Identités numériques : gestion inter-organisationnelle centrée sur l'utilisateur et respectueuse de la vie privée

Mikaël Ates

Thèse

Pour obtenir le grade de

Docteur de l'université Jean Monnet de Saint-Étienne

Génie Informatique, Automatique et Traitement du Signal

Présentée et soutenue publiquement le 2 octobre 2009

par

Mikaël ATES

Ingénieur TELECOM Saint-Étienne – Maître ès Sciences

Identités numériques : gestion inter-organisationnelle centrée sur l'utilisateur et respectueuse de la vie privée

Directeur de thèse :
Jacques FAYOLLE

Co-Directeur de thèse :
Bruno SAUVIAC

Composition du Jury :

Frédéric Cuppens	Professeur, TELECOM BRETAGNE	*Rapporteur*
Lionel Brunie	Professeur, INSA de Lyon	*Rapporteur*
Michel Riguidel	Professeur, TELECOM PARISTECH	
François Jacquenet	Professeur, Université de Saint-Etienne	
Laurent Vercouter	Maître de Conférences, Ecoles des Mines de Saint-Etienne	
Frédéric Péters	Ingénieur, Société Entrouvert	
Christophe Gravier	Docteur, TELECOM SAINT-ETIENNE	
Jacques Fayolle	Maître de Conférences, TELECOM SAINT-ETIENNE	*Directeur*
Bruno Sauviac	Professeur, TELECOM SAINT-ETIENNE	*Co-directeur*

Remerciements

Ce travail fut réalisé au sein de l'équipe SATIN - Laboratoire DIOM - TELECOM SAINT-ETIENNE - Université Jean Monnet de Saint-Étienne - Université de Lyon, grâce à un financement sur fonds propres de l'école d'Ingénieurs TELECOM SAINT-ETIENNE du 1^{er} octobre 2006 au 30 Septembre 2009.

Je tiens en premier lieu à remercier la société LOTIM Télécoms et le Conseil Général de la Loire ayant permis de constituer ce financement.

Je remercie mon directeur de thèse, Jacques Fayolle, pour son enthousiasme, son soutien et la confiance sans faille qu'il m'a accordée durant ces trois années.

Je remercie également chaleureusement mon co-directeur de thèse, Bruno Sauviac, pour sa disponibilité et sa bonne humeur.

Je remercie Frédéric Cuppens et Lionel Brunie qui ont accepté de rapporter sur mes travaux. Ils ont apporté des critiques constructives et enrichissantes qui m'ont notamment permis d'élargir ma vision sur les qualités essentielles d'un travail scientifique.

Je remercie Michel Riguidel, François Jacquenet et Laurent Vercouter d'accepter de participer à mon jury.

Je remercie mes collègues et camarades de jeux, Jérémy, Christophe et Abakar, avec qui j'ai partagé beaucoup de bons moments au cours de ces trois années, aussi bien sur un terrain de sport qu'autour d'un café.

Je tiens à remercier l'équipe d'Entrouvert, Pierre Cros, Frédéric Péters, Christophe Boutet et Benjamin Dauvergne, pour les multiples et passionnantes discussions techniques mais aussi, et surtout, pour leurs encouragements, leurs accueils chaleureux, leur gentillesse et leur vision éthique du monde de l'industrie informatique.

Je remercie tous mes amis, passionnés, irresponsables, flemmards ou inconscients, tous géniaux.

Je remercie ma famille, vous êtes incroyables et surtout formidables.

Enfin, je te remercie toi, Evangéline, pour tes encouragements, tes relectures, tes critiques, tes conseils, ta patience, notre vie ensemble.

Résumé

Cette thèse a pour objet d'étude le paradigme de la gestion des identités numériques entre organisations. L'accent est porté sur l'usager, consommateur de services hébergés par des organisations dans un environnement ouvert. Le terme « environnement ouvert » résume l'idée d'un environnement où il ne peut exister d'autorité centrale régissant toutes les mises en relation entre entités qui le peuplent, ni tous les accès que ces dernières requièrent. Ainsi, dans un tel environnement, diverses entités, potentiellement inconnues, ont à établir des relations qui visent, dans ces travaux, à satisfaire les conditions de contrôle d'accès des fournisseurs de services et à donner à l'usager des moyens de contrôle et de confiance envers les organisations. Le « WEB » au travers de l'« Internet » est une implémentation qui constitue un tel environnement.

L'emploi de tiers de confiance et leur potentielle croissance au sein d'un tel environnement sont des propositions argumentées. En effet, les certificats numériques sont une réalisation technologique qui permet la diffusion d'informations certifiées issues de tiers de confiance, et les échanges d'informations certifiées entre usagers et organisations sont une réponse aux deux objectifs précédents. Cela suppose donc le déploiement d'une architecture globale d'échanges de certificats.

La thèse repose sur un modèle de négociation de confiance permettant l'établissement graduel d'une relation de confiance, potentiellement entre inconnus, reposant sur des tiers de confiance et intégrant l'idée d'une diffusion d'information maîtrisée. Il est alors justifié que les échanges de certificats sont une implémentation pertinente de ce concept.

La réalisation d'une possible architecture, à l'échelle globale, implique de nombreuses problématiques, dont les principales sont décrites et étudiées. Cette architecture suppose notamment des échanges entre tiers de confiance et organisations au sujet des usagers, ce qui représente une menace potentielle pesant sur le respect de la vie privée des usagers. L'enrichissement de l'environnement des usagers est identifié comme une condition au déploiement d'une architecture permettant d'adresser cette problématique. À cette fin, il est étudié l'emploi d'un schéma de signature permettant de bâtir des certificats offrant la non-associativité des transactions de génération et de présentation, la présentation sélective de contenu, les preuves de possessions et les preuves de propriétés sur le

contenu. Ces propriétés permettent notamment de réaliser le statut d'anonymat au sens de la non-associativité. Le statut d'anonymat des interlocuteurs au sein des négociations de confiance et les problématiques que ce statut engendre sont alors étudiés.

Des négociations conduites par l'usager impliquent des problématiques d'ergonomie et d'utilisabilité. Un outil de gestion des identités numériques mis à disposition des usagers est une première réponse. Une interface graphique de l'agent de négociation pour l'usager est décrite à cette fin. Les notions d'automatisation des négociations de confiance sont introduites dans le but de proposer une solution complémentaire permettant d'assister l'utilisateur.

Le modèle est au départ relativement « dissymétrique », phénomène accentué par une vision « centrée sur l'utilisateur » faisant de l'usager le chef d'orchestre de la diffusion de ses informations. Puis, au travers d'une étude sur l'universalité d'un agent de négociation, ce modèle est affiné pour aboutir à la description d'un agent de négociation s'adaptant autant à l'environnement utilisateur comme outil de gestion des identités numériques, qu'à celui des organisations employé à des fins de contrôle d'accès aux applications.

L'idée de l'universalité d'un tel agent implique l'étude des problématiques d'interopérabilité et de standardisation, incluant le besoin d'espaces de noms communs et de protocoles interopérables. Il est pour cela présenté une mise en œuvre des certificats anonymes basée sur la diffusion publique de méta-données des générateurs ayant aboutie à l'élaboration d'un schéma de données XML baptisé x23.

Enfin, le concept d'« identité en tout lieu » et l'emploi de ce travail dans les environnements informatiques pervasifs et ubiquitaires sont discutés.

Abstract

The topic of this thesis is the paradigm of the cross-organizationnal digital identity management. The focus is on the user, consumer of services hosted by organizations. The scene takes place in an « open environment », which refers to an environment where it cannot exist a central authority able to manage neither all the relationship establishments nor all the access requests. In such a world, various entities, potentially unknown, have to establish relationships in order to satisfy service providers' access control policies and to provide users with control and trust about organizations.

The use of trusted third parties, and their expected growth, are propositions which are defended. As a matter of fact, digital certificates are a technical implementation allowing to spread certified information issued from trusted third parties. Moreover, the certified information exchanges, between users and organizations, are a way to match both previous expectations. However, it implies a global architecture for exchanging digital certificates.

Along the thesis, a model of trust negotiation allowing a gradual establishment of trust relationships, potentially between strangers, relying on trusted third parties and on a thinly-controlled spreading of information, is described. Then, the digital certificates as a relevant implementation of this concept are justified.

The realization of a possible architecture, at a global scale, implies many stakes and issues. For instance, this architecture implies exchanges about users between organizations and trusted third parties, which means a possible threat on the users' privacy. The enrichment of the user side is identified as a condition in order to deploy a privacy-respectful architecture. Following through this goal, it is studied the use of a signature schema allowing unlinkable certificates issuing and showing transactions, selective disclosure of certificates content, proofs of possession and proofs on the certificates content. These properties especially allow to realize the anonymity status in the sense of the unlinkability. The anonymity status of interlocutors and the implied stakes and issues are then studied.

Negotiations by users raise a usability concern. An identity management tool dedicated to users is a first answer. A suitable graphical interface is depicted as an illustration. The basics of automated trust negotiations are also introduced in order to propose a com-

plementary solution allowing to assist users in their negotiations.

The model is, at first, quite asymmetrical, phenomena highlighted by the « user-centric » vision making the users the conductors of the certificates exchanges. But, through a study about the possible universality of a negotiation agent, the model is refined to lead to a universal negotiation agent suitable as well as an identity management tool for users as an access control tool for organizations.

Talking about the possible universality of such an agent implies to study the interoperability and standardization questions, including the need of common namespaces and interoperable protocols. In this way, an implementation of anonymous certificates based on public meta-datas of certificates issuers is presented. It reaches to a new XML schema called x23.

Finally, the concept of « identity everywhere » and the use of this work in pervasive and ubiquitous environments are discussed.

Table des matières

CHAPITRE I

Introduction

Sommaire

"Je transforme ce « je pense donc je suis » qui m'a tant fait souffrir - car plus je pensais, moins il me semblait être - et je dis : on me voit, donc je suis."

Jean-Paul Sartre

I.1 Identité réelle et identité civile

Les enjeux liés à l'identité numérique sont inhérents à ceux des individus dans le monde physique. Ils révèlent l'intérêt du sujet de la gestion des identités entre organisations et mettent en lumière les difficultés de retranscrire des procédures basées sur des relations sociales en des procédures opérées aux travers de réseaux de communications et d'interfaces homme-machine. Nous utilisons dans l'introduction de nombreux termes qui sont précisés dans les chapitres suivants.

I.1.1 Identité civile

L'Académie Française définit l'identité comme « la personnalité civile d'un individu, légalement reconnue ou constatée, établie par différents éléments d'état civil et par son signalement ». Cette définition, notamment utilisée dans les sphères régaliennes et judiciaires, permet de décrire l'identité comme la reconnaissance par un tiers, ici l'État, au travers d'une entité organisationnelle compétente, l'état civil, l'existence d'un individu. Cela se traduit en pratique par une procédure administrative qui officialise l'existence de cet individu, et qui définit les moyens de désignation.

La naissance d'un individu est en France actée en mairie puis enregistrée à l'état civil. Le registre des naissances est tenu en double original dont un est déposé au tribunal de grande instance et vérifié par le procureur de la République. Il permet une identification des individus nés sur le territoire français et constitue l'une des références de l'identité civile d'un individu. Une copie intégrale de l'acte de naissance, souvent appelé extrait de naissance, permet à un individu de fournir la preuve de son identité dans différentes procédures. Il s'agit d'un document émis en préfecture. Il est certifié par le cachet de celle-ci et la signature du préfet, ou d'un délégataire. Cette certification permet aux destinataires d'en vérifier l'authenticité et son émission par un tiers compétent.

L'extrait de naissance peut être requis lors d'une procédure administrative afin d'apporter la preuve de l'existence d'une identité civile. Lorsqu'il s'agit du seul document certifié requis pour établir l'identité du sujet au sein de cette procédure, et que le porteur du document est associé au sujet de l'extrait, cela fait de celui-ci le moyen pour un individu d'apporter la preuve de son identité. Cela peut être le cas pour les procédures permettant l'obtention de pièces d'identité, documents permettant à leur détenteur d'apporter la preuve de leur identité. Considérons dans un premier temps l'authentification comme une procédure permettant d'établir une identité suite à l'apport d'une preuve d'identité. À ce titre, les pièces d'identité, et parfois l'extrait de naissance, sont souvent acceptés comme des moyens d'authentification. Nous verrons, lors de définitions plus précises, que

la notion de preuve est toute relative.

I.1.2 Identité réelle

Appelons l'identité réelle d'un individu le fait de pouvoir désigner de manière infaillible un être unique. Si les procédures ayant permis l'enregistrement d'une identité civile, puis à l'individu d'apporter la preuve de son identité, peuvent être considérées comme infaillibles, alors, il est possible de considérer l'identité civile comme la matérialisation d'une identité réelle. Si par contre ces mécanismes sont faillibles, il est nécessaire de distinguer identité réelle et identité civile.

Il y a encore peu de temps, l'obtention d'un extrait de naissance se faisait en préfecture. Cette procédure nécessitait que l'individu, sujet de l'extrait, se présente avec son livret de famille et une pièce d'identité. Cela peut paraître paradoxal du fait qu'il faille présenter un extrait de naissance dans la plupart des procédures permettant l'obtention d'une pièce d'identité. Cependant, la délégation auprès d'un tiers, soit de tutelle lorsque l'individu est mineur, soit par procuration lorsque l'individu est majeur, permet à celui-ci d'obtenir un premier extrait de naissance. Aujourd'hui, au travers de l'informatisation des procédures administratives, il est possible d'obtenir un extrait de naissance par l'accomplissement d'une procédure en ligne. Celle-ci requiert la fourniture d'un ensemble d'informations sur l'identité civile du sujet de l'extrait (nom, prénom, date et lieu de naissance) et sur celles de ses parents. La connaissance de ces informations constitue le moyen d'apporter la preuve de son identité, ce qu'il est possible d'assimiler à un mécanisme d'authentification. L'extrait de naissance est ensuite envoyé par courrier postal. Si l'extrait de naissance est utilisé dans une procédure comme seul moyen offert à l'individu pour apporter la preuve de son identité, alors les quelques failles potentielles suivantes nous obligent à distinguer son identité réelle de son identité civile :

- la connaissance par un tiers des informations nécessaires à l'obtention d'un extrait de naissance en ligne et la non vérification de l'adresse postale comme celle du sujet,
- l'obtention d'un extrait de naissance par un membre de la famille sans procuration,
- une boîte postale compromise (cambriolage).

Les registres de l'état civil étant la référence de l'identité d'un individu, l'ensemble des mécanismes d'enregistrement et de déclinaison de l'identité sont les fondamentaux pour rapprocher au maximum l'identité civile de l'identité réelle.

I.1.3 Décliner son identité

Il est possible de décrire sommairement une procédure générique permettant à un individu de décliner son identité. Un premier mécanisme permet d'obtenir une preuve matérielle de l'identité. Un second mécanisme permet d'établir l'identité auprès d'un tiers grâce à cette preuve. Si ces mécanismes sont faillibles, il existe un risque pour que l'identité établie ne soit pas celle du porteur de la preuve, conduisant à une usurpation d'identité. Une organisation établissant une identité à l'aide d'une preuve fournie par un tiers peut elle-même être une source de preuves d'identité employées auprès d'autres tiers. Ainsi, au fil des établissements d'identité successifs, la confiance dans le fait que l'identité établie soit celle du porteur de la preuve diminue.

I.1.4 Certification et authenticité

L'établissement d'une identité se basant sur des éléments émis par des tiers implique la nécessité de s'appuyer sur des mécanismes permettant de :

- vérifier l'authenticité d'une preuve,
- authentifier l'émetteur de cette preuve.

Il s'agit d'empêcher la production de pièces falsifiées et de s'assurer qu'elles proviennent de la source attendue. Ces mécanismes sont souvent couplés. Si l'on prend l'exemple de l'extrait de naissance, le cachet signé sert à vérifier l'authenticité du document, c'est-à-dire à lutter contre la falsification, si l'on considère cette certification comme non reproductible. Le cachet assure également l'authentification de l'émetteur, ici la préfecture, dont le nom est décliné par le cachet.

Un élément physique contrefait est généralement appelé « faux ». Son équivalent authentique est appelé « original ». Il existe plusieurs moyens permettant de vérifier l'authenticité d'éléments physiques, par exemple la difficulté de reproduction (les hologrammes, les filigranes, les signatures, et les encres spéciales) ou le secret (les encres invisibles). Les justificatifs de domicile, autres éléments utilisés comme preuve de l'identité, sont couramment utilisés dans les procédures administratives alors qu'ils ne sont que très rarement certifiés. Cela rend donc impossible la distinction entre faux et originaux.

Un élément utilisé au sein d'un mécanisme d'établissement de l'identité peut être falsifié et conduire à l'établissement d'une identité différente de celle du porteur de la preuve. Un individu peut ainsi usurper une identité par l'usage de faux. Si cette première procédure conduit à la délivrance d'une pièce d'identité, la détention de celle-ci par l'individu lui permettra d'usurper à nouveau cette identité dans les procédures successives. La contrefaçon est cependant une menace souvent moins difficile à détecter, et à contrer, qu'une

faille dans un mécanisme d'établissement de l'identité. En effet, la falsification est détectable par les contre-mesures de la falsification ce qui n'est pas le cas de telles failles. Ainsi, un mécanisme défaillant peut permettre l'accomplissement avec succès d'une procédure à partir d'éléments authentiques alors qu'une identité est usurpée.

La problématique des failles dans les procédures administratives ouvre la voie de l'obtention de « vraies/fausses » pièces certifiées. Il existe plusieurs moyens de lutte dont le plus simple est la durée de validité qui impose le renouvellement des procédures d'établissement de l'identité. Cela n'a de sens que si la procédure est régulièrement remise en question et mise à jour au vue de ses failles potentielles, et si la procédure de vérification de l'élément intègre la vérification de la date de validité.

En résumé, les identités réelles et civiles doivent être distinguées afin de ne pas se méprendre quant aux attentes de la gestion des identités. En outre, l'établissement d'identité s'appuyant sur des preuves fournies par des tiers requiert des mécanismes forts pour lutter contre l'usurpation d'identité.

I.2 Négociation de confiance

Dans cette section, nous introduisons la terminologie de la négociation que nous utiliserons par la suite. Les termes figurent en italique. Nous employons volontairement des répétitions lorsque cela apporte un bénéfice pour la définition de la terminologie.

I.2.1 Introduction

La vie civile, dans la sphère régalienne ou économique (les services et le milieu bancaire inclus), est ponctuée d'interactions entre individus et organisations. Ces interactions peuvent prendre la forme d'échanges multiples entre intervenants, et aboutir à l'accomplissement d'un *objet*, d'un achat ou d'une signature de contrat par exemple. Nous appellerons ces échanges multiples une *négociation*. Du point de vue de l'un des intervenants, la négociation est assimilable à une *procédure administrative* à accomplir pour voir l'accomplissement de l'*objet*, ou bien encore, à une séquence de tâches que l'on peut voir comme la constitution d'un *dossier administratif* à partir de divers *éléments*, notamment acquis auprès d'organisations ou d'individus tiers de l'interlocuteur. Les *éléments* requis sont indiqués par chacun des interlocuteurs durant la négociation. Ils peuvent être vus comme les moyens de satisfaire les *règles* d'accès de chacun pour permettre l'accomplissement de l'*objet*.

I.2.2 Généralisation

Une généralisation informelle de la négociation est ici présentée et sera utilisée au sein de la thèse. La *négociation* vise à satisfaire un *objet*, une ressource ou un service, qu'un *initiateur* requiert d'un *fournisseur*. Ce dernier indique ses conditions sous la forme de *règles*. L'*initiateur* peut alors les satisfaire ou imposer les siennes. La satisfaction d'une *règle* se fait par la fourniture d'*éléments*. Débute donc une phase de négociation. Cette phase doit permettre d'établir des compromis, chacun souhaitant ne diffuser qu'un minimum d'*éléments*. Il s'agit donc de déterminer une séquence d'échanges d'*éléments* permettant d'aboutir à un consensus satisfaisant les *règles* d'accès de chacun sur les *éléments* qu'il diffuse. Il résulte d'une négociation menée avec succès la fourniture de l'*objet* à l'*initiateur*. Cela est illustré à la figure VI.1 :

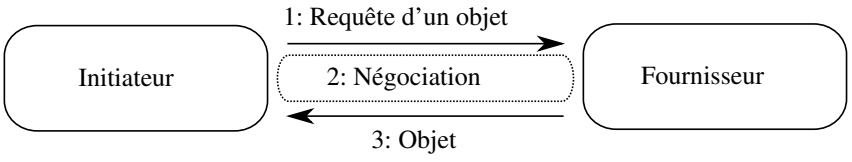

FIG. I.1 – *Vue générale d'une negociation.*

La majeure partie de ce que l'on considère comme des négociations dans le monde physique sont des cas d'usage simples où il n'y a pas de réelle négociation. L'achat d'un *objet* par exemple, dans son expression la plus simple, peut se représenter par la requête de l'*objet* par l'*initiateur*, l'indication de la *règle* « prix » par le *fournisseur*, la fourniture de l'*élément* « argent » par l'*initiateur* et la fourniture de l'*objet* par le *fournisseur*.

I.2.3 Sources des *éléments* à fournir

Les *éléments* fournis peuvent être issus des interlocuteurs eux-mêmes, ou de tiers distincts de nos deux interlocuteurs principaux. Le terme « issus » est employé pour désigner la source de l'*élément*. Par le suite, nous emploierons les termes *générer* et *générateur* pour indiquer la source[1]. Le terme « générer » peut apparaître déconcertant dans le monde physique, il est intuitif dans le monde numérique.

Les rôles d'*initiateur* et de *fournisseur* sont concurrents dans une négociation. Ils peuvent par contre être endossés conjointement avec un autre rôle tel que *générateur* ou *consommateur*. Il existe donc plusieurs cas de figures suivant les rôles empruntés, notamment par les sujets des éléments.

Lorsque le *générateur* est un tiers distinct du sujet de l'*élément* généré, et que ce dernier présente l'élément au *consommateur*, il est alors nommé *porteur*. Ceci est illustré à la figure I.2.

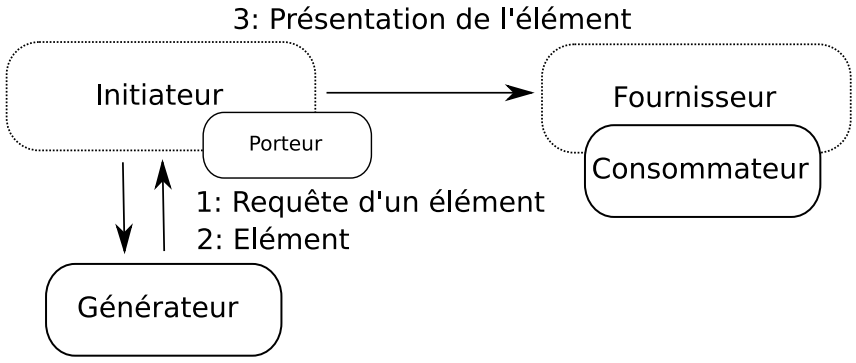

FIG. I.2 – *Notion de porteur.*

Ce n'est cependant pas une règle. Si l'intervenant *consommateur* de l'*élément* est en relation directe avec le *générateur*, l'intervenant pour qui l'*élément* a été généré n'est pas considéré comme un *porteur*. Cependant, il est considéré comme le *sujet* de l'*élément* si le *consommateur* le lui associe. Si l'*élément* est généré par l'intervenant, il est naturellement

1. En anglais, le terme "issuer" est couramment employé.

le *porteur*.

La notion de *négociation* suppose des échanges bilatéraux. Cela implique que les *initiateurs* et les *fournisseurs* puissent assumer tour à tour le rôle de *porteur* ou de *consommateur*, et qu'ils présentent des éléments qu'ils ont générés ou issus de *générateurs* tiers.

I.2.4 Nature des relations

La notion de confiance est définie au chapitre suivant, il est cependant intéressant d'introduire ce concept. La confiance est ce qui permet à deux individus d'entrer en relation alors qu'ils n'ont pas la certitude de satisfaire leurs attentes envers cette relation. Si l'on rapporte cette notion à la dimension organisationnelle, chaque organisation représente une entité distincte. Chaque organisation est administrée indépendamment et peut donc être considérée comme un domaine de sécurité distinct. Ainsi, plusieurs organisations sont des domaines de sécurité distincts, ce qui implique que le contrôle par une organisation des informations qu'elle consomme n'est pas total, puisqu'elles proviennent de l'« extérieur ». Il existe donc une part d'incertitude dans les échanges inter-organisationnels. Les relations entre organisations qui s'échangent des informations sont alors qualifiées de relations de confiance. La confiance prend des formes multiples sur lesquelles nous reviendrons par la suite. Notons qu'il peut par exemple s'agir de partenariats comportant certains engagements. Ce peut être également des notions plus subjectives telles que le fait qu'une organisation soit considérée de confiance pour fournir un type d'élément dès lors qu'elle accorde elle-même de l'importance à cet élément.

Reprenons notre système de négociation. Les parties négociatrices sont intrinsèquement des « domaines de sécurité » différents. Il est supposé qu'elles ne peuvent avoir un contrôle total l'une sur l'autre. La relation établie entre parties négociatrices se base donc sur la confiance. Chaque partie souhaite une part de contrôle sur son interlocuteur afin de diminuer le sentiment d'incertitude. Notre modèle de négociation de confiance se base donc sur le parti-pris de la confiance basée sur le contrôle. En d'autres termes, l'incertitude issue d'un contrôle limité suppose la confiance pour établir une relation. Les éléments présentés visent donc à satisfaire des besoins de contrôle afin de pouvoir établir une relation de confiance. L'*initiateur* et le *fournisseur* interagissent dans le but de permettre la fourniture de l'*objet*. Il est donc nécessaire qu'ils acquièrent l'un envers l'autre un niveau de confiance suffisant pour permettre cet accomplissement. Selon la connaissance qu'ils ont au préalable l'un de l'autre, et éventuellement d'un historique de négociations passées, ils ont l'un envers l'autre un certain sentiment de confiance, qui peut être nul. La négociation va permettre à chacun de spécifier les informations qu'il souhaite obtenir afin d'élever celui-ci. Autrement dit, ils vont devoir satisfaire aux exigences de leur inter-

locuteur afin d'établir une relation de confiance l'un envers l'autre, d'entrer en relation, et ainsi, de permettre l'accomplissement de l'*objet* de la négociation. La négociation est dite de confiance. Ce lien de confiance est illustré par le lien numéroté « 1 » sur la figure I.3. Notons que cette figure n'illustre pas le fait qu'au cours d'une même négociation l'*initiateur* et le *fournisseur* puissent être tour à tour *consommateurs*.

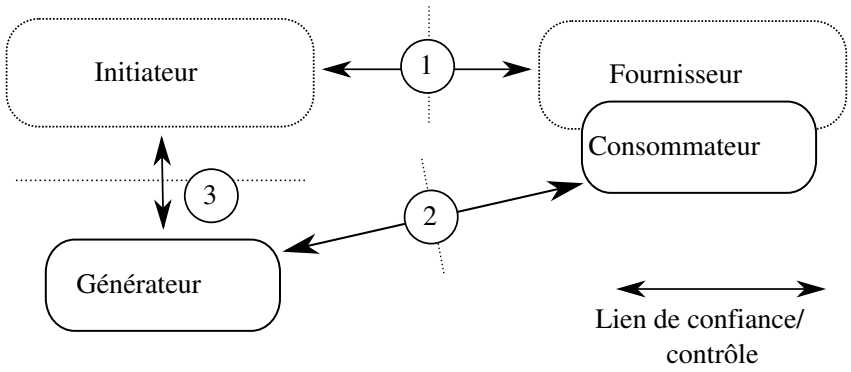

FIG. I.3 – *Les liens de confiance et de contrôle.*

La négociation de confiance entre l'*initiateur* et le *fournisseur* repose notamment sur la présentation d'*éléments* issus de *générateurs*. Si un *générateur*, distinct du *porteur*, et le *consommateur* appartiennent à des organisations différentes, leur relation est de confiance. Ce lien de confiance est numéroté « 2 » sur la figure I.3. La figure I.4 illustre la présentation d'un *élément* issu d'un *générateur*, *tiers de confiance*, appartenant au *domaine de confiance* du *consommateur*.

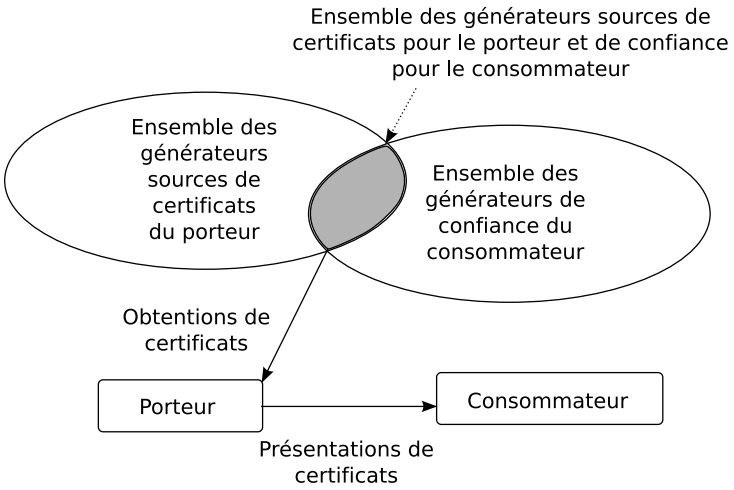

FIG. I.4 – *Présentation d'un certificat issu du domaine de confiance de son interlocuteur.*

Il est possible qu'il n'y ait pas de relation de confiance entre un *générateur*, distinct du

porteur, et le *consommateur*. Le *générateur* est alors en quelque sorte simplement un « espace de stockage » d'*éléments* utilisés par le *porteur*. Nous verrons plus précisément cette notion au chapitre 3, qui en pratique peut être assimilée à ce que l'on peut qualifier de « portefeuille en ligne ». Ainsi, le *consommateur* fait confiance au *porteur* pour fournir ces éléments, et le *porteur* fait confiance au *générateur*. Ce lien est numéroté « 3 » sur la figure I.3. Nous sommes donc en présence de deux types de relations de confiance, entre les *initiateurs* et les *fournisseurs*, d'une part, et entre les *générateurs* et les *consommateurs*, d'autre part.

L'environnement de négociation est un environnement où l'on souhaite voir négocier des entités inconnues, qui doivent donc établir une relation de confiance au travers de la négociation. Nous pouvons dès lors introduire la notion de confiance transitive employée pour résoudre le paradigme de la confiance en environnement ouvert. Il s'agit d'accepter que des inconnus puissent établir une relation de confiance en s'appuyant sur des tiers de confiance qu'ils ont en commun. La confiance est obtenue d'un tiers de confiance envers un inconnu par transitivité. Ainsi, une part de la confiance est acquise durant la négociation par un *élément* provenant d'un tiers de confiance. Cela suppose que le *consommateur* de l'*élément* ait confiance dans le *générateur* de manière à attribuer au *porteur* un niveau de confiance plus élevé suite à la consommation de cet *élément*. Le *générateur* est ainsi qualifié de *tiers de confiance* appartenant au *domaine de confiance* du *consommateur*.

Il doit être possible pour les *consommateurs* de s'assurer que les *éléments* proviennent d'un tiers de confiance. Prenons l'exemple d'un *initiateur* souhaitant ouvrir des droits auprès d'une administration française. Supposons qu'il présente l'*élément* passeport au *fournisseur*, l'administration concernée. Celle-ci fait confiance aux préfectures françaises pour délivrer des pièces d'identité aux citoyens. Il s'agit donc de vérifier que le générateur est une préfécture française. Ainsi, pour pouvoir vérifier qu'un *élément* provienne d'un *générateur* en lequel un *consommateur* a confiance, il est nécessaire que cet *élément* soit accompagné, ou soit porteur, d'une preuve de l'identité de son *générateur*, et que cette identité soit connue du *consommateur* de l'*élément*. La *certification* de l'*élément* est le mécanisme qui permet au *consommateur* d'authentifier le *générateur*. Un *élément certifié* sera désormais appelé *certificat*.

I.2.5 Établissement de l'identité et pièces d'identité

Un des intervenants peut requérir des *éléments* permettant d'établir l'identité de son interlocuteur. Par exemple, parce qu'il est capable de lui attribuer un ensemble de droits attachés à une identité connue.

Comme nous l'avons vu, une pièce d'identité permet à une entité d'établir une identité auprès d'un tiers. La pièce d'identité peut également être employée pour permettre un recours légal contre un individu en cas de litige. Les informations de l'état civil ne sont dans ce cas pas utiles. Il suffit à l'*initiateur* d'apporter la preuve de possession d'une telle pièce, preuve porteuse d'un identifiant. Le *fournisseur* aurait ainsi un moyen de recours en cas de litige. Il s'agit en résumé d'une pièce d'identité certifiée identifiable ne présentant pas d'informations d'état civil. La mise en œuvre des mécanismes qui permettent au *consommateur* de vérifier l'authenticité de la pièce et d'obtenir la révocation de l'anonymat de l'individu en cas de préjudice avéré est nécessaire.

Comme nous le verrons aux chapitres 4 et 5, la notion d'établissement d'une identité prend des formes multiples dans un environnement ouvert. Les notions d'expérience passée et de construction d'une réputation, éventuellement avec un tiers unique, peuvent être réalisées à l'aide de pseudonymes. Il est cependant également attendu de pouvoir mener de multiples négociations sans établir d'identité connue, et de préserver ainsi son anonymat par la non-associativité des négociations. Cela n'empêche pas qu'une négociation anonyme, c'est-à-dire qui ne peut être associée à aucune autre négociation de l'interlocuteur, soit identifiable, et que l'anonymat puisse être révoqué.

I.2.6 Négociation et contrôle d'accès

L'accès à l'*objet* est conditionné par la fourniture d'*éléments* provenant de tiers de confiance. Ceci revient à baser sur ces *certificats* une partie du contrôle d'accès, ce que l'on nomme « gestion de la confiance ». Les droits ouverts peuvent dépendre du contenu des *certificats*, ou plus simplement du fait qu'ils proviennent d'un *générateur* de confiance du *consommateur*. Prenons l'exemple de certains services de l'administration française qui sont ouverts à tout citoyen français et pour lesquels la présentation d'une carte d'identité française suffit à exercer ces droits. Ce qui importe, dans ce cas, ce n'est pas les informations personnelles contenues dans la pièce d'identité, mais simplement l'appartenance à un ensemble. La pièce d'identité est ici utilisée comme le moyen de prouver l'appartenance à l'ensemble « citoyens français » sur lequel se base le contrôle d'accès.

Les *certificats* servant au contrôle d'accès sont très nombreux dans la vie courante. Citons par exemple les diplômes qui permettent l'inscription à des niveaux d'études supérieurs, les brevets d'aptitude divers et variés, les permis de conduire, l'extrait de casier judiciaire, le décompte des bonifications d'assurance, l'extrait du registre des interdits bancaires, les fiches de paie, les factures, les attestations d'assurance, les timbres postaux, fiscaux et amendes, et le plus courant, la monnaie (billets, pièces et chèques). Il est aussi possible d'ajouter à cette liste les monnaies non officielles, comme les « chèques cadeaux » et les

« points de fidélité » valables dans des organisations partenaires. Notons, d'une part, que dans le monde physique la plupart de ces *éléments* ne sont en fait pas certifiés, et d'autre part, qu'il est possible de rendre anonyme la plupart d'entre eux.

I.2.7 Signature

Au-delà de vouloir établir l'identité d'un interlocuteur, un intervenant peut souhaiter obtenir une preuve de son identité qu'il pourra faire valoir auprès d'un tiers. Cette preuve pourra par exemple attester de la participation d'un interlocuteur à une négociation, ou de son acquittement sur un ensemble d'informations. La signature est la preuve qui permet de satisfaire ces cas d'usage. La signature doit pour cela avoir la propriété d'unicité et n'être reproductible que par son auteur. La signature doit également être attachée à l'identité de l'individu pour avoir un sens, c'est-à-dire qu'il doit être possible de s'assurer que la signature provient bien d'un individu identifiable. Les mécanismes mis en place doivent ainsi assurer la non-répudiation du signataire. Dans le monde physique, il n'existe que le mécanisme de signature manuscrite, signature que l'on suppose unique et non-reproductible excepté par son auteur. Une signature ne peut être vérifiée que si elle existe au sein d'un référentiel qui va servir de point de comparaison. La signature d'un document doit donc être accompagnée d'un moyen de vérification auprès d'un référentiel associant la signature à l'identité du signataire. La signature sur une pièce d'identité peut donc servir de référentiel et permettre à un tiers de vérifier la validité d'une signature apposée, en comparaison de celle portée sur la pièce d'identité. Dans le monde physique, ce principe est rarement respecté. Lorsque l'on apporte un élément certifié par une signature, dans laquelle on peut englober un cachet, il est très rarement utilisé un référentiel de comparaison. L'authentification du *générateur* par la certification d'un *élément* par signature manuscrite est donc faible. A l'inverse, dans le monde numérique, la signature numérique est un mécanisme sûr employé pour la certification.

I.3 Contenu de la thèse

Les travaux présentés dans la thèse se focalisent sur un initiateur qui est une personne physique, et sur un fournisseur de services hébergé par une organisation. Cette approche permet de mettre en lumière la problématique du respect de la vie privée que l'on pense *a priori* de moindre importance lorsque les interlocuteurs sont des entités organisationnelles. Ce choix présente aussi l'avantage de mettre en valeur la notion de négociation s'appuyant sur des certificats, aussi riche entre usagers et organisations, qu'entre organisations. Pour autant, ces travaux n'écartent en aucun cas les négociations entre organisations, ou entre personnes physiques.

L'utilisateur se situe au cœur des échanges, il a le rôle de l'initiateur et il souhaite consommer de multiples services et ressources offerts par des fournisseurs. Ce sont les objets de la négociation. Les organisations qui hébergent ces derniers basent une partie des conditions d'accès sur des informations certifiées, les certificats. L'initiateur en diffusera certaines de manière contrôlée. En effet, il ne souhaite révéler certaines informations aux fournisseurs que pour un certain niveau de confiance. De manière générale, moins il révèle d'informations sur lui-même, plus il s'en satisfait. Il estime en quelque sorte la sensibilité et la valeur de ces informations, et les diffusent en fonction de son sentiment de confiance. Réciproquement, pour obtenir la confiance de l'utilisateur, le fournisseur diffusera lui aussi des informations certifiées avec les mêmes exigences. Les échanges multiples de règlements et de certificats constituent la négociation. Les informations certifiées proviennent du domaine de confiance de leur interlocuteur. Il est possible que leur fourniture agisse sur le sentiment de confiance de chacun par transitivité. Cela conduit alors à une négociation visant à établir une relation de confiance graduelle permettant d'aboutir à un consensus satisfaisant les conditions de chacun. Il résulte d'une négociation menée avec succès la fourniture de l'*objet* à l'*initiateur*.

L'établissement d'une relation de confiance est une notion subjective. Dans le monde physique, l'ouïe et la vue sont les interfaces de capture de l'information qui permettent à notre système cognitif d'interpréter le contexte, avec pour paramètres les plus influents l'interprétation de comportements et l'expérience. Il est également possible de traduire abusivement cette interprétation par le concept d'intuition. Dans le monde numérique, celui des télécommunications, les interfaces de l'homme sont celles offertes par son terminal d'accès. La notion d'interface homme-machine a alors une place prépondérante dans cette étude. Une partie des travaux est donc dédiée, d'une part, aux interactions de l'utilisateur, et d'autre part, au rendu visuel de l'interface. Il s'agit de retranscrire la notion de négociation pour la rendre intuitive dans le monde numérique, même face à une machine pour interlocuteur. Cela suppose d'apporter une dimension interactive à la négociation

afin que l'utilisateur ressente qu'il en est l'acteur et qu'il n'est pas seulement soumis aux exigences des fournisseurs.

Il est également nécessaire de pouvoir constituer des domaines de confiance, et d'obtenir et de présenter des informations en provenance de ceux-ci. Cela soulève le besoin d'une architecture de confiance permettant de véhiculer entre organisations des informations sur les interlocuteurs.

En outre, les informations véhiculées sont synonymes de descriptions des interlocuteurs et de leurs comportements et permettent donc leur profilage. Une seconde problématique est alors celle du respect de la vie privée dans un monde numérique où la puissance de calcul, les dimensions vertigineuses des espaces de stockage ainsi que l'exposition des canaux de communication, combinées à la facilité attendue de consommation des services, peuvent grandement mettre ce respect en péril. Par conséquent, une attention toute particulière est portée à l'association des identités numériques que nous décrivons comme une menace potentielle au respect de la vie privée. Nous nous attachons donc à produire une architecture d'échange des informations d'identité respectueuse de la vie privée.

L'enjeu de ces travaux est donc de définir une couche de gestion des identités qui n'a de sens que si elle est pervasive. **Si les travaux présentés ici devaient se résumer en une seule phrase, ce serait : *l'étude des échanges d'informations certifiées pour les négociations de confiance dans un environnement numérique ouvert.*** Les contributions attendues ont trait en particulier à la description du domaine, des concepts et des mécanismes technologiques, ainsi que des enjeux humains et sociétaux. Les études menées portent sur les protocoles cryptographiques, la négociation de confiance, le contrôle d'accès basé sur les échanges d'informations certifiées, la prise en considération des interactions utilisateurs et, enfin, la conception d'une architecture et d'une interface utilisateur apparentées aux résultats de recherche attendus. Nous utiliserons donc au cours de la thèse la terminologie issue de la première généralisation du concept de négociation introduite dans ce chapitre.

La première partie vise à définir les concepts généraux mais également à étudier les manques des architectures existantes. Le but de cette partie est de mettre en lumière les enjeux de ces travaux et de justifier pourquoi la prise en compte des notions d'universalité et de pervasivité est fondamentale.

Le **chapitre 2** décrit les notions générales de la gestion des identités numériques, précise celles de confiance et d'anonymat, décrit le besoin de respect de la vie privée inhérent à ces travaux et liste sommairement les enjeux d'une telle architecture pour les utilisateurs

et les organisations.

Au **chapitre 3** sont étudiées les architectures existantes adressant les échanges de certificats entre organisations. Il ne s'agit pas ici de faire une étude comparative de tout ce qui pourrait se référer aux domaines étudiés. En effet, les architectures existantes n'adressent qu'une partie des problématiques soulevées ici. Cependant, cela permet de mettre en relief les attentes énumérées au chapitre précédent et les technologies couramment employées aujourd'hui, d'étudier les sources de normes et de standards qui seront employées en troisième partie, et surtout, de rendre compte d'un constat, celui du besoin d'une architecture plus respectueuse de la vie privée. Nous verrons que ce constat pousse à prendre en considération un environnement utilisateur enrichi, ce qui justifie les besoins en termes d'universalité et de pervasivité.

La seconde partie a pour objectif de décrire les briques technologiques nécessaires à la réalisation d'une architecture d'échanges de certificats et de négociation de confiance. Pour cela, les états de l'art des domaines concernés sont menés afin, d'une part, de mettre en relation différentes contributions existantes, et d'autre part, d'étendre au besoin certaines d'entre elles.

Au **chapitre 4** est faite une étude des besoins en matériel cryptographique afin de permettre des échanges de certificats anonymes, de mener de multiples négociations non-associables, et de permettre la présentation sélective d'informations contenues dans les certificats. Sont également présentés la notion de système à pseudonymes, ainsi que les besoins architecturaux pour permettre la mise en œuvre de pièces d'identité civile anonymes, de la révocation de l'anonymat et, enfin, de la non-transférabilité des certificats. Un bilan des travaux scientifiques existants est présenté et des composants pour bâtir notre architecture de certificats sont choisis. Une description générale et quelques notes d'implémentations sont présentés concernant les réalisations menées en langage de programmation C.

Le **chapitre 5** précise les notions de connaissance et de reconnaissance d'un tiers, d'identité connue publiquement et de confiance acquise en dehors du système de négociation. La notion d'anonymat est discutée à la vue de ces concepts. L'apport des travaux du chapitre précédent permet notamment de discuter plusieurs considérations pratiques sur l'emploi de pseudonymes qu'il est possible d'envisager entre deux interlocuteurs. La confidentialité des échanges basée sur le pseudonyme employé comme clé publique permettant l'échange du secret de confidentialité est ensuite étudiée. Nous justifions la certification de la clé publique dans chacun des certificats, par une signature à l'aveugle si la non-associativité est requise. Il est alors justifié le concept de confiance croissante dans la confidentialité du

canal de communication. Le pseudonyme étant une information sensible, il est supposé renouvelable d'un pseudonyme à usage unique vers un pseudonyme déjà employé. Cette étude est illustrée à l'aide du protocole TLS.

Au **chapitre 6**, la négociation de confiance est dans un premier temps justifiée au regard des objectifs de l'architecture, notamment de la diffusion fine et contrôlée de l'information par les usagers. L'utilisateur est considéré comme étant au centre de l'architecture et « aux commandes » des échanges. Il est nécessaire de l'assister et d'améliorer son expérience par l'automatisation de ses choix. Nous nous appuyons sur les travaux scientifiques portant sur les négociations de confiance automatisées pour traiter ces problématiques d'utilisabilité. Une étude est faîte pour déterminer un langage de contrôle d'accès adapté à la négociation. Il est enfin présenté la faisabilité de ces objectifs par un cas d'étude. Outre la description de cet objectif de recherche sur l'utilisabilité, ce chapitre permet de présenter plusieurs considérations de mise en œuvre, notamment la détermination des générateurs disponibles satisfaisant les conditions de contrôle d'accès d'un consommateur.

La troisième partie vise à mettre en œuvre les mécanismes précédemment décrits. Il s'agit notamment de décrire quels sont les moyens qui permettent d'espérer satisfaire aux conditions de l'universalité et de la pervasivité.

Le **chapitre 7** explore l'idée d'une couche de gestion des identités dédiée au contrôle d'accès des applications. L'objectif est de soulever les enjeux et les problématiques majeurs d'une telle ambition. Une description fonctionnelle de l'agent de négociation est ensuite donnée de manière à ce qu'il soit adapté à l'environnement des utilisateurs comme outil de gestion des identités numériques et aux organisations comme outil de contrôle d'accès aux applications.

Le **chapitre 8** constitue la synthèse des besoins affiliés à la notion d'universalité en vue de parvenir à la pervasivité. Il est donné un sens pratique à la notion de confiance entre organisations. Les notions d'interopérabilité, d'espaces de noms communs et de standardisation, notamment par les standards du Web, sont présentées. Il est proposé une solution pour la sérialisation des certificats anonymes basée sur des données publiques des générateurs de certificats. La réalisation d'une application XML de ces données implémentée en langage C à l'aide des librairies libxml2 et xmlsec1 est présentée. Une solution de sérialisation du protocole de négociation basée sur l'enrichissement de documents XML est également proposée. La mobilité des usagers est un paradigme pour lequel des propositions sont faites, notamment basées sur une plateforme de confiance. Enfin, l'emploi de la négociation de confiance dans les environnements pervasifs et ubiquitaires et la notion

d'« identité en tout lieu[2] » sont discutés.

Le **chapitre 9** vise à « donner un visage » à l'environnement client. Cela permet notamment de comprendre en quoi il est possible que celui-ci soit une source de confiance pour l'utilisateur. Les questions d'ergonomie et d'acceptation utilisateur sont abordées afin d'introduire les tests utilisateurs permettant d'initier l'expérimentation nécessaire pour évaluer la proposition faite au chapitre 6.

2. trad. Identity Everywhere.

Partie I: L'identité et le monde numérique

CHAPITRE II

Quelle vie numérique pour demain ?

*Le **chapitre 2** décrit les notions générales de la gestion des identités numériques, précise celles de confiance, d'anonymat et de pseudonymat, décrit le besoin de respect de la vie privée inhérent à ces travaux, et enfin, liste sommairement les enjeux d'une telle architecture pour les utilisateurs et les organisations.*

Sommaire

"[...]
A l'oiseau: "Seigneur Cormoran, d'où vous vient cet avis ? Quel est votre garant ? Etes-vous sûr de cette affaire ? N'y savez-vous remède ? Et qu'est-il bon de faire ?
- Changer de lieu, dit-il.
- Comment le ferons-nous ?
- N'en soyez point en soin: je vous porterai tous l'un après l'autre en ma retraite. Nul que Dieu seul et moi n'en connaît les chemins, il n'est demeure plus secrète. Un vivier que Nature y creusa de ses mains, inconnu des traîtres humains, sauvera votre république."
On le crut. Le peuple aquatique l'un après l'autre fut porté sous ce rocher peu fréquenté. Là Cormoran le bon apôtre, les ayant mis en un endroit transparent, peu creux, fort étroit, vous les prenait sans peine, un jour l'un, un jour l'autre. Il leur appris à leurs dépens que l'on ne doit jamais avoir de confiance en ceux qui sont mangeurs de gens.
[...]"

Jean de La Fontaine, *Les Poissons et le Cormoran.*

II.1 L'identité numérique

II.1.1 Introduction

Il est possible de décrire l'identité de manière très générique comme l'existence d'une entité pour une autre et le fait que cette dernière soit à même de traduire cette existence sous une forme quelconque. Dans le monde numérique, une entité sujet, respectivement, objet, d'un processus informatique, revêt, respectivement, se voit associer, une identité au sein de ce processus. Il est alors possible de distinguer un premier aspect fonctionnel de l'identité, celui du référencement et de la description. L'identité numérique est ainsi un ensemble de données descriptives que l'on peut désigner par un identifiant, une valeur unique dans l'espace des valeurs servant à l'identification des identités pour un système. Lorsque l'identité représente un individu, une partie de sa description peut être faite par des attributs. Ce sont les attributs d'identité qui constituent le profil de l'individu. Cette notion est similaire à celle de (Bishop, 2002) qui définit simplement l'identité numérique comme la représentation informatique d'une entité. L'identité possède un deuxième aspect fonctionnel inhérent à l'entité interagissant avec un système. Celle-ci peut obtenir un ensemble de droits auprès du système, qui se traduisent en pratique par des autorisations d'accès à des données et des processus contrôlés par le système, appelé contexte de sécurité (Benantar, 2005). L'entité se voit alors associée une identité dès lors que l'accès est autorisé. Il est courant que cet accès soit soumis au fait qu'une entité ait à emprunter une identité déjà existante sur le système. L'entité doit donc établir une identité existante, généralement à l'aide d'une preuve. L'identité existante permet donc à une entité de l'emprunter afin d'exercer un ensemble de droits qui lui sont associés. Il est notamment possible qu'une entité puisse revêtir une identité distincte sur différents systèmes, ou plusieurs identités sur un même système. L'établissement d'une identité n'est cependant pas un pré-requis à des accès autorisés auprès d'un système. En effet, il s'agit de l'un des enjeux des travaux de la thèse, permettre un accès à une entité préalablement inconnue, c'est-à-dire n'établissant pas d'identité connue du système. Ainsi, une identité peut être créée dynamiquement lors d'un accès comme créée préalablement à celui-ci.

Il est possible de résumer ces deux aspects fonctionnels de l'identité numérique. Selon (Damiani *et al.*, 2003), il existe l'identité :

- au sens de l'identification d'une entité auprès d'un système, nommée « nym »,
- comme un ensemble de données descriptives d'une entité, nommée « identité partielle ».

II.1.2 Contrôle d'accès et gestion de compte

La gestion des identités numériques a deux applications classiques, la *gestion de compte* et le *contrôle d'accès*.

La *gestion de compte* est intimement liée aux notions d'audit et d'enregistrement d'activité d'une identité au sein d'un système. L'ensemble des informations ainsi glanées est appelé « compte » (Benantar, 2005). D'après la définition faite précédemment de l'identité numérique, sous son aspect descriptif, le compte peut être assimilé à l'identité numérique. Cela permet de rationaliser le fait que soit parfois associé à la notion de compte l'ensemble des paramètres de personnalisation généralement issus de l'activité d'une entité auprès d'un système, et le fait qu'une entité puisse revêtir de manière répétée une même identité au sein d'un système. L'association d'une entité à une identité, et abusivement à un compte, permet d'auditer l'activité de cette entité auprès d'un système, et de personnaliser ses interactions avec celui-ci, mais également de maintenir des droits précédemment acquis.

Le *contrôle d'accès* est aussi appelé *autorisation*[1]. Le contrôle d'accès consiste en l'implémentation d'une politique de sécurité appliquée au contrôle des accès à des services et des ressources. La politique prend la forme de règlements appliqués au travers de mécanismes. L'utilisation de modèles de contrôle d'accès permet de rationaliser les implémentations et d'assurer certaines propriétés du système prouvées par le modèle. Une identité se voit ainsi autorisée à exercer un ensemble de *droits* au sein d'un système. Une entité qui revêt une identité peut ainsi exercer les droits de celle-ci au sein du système. L'ensemble des données accessibles, et des processus exécutables, au sein d'un système au cours d'une session est appelé *contexte de sécurité*. Le contexte de sécurité, et la restriction des accès de l'entité à celui-ci, sont régis par un *moniteur de référence*. La représentation de l'entité au sein du moniteur de référence est appelée « principal » (Benantar, 2005).

II.1.3 Authentification

Encore une fois, nous décrivons ce concept par son aspect fonctionnel. L'authentification est parfois assimilée à la certification. Autrement dit, il est parfois appelé « authentification » le fait de pouvoir vérifier qu'une information est intègre et certifiée par un tiers. La certification de l'information est alors porteuse d'une preuve qui permet d'établir l'identité de ce tiers. Or, il est possible de considérer l'authentification comme un procédé permettant d'apporter la preuve de possession d'une identité. L'authentification est donc

1. Cela justifie l'acronyme Anglais AAA (Authentication Authorization Accounting) pour l'authentification, le contrôle d'accès et la gestion de compte.

un procédé employé pour la certification auquel s'ajoute le procédé visant l'intégrité de l'information.

Nous considérerons donc l'authentification comme un ensemble de mécanismes permettant d'établir l'identité d'une entité, et réciproquement, permettant à une entité d'établir une identité auprès d'un système. Les mécanismes d'authentification se basent sur la notion de preuve. Ainsi, on parle généralement d'apporter une *preuve* de connaissance ou de possession. Il est d'usage de classer les preuves apportées selon trois facteurs qui reflètent l'idée qu'une identité serait la déclinaison numérique unique d'une entité pour un système. Ces catégories permettent à une entité d'apporter la preuve de son identité selon ce qu'elle « sait », « possède » ou « est » (Bishop, 2002). Ces catégories ont un impact fort sur l'implémentation des mécanismes d'authentification, cependant, il est difficile de leur donner un sens lorsque l'on parle de protocole d'authentification par exemple. En effet, le mot de passe pris comme l'exemple le plus courant de ce que l'on « sait », devient une preuve que l'on possède dès lors qu'il est inscrit dans un fichier. De la même manière, la biométrie, preuve par ce que l'on est, fournit une preuve équivalente à une clé, qui a le désavantage de ne pas être révocable. Nous appellerons par la suite *établissement d'une identité* l'événement à l'issu duquel une entité emprunte une identité auprès d'un système. Ce terme a le mérite de faire abstraction des mécanismes sous-jacents. Pour cela, il n'est plus fait de distinctions concernant les mécanismes d'authentification dans la suite de ces travaux, et afin de faire abstraction de la notion de mécanisme, le terme *établissement d'une identité* sera préféré à *authentification*, de même que *validation de certificat*, en lieu et place du terme *authentification de certificats*.

Intéressons-nous cependant brièvement à un mécanisme d'authentification qui se distingue particulièrement et qui porte parfois à confusion avec la présentation de certificats. Il s'agit de l'authentification par contrôle d'un emplacement physique ou virtuel. Il est par exemple adressé un secret à une adresse électronique, de messagerie instantanée ou Web. Il est supposé que l'entité sujet du mécanisme d'authentification contrôle cet emplacement, ou tout du moins, sera seule à pouvoir y accéder. Cela passe donc généralement par un autre moyen d'authentification auprès du système qui héberge cet emplacement. L'emplacement est alors en quelque sorte l'identifiant de l'identité, et le fait que l'entité puisse retourner le secret au système, la preuve de possession de cette identité. Ce genre de mécanisme repose sur le choix de la destination, choix qui est généralement fait par l'usager. C'est donc à celui-ci de s'assurer que la destination est protégée, notamment par un mécanisme d'authentification fiable. Ce type d'authentification est appelé authentification par délégation. En étendant ce mécanisme, il est possible d'obtenir du système délégataire la génération d'une preuve, que l'entité emploiera pour établir son identité. Comme nous l'avions présenté au premier chapitre, il peut exister ou non une relation

entre le consommateur de la preuve et le fournisseur de celle-ci. S'il n'existe pas de relation, le délégataire est un espace de stockage d'éléments, une sorte de « portefeuille de preuves en ligne ». Citons par exemple le système OpenID (OpenID-Community, 2008). Si le consommateur possède un lien de confiance avec le délégataire, celui-ci devient un générateur, la preuve est un certificat, et il y a réellement délégation de l'authentification. Citons à présent l'exemple de SAML (Maler, 2006). Dans ce cas, le certificat est employé comme une preuve permettant d'établir une identité. Nous verrons au chapitre suivant que la délégation de l'authentification est une application contestable lors d'échanges inter-organisationnels.

L'association d'une entité physique à une identité numérique par un mécanisme d'établissement d'identité auprès d'un système est un paradigme qui n'a pas de solution fiable à 100% connue à ce jour. Cela est valable dans le monde numérique comme dans le monde physique. Dans le monde des télécommunications, cela est encore plus problématique. Les mécanismes d'authentification permettent la fourniture de preuves que l'on sait productibles par une entité. La tentation est grande de vouloir associer une identité numérique à une entité unique au travers de l'authentification. Cependant, vu du système, dès lors qu'une entité produit une preuve, elle est l'identité correspondante pour le système. Le terme « possession » d'une identité, très couramment employé, n'a donc pas réellement de sens. Les identités existent, et n'importe quelle entité, à même de produire une preuve, peut revêtir l'identité correspondante auprès du système. Nous verrons au chapitre 4, que l'authentification peut faire appel à des mécanismes supplémentaires, afin notamment d'éviter la cession de preuves ou la coalition d'utilisateurs, et cela par des moyens de coercition.

Il est enfin nécessaire de préciser deux notions qui sont proches des mécanismes d'authentification, la liaison de compte et la signature numérique.

Il est dans certaines circonstances appelé *liaison de compte*, le fait de modifier la preuve permettant à une entité d'établir une identité auprès d'un système. Prenons l'exemple d'une identité, représentant une entité, déjà existante au sein d'un système. Lors de la première interaction de l'entité avec le système, il lui sera demandé un ensemble d'informations permettant d'apporter la preuve qu'elle est l'entité que l'on veut associer à cette identité. Il est supposé que ces informations constituent un secret permettant l'authentification, et donc d'associer, le temps d'une session initiale, l'entité à cette identité. Une fois cette identité établie, le système et l'entité vont négocier un secret qui servira de preuve pour les authentifications suivantes. Citons l'exemple d'une administration quelconque qui possède dans son système d'information une identité pour chaque citoyen. Lors d'un premier accès au site en ligne de cette administration, un ensemble d'informations d'état

civil (ceux cités pour l'obtention de l'extrait de naissance) est demandé en guise de secret. Lorsque la session est établie, l'usager est par exemple invité à choisir un identifiant et un mot de passe pour les authentifications suivantes.

La *signature numérique* doit avoir les mêmes propriétés que dans le monde physique, être unique et n'être reproductible que par son auteur. La signature repose également sur la notion de secret, et afin d'assurer la non-répudiation, ce secret doit n'être connu que de l'entité qui l'emploie. La signature numérique repose sur le chiffrement asymétrique (Menezes *et al.*, 1996). L'auteur de la signature est détenteur d'une clé privée qui lui permet de signer. À celle-ci est associée une clé publique. La clé publique est diffusée au tiers souhaitant vérifier la signature accompagnée de l'identité de l'auteur pour ce jeu de clés. Si l'association de l'identité et de la clé publique est considérée comme sûre, vérifier la signature produite à l'aide de la clé privée à partir de la clé publique apporte l'information que l'élément signé l'a été par l'identité associée à la clé publique. La signature est donc un moyen d'authentification d'une identité. Il est considéré que la signature numérique est un mécanisme plus fort que la signature dans le monde physique, à la condition d'employer des clés de chiffrement suffisamment grandes. Les propriétés d'unicité et de non-reproductibilité sont notamment démontrables et vérifiables. La signature numérique offre en outre des fonctionnalités qui ne sont pas physiquement possibles, le fait qu'une signature numérique puisse servir à la vérification de l'intégrité du contenu d'un document par exemple.

II.1.4 Anonymat, « Pseudonymat » & Non-associativité

L'anonymat est un concept qui peut prendre différentes significations et posséder différentes propriétés. Nous partons d'une définition qui fait souvent l'unanimité dans le domaine des communications. L'anonymat est décrit comme le fait qu'un sujet ne soit pas identifiable au sein d'un ensemble de sujets, appelé l'ensemble d'anonymat (Pfitzmann & Kohntopp, 2001). Notons une remarque intuitive et formulée par (Diaz & Preneel, 2007) qui précise qu'une large population de sujets est nécessaire et que l'anonymat croît en fonction de cette taille et de l'impossibilité de distinguer les sujets au sein de l'ensemble d'anonymat. (Pfitzmann & Kohntopp, 2001) restreint cet ensemble, dans un environnement où les sujets peuvent être actifs ou non, aux sujets acteurs. Cette définition est particulièrement bien adaptée pour les systèmes décrivant des communications, les acteurs pouvant être émetteurs ou récepteurs, et donc, appartenir à l'ensemble d'anonymat restreint aux émetteurs ou aux récepteurs. Il est important de noter que cette définition induit la notion d'observation d'un système et des ensembles d'anonymat qui le composent.

Considérons le cas où un initiateur mène plusieurs négociations auprès de multiples four-

nisseurs. Les points d'observation de l'anonymat sont celui d'un attaquant extérieur au système (parfois appelé « outsider »), ou d'un acteur de notre système (parfois appelé « insider ») distinct de celui dont on souhaite préserver l'anonymat. Si l'on se focalise sur l'initiateur, les menaces représentant les points d'observation internes sont les générateurs et les fournisseurs.

D'un point de vue extérieur, l'attaquant peut avoir une connaissance préalable d'une entité. Cette connaissance peut être constituée des actions préalables de cette entité au sein du système, ou en dehors de celui-ci, autant que d'une identité de cette entité. L'anonymat implique que l'attaquant ne soit pas capable, en observant le système, de déterminer quelles sont les communications liées à cette information. Autrement dit, les communications d'un sujet doivent être indistinguables des autres communications. Cela implique qu'il ne soit pas possible de distinguer deux communications comme étant liées à un même sujet si tel est le cas.

D'un point de vue interne, assurer la propriété d'anonymat d'un initiateur vis-à-vis des points d'observation que sont les autres acteurs du système signifie, par exemple, que lorsqu'un générateur a émis un certificat utilisé par l'initiateur auprès d'un fournisseur, le générateur et le fournisseur ne puissent pas associer ces deux transactions. Cette propriété est appelée « inassociativité »[2], « non-associativité » ou « impossibilité de lier ». L'anonymat est ici assuré par la non-associativité des transactions qui implique qu'elles soient « non corrélables » ou « indistinguables » au sein d'un ensemble de transactions. Il doit également être possible de rendre de multiples négociations de l'initiateur avec un même fournisseur inassociables, même lorsque les mêmes certificats sont présentés de multiples fois. Cela est d'autant plus vrai lorsqu'un même initiateur négocie avec plusieurs fournisseurs, ceux-ci ne doivent pas pouvoir distinguer ces négociations. A l'inverse, l'établissement d'une identité connue signifie l'association de l'interlocuteur à un ensemble d'informations préalablement connues. Il s'agit donc de définir et de contrôler les associations attendues au sein d'un tel système et de prévenir celles qui ne le sont pas.

Il est nécessaire pour permettre la gestion de compte que les actions d'un acteur auprès d'un tiers soient associables et cela au travers de l'établissement d'une identité. Cet établissement peut notamment être mené en déclinant un identifiant que l'entité souhaite volontairement associable à son identité réelle. Ces identifiants sont appelés « alias ». Cependant, l'entité peut également souhaiter utiliser un identifiant qui ne soit pas associable, ni à son identité réelle, ni à aucune action en dehors de celles qu'elle mène en déclinant cet identifiant. Celui-ci est alors appelé « pseudonyme ». Le statut de l'entité qui emploi un pseudonyme pour décliner une identité est appelé « pseudonymat » (Pfitz-

2. trad. de "Unlinkability" par Yves Deswarte.

mann & Kohntopp, 2001). Le pseudonymat implique que les négociations menées sous un même pseudonyme soient associables. L'établissement d'une identité implique de prouver la possession d'un pseudonyme.

Une entité peut utiliser un pseudonyme différent auprès de chacun des tiers sur lequel est hébergée une identité. Si les pseudonymes d'un utilisateur sont indistinguables dans l'ensemble des pseudonymes, les différentes identités sont non-associables par la déclinaison des pseudonymes. Ainsi, l'emploi de pseudonymes indistinguables avec tout interlocuteur, générateurs y compris, lorsque l'établissement d'une identité est requis, est une condition nécessaire mais non suffisante pour permettre de rendre non-associables les délivrances et les présentations de certificats. Notons dès lors qu'une signature peut être un identifiant. Ainsi, si un certificat est délivré au consommateur tel qu'il est issu d'un générateur, les transactions qui impliquent ce certificat deviennent associables. L'association de ces transactions rend les pseudonymes, et donc les identités d'une même entité, associables. Nous reviendrons plus en détails sur ces notions au chapitre 4.

En résumé, pour satisfaire aux conditions d'anonymat dans notre cas d'étude, nous souhaitons qu'un système d'échange de certificats puissent permettre, pour une même entité, que :

- de multiples négociations sur un même fournisseur soient non-associables si aucune identité n'y est établie, et ce même en présentant plusieurs fois un même certificat,
- sous le couvert du pseudonymat, les transactions avec des tiers soient non-associables afin que ces multiples identités ne le soient pas non plus.

II.2 Introduction à la notion de confiance

La confiance a été définie au premier chapitre comme le moyen permettant à deux individus d'entrer en relation alors qu'ils n'ont pas la certitude de satisfaire leurs attentes envers cette relation. Les mécanismes de confiance, dans un univers numérique, peuvent reposer sur des mécanismes de sécurité. Mais ils vont bien au-delà puisqu'ils font appel à de multiples notions telles que la rationalité des individus ou la gestion des risques par les organisations par exemple.

(Cofta, 2007) définit un concept précis et intéressant de la confiance dans les communications. Il exprime le fait qu'il est nécessaire d'opposer les notions de confiance et de contrôle. La confiance est une notion subjective qui intervient dès que l'on souhaite entretenir une relation avec un tiers que l'on ne contrôle pas. Les moyens de contrôle assurent dans une certaine mesure que le comportement sera celui attendu. A l'inverse, la confiance a trait au comportement attendu d'un tiers, introduisant une incertitude, celle que le tiers pourrait ne pas se comporter ainsi. Un comportement est donc attendu avec un risque estimé que ce ne soit pas le cas. Ainsi, pour pouvoir entrer en relation avec un tiers, c'est-à-dire lui faire confiance[3], il est nécessaire d'avoir un certain niveau de confiance[4]. Pour cela, les intervenants utilisent divers moyens pour influencer le sentiment de confiance de leurs interlocuteurs[5].

Illustrons ce propos par deux exemples. Un commerçant peut se faire connaître grâce à une campagne publicitaire. Cela n'apporte aucune garantie sur son comportement, et la notion de connaissance est totalement subjective. Cependant, cela a pu déclencher chez certains sujets un sentiment de confiance, suffisant pour qu'ils puissent entrer en relation. Le client a cependant quelques moyens de contrôles, le service de répression des fraudes ou les associations de consommateurs par exemple, mais dont il ne pourra faire usage qu'*a posteriori* en cas de litige. Par contre, la connaissance de ces moyens de contrôle par le commerçant peut l'influencer pour qu'il honore ses engagements.

Prenons un second exemple qui illustre le fait que la notion de confiance est omniprésente dans la vie quotidienne. Un piéton souhaite traverser la chaussée, une voiture arrivant, et la signalétique piéton étant au vert. Le piéton se sent en confiance et entame sa traversée : il s'attend à ce que le conducteur respecte la signalisation et donc s'arrête au feu. Le piéton se sent en confiance grâce au contexte, c'est-à-dire grâce à l'ensemble des éléments significatifs de son environnement (le feu vert est par exemple un facteur influent). Ce-

3. trad. "To trust."
4. trad. "To be confident."
5. trad. "Trustworthiness."

pendant, certains facteurs ont une valeur difficilement estimable, donc, même si l'on sait que certains critères sont influents (l'inconscient, l'expérience, la météorologie, l'éventuel ralentissement de la voiture, etc.), ils restent difficiles à interpréter et à modéliser. Lors d'une situation similaire mais en changeant certains paramètres, la nuit par exemple, le piéton peut ne pas se sentir en confiance et ne pas entrer en relation, ne pas traverser. Disons que le piéton entame sa traversée. Il n'a aucune garantie sur le bon déroulement de sa traversée. Il n'a pas le contrôle du conducteur qui lui-même n'a pas le contrôle de tous les mécanismes de sa voiture. Il y a donc une relation de confiance qui s'établit entre le piéton et le chauffeur alors qu'ils ne se connaissaient pas avant cette interaction. Cet exemple permet d'introduire la notion de subjectivité de la confiance. Dans une situation donnée, les relations de confiance sont multiples et leur recensement est quasiment impossible. En effet, le piéton fait également confiance dans le système de freinage, dans le garagiste ayant fait la révision du système de freinage, etc. On pourrait introduire les notions de confiance directe et indirecte mais leur distinction est souvent difficile. Le piéton fait indirectement confiance dans les procédés de fabrication du système de freinage du constructeur automobile par exemple, mais également dans l'automate ayant fait le montage, ou dans l'opérateur de l'automate, ou le développeur du logiciel embarqué de l'automate, etc. Enfin, les contrôles sont nombreux. Ils permettent au piéton de se sentir en confiance, et donc de faire confiance. Citons par exemple la signalisation au sol ou celle des feux. Cependant, les notions de contrôle sont également subjectives. Citons par exemple la peur par le chauffeur des contrôles routiers qui le poussent à respecter le code de la route et à s'arrêter au feu.

Revenons à notre première modélisation de l'environnement de négociation. Au chapitre précédent nous avons précisé l'existence de deux types de relation de confiance, entre les générateurs et consommateurs de certificats, et entre les deux parties négociatrices. Cette supposition vient du fait que nous avons considéré que l'ensemble des acteurs puissent appartenir à des domaines de sécurité différents. Selon la notion de confiance introduite ici, il ne peut y avoir un contrôle total entre les différents acteurs, ce qui nécessite d'introduire la confiance pour leur permettre d'entrer en relation. A l'inverse, si le *générateur* et le *consommateur* sont administrés par une même autorité, leur relation est de contrôle et non de confiance. Il est par exemple considéré qu'il s'agit du cas des architectures d'authentification unique intra-organisationnelles. Au chapitre 6 est détaillée la nature des liens de confiance des acteurs de la négociation.

Il est attendu que la négociation, visant à établir une relation de confiance entre un initiateur et un consommateur, repose sur un équilibre entre confiance et contrôle. Lors d'une première interaction entre initiateur et fournisseur, sans aucune connaissance préalable l'un de l'autre, ceux-ci vont établir une relation de confiance, au travers des échanges

de certificats de leur propre domaine de confiance. Or, le risque est que chacun essaye d'augmenter au maximum son pouvoir de contrôle. En effet, l'intérêt de la négociation peut être d'enrayer la tendance du recours à un contrôle maximum. De plus, le contrôle ne peut répondre à toutes les situations. Il est souvent admis que les niveaux de confiance fluctuent, tant et si bien que la confiance peut se perdre. Et cela, aussi bien entre usagers qu'entre organisations, notamment lorsqu'un des interlocuteurs requiert trop de contrôle (Cofta, 2007). L'usager souhaite bien-sûr avoir des moyens de contrôle, mais il préfèrera sûrement interagir avec des personnes de confiance, avec lesquels la confiance se justifie, rendant ainsi les moyens de contrôle obsolètes.

Les échanges de certificats permettent de réaliser l'établissement d'une relation de confiance. Ainsi, chaque certificat contribue à l'établissement de la relation. Cependant, il est difficile de déterminer le besoin, de contrôle ou de confiance, que chaque certificat permet de satisfaire. La contribution de chaque certificat à l'établissement de la relation justifie le fait que nous puissions dire que les échanges de certificats, provenant de tiers de confiance, permettent l'établissement d'une relation basée sur la confiance. Cependant, la remarque précédente justifie qu'en première partie nous ayons indiqué que les éléments présentés visent à satisfaire des besoins de contrôle afin de pouvoir établir une relation de confiance.

En résumé, la confiance dénote une part d'incertitude dans l'attente d'un fait. Elle est périssable et une fois accordée, elle nécessite d'être entretenue. Par simplicité, dans le reste de ce document, nous parlons de confiance sans faire la distinction entre contrôle et confiance, cela afin de désigner une complémentarité entre un sentiment de confiance et certains moyens de contrôle en vue d'établir une relation. Lorsque cela est nécessaire nous revenons sur cette notion, notamment de manière concrète et appliquée au chapitre 8.

II.3 Respect de la vie privée

II.3.1 Introduction

Le respect de la vie privée[6] est aujourd'hui considéré comme un droit fondamental qui prend place aussi bien dans des traités internationaux (la convention européenne des Droits de l'Homme par exemple) que dans les constitutions nationales. D'un point de vue historique, ces droits avaient pour but de protéger les citoyens de leur gouvernement. Le droit au respect de la vie privée fut définie dès 1890 par (Warren & Brandeis, 1890) comme "Le droit d'être laissé seul"[7] suite à une intrusion dans sa vie privée par un journal de Boston. Le débat refit surface dans les années 60 suite à l'arrivée des premiers ordinateurs synonymes d'une puissance de calcul pouvant servir au traitement de données personnelles. Ce qui fit naître le droit de protection des données. (Schoeman, 1984) livre cette définition :

> "Une personne voit sa vie privée respectée dans la mesure où des tierces personnes ont un accès limité aux informations la concernant, aux aspects intimes de sa vie, à ses pensées ou à son corps."[8].

Cette définition nous permet d'élargir le concept de respect de la vie privée à l'observation du comportement d'une personne et de ses relations, ses biens, sa connaissance ou bien encore son intégrité physique. Concernant notre problématique, nous retiendrons les enjeux du traitement des données personnelles et du suivi d'activité intégrant les aspects comportementaux et relationnels d'un individu.

L'objectif de la protection de la vie privée des personnes est de prévenir des menaces sociétales telles que la diffamation, la ségrégation, l'exclusion, ou bien encore, la discrimination. Dans ces cas, les informations confidentielles sont par exemple : les origines ethniques, les orientations sexuelles, ou bien encore, la confession religieuse. Mais les menaces sont également d'ordre économique, avec par exemple les campagnes de publicité ciblées ou la vérification implicite du respect des droits d'auteurs. En psychologie, le respect de la vie privée est nécessaire à l'épanouissement des personnes, aussi appelé autonomie, qui peuvent expérimenter la vie sans avoir une peur constante du jugement.

Il existe plusieurs domaines de contre-mesures à la violation de la vie privée. Les principaux sont les contre-mesures techniques, comportementales et juridiques. Dans les travaux de cette thèse nous traiterons des deux premiers. Ajoutons un mot concernant le troisième.

6. trad. "Privacy."
7. trad. "The right to be left alone."
8. trad. "A person has privacy to the extent that others has limited access to information about him, limited access to the intimacies of his life, or limited access to his thoughts or his body."

La loi repose sur la généricité de manière à pouvoir être appliquée à de nombreuses situations. Et savoir si la vie privée n'a pas été respectée au sens de la loi dépendra de l'interprétation de la situation par la justice, et notamment des intentions de la victime présumée. Par exemple, une célébrité sur une plage publique prise en photographie pourra sûrement poursuivre l'auteur pour une atteinte à son droit à l'image, et non, pour violation de sa vie privée.

II.3.2 Protection des données personnelles

La protection des données personnelles est une facette importante du respect de la vie privée. Elle s'appuie sur deux nécessités fondamentales :

- Obtenir le consentement d'un individu lors de la divulgation ou de la rétention d'informations personnelles le concernant.
- La nécessité de sécuriser les données personnelles. Citons un jugement de 2005 de la commission fédérale américaine du commerce[9] :

  > "Les consommateurs doivent avoir la certitude (intime conviction) que les sociétés qui possèdent des données confidentielles les concernant les manipuleront avec le soin qui leur incombe et y apporteront les moyens de sécurisation appropriés"[10].

Ce jugement fut émis suite à une transaction financière en ligne dont les communications ont circulé « en clair ».

II.3.3 Protection des communications

Il s'agit de l'autre facette du respect de la vie privée dans le monde numérique. Le mythe de « Big brother »[11], et plus sérieusement, les projets dans la verve du projet Echelon[12] représentent les menaces les plus visibles de la surveillance. Celle-ci regroupe l'ensemble des procédés de traitement des observations d'individus ou de groupes. Les objectifs sont variés. Par exemple, les états y voient un moyen de lutte contre le terrorisme ou le crime, les employeurs un moyen de vérifier l'efficacité de leurs employés, etc. Les systèmes informatiques et de télécommunications offrent une opportunité jusque-là jamais égalée en terme de surveillance. Appelée la « dataveillance », celle-ci représente un moyen de collecter et de traiter des informations personnelles à grande échelle (Clarke, 1988).

9. US Federal Trade Commision
10. trad. "Consumers must have the confidence that companies that possess their confidential information will handle it with due care and appropriately provide for its security."
11. Personnage de fiction du roman 1984 de George Orwell.
12. Système de renseignement élaboré par les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande dans le cadre du traité UKUSA.

Le traitement des données repose sur plusieurs techniques qui peuvent mettre à l'épreuve le respect de la vie privée. Citons par exemple la fusion de bases de données couplée à la comparaison d'enregistrements concordants sur les identités. En effet, mettre en comparaison des relevés bancaires et des déclarations d'impôt est un moyen de lutte efficace contre la fraude fiscale. Citons également les traitements statistiques de données ou suivant des modèles de données qui permettent d'extraire de bases de données des comportements de consommation. Une banque pourrait faire une étude statistique sur les faillites personnelles par région, et ainsi appliquer des quotas de prêts bancaires différents selon la provenance géographique du demandeur. Il est également possible que les télécommunications soient un préjudice pour l'intégrité physique d'un sujet, citons notamment la géo-localisation horodatée avec des technologies telles que les téléphones mobiles ou les transpondeurs RFID.

II.3.4 Savoir que l'on est une victime

Pato et Casassa-Mont (Pato, 2003 ; Mont *et al.*, 2002) présentent une vision de ce qu'un sujet perçoit de lui-même et cela selon ce qu'il sait de lui, selon ce qu'il sait que l'on sait de lui, et selon ce qu'il ne sait pas que l'on sait de lui[13]. Bien qu'intuitive, cette distinction est rarement faite consciemment par les individus. La perception de leur vie privée, et la violation de leurs droits à ce sujet, sont floues. La preuve en est que la plus grande menace connue à ce jour vient de ce que les usagers diffusent délibérément. Les réseaux sociaux sont au cœur de ces problématiques, les utilisateurs y révèlent des informations qui peuvent leur être préjudiciables en sous-estimant leur impact potentiel. Comme Baker (Baker, 1996), alors chef du conseil de la NSA le souligna:

> "La plus grande menace pour notre vie privée dans le monde digital ne vient pas de ce que nous conservons secret mais de ce que nous révélons volontairement.[...] Restreindre cet envahissement de la vie privée est un challenge, mais ce n'est pas une tâche pour le chiffrement. Le chiffrement ne peut pas vous protéger contre les mauvaises utilisations des données que vous avez fournies volontairement."

Cela conduit à étudier la perception par les utilisateurs des violations potentielles et avérées. Nissenbaum (Nissenbaum, 1998) parle, pour la surveillance dans des lieux publics, d'« intégrité contextuelle ». En effet, les usagers considèreront (à juste titre) que leur intégrité, le respect de leur vie privée, a été violée si les données collectées en un lieu, et pour les besoins de l'activité en ce lieu, sont connues ou exploitées dans un autre. Si la perception n'est pas effective, le sentiment des usagers peut tendre simplement vers la sensation de gène ou de doutes répétés, ce qui les conduiraient à ne plus faire confiance dans les

13. trad. respectivement "Me-Me", "Known-Me" et "Unknown-Me".

systèmes informatiques et de télécommunications, sans pour autant pouvoir l'expliquer clairement. Sans céder à la technophobie, cela pourrait cependant poser des problèmes d'acceptabilité.

Nombre d'« acteurs de l'identité numérique » ont conscience du fait que le non-respect de la vie privée est un risque latent qui met en péril le monde numérique, citons par exemple la commission européenne (Directorate-General XIII, 1997) :

> "Si les citoyens et les sociétés ont à craindre que leurs communications et leurs transactions soient auditées avec l'aide de systèmes de contrôle d'accès, ou d'architectures similaires, élargissant injustement les capacités de surveillance des agences gouvernementales, ils préfèreront rester dans le monde hors ligne anonyme et l'avènement du commerce électronique n'aura jamais lieu. " [14].

Il est cependant nécessaire de nuancer ces propos, notamment au regard des réseaux sociaux qui sont le contre-exemple de ces propos.

Enfin, les environnements informatiques ubiquitaires et pervasifs, en devenir, visent à permettre à tout un chacun de bénéficier de tous les services numériques auxquels il a droit, en tout lieu, à tout instant. Ces environnements s'appuient sur des technologies telles que l'intelligence ambiante, les réseaux de capteurs et l'identification automatisée notamment afin d'offrir l'automatisation de la fourniture de services personnalisés. (Langheinrich, 2001) et (Brey, 2006) ont identifié six menaces pour la vie privée liées à l'informatique ubiquitaire : l'ubiquité, l'invisibilité, la détection automatisée [15], l'amplification de la mémoire [16](enregistrement et analyse des actions), la détermination d'un profil usager aussi appelé profilage [17] et l'inter-connectivité [18](connexions des objets entre eux). Nous reviendrons sur les environnements pervasifs et ubiquitaires au chapitre 8.

Nous considérons dans la thèse l'« Internet » comme le support universel de l'infrastructure de télécommunication incluant l'ensemble des réseaux augmentant son nombre de points d'accès. Dès lors qu'un réseau offre la possibilité de connecter un terminal au reste du réseau, c'est un réseau qui sera assimilable à l'Internet, réseaux d'opérateur mobile et de capteurs y compris. A ce titre, l'Internet représente une menace difficile à juger pour un usager non averti, tant il est difficile de quantifier le volume d'informations personnelles disséminées au fil des connexions et le nombre de canaux exposant les flux de

14. trad. "If citizens and companies have to fear that their communication and transactions are monitored with the help of key access or similar schemes unduly enlarging the general surveillance possibility of government agencies, they may prefer remaining in the anonymous off-line world and electronic commerce will just not happen."
15. trad. "Sensing."
16. trad. "Amplification of memory."
17. trad. "User profiling."
18. trad. "Connectedness."

communication. Il est dès lors possible de mesurer la « surexposition » des architectures d'échanges d'informations sur les usagers et entre organisations, au travers de l'Internet, et cela en cours de consommation de services.

II.3.5 Vie privée et identité numérique

Ce que nous avons appelé l'identité réelle dans le premier chapitre, (Giddens, 1991) l'appelle l'identité selon soi-même[19], et la définit comme :

> "une mémoire perçue par soi-même et qui devrait être continuellement ajustée pour construire le récit de sa vie[20]."

Cette identité symbolise le soi. Nous avons tenté de montrer qu'il n'était pas possible pour un individu de prouver sans une incertitude qu'il est bien cette identité auprès d'un tiers. Cependant, cette notion apporte une dimension qui n'est pas physique à l'identité, et qui est l'ensemble des informations d'une vie, non totalement descriptibles puisque perçues de soi-même. L'identité est alors vue comme un tout. Lorsqu'un individu communique, il s'expose au reste du monde et il existe. Pour autant, l'humain s'évertue généralement à ne présenter qu'un sous-ensemble des informations le concernant au monde extérieur, et cela suivant le contexte ou l'interlocuteur par exemple. Chacun de ces sous-ensembles peut être considéré comme une identité visible d'une entité. Comme (Giddens, 1991) l'exprime, les communications numériques ont permis une virtualisation de ces identités. Ce que l'on a nommé identité numérique au sein d'un système n'est ainsi qu'une identité visible d'une identité. A l'instar du monde physique, une observation peut permettre de créer une identité sans que l'entité observée puisse en être consciente. A l'inverse, un usager devrait pouvoir développer un ensemble d'identités distinctes qui ne seraient pas assimilables à une même entité, et cela afin de garder éloigné au maximum ce qui est connu de lui-même.

Si l'on rapproche ces notions de celle de l'identité numérique, au sein d'un environnement distribué, l'enjeu de la protection de la vie privée consiste en :

- la gestion de la diffusion des information d'identité,
- l'inassociativité des multiples identités empruntées par une même entité et de ses activités entre différents systèmes.

Or, notre problématique nécessite la convergence de ces identités dans le but de véhiculer des informations de l'une vers l'autre. En effet, on considère que les organisations, générateurs et consommateurs, possèdent des identités visibles distinctes d'une même entité, et l'on souhaite qu'ils puissent échanger des informations sur celles-ci. Cela revient à faire correspondre les identités, ce qui va à l'encontre des précautions liées au respect de la vie

19. trad. "Self-identity."
20. trad. "A self-reflective memory of oneself that should be reconciled to construct the narrative of life."

privée qui veulent que ces identités ne soient pas associables. Il s'agit donc de mettre en œuvre des mécanismes permettant d'assurer les conditions de l'anonymat décrites précédemment. Autrement dit, l'association des identités d'une même entité ne doit être possible que par l'entité elle-même. Il s'agira pour autant de permettre une négociation faisant intervenir de multiples organisations et identités visibles d'une entité, en offrant à celle-ci des moyens de diffusion de ses informations simples et contrôlables. Voici donc l'un des enjeux majeurs soulevés par les travaux de cette thèse, permettre une négociation faisant intervenir de multiples organisations et identités visibles d'une entité en assurant qu'elle soit la seule à pouvoir les faire concorder. Et selon la reflexion de (Pato, 2003 ; Mont *et al.*, 2002), qu'une entité ait le contrôle maximum sur les informations diffusées à son égard.

II.4 Les enjeux de la vie numérique

Il est désormais temps de définir les attentes de chacun des acteurs et de répondre à la question fondamentale : « qu'est ce que chacun a à gagner et à perdre ? ». Avant de tenter de répondre à cette question, quelques cas d'usage communs sont décrits afin d'étayer notre argumentaire.

II.4.1 Cas d'usage

La négociation requiert dans un premier temps de traiter les attentes de chacun envers les échanges de certificats. Nous nous intéressons plus particulièrement au cas d'un initiateur humain, qui requiert un objet d'un fournisseur hébergé par une organisation. Il présente pour cela des certificats qu'il a obtenu d'organisations du domaine de confiance du fournisseur. La problématique de la détermination de l'appartenance des sources de certificats au domaine de confiance du fournisseur est abordé par la suite. Notons pour l'instant qu'un règlement énumère les certificats requis pour satisfaire les conditions du contrôle d'accès, ainsi que les sources potentielles des certificats attendus.

II.4.1.1 La monnaie électronique

L'un des cas d'usage est le paiement en ligne. Celui-ci doit pouvoir se faire dans le domaine financier international. Il est en outre intéressant de considérer le traitement de n'importe quel type de monnaie, celles qui n'ont de valeur que dans des sphères réduites particulières[21] : bons d'achats valables dans une chaîne de magasins, monnaie de jeux vidéos valable pour tous les jeux d'un éditeur, points de fidélité, etc. Cependant, le but recherché est un paiement avec une propriété de l'argent liquide du monde physique, le fait qu'une banque ne puisse pas savoir où un individu dépense son argent. On appelle cela la *monnaie électronique*[22](Chaum *et al.*, 1990), que l'on distingue du paiement électronique. En effet, lorsqu'un individu retire de l'argent liquide à un distributeur, la banque ne sait pas quand, ni où, il sera dépensé.

L'une des premières difficultés soulevées vient du support, les données digitales. Cela soulève une problématique qui n'existe pas dans le monde physique : lorsqu'une pièce de monnaie est dépensée dans le monde physique, l'acheteur n'est plus en possession de celle-ci. Or, dans le monde numérique, le certificat reste en sa possession, il ne fait que le présenter au consommateur. Les certificats utilisés pour la monnaie électronique doivent donc être à usage unique. Il faut ajouter le fait que le consommateur (le commerçant) ne

21. trad. "Scrip."
22. trad. "e-cash."

doit pas non plus pouvoir encaisser cet argent plusieurs fois. Il s'agit donc de gérer l'usage des certificats.

La deuxième difficulté de la monnaie électronique est de ne pas permettre la mise en correspondance des transactions de génération et de consommation d'un même certificat entre le commerçant et la banque. Cette propriété assure que les activités menées auprès de chacun ne puissent pas être associées par l'intermédiaire des certificats de monnaie.

II.4.1.2 La pièce d'identité

Nous avons soulevé à plusieurs reprises la problématique de la pièce d'identité civile. Les enjeux de la pièce d'identité civile numérique sont multiples :

- fournir un moyen de contrôle permettant un recours juridique en cas de litige auprès d'une entité juridique compétente,
- octroyer des droits d'accès aux citoyens du fait qu'ils appartiennent à un ensemble, celui des citoyens français,
- permettre l'établissement de l'identité auprès des fournisseurs de l'état,
- permettre la fourniture d'informations d'état civil certifiées.

Les deux premières applications ne nécessitent pas de révéler d'attributs de l'identité civile. La première application peut être réalisée à l'aide d'une pièce d'identité anonyme dont chaque nouvelle présentation serait non-associable aux précédentes. Pour la seconde, il suffit de prouver la possession d'une pièce d'identité valable. La troisième application peut prendre deux formes. La pièce d'identité peut permettre de produire une preuve d'identité, par signature par exemple, ou les attributs certifiés peuvent servir de moyens d'authentification (quatrième application). Notons que si la pièce d'identité se matérialise par un unique certificat, cela suppose que sa possession puisse être prouvée sans ne révéler d'autre information que sa possession (répond aux deux premières applications), qu'il contienne une clé publique pour la signature et que les attributs qu'il contient puissent être présentés indépendamment les uns des autres, ce qui est nommé « présentation sélective » du contenu d'un certificat.

À la différence de la monnaie électronique où il peut être souhaité que l'anonymat ne soit révoqué que lors d'une action de l'individu, tel qu'essayer de « dépenser » deux fois le même certificat, la révocation de l'anonymat d'une pièce d'identité doit pouvoir être faite même si l'utilisateur n'utilise pas directement ce certificat de manière frauduleuse. La révocation pourrait être faite par le générateur du certificat, cependant cela n'apporterait pas un niveau de protection de la vie privée suffisant. Il est en effet nécessaire de concevoir une architecture où ni le générateur, ni le consommateur ne puissent révoquer l'anonymat. Il est donc nécessaire d'introduire un tiers de confiance de l'utilisateur et du

consommateur qui soit indépendant des deux.

Revenons sur le concept d'identités réelles et civiles. Pour que l'identité civile empruntée dans le monde numérique soit la plus proche de l'identité réelle, il serait judicieux que les certificats soient émis par l'état civil lui-même. Il faut ajouter à cela qu'il est fort probable que l'on assiste à la convergence des mondes physique et numérique pour ce qui est de l'établissement de l'identité civile à travers une unique pièce d'identité. En effet, les pièces d'identité physiques intègrent désormais des composants numériques qui sont promis à des fonctionnalités telles que la signature. Il est donc envisageable qu'un utilisateur puisse générer ses propres certificats à partir d'une clé contenue dans sa pièce d'identité, elle-même signée du générateur qui serait l'état civil. Le porteur crée le certificat au nom du générateur en apposant une signature avec une clé signée, directement ou indirectement, par le générateur. Cela permet donc d'apporter au consommateur un certificat indirectement signé d'un générateur de confiance alors que ce celui-ci ne l'a pas généré.

Ce cas d'usage soulève diverses problématiques telles que le renouvellement et la révocation des certificats. Le fait de vouloir des certificats à usages multiples accentue la problématique de la durée de validité et de la révocation des certificats. En outre, diverses fonctionnalités des certificats, qui seront détaillées au chapitre 4, ont été mises en lumière.

II.4.1.3 Un cas banal

Terminons par le désormais célèbre cas d'usage de la location de voiture (Camenisch & Pfitzmann, 2007). Celui-ci nécessite un paiement, la présentation d'une pièce d'identité, d'un permis de conduire et d'une assurance. Le permis de conduire peut être anonyme, de même que la pièce d'identité et l'attestation d'assurance. Autrement dit, seule la preuve de leur possession est requise. Nous avons dit qu'il était difficile de s'assurer lors de télécommunications que le sujet est bien le porteur des certificats. Ainsi, il est possible que l'utilisateur cède ses secrets, donc ses certificats. La nouvelle difficulté intéressante de ce cas d'usage est de pouvoir traiter des pièces d'identité anonymes comme provenant d'une même entité. La problématique est de s'assurer, d'une part, que ces pièces sont toutes relatives à une même entité, et cela, sans que les générateurs puissent lier leur identité respective de l'individu, d'autre part, que le porteur soit l'individu sujet.

II.4.1.4 Remarques

Ces cas d'usage soulèvent deux problématiques majeures, à savoir :

1. Le besoin d'une architecture de confiance globale. Il s'agit de mettre en œuvre un nombre suffisant de sources de confiance pertinentes afin que deux interlocuteurs

puissent espérer déterminer les sources du porteur qui soient de confiance pour le consommateur. Il s'agit également de mettre en œuvre les mécanismes permettant de découvrir quelles sont ces sources, c'est-à-dire des mécanismes de découverte de chemins de confiance. Notons qu'il apparaît inévitable de constituer des ensembles de sources dédiées à des pans de métiers (services de l'État, assureurs, banques, etc.) et que ces ensembles aient une source racine dont le certificat à clé publique soit publiquement connue permettant ainsi de déterminer « simplement » un chemin de confiance pour les sources sous-jacentes.

2. Le besoin d'interopérabilité. Pour prétendre à la pervasivité, il est nécessaire que tous les acteurs puissent interopérer. Il s'agit, d'une part, de définir des algorithmes communs ou interopérables, et d'autre part, des espaces de nom communs, ou qu'il est possible de mettre en correspondance. L'interopérabilité des algorithmes touche aussi bien les primitives cryptographiques que les protocoles. Les espaces de noms portent sur les informations d'identités, les certificats, les règlements de contrôle d'accès, ou bien encore, les messages protocolaires.

Nous reviendrons concrètement sur les moyens d'adresser ces deux problématiques au chapitre 8.

II.4.2 Les enjeux du point de vue des organisations

Les enjeux et attentes pour les organisations peuvent se résumer à :

- augmenter l'offre de services aux consommateurs,
- réduire la complexité des démarches administratives,
- réduire le coût de la gestion des démarches administratives,
- réduire les coûts d'administration des identités numériques.

Au paragraphe précédent, nous avons soulevé les deux problématiques majeures que les organisations auront à résoudre. Concernant les certificats, résumons les problématiques des utilisations frauduleuses potentielles :

- parer à la cession de certificats par l'utilisateur,
- lier les certificats à propos d'un même sujet, autrement dit, que plusieurs utilisateurs ne puissent pas s'allier pour cumuler leurs certificats, dans le but par exemple d'obtenir des droits d'accès supérieurs à leur droits respectifs,
- gérer le cycle de vie des certificats (utilisables une ou plusieurs fois),
- gérer les renouvellements et les révocations de certificats,
- se conformer à la législation sur le respect de la vie privée.

Les organisations ont le souci de l'adoption de ces technologies sans laquelle rien n'est possible. Cela implique une simplicité d'utilisation par un utilisateur non averti et de

mise en œuvre (installation/configuration/maintenance). Cela signifie également que les organisations veulent la confiance des utilisateurs, donc qu'elles sont enclines à mettre en œuvre des mécanismes leur permettant de « donner l'impression » aux usagers que leur vie privée est respectée. Enfin, ajoutons une problématique qui est soulevée dès le prochain chapitre, est celle de l'universalité. En effet, l'architecture présentée dans cette thèse repose sur l'enrichissement de l'environnement de l'utilisateur afin de gérer ses identités numériques et ses certificats, et l'enrichissement de l'environnement fournisseur afin de gérer le contrôle d'accès. Nous supposons pour cela le déploiement d'un outil logiciel universel. Nous justifierons au chapitre 7 le fait qu'il puisse s'agir d'un même module pour les deux applications et que nous souhaitons universel.

II.4.3 Les enjeux du point de vue des usagers

Les enjeux du point de vue de l'usager sont principalement le respect de sa vie privée, l'ergonomie d'utilisation des services et d'obtention des ressources. Les attentes envers le respect de leur vie privée dépend de la perception qui en est faite, différente pour chaque individu. Cependant, nous avons fait le choix de « décider » pour l'individu quels sont ses attentes, soit :

- contrôler l'ensemble des informations diffusées à son sujet,
- diffuser le minimum d'informations afin de satisfaire sa requête,
- que l'on ne puisse pas usurper son identité,
- que l'on ne puisse pas présenter des certificats qui auraient pu être générés pour lui,
- que les certificats qu'il présente aux consommateurs ne puissent pas être réutilisés par ceux-ci auprès d'autres consommateurs,
- un consommateur ne doit pas pouvoir prétendre auprès d'un tiers qu'un utilisateur lui a présenté plusieurs fois un même certificat si ce n'est pas le cas (palier au double encaissement de l'argent par exemple),
- les générateurs et les consommateurs ne doivent pas pouvoir lier les transactions afin de ne pas pouvoir lier leur identité numérique respective de l'utilisateur,
- il doit être possible de fournir des certificats aux consommateurs sans que les générateurs puissent en avoir connaissance afin d'éviter le suivi d'activité des usagers.

Nous déduisons de ceci qu'il est nécessaire que l'utilisateur puisse contrôler les informations contenues dans les certificats, donc qu'il puisse intervenir sur le contenu présenté en fonction de l'information demandée par le consommateur. Ainsi, l'information présentée pourra être différente de celle contenue dans un certificat, par exemple n'indiquer que sa majorité à partir de sa date de naissance, ou bien encore n'indiquer que si un conducteur possède encore des points sur son permis de conduire et non le nombre de points restants, etc.

L'interface « homme-machine », composante de l'agent de négociation de l'usager, est un enjeu majeur. Celle-ci doit être conçue de manière à ce que l'utilisateur non-spécialiste en ait un usage aisé et qu'il souhaite s'en servir. Il s'agit également de présenter à l'utilisateur les indications lui rendant compte des interactions de la négociation avec son interlocuteur.

Dans l'ensemble, les enjeux pour les organisations et les usagers se rejoignent. Il y a tout de même une distinction à faire, les organisations ayant un facteur économique majeur. Elles ne dépenseront, au maximum, pas plus que ce qu'elles peuvent y gagner. Le facteur économique est en balance avec le respect de la vie privée, critère qui influe fortement sur le coût et la complexité de l'architecture.

CHAPITRE III

Architectures d'échanges de certificats existantes

*Au **chapitre 3** sont étudiées les architectures existantes adressant les échanges de certificats entre organisations. Il ne s'agit pas ici de faire une étude comparative de tout ce qui pourrait se référer aux domaines étudiés. En effet, les architectures existantes n'adressent qu'une partie des problématiques soulevées ici. Cependant, cela permet de mettre en relief les attentes énumérées au chapitre précédent et les technologies couramment employées aujourd'hui, d'étudier les sources de normes et de standards qui seront employées en troisième partie, et surtout, de rendre compte d'un constat, celui du besoin d'une architecture plus respectueuse de la vie privée. Nous verrons que ce constat pousse à prendre en considération un environnement utilisateur enrichi, ce qui justifie les besoins en termes d'universalité et de pervasivité.*

Sommaire

"L'histoire doit nous servir de miroir ; l'avenir s'y réfléchit."

Qianlong, *Empereur de Chine, XVIII^{ieme} siècle.*

III.1 Introduction

Il existe de nombreux travaux scientifiques et technologiques qui adressent les problématiques d'échanges de certificats entre organisations, ou qui pourraient être utilisés à cette fin. Par mesure de généricité, on considèrera qu'une architecture permet de véhiculer un certificat dès lors que deux parties peuvent échanger une information signée. Ainsi, une architecture peut entrer dans cette étude dès lors que les certificats peuvent porter sur un tiers distinct du générateur et du consommateur du certificat.

Nous avons cependant restreint cette étude aux architectures ayant fait l'objet d'efforts de normalisation. Nous entendons par le fait qu'une architecture ait fait l'« objet d'efforts de normalisation », le fait que, s'agissant d'architectures protocolaires, les échanges aient été normalisés. Cela a trait aux espaces de noms employés, aux algorithmes des rôles principaux de l'architecture et aux formats des messages. Les architectures cryptographiques et systèmes de négociation, qui ne sont pour l'instant qu'au stade de la « proposition scientifique », et sur lesquelles nous nous appuierons, sont étudiées en seconde partie.

Cette étude ne prétend pas à une évaluation exhaustive, aussi bien pour les cas étudiés, que pour les critères choisis. Cependant, les choix seront justifiés. Notons simplement que l'évaluation devra permettre de déterminer dans quelles proportions ces cas satisfont les attentes soulevées au chapitre précédent, pour les organisations, d'une part, et les utilisateurs, d'autre part. L'intérêt de cette étude est également de mettre en lumière les standards qui pourront être réemployés par la suite. L'évaluation repose sur des critères génériques qui, s'ils sont satisfaits, entraînent une évaluation avec des critères plus précis.

Ce chapitre met l'accent sur la technologie de fédération d'identité qui est aujourd'hui privilégiée dans diverses architectures d'échanges de certificats inter-organisationnels. Est discuté le fait qu'elle repose sur des concepts qui ne peuvent satisfaire nos attentes. Nombre de publications scientifiques adressent ces problématiques en modifiant les principes de la fédération, notamment à l'aide d'outils cryptographiques tels que les preuves de connaissances. Cependant, les objectifs, même s'ils sont rarement affichés comme tels, sont de changer les concepts fondamentaux de la fédération, donc de ne plus faire de la fédération d'identité. Or, ce que nous proposons dans cette thèse, c'est de définir les concepts attendus puis l'architecture correspondante. Ce chapitre se termine sur une discussion sur l'implémentation d'un environnement utilisateur enrichi et sur les questions d'universalité.

III.2 Les critères d'évaluation

Comme cela a été souligné au précédent chapitre, l'enjeu des organisations est principalement l'acceptation de la technologie par les usagers dans le but d'obtenir un retour sur investissements. L'évaluation de l'acceptation des usagers peut être faite selon des critères objectifs, même si elle est fonction du sentiment de confiance de l'utilisateur, critère difficilement évaluable à la vue d'une technologie. Les critères choisis sont présentés figure III.1 puis expliqués.

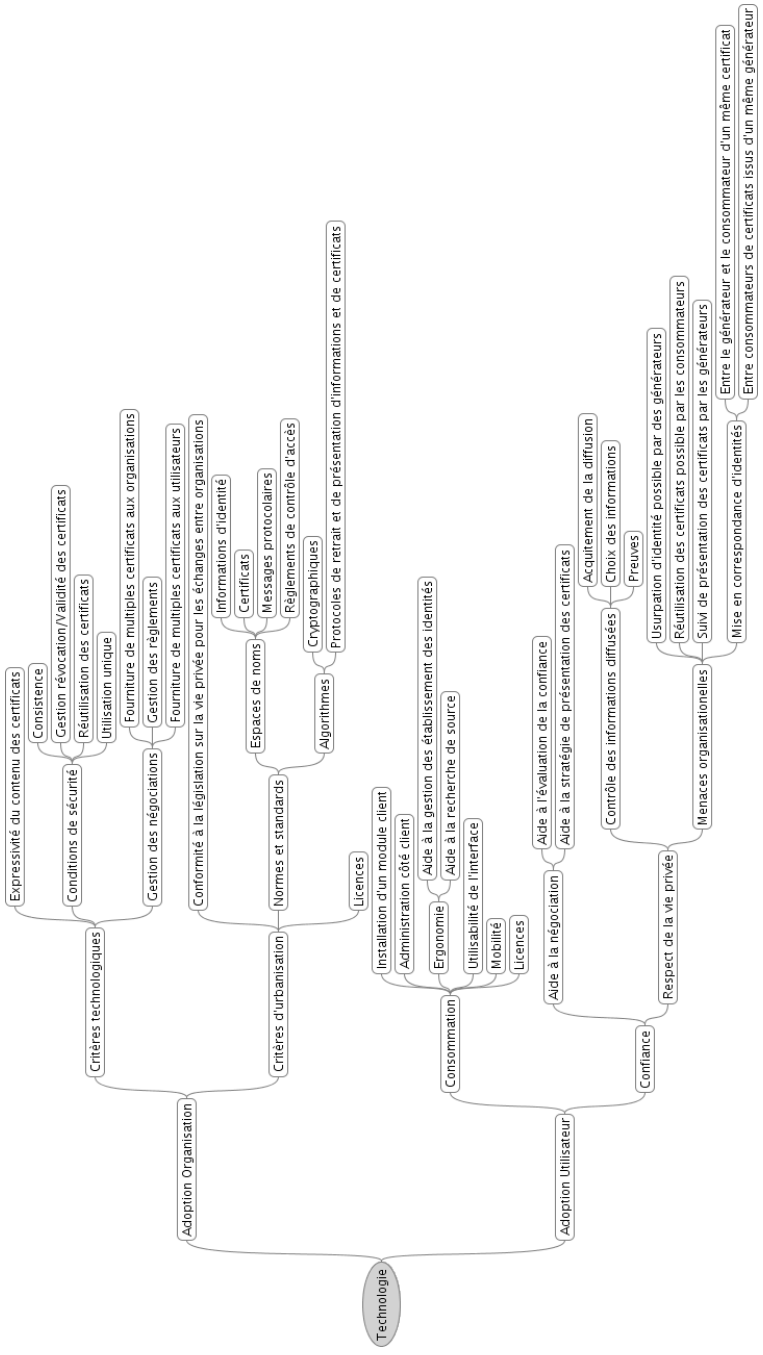

FIG. III.1 – *Critères d'évaluation des architectures d'échanges de certificats.*

III.2.1 Les critères d'évaluation pour l'adoption des organisations

L'évaluation du coût de l'adoption d'une technologie par une organisation est une tâche difficilement réalisable compte tenu de la nature de cette étude. A défaut, des critères simples à évaluer et ayant un impact fort sur le coût ont été choisis. Ils sont scindés en deux ensembles, les critères technologiques et les critères d'urbanisation. Les critères technologiques englobent l'expressivité du contenu des certificats, les conditions de sécurité et la gestion de la négociation. Les conditions de sécurité regroupe ce que nous considérons comme des pré-requis. Le terme consistance ou cohérence[1] (Camenisch & Lysyanskaya, 2001) correspond au fait que plusieurs usagers ne puissent pas cumuler leurs certificats. La gestion de la négociation du point de vue des organisations consiste à mesurer s'il est possible d'établir graduellement la confiance par un échange bilatéral de certificats. Les critères d'urbanisation regroupent des critères plus génériques. Le respect de la vie privée sur un plan juridique est une condition que nous considérons comme *sine qua non*. À celle-ci, il faut ajouter l'utilisation de normes et de standards sans quoi le déploiement d'une architecture, dont le sens premier est l'interopérabilité des organisations, n'a pas de chance d'aboutir. Enfin, les licences qui concernent l'architecture peuvent être un frein au déploiement par les organisations.

III.2.2 Les critères d'évaluation pour l'adoption des usagers

Les critères d'évaluation pour l'adoption des usagers sont également scindés en deux ensembles. Les critères de consommation regroupent de multiples questions pratiques, la nécessité pour l'utilisateur d'installer un logiciel, qui ne serait donc pas « natif » aux environnements utilisateurs, ou une évaluation des besoins d'administration de celui-ci par l'usager par exemple. Il y est également inclus l'ergonomie de la négociation, suivant que l'utilisateur ait à s'authentifier de multiples fois au cours d'une négociation ou que des mécanismes d'authentification unique facilitant l'utilisabilité soient intégrés par exemple. L'utilisabilité de l'interface graphique n'a de sens que s'il existe une implémentation d'une interface client. Ce critère est surtout utile dans ce chapitre pour qualifier la technologie Cardspace (Nanda & Jones, 2008). Le critère de mobilité indique si l'architecture est prévue pour que l'utilisateur retrouve son environnement de gestion des négociations lorsqu'il change de terminal ou de point d'accès. Le second ensemble de critères a trait à la confiance. Ces critères ont en quelque sorte été rationalisés afin de permettre une évaluation objective. Nous considérons deux axes majeurs permettant de « travailler » sur la confiance des usagers : la négociation et le respect de la vie privée. L'aide à la négociation regroupe les mécanismes qui visent à renforcer le sentiment de confiance de l'usager par des mécanismes d'évaluation des organisations et d'aide à la diffusion des

1. trad. Consistency

certificats. Le respect de la vie privée est évalué en fonction des possibilités de contrôle de la diffusion d'information ou des menaces potentielles que les organisations représentent. Le contrôle de la diffusion est un critère graduel :

- Acquittement de la diffusion d'information.
- Choix des informations diffusées. Cela sous-entend que le règlement du consommateur permette un choix aboutissant tout de même à l'objet de la négociation.
- Possibilité pour l'utilisateur de fournir des preuves de possession de certificats ou des preuves de propriétés sur les attributs qu'ils contiennent.

Concernant les menaces organisationnelles, le premier critère indique s'il existe des autorités délégataires de l'authentification au sein de l'architecture, ce qui signifierait qu'elles soient génératrices de certificats permettant l'établissement des identités entre organisations, donc qu'elles posent le problème d'une usurpation possible des identités des usagers par les organisations. Le second critère indique s'il est possible qu'un consommateur puisse se faire passer pour un porteur auprès d'un autre consommateur, ce qui signifie par exemple que la possession d'un certificat n'est pas prouvée. Le suivi de présentation des certificats indique si le générateur connaît au cours des négociations le consommateur pour lequel il délivre un certificat, auquel cas, le générateur peut tracer certaines activités de l'usager. Enfin, la mise en correspondance d'identités inclut deux conditions portant sur la non-associativité. Premièrement, le générateur et le consommateur ne doivent pas à partir du certificat pouvoir lier leur identité respective de l'usager. Deuxièmement, un même certificat présenté à deux consommateurs ne doit pas non plus leur permettre cette association d'identité.

III.2.3 Légende

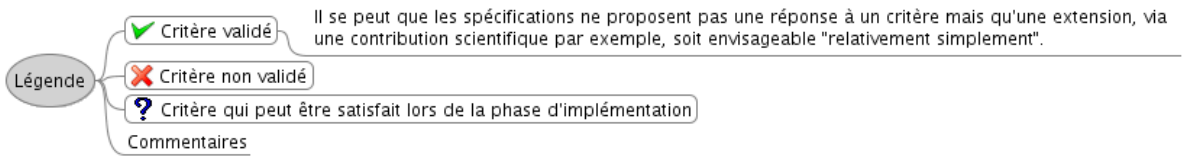

FIG. III.2 – *Legende de l'évaluation.*

III.3 Évaluations

La description et l'analyse des architectures étudiées ainsi que les évaluations « graphiques » selon les critères précédemment définis peuvent nuire au flot de lecture de la thèse ce qui justifie leur report en annexes (Annexes A). Sont présentées ici les synthèses de ces études. Ce choix implique que les références et les définition des termes requises soient en annexes.

III.3.1 Kerberos

Kerberos répond à plusieurs problématiques mais ne répond pas à la problématique de respect de la vie privée. Le KDC peut potentiellement usurper n'importe quelle identité pour laquelle il délivre des tickets d'authentification. Il peut également traquer les activités de l'usager puisqu'il est directement impliqué dans les accès applicatifs. De plus, le chiffrement symétrique implique que le ticket délivré par un KDC soit chiffré avec un secret partagé entre le KDC et l'application, ou un autre KDC. Outre la problématique pour gérer une architecture de confiance globale, cette partie du ticket est opaque pour le porteur ce qui ne permet pas à l'usager de contrôler son contenu. Les certificats n'offrent pas les fonctionnalités permettant un contrôle fin de l'information diffusée. Enfin, Kerberos n'intègre aucun des besoins de la négociation. Cette évaluation se justifie du fait que Kerberos fut conçu pour des mises en œuvre intra-organisationnelles. Kerberos n'est donc pas adapté pour être le support d'une architecture de confiance globale.

III.3.2 RADIUS

Il est possible de considérer que le serveur RADIUS qui authentifie l'initiateur est un générateur. Il délivre une autorisation au serveur relais qui se comporte également en générateur en délivrant à son tour une autorisation au NAS. Celui-ci consomme l'autorisation et fournit le service d'accès au réseau. Les informations sont donc directement échangées entre le consommateur et les générateurs ce qui permet intrinsèquement à ces derniers de pouvoir usurper l'identité de l'usager. Les activités de l'usager peuvent être suivies par les serveurs RADIUS. Pour ces inconvénients majeurs, l'architecture RADIUS n'est pas adaptée et évaluée plus précisément. L'architecture RADIUS est cependant intéressante car elle symbolise la problématique de l'accès réseau vu comme un service, et qui devrait donc être négocié. Nous reviendrons sur la problématique d'accès au réseau au chapitre 8.

III.3.3 Infrastructures à clés publiques X509 couplées à TLS

Les schémas de signature standardisés pour les certificats X509 permettent de lier les transactions entre générateurs et consommateurs et, intrinsèquement, ils ne permettent pas de faire de la présentation sélective de contenu ni de conduire des preuves. Concernant l'aspect protocolaire, le protocole TLS ne satisfait pas nos besoins. Le protocole TLS permet une authentification mutuelle, mais n'est pas adapté pour l'échange de multiples certificats. Une proposition de Hess (Hess *et al.*, 2002) propose une modification de TLS pour le support des négociations de confiance. L'architecture se rapproche alors sur certains points de ce qui est attendu. Il est cependant nécessaire d'y apporter de nombreuses modifications et de l'enrichir comme nous le verrons par la suite. Il est notamment nécessaire de définir les protocoles permettant l'obtention de certificats dynamiquement auprès des générateurs ainsi qu'un schéma de signature permettant des certificats aux fonctionnalités plus avancées.

III.3.4 La fédération d'identités

La délégation de l'authentification puis de l'autorisation, dans le but de faire des requêtes d'attributs, confèrent aux autorités des pouvoirs qui sont des menaces pour le respect de la vie privée des utilisateurs : usurpations d'identités et suivi d'activités. Il est possible, dans certains cas, de ne pas utiliser la délégation de l'authentification au détriment des interactions utilisateurs qui s'ajoutent à celles de sélection de la source des certificats et de fédération des identités. Enfin, la fédération d'identités est très peu adaptée à la gestion de la vie numérique en dehors des cercles de confiance des fédérations, c'est-à-dire où les générateurs et les consommateurs ne sont pas liés de confiance. L'utilisateur doit alors avoir recours à des mécanismes complémentaires pour gérer ses authentifications multiples ou pour faire de l'auto-saisie de champs redondants.

La délégation de l'authentification est « utile » dès lors que l'on souhaite réduire le nombre d'interactions de l'utilisateur requises pour fournir les preuves de son identité, et que l'utilisateur n'est pas doté d'un environnement dédié à la gestion de ses multiples identités. A l'inverse, un environnement utilisateur enrichi, en facilitant la fourniture de preuves d'identité, rend la délégation de l'authentification obsolète (Ates *et al.*, 2008a). Il est en effet possible de gérer autant de preuves que d'identités si l'environnement est adapté. Un navigateur Web n'est pas supposé implémenter de tels mécanismes ce qui implique la nécessité de la délégation pour faire face aux multiples authentifications requises par les mécanismes de la fédération. La localisation des sources, et l'obtention des certificats par l'initiateur, afin qu'il en soit le porteur, sont aussi des problématiques qui sont solvables par un environnement utilisateur enrichi. C'est l'emploi d'un navigateur Web

standard qui entrave la gestion de ces problématiques et fait peser diverses menaces sur la vie privée des usagers. Enfin, un environnement client enrichi est nécessaire pour permettre la négociation par l'utilisateur, afin qu'il puisse faire des requêtes de certificats au fournisseur et les valider selon son propre domaine de confiance. En outre, les schémas de signature proposés n'offrent pas les fonctionnalités attendues. Notons dès lors que les mécanismes cryptographiques, impliqués par un schéma de signature satisfaisant nos attentes, nécessitent également un environnement utilisateur adapté.

III.3.5 Le client avancé Liberty Alliance ID-WSF

Cette architecture, qui suppose l'enrichissement de l'environnement utilisateur, permet de résoudre plusieurs problèmes évoqués précédemment, notamment ceux cités comme étant dûs au navigateur Web standard lors de l'étude des architectures de fédération d'identités : la délégation de l'authentification, le suivi d'activité par les autorités et le choix des sources par exemple. Cependant, un schéma de signature correspondant à nos attentes n'est pas proposé. Enfin, il n'est pas spécifié si l'utilisateur peut requérir des certificats des organisations ce qui empêche de considérer la négociation de confiance comme faisable. Le partage et la cession des certificats sont des problématiques qui sont à traiter indépendamment.

Cette architecture ouvre la voie d'un environnement utilisateur riche. Notons qu'il n'y a pas d'implémentation officielle connue à ce jour.

III.3.6 CardSpace

CardSpace souffre des mêmes « maux » que le client avancé ID-WSF. Il n'est pas proposé de schéma de signature aux fonctionnalités avancées. Il n'y a pas non plus de négociation possible, la fourniture de certificats est unidirectionnelle si l'on exclut le certificat du fournisseur servant à l'établissement d'un canal sécurisé. Le partage et la cession des certificats sont des problématiques qui sont à traiter indépendamment.

Cette architecture implémente cependant divers principes que nous considérons comme fondamentaux pour l'architecture attendue. Il s'agit notamment de la conception d'un outil de gestion des identités adapté aux besoins d'un utilisateur non-averti, permettant la gestion des authentifications multiples et le contrôle des informations diffusées, et la mise en œuvre de moyens d'intégration aux applications existantes.

III.4 Architecture centrée sur l'utilisateur

L'étude qui vient d'être présentée illustre deux manques principaux des architectures existantes, d'une part, celui d'un schéma de signature permettant l'élaboration de certificats satisfaisant nos attentes, et d'autre part, le fait qu'il n'existe pas de réelle proposition visant un échange bilatéral de certificats.

Ce que fait également ressortir cette étude, c'est la nécessité d'un environnement utilisateur suffisamment riche, notamment pour pouvoir satisfaire aux conditions du respect de la vie privée. Ainsi, les architecture présentées souffrent de certaines des problématiques suivantes dues à un environnement utilisateur pauvre au regard des besoins de la gestion des identités et des certificats :

1. La délégation de l'authentification offre le pouvoir à une autorité d'usurper les identités pour lesquelles elle est délégataire de l'authentification (ce principe, bien qu'évident et intrinsèque au principe de la délégation, n'en fait pas moins un mécanisme inacceptable entre certaines organisations),
2. L'obtention et la présentation de certificats se fait par un dialogue directe entre organisations. Cela permet aux organisations de suivre les activités des utilisateurs en connaissant les organisations auprès desquelles les certificats sont dépensés.
3. L'obtention et la présentation d'un même certificat permet aux organisations impliquées de lier les transactions et, ainsi, d'associer les identités d'une même entité.
4. Lorsqu'une information certifiée requise est contenue dans un certificat de l'utilisateur, l'intégralité du contenu du certificat est présenté.
5. L'utilisateur ne peut requérir de multiples certificats des organisations, ni négocier les informations que les organisations requièrent de sa part.

Les architectures de fédération d'identités sont sources de ces menaces, notamment du fait du concept de l'identité fédérée. A l'inverse, le concept de l'identité centrée sur l'utilisateur[2] signifie que l'association des identités ne peut être faite que par le sujet de ces identités, ce qui est conforme à ce que nous évoquions section II.3.5. Cette définition de l'identité centrée sur l'utilisateur est simple, et nous pensons qu'il s'agit de la seule intéressante. Cela va à l'encontre d'une vision répandue où ce terme est employé dès lors que seules les interactions de l'utilisateur sont prises en considération. Ce que l'on nomme le traitement de données personnelles[3] sur les identités numériques multiples ne doit être alors possible que par le sujet de celles-ci. Cela implique que la délégation de l'authentification soit bannie au profit d'un établissement de l'identité seulement possible par le sujet de ces identités. Autrement dit, le concept d'identité centrée sur l'utilisateur implique de

2. trad. "User centric-identity."
3. trad. "Private data mining."

découpler l'apport de certificats de l'établissement d'une identité (Ates *et al.*, 2009b).

En résumé, il est attendu d'un environnement utilisateur riche que l'utilisateur puisse :

1. être capable d'obtenir et de présenter lui-même ses certificats,
2. être capable de rendre ses multiples négociations (et identités donc) non associables,
3. être le seul à pouvoir établir ses multiples identités,
4. contrôler, choisir et négocier les informations qu'il diffuse,
5. disposer d'un outil d'aide à la négociation,
6. établir à l'aide d'une négociation de confiance une relation de confiance avec un inconnu,
7. disposer d'une interface homme-machine d'établissement de ses identités et de négociation adaptée.

La négociation n'est pas traitée dans les architectures existantes. En d'autres termes, il n'est pas possible de mener des échanges mutuels de certificats comme support à un établissement graduel de la confiance. Il est très rarement pris en compte le fait qu'un utilisateur puisse être amené à requérir des certificats avant d'accepter d'en présenter. Cela empêche toute négociation basée sur ce principe. Négocier, c'est aussi gérer les sources multiples de certificats afin d'aider l'utilisateur à satisfaire les conditions exprimées au sein des règlements des fournisseurs. Il s'agit également d'aider l'utilisateur à prendre des décisions concernant la diffusion de certificats et l'établissement d'une identité, voire, à automatiser ces opérations.

Concevoir une interface homme-machine ergonomique est une condition essentielle à l'obtention du sentiment de confiance de l'utilisateur, nécessaire à son adoption du système. Il s'agit d'assurer un confort d'utilisation lors des négociations. Cela englobe la gestion des authentifications multiples mais également de présenter une interface simple suite à l'analyse de règlements de contrôle d'accès complexes par exemple.

Le besoin d'interopérabilité n'est pas directement lié à l'environnement utilisateur enrichi. L'interopérabilité est un besoin commun à toutes les architectures visant les échanges entre systèmes, et plus encore entre organisations. Il s'agit d'employer des espaces de noms communs pour exprimer les informations d'identités et les certificats, de s'accorder sur un ensemble d'algorithmes cryptographiques, sur des protocoles communs ou interopérables, et sur des sérialisations « standardisées ». Il s'agit d'un sujet que nous aborderons lors de l'implémentation. Notons pour l'instant que nous avons conscience que l'« ambition de la pervasivité » suppose, pour une architecture comme celle-ci, que l'interopérabilité soit un acquis.

La problématique majeure de l'environnement utilisateur enrichi est celle de l'universalité. Il est requis que cet environnement soit disponible sur tout système destiné aux utilisateurs, autrement dit, qu'il soit natif. Il faut également que les applications existantes, que l'on souhaite voir s'appuyer sur cette architecture, puissent dialoguer avec celui-ci. Il s'agit de la condition d'« universalité » nécessaire pour pouvoir prétendre à l'appellation de « couche de gestion des identités ».

À cela s'ajoute enfin le problème de la mobilité des utilisateurs. Un client riche, tel qu'il est décrit ici, repose sur un ensemble de paramètres et de données (clés, méta-données, historique, etc.). Pour que l'utilisateur puisse acquérir la mobilité, il est nécessaire de rendre l'ensemble de ces données « transportables ». Autrement dit, il est nécessaire que l'utilisateur retrouve son environnement lorsqu'il change de terminal. Nous verrons qu'il est possible d'envisager deux solutions. Premièrement, la solution « mobile » qui suppose l'utilisation d'un support physique. Deuxièmement, la solution « nomade » qui suppose que l'utilisateur maintienne en ligne l'ensemble de ses paramètres, à la condition évidente que cela ne revienne pas à remettre aux hébergeurs de ses données « les clés de sa vie numérique ».

Partie II: Étude

CHAPITRE IV

Systèmes cryptographiques de certificats

*Au **chapitre 4** est faite une étude des besoins en matériel cryptographique afin de permettre des échanges de certificats anonymes, de mener de multiples négociations non-associables, et de permettre la présentation sélective d'informations contenues dans les certificats. Sont également présentés la notion de système à pseudonymes, ainsi que les besoins architecturaux pour permettre la mise en œuvre de pièces d'identité civile anonymes, de la révocation de l'anonymat et, enfin, de la non-transférabilité des certificats. Un bilan des travaux scientifiques existants est présenté et des composants pour bâtir notre architecture de certificats sont choisis. Une description générale et quelques notes d'implémentations sont présentés concernant les réalisations menées en langage de programmation C.*

Sommaire

"Dans la théorie des nombres, un problème est aussi immortel qu'une oeuvre d'art."

David Hilbert, *Introduction aux Eléments de la théorie des nombres algèbriques de Legh Wilber Reid.*

IV.1 Systèmes à pseudonymes

Nous avons soulevé à plusieurs reprises les fonctionnalités et propriétés attendues du système de négociation. Nous reprenons ici celles qui ont trait aux besoins en primitives cryptographiques. Dans un second temps, les différentes propositions scientifiques sont étudiées afin de déterminer les plus pertinentes.

Au cours de la section II.1.4, nous indiquions que pour satisfaire aux conditions d'anonymat, le système devait permettre d'échanger des certificats de sorte que :

- de multiples négociations sur un même fournisseur soient non associables si aucune identité n'y est établie, et ce même en présentant plusieurs fois un même certificat,
- sous le couvert du pseudonymat, les transactions soient non associables entre tiers afin que de multiples identités d'une même entité ne le soient pas non plus.

Il s'agit donc de permettre l'inassociativité des transactions et de mettre en œuvre le statut d'anonymat ou de pseudonymat si l'établissement d'une identité est requis.

Une architecture permettant l'échange de certificats en satisfaisant la propriété de non associativité des identités est couramment appelée « système à certificats anonymes » ou « système à pseudonymes » (Lysyanskaya *et al.*, 2000 ; Pashalidis & Mitchell, 2004). Les pseudonymes ont trait à l'établissement de l'identité et sont une condition à l'inassociativité des transactions lorsque l'établissement d'une identité est requis. Les pré-requis d'une telle architecture sont introduits par (Chaum, 1981).

Le principe de l'utilisation de multiples certificats numériques non associables présentés sous divers pseudonymes est introduit par (Chaum, 1985 ; Chaum & Evertse, 1987). Diverses briques ont été proposées (Chaum, 1983 ; Chaum *et al.*, 1990 ; Chaum, 1991 ; Damgård, 1990 ; Brands, 1993, 1994, 1995 ; Chen, 1995) pour enfin voir présentés des systèmes plus complets (Lysyanskaya *et al.*, 2000 ; Brands, 2000 ; Camenisch & Lysyanskaya, 2001). Le cœur de l'architecture repose sur les certificats et sur leurs propriétés, c'est-à-dire sur le schéma de signature des certificats.

Nous décrivons dans cette section les difficultés techniques, architecturales et d'acceptabilité que soulève une telle architecture.

IV.1.1 Les certificats

L'inassociativité des transactions suppose un schéma de signature des certificats permettant cette propriété. Plus précisément, ce qui est attendu, c'est un schéma de signatures

permettant de vérifier la validité d'une signature sans que sa génération et sa vérification puissent être associées. Il est également nécessaire que ce schéma permette que les multiples vérifications d'une même signature soient inassociables. Les vérifications d'un même certificat par une même entité, ou par de multiples entités, sont ainsi non-associables. Lorsque des certificats ont cette propriété, ils sont abusivement appelés certificats anonymes.

Le certificat est un ensemble d'informations et une signature de cet ensemble. Lorsqu'il s'agit d'un "certificat d'identité", l'information est un ensemble d'attributs portant sur un sujet ou sur les propriétés du certificat. Une des fonctionnalités majeures attendues des certificats est la présentation sélective[1] de certaines informations qu'ils contiennent. Le schéma de signature doit donc permettre de vérifier la signature en présentant indépendamment chacun des attributs, sous-ensemble de l'information signée. La signature n'est donc pas une donnée constante mais une donnée variable selon le contenu présenté lors de la vérification.

Les certificats et les protocoles de vérification représentent l'opportunité d'implémenter des mécanismes de preuves. Cela permet d'apporter la preuve de possession d'une signature d'un générateur sans divulguer les données signées. En outre, en règle générale, la possession d'un certificat devrait toujours être prouvée, rendant le certificat assimilable à une clé publique que l'on prouve à l'aide d'une ou plusieurs clés privées. Il est ainsi possible de prouver la possession d'un certificat, voir l'appartenance à un ensemble lorsque le générateur représente cet ensemble, sans avoir à présenter le contenu du certificat.

Il est également souhaité que le schéma de signature permette de prouver des propriétés sur les informations signées. Donnons par exemple l'âge prouvé à partir d'une date de naissance chiffrée dans l'un des attributs contenus dans un certificat. Les preuves qu'il est possible d'apporter ont trait à des expressions numériques qui dans cet exemple serait : « date actuelle - date de naissance = âge ». Il est donc important de raisonner en termes de données numériques pour savoir ce qu'il est possible de prouver. Les données qui sont prouvées sont généralement appelées engagements[2].

Une partie des attributs contenus dans un certificat sert à définir les propriétés du certificat. Il s'agit notamment des propriétés de validité. Un certificat peut être généré pour une durée de validité illimitée. Dans le cas contraire, il lui est associé une date d'échéance dont peut être déduite la durée de validité. Un certificat peut également être révoqué. La propriété de non-associativité empêche cependant de gérer une liste de révocation des

1. trad. Selective disclosure.
2. trad. Commitments.

certificats révoqués puisque le générateur ne peut pas désigner les certificats qu'il a émis aux consommateurs des certificats. Nous verrons que des solutions existent. Les certificats peuvent également être limités en nombre d'utilisations. Avec un certificat n'ayant pas la propriété de non-associativité une vérification auprès du générateur lors de sa présentation permet au générateur de compter le nombre d'utilisations, donc d'indiquer si un certificat est toujours valide. Les certificats anonymes supposent que chaque présentation de signature laisse une « trace » différente, ce qui empêche ce procédé. Il existe cependant des mécanismes permettant de « libérer » un identifiant du certificat dès qu'une utilisation de celui-ci est faite au-delà du nombre permis. Il est également possible de coupler ces mécanismes avec un environnement utilisateur contrôlé à l'aide d'une plateforme de confiance[3]. Les certificats sont présentés par l'intermédiaire de la plateforme de confiance, plateforme qui a la charge de garantir le nombre de présentations autorisées. Il est également nécessaire que l'environnement client puisse aider l'utilisateur à gérer la validité de ses certificats, c'est-à-dire leur durée de validité et leur nombre d'utilisations. Cela est d'autant plus important si des moyens répressifs sont employés envers l'utilisateur en cas de mauvaise utilisation.

IV.1.2 Systèmes à pseudonymes

Un pseudonyme est un identifiant d'une identité qui n'est pas associable à l'identité réelle d'une entité comme le définit (Pfitzmann & Kohntopp, 2001). L'établissement d'une identité sous un pseudonyme est appelé « pseudonymat ». Le pseudonymat se réduit le plus souvent à l'utilisation de pseudonymes. Nous y attachons l'idée de pseudonymes indistinguables, c'est-à-dire qui ne peuvent être corrélés, afin d'assurer la non-associativité des identités comme nous l'avons indiqué section II.1.4. Nous distinguons ainsi le pseudonymat, où les pseudonymes employés sont indistinguables, du « pseudonymat » public lorsqu'un pseudonyme est employé avec plusieurs parties.

Le pseudonyme est le moyen de désigner une identité et d'établir une identité. Cela suppose un protocole permettant l'établissement d'un pseudonyme entre un utilisateur et une organisation qui génère une donnée privée pour le possesseur de l'identité. Cela suppose également qu'il soit difficile que deux entités puissent présenter un même pseudonyme. Le pseudonymat permet de rendre les multiples transactions avec un même interlocuteur associables, donc d'associer de multiples négociations, ou plus généralement, de multiples actions à une identité.

Le pseudonymat est donc requis pour bénéficier de la propriété de non-associativité des identités lorsque l'établissement d'identités est requis auprès de plusieurs entités.

3. trad. Trusted plateform.

Enfin, il est possible d'exploiter l'inassociativité des multiples vérifications d'un même certificat pour permettre de mener des négociations anonymes. Pour cela, soit aucun pseudonyme n'est employé, soit un pseudonyme n'est jamais réutilisé. Cela n'empêche en rien d'associer à une négociation menée dans de telles conditions un mécanisme permettant de révoquer l'anonymat.

IV.1.3 Besoins de l'architecture

IV.1.3.1 Révocation de l'anonymat

L'un des intérêts majeurs d'un système à pseudonyme est l'anonymat par l'inassociativité. Pour autant, il est nécessaire de prévoir des « échappatoires » contrôlées permettant de révoquer cet anonymat. Au vue des concepts précédemment définis, il est possible d'envisager deux types de révocation de l'anonymat suivant la propriété d'anonymat remise en cause : l'inassociativité ou le pseudonymat. Les deux types de révocation sont ainsi (Camenisch & Lysyanskaya, 2001) :

- la révocation de l'inassociativité entre générateurs et consommateurs, aussi appelée révocation locale,
- la révocation du pseudonymat permettant de révéler un pointeur vers une identité civile, aussi appelée révocation globale.

Vient ensuite la notion événementielle signifiant les circonstances de la révocation. Là encore, il existe deux possibilités :

- la révocation devient possible dès lors que l'utilisateur commet une action spécifique, détectable par le système, et que nous appelons révocation *synchrone*,
- la révocation est possible indépendamment d'une action quelconque de l'utilisateur vis-à-vis du système. Il s'agit par exemple de déterminer qu'il y a eu une action frauduleuse de l'utilisateur, non-détectable par le système affilié au premier cas. Il s'agit donc de permettre une révocation à « contre-coup ». Nous qualifions cette révocation d'*asynchrone*.

La révocation asynchrone est une problématique délicate qui nécessite une architecture particulière comme nous le verrons par la suite. Il est cependant possible, dès à présent, de noter qu'il s'agit d'une responsabilité importante qui devrait être répartie entre plusieurs organismes indépendants (police et justice par exemple).

IV.1.3.2 Non-transférabilité

La non-transférabilité est un paradigme majeur de l'identité numérique et qui par ailleurs n'est restreint ni à ce domaine, ni à celui des certificats. Comme nous l'évoquions à la section II.1.3, une entité emprunte une identité dès lors qu'elle est à même de fournir la preuve de cette identité. Il s'agit ici de la problématique de la transférabilité de la preuve de l'identité. Cette problématique existe également pour les certificats.

Il existe divers mécanismes qui visent à adresser cette problématique et que l'on peut classer en deux catégories : ceux qui s'appuient sur la technologie et ceux qui s'appuient sur la psychologie. Les solutions technologiques sont par exemple les plateformes de confiance. Elles ne constituent cependant pas une réponse suffisante lorsqu'il s'agit d'établir l'identité d'une entité. En effet, rien n'empêche un individu de céder sa carte de paiement et de révéler son code d'accès par exemple. Les solutions psychologiques ont trait à la dissuasion, ce que (Dwork *et al.*, 1996) nomme l'auto-réglementation[4]. Il s'agit par exemple de mesures de répression. Dans le cas de cartes de paiements, il s'agit d'attribuer la responsabilité des actes à son possesseur légitime tant qu'il ne déclare pas la perte. Ce peut être également la mise en gage d'une somme d'argent. Son obtention serait basée sur le secret dont on veut dissuader la cession, donc céder ce dernier reviendrait à céder la somme d'argent mise en gage. Cependant, comme tout mécanisme basé sur la psychologie, son efficacité est variable. Cela fait appel à la rationalité des individus mais également à la confiance, notamment dans le bénéficiaire de la cession du secret. La confiance est alors à mettre en balance avec la valeur du gage et les préjudices éventuels résultant de la cession du gage. Il apparaît évident que ces deux types de mécanismes sont complémentaires.

En résumé, nous sommes face à deux problématiques : la cession des certificats[5] et la mise en commun de certificats par deux entités que l'on appelle le partage de certificats[6]. Assurer la première propriété implique de résoudre la seconde, alors que la réciproque n'est pas vrai. La seconde problématique, parfois appelée coalition en équipe[7] (Camenisch & Lysyanskaya, 2001), peut paraître de prime abord solvable techniquement de manière relativement aisée. Citons par exemple un identifiant unique associé à une entité que chaque générateur de certificat aurait à charge de mettre dans les certificats. Cette solution ne satisfait cependant pas la propriété de non-associativité des certificats. Nous verrons donc qu'il existe un mécanisme permettant de mettre un secret dans chacun des certificats et permettant à l'utilisateur de prouver que ce secret est le même dans chacun des certificats, sans remettre en question la propriété de non-associativité. Cette solution

4. trad. Self-Policing
5. trad. Lending.
6. trad. Sharing.
7. team-up

débouche alors sur la problématique de non-transférabilité du secret.

Enfin, il est nécessaire d'ajouter une dernière problématique. Il est souhaité que certains certificats soient non-cessibles et que d'autres le soient (les tickets de cinéma ou de la monnaie par exemple). Ces certificats ne devraient donc pas contenir d'informations liées à une identité. Cependant, la difficulté réside dans la responsabilité d'une action frauduleuse du fait que, de la même façon que dépenser de l'argent ne revient pas à ne plus avoir les certificats à disposition, céder un certificat ne signifie pas ne plus en avoir la possession.

IV.1.3.3 Recouvrement, renouvellement et portabilité

La dernière nécessité architecturale est celle de la gestion du cycle des secrets, et notamment des pseudonymes. Si l'on imagine que les utilisateurs batissent leur vie numérique autour des pseudonymes, leur perte ou leur compromission peuvent être extrêmement préjudiciables.

La problématique de la perte implique de permettre à un individu d'« externaliser » ses secrets sans « céder sa vie numérique » comme nous l'évoquions à la section III.4. Les solutions se rapprochent également des besoins de portabilité des secrets. Il est donc envisageable que l'une des solutions, à l'instar de celle de la révocation de l'anonymat asynchrone, repose sur des organismes indépendants (la préfecture et le notaire de l'usager par exemple). En effet, le recouvrement n'est réalisable que s'il est possible de dupliquer la base des secrets, et le dépositaire des clés[8] devient une menace en tant qu'« usurpateur » d'identités potentiel.

La problématique de la compromission née du fait que l'utilisateur a la responsabilité de ses pseudonymes. Il doit pouvoir détecter une telle compromission et le prouver en cas de litige. Il est également nécessaire qu'il puisse renouveler ses pseudonymes auprès des organisations où il les avait établis. Un mécanisme d'établissement d'identité « de secours » prenant l'ascendant sur celui fait à l'aide des pseudonymes est donc à prévoir.

8. trad. Key Escrow.

IV.2 Bases

Cette section présente les bases cryptographiques nécessaires à la compréhension de ce chapitre. Elles ne sont pas présentées aussi formellement que ce qu'il est coutume de rencontrer dans les travaux dédiés à ce sujet. Elles sont cependant présentées de manière intuitive et concise.

IV.2.1 Notation

Nous utiliserons par la suite les notations courantes suivantes :

- Lorsqu'il sera évoqué une valeur choisie aléatoirement dans un ensemble E, cela suppose une distribution de probabilité uniforme indépendante, notée $x \in_{\mathcal{R}} E$.
- On note $\mathbb{Z}_t$ l'anneau des entiers modulo t.
- On note $\mathbb{Z}_t^*$ son groupe multiplicatif. Le nombre d'éléments d'un groupe est appelé ordre du groupe.
- QR_t est le groupe des résidus quadratiques modulo t.
- Le plus grand diviseur commun de a et de b égal à c est noté $pgcd(a,b) = c$. Si $c = 1$, a et b sont dits co-premiers.
- Si a est un facteur de b on dit que a *divise* b noté $a \mid b$ ou a *div* b. Si a ne divise pas b, on le note $a \nmid b$
- $a \| b$, la concaténation de deux chaînes binaires.
- Soit $\mathcal{H} : \{0,1\}^* \longrightarrow \{0,1\}^l$ une fonction de hachage résistante aux collisions qui associe à une représentation binaire en argument une chaîne binaire de longueur l.

Notons que nous utilisons à de multiples reprises des éléments mathématiques appelés « générateurs ». Ce terme porte à confusion avec le terme générateur employé pour les générateurs de certificats. Ainsi, lorsque le mot *générateur* suppose l'élément mathématique, il est noté en italique.

IV.2.2 Problèmes cryptographiques

Soit une fonction f associant une valeur du domaine X à une valeur unique dans le co-domaine Y, notée $f : X \longrightarrow Y$. L'image $y \in Y$ de $x \in X$ est notée $y = f(x)$. Une fonction cryptographique f est considérée comme étant à sens unique s'il est possible de considérer comme simple le calcul de $f(x)$ à partir de x et difficile celui de x à partir de $f(x)$. Il est attendu que les fonctions à sens uniques soient libres de collisions, c'est à dire que si $f(a) = f(b)$ alors $a = b$.
Les fonctions à sens unique constituent la base de nombre de primitives cryptographiques et de cryptosystèmes à clés publiques. Considérons une clé publique et une clé privée.

La primitive de chiffrement consiste à utiliser une fonction à sens unique permettant de chiffrer une donnée à l'aide d'une clé publique et de ne rendre celle-ci déchiffrable qu'à l'aide de la clé privée. Il est donc possible de supposer que la fonction de chiffrement soit simple pour le chiffrement à l'aide de la clé publique et difficile pour le déchiffrement si l'on ne possède pas la clé privée.

La constitution de telles fonctions peut reposer sur des problèmes de la théorie des nombres considérés comme difficiles. Cela suppose qu'ils soient solvables en des temps de calculs fonction de la taille des ensembles. Ainsi, en augmentant ces tailles, il est possible de rendre les problèmes suffisamment difficiles à calculer pour les rendre utilisables pour des applications pratiques de fonctions à sens unique.

Les cryptosystèmes à clés publiques reposent sur des problèmes considérés comme difficiles bien que leur appartenance à cette classe n'ait pas été démontrée. Voici quelques exemples de problèmes employés par la suite (Menezes *et al.*, 1996).

1. Le problème de la décomposition d'un entier positif n en facteurs premiers (FACTORING) : il est considéré comme difficile d'écrire $n = p_1^{e_1}...p_k^{e_k}$ où les p_i sont des nombres premiers distincts et les e_i des entiers positifs.

2. Le problème RSA (RSA) : il est considéré comme difficile de trouver un entier m tel que $m^e \equiv c \ mod \ n$ avec n un entier positif produit de deux premiers p et q, e tel que $pgcd(e,(p-1)(q-1)) = 1$.

3. Le problème RSA fort (SRSA) : il est considéré comme difficile de trouver un entier m et $e > 1$ tel que $m^e \equiv c \ mod \ n$ avec n un entier positif produit de deux premiers p et q.

4. Le problème du logarithme discret (DL) : il est considéré comme difficile de trouver un entier x avec $0 \leq x \leq p-2$ noté $log_\alpha \beta$ tel que $\alpha^x \equiv \beta \ mod \ p$ avec p premier, α un *générateur* de $\mathbb{Z}_p^*$ et $\beta \in \mathbb{Z}_p^*$.

5. Le problème du logarithme discret généralisé(GDL) : il est considéré comme difficile de trouver un entier x avec $0 \leq x \leq n-1$ noté $log_\alpha \beta$ tel que $\alpha^x = \beta$ avec G un groupe cyclique d'ordre n, α un *générateur* de G et $\beta \in G$.

6. Le problème de Diffie-Hellman (DH) : il est difficile de trouver $\alpha^{ab} \ mod \ p$ avec p premier, α un *générateur* de $\mathbb{Z}_p^*$ et les éléments $\alpha^a \ mod \ p$ et $\alpha^b \ mod \ p$.

7. Le problème de Diffie-Hellman généralisé (GDH) : il est difficile de trouver α^{ab} avec G un groupe cyclique, α un *générateur* de G et les éléments α^a et α^b de ce groupe.

Notons également le théorème suivant (Camenisch & Shoup, 2003) :

> *Selon la supposition SRSA, étant donné n tel que défini et les éléments aléatoires g,$h \in (\mathbb{Z}_n^*)^2$, il est difficile de calculer un élément $w \in \mathbb{Z}_n^*$ et les entiers a, b et c tels que $w^c \equiv g^a h^b \ mod\ n$ avec $c \nmid a$ et $c \nmid b$.*

Il existe deux méthodes connues permettant de construire les groupes nécessaires à ces problèmes, par les sous-groupes et par les courbes elliptiques. Ainsi, avec la méthode des sous-groupes : soit G_q un sous-groupe de $\mathbb{Z}_p^*$ où p est un premier tel que $q|(p-1)$.

Enfin, voici quelques fonctions à sens unique que nous utiliserons par le suite [9] :

1. Soit q un premier de taille binaire k qui spécifie un groupe G_q d'ordre q. g est un *générateur* de G_q. Soit $x \in \mathbb{Z}_q$ le logarithme discret de g^x. Soit f une fonction DL telle que :
$$f_{q,g} : x \longrightarrow g^x$$
2. Soit q un premier de taille binaire k qui spécifie un groupe G_q d'ordre q. $g_1,...,g_l$ sont des *générateurs* de G_q avec $l \geq 1$ et $g_l \neq 1$. Soit le tuple $x_1,...,x_l \in \mathbb{Z}_q$. Soit f une fonction $DLREP$ telle que :
$$f_{q,g_1,...,g_l} : (x_1,...,x_l) \longrightarrow \prod_{i=1}^{l} g_i^{x_i}$$
dans le domaine $(\mathbb{Z}_q)^l$. Le tuple $(x_1,...,x_l)$ est alors appelé une représentation-DL de $h := \prod_{i=1}^{l} g_i^{x_i}$ respectant le tuple de bases $(g_1,...,g_l)$.

3. Soit n un entier supérieur à 4, produit de deux premiers p et q. Soit v un nombre inférieur à $\varphi(n)$, l'indicatrice d'Euler, $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$. Soit $x \in \mathbb{Z}_n^*$. Soit f une fonction RSA telle que :
$$f_{n,v} : x \longrightarrow x^v$$
4. Soit n un entier supérieur à 4, produit de deux premiers p et q. Soit v un nombre inférieur à n et co-premier avec $\varphi(n)$. $g_1,...,g_l$ sont les éléments de $\mathbb{Z}_n^*$ avec $l \geq 1$. Soit le tuple $(x_1,...,x_{l+1})$ avec $x_1,...,x_l \in \mathbb{Z}_v$ et $x_{l+1} \in \mathbb{Z}_n^*$. Soit f une fonction $RSAREP$ telle que :
$$f_{n,v,g_1,...,g_l} : (x_1,...,x_l,x_{l+1}) \longrightarrow \prod_{i=1}^{l} g_i^{x_i} x_{l+1}^v$$
dans le domaine $(\mathbb{Z}_v)^l \times \mathbb{Z}_n^*$. Le tuple $(x_1,...,x_l,x_{l+1})$ est alors appelé une représentation-RSA de $h := \prod_{i=1}^{l} g_i^{x_i} x_{l+1}^v$ respectant $(g_1,...,g_l,v)$.

9. Pour plus de détails sur les problèmes de représentations voir (Brands, 1993).

IV.2.3 Les preuves de connaissance

On introduit ici le concept de preuves de connaissance, aussi appelé preuve par protocole (Goldwasser *et al.*, 1985). Une preuve de connaissance permet à une entité appelée *prouveur*[10] de convaincre (prouver à) une entité appelée *vérifieur*[11] qu'il connait la solution d'un problème difficile tel que les propriétés suivantes soient respectées (Camenisch & Stadler, 1997) :

1. la propriété de complétude[12] : un prouveur honnête connaissant la solution peut convaincre avec succès le vérifieur,
2. la propriété de cohérence[13] : avec une probabilité quasi-certaine, un prouveur tricheur, ne connaissant aucune solution, échouera dans ses tentatives de convaincre un vérifieur,
3. la propriété de divulgation nulle de connaissance[14] : le vérifieur obtient seulement l'information de connaissance de secret du prouveur.

Une preuve de connaissance ayant la propriété de divulgation nulle de connaissance est appelée : « preuve de connaissance à divulgation nulle de connaissance[15] ». Les preuves de connaissance sont formellement définies par (Feige *et al.*, 1988). Il existe à ce jour de tels protocoles, efficaces, reposant sur les problèmes RSA et DL, et prouvés sûrs selon le modèle de l'oracle aléatoire (Bellare & Rogaway, 1993) permettant de supprimer l'obstacle de la fonction de hachage dans les preuves de sécurité.

Le protocole se fait en trois phases, le prouveur fait un engagement aussi appelé témoin[16]. Le vérifieur produit alors un challenge auquel le prouveur répond. Ce processus est répété un nombre de fois nécessaire à réduire la probabilité de pouvoir répondre correctement aux challenges sans connaître le secret. Il ne s'agit donc pas d'une preuve au sens mathématique strict mais plutôt d'un jeu probabiliste. Un exemple est donné entre un prouveur A et un vérifieur B, ce protocole étant répété un nombre t de fois :

$$A \longrightarrow B : Engagement$$
$$A \longleftarrow B : Challenge$$
$$A \longrightarrow B : Reponse$$

10. trad. Prover.
11. trad. Verifier.
12. trad. Completeness.
13. trad. Soundness.
14. trad. Zero-Knowledge.
15. trad. Zero-Knowledge proof of Knowledge.
16. trad. Commitment ou Witness.

Le premier protocole de ce type est dû à (Fiat & Shamir, 1987). Il n'est cependant pas considéré comme efficace du fait que le challenge a une longueur de un bit. Prenons à titre d'exemple l'un des protocoles les plus couramment utilisés : le protocole de Shnorr (Schnorr, 1990). Le prouveur convainc le vérifieur qu'il connaît le logarithme discret de y en base g soit $log_g y$, g *générateur* de G_q et q premier. Le prouveur prouve qu'il connaît le secret, aussi appelé la quantité x, tel que $y = g^x$. La valeur y est connue du vérifieur. Soit $r_\alpha \in_{\mathcal{R}} \mathbb{Z}_q$, le prouveur s'engage en envoyant $t = g^{r_\alpha}$:

$$P \longrightarrow V : t$$

Le vérifieur envoie un challenge $c \in \{0,1\}^{l_c}$ avec l_c la longueur du challenge :

$$P \longleftarrow V : c$$

Le prouveur répond par $s_\alpha := r_\alpha - cx \ mod \ q$:

$$P \longrightarrow V : s_\alpha$$

Le vérifieur vérifie alors la réponse: $t' = g^{s_\alpha} y^c \stackrel{?}{=} t$ que l'on peut justifier ainsi :

$$\begin{aligned} s_\alpha = r_\alpha - cx &\Leftrightarrow s_\alpha + cx = r_\alpha \\ &\Leftrightarrow g^{s_\alpha + cx} = g^{r_\alpha} \\ &\Leftrightarrow g^{s_\alpha} g^{cx} = g^{r_\alpha} \\ &\Leftrightarrow g^{s_\alpha} y^c = g^{r_\alpha} \end{aligned} \tag{IV.1}$$

La probabilité de cohérence, aussi appelée erreur de connaissance [17], est alors de 2^{-l_c}.

Selon (Fiat & Shamir, 1987), il est possible de dériver ce protocole pour en faire un protocole de signature. Cela est généralement appelé l'« heuristique Fiat-Shamir » (Fiat & Shamir, 1987 ; Pointcheval & Stern, 1996). Au lieu d'envoyer un challenge, le vérifieur envoie une valeur de hachage contenant un message $m \in \{0,1\}^{l_m}$ à signer. Ainsi, le challenge est remplacé par $c = \mathcal{H}(g \| y \| t \| m)$. La signature de m consiste en la paire (s,c). La vérification de la signature consiste en la vérification des valeurs de hachage :

$$\hat{t} = g^s y^c \ et \ c \stackrel{?}{=} \mathcal{H}(g \| y \| \hat{t} \| m)$$

Dans la suite de ce chapitre nous utiliserons la notation introduite par Camenish et Stadler (Camenisch & Stadler, 1997) pour noter les preuves de connaissance. Ainsi, une preuve de connaissance d'une quantité α est notée :

$$PK\{(\alpha) : y \equiv g^\alpha\}$$

Cela correspond à prouver la valeur secrète x de l'exemple précédent, alors que y est connu du vérifieur. Le protocole dérivé pour en faire un protocole de signature est noté :

$$SPK\{(\alpha) : y \equiv g^\alpha\}(m)$$

17. trad. Knowledge error.

Il est également possible de prouver la connaissance d'une représentation. Soient l bases $g_1,...,g_l \in G_q$ avec $l \geq 1$ et $g_l \neq 1$. Le protocole noté :

$$PK\{(\alpha_1,...,\alpha_l) : y \equiv \prod_{i=1}^{l} g_i^{\alpha_i}\}$$

est une preuve de connaissance de la représentation x_i de $y \in G_q$ respectant les bases g_i. Ainsi, les prouveurs et vérifieurs ont en entrée : $y,g_1,...,g_l$, l'ordre q du groupe et le paramètre k (taille de q). Les secrets connus du prouveur sont les $x_i \leq q-1$ tels que $y = \prod_{i=1}^{l} g_i^{x_i}$. Les secrets x_i sont les quantités α_i à prouver. Voici donc le protocole.

Le prouveur choisi l valeurs aléatoires $r_{\alpha_i} \in_{\mathcal{R}} \mathbb{Z}_q$ et s'engage en envoyant $t = \prod_{i=1}^{l} g_i^{r_{\alpha_i}}$:

$$P \longrightarrow V : t$$

Le verifeur envoie un challenge $c \in \{0,1\}^{l_c}$ avec l_c la longueur du challenge :

$$P \longleftarrow V : c$$

Le prouveur calcule l réponses $s_{\alpha_i} := r_{\alpha_i} - cx_i \ mod \ q$:

$$P \longrightarrow V : s_{\alpha_1},...,s_{\alpha_l}$$

Le vérifieur vérifie alors la réponse: $t' = y^c \prod_{i=1}^{l} g_i^{s_{\alpha_i}} \stackrel{?}{=} t$ que l'on peut justifier ainsi :

$$\begin{aligned} s_{\alpha_i} = r_{\alpha_i} - cx_i &\Leftrightarrow s_{\alpha_i} + cx_i = r_\alpha \\ &\Leftrightarrow g_i^{s_{\alpha_i}+cx_i} = g_i^{r_{\alpha_i}} \\ &\Leftrightarrow g_i^{s_{\alpha_i}} g_i^{cx_i} = g^{r_{\alpha_i}} \end{aligned} \tag{IV.2}$$

et

$$\prod_{i=1}^{l} g_i^{s_{\alpha_i}} g_i^{cx_i} = \prod_{i=1}^{l} g_i s^{r_{\alpha_i}} \Leftrightarrow y^c \prod_{i=1}^{l} g_i^{s_{\alpha_i}} = \prod_{i=1}^{l} g_i^{r_{\alpha_i}} \tag{IV.3}$$

La notation de Camenisch permet d'exprimer aisément un ensemble de preuves de plusieurs quantités par l'utilisation de plusieurs protocoles fonctionnant en parallèle. Ainsi,

$$PK\{(\alpha_1,...,\alpha_l,\beta_1,...,\beta_{l'}) : y \equiv \prod_{i=1}^{l} g_i^{\alpha_i} \wedge z \equiv \prod_{i=1}^{l'} h_i^{\beta_i}\} \tag{IV.4}$$

avec $g_i,h_i,y,z \in G_q$, est obtenu à l'aide des deux protocoles suivants :

$$PK\{(\alpha_1,...,\alpha_l) : y \equiv \prod_{i=1}^{l} g_i^{\alpha_i}\} \quad et \quad PK\{(\beta_1,...,\beta_{l'}) : z \equiv \prod_{i=1}^{l'} h_i^{\beta_i}\} \tag{IV.5}$$

Notons simplement que les engagements de chaque protocole sont envoyés en premier, puis le vérifieur envoie un seul challenge que le répondeur utilisera pour calculer les réponses de chaque protocole.

Il est également possible de prouver l'égalité de deux logarithmes discrets respectant des bases différentes. Ainsi, si la quantité α est prouvée égale pour deux représentations avec deux bases distinctes, la valeur aléatoire r_α doit être la même pour les deux protocoles qui impliquent α. Prenons l'exemple suivant :

$$PK\{(\alpha,\beta) : y \equiv g^\alpha h^\beta \wedge z \equiv i^\alpha\} \tag{IV.6}$$

Ce protocole sert à démontrer la connaissance de x_α et x_β par le prouveur, et le fait que le logarithme discret de z en base i soit égal au premier élément de y en base g. Les engagements sont $t_y = g^{r_\alpha} h^{r_\beta}$ et $t_z = i^{r_\alpha}$, le challenge $c \in_{\mathcal{R}} \{0,1\}^k$, et les réponses $s_\alpha = r_\alpha - c x_\alpha \ mod\ q$ et $s_\beta = r_\beta - c x_\beta \ mod\ q$. Les équations de vérification sont $t_y \stackrel{?}{=} y^c g^{s_\alpha} h^{s_\beta}$ et $t_z \stackrel{?}{=} z^c i^{s_\alpha}$.

Enfin, notons quelques exemples utiles donnés par (Camenisch, 2008) :

- $PK\{(\alpha,\beta) : y_1 \equiv g^\alpha \wedge y_2 \equiv g^\beta \wedge y_3 \equiv y_1^\beta\}$ permet de prouver que $log_g y_3$ est le produit de $log_g y_1$ et $log_g y_2$.
- $PK\{(\alpha) : y_1 \equiv g^\alpha \wedge y_2 \equiv y_1^\alpha\}$ permet de prouver que $log_g y_2 = (log_g y_1)^2$.
- $PK\{(\alpha) : \frac{y}{g^{(a+b)/2}} \equiv g^\alpha \ mod\ n \ \wedge \ \alpha \in [-\frac{b-a}{2}, \frac{b-a}{2}]\}$ permet de prouver qu'un logarithme discret est contenu dans un intervalle $[a,b]$.

IV.2.4 Les signatures à l'aveugle

Les signatures à l'aveugle sont des protocoles cryptographiques introduits par (Chaum, 1983). Elles permettent à une entité de produire une signature sur un message, et à un tiers interlocuteur du signataire de modifier celui-ci sans altérer la signature. Le message ainsi signé pourra être reconnu comme signé du signataire sans que celui-ci ne puisse l'associer à une signature qu'il a produite.

Prenons un exemple basé sur le cryptosystème à clé publique RSA (Rivest *et al.*, 1978). Soit n le produit de deux premiers p et q. Soit e un nombre premier avec $\varphi(n)$. Soit d l'inverse de e modulo $\varphi(n)$, soit $ed \equiv 1 \ mod\ \varphi(n)$. Dans le cadre d'un cryptosystème à clé publique, soit (e,n) la clé publique du signataire et $(d,\varphi(n))$ sa clé privée. Notons, pour tout entier a, $a^{ed} \equiv a \ mod\ n$. Le processus de signature du message m est le suivant :

$$s \equiv m^d \ mod\ n \tag{IV.7}$$

La vérification consite à vérifier :

$$m \stackrel{?}{=} s^e \ mod\ n \tag{IV.8}$$

La signature à l'aveugle se fait en trois phases : l'aveuglement, la signature et le « désaveuglement ». Considérons un tiers A souhaitant faire signer un message m à un signataire B sans que celui-ci n'ait connaissance ni de ce message ni de la signature de m. Pour cela, A génère un entier aléatoire k co-premier avec n. A procède à l'aveuglement de m par la fonction f, $f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$, définie par $f(m) \equiv mk^e \ mod \ n$. A envoie $f(m)$ pour signature à B. B signe, soit $s \equiv f(m)^d \ mod \ n$, et fournit s à A. On note que $s \equiv (m.k^e)^d \equiv m^d k^{ed} \equiv m^d k \ mod \ n$. Le désaveuglement de la signature se fait par la fonction g, $g : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$, définie par $g(m') \equiv m'k^{-1} \ mod \ n$. Il en résulte $g(s) \equiv g(m^d k \ mod \ n) \equiv m^d \ mod \ n$. *A* obtient donc une signature valide sur m par B sans que celui-ci puisse comparer celle-ci avec un message qu'il aurait auparavant signé.

En résumé, A génère $k \in_{\mathbb{R}} \mathbb{Z}_n$, avec $pgcd(k,n) = 1$. et aveugle m par $m' \equiv mk^e \ mod \ n$:

$$A \xrightarrow{m'} B \tag{IV.9}$$

B signe m', $s_{av} \equiv m^d k \ mod \ n$:

$$A \xleftarrow{s_{av}} B \tag{IV.10}$$

A désaveugle la signature, $s \equiv m^d \ mod \ n$.

Il est nécessaire de compléter la présentation de la signature par le mécanisme de sélection aléatoire[18] par le signataire, introduite par (Rabin, 1989). En effet, le signataire peut requérir la connaissance du message à signer, ou tout simplement s'assurer que le message à signer possède un certain format. Cependant, l'aveuglement de celui-ci lui empêche de vérifier que le message est bien celui attendu. Pour pallier à cela, le signataire va exiger k candidats à la signature et n'en signera que $k/2$. Pour les $k/2$ autres pris au hasard, l'utilisateur devra fournir les valeurs d'aveuglement. Cela permet au signataire de vérifier si l'utilisateur a triché ou non. L'utilisateur peut tenter de tricher en espérant que les candidats pour lesquels il a triché ne soient pas ceux choisis par le signataire pour être analysés. La probabilité de pouvoir tricher est donc déterminée par la taille de k. Ainsi, A génère i candidats :

$$C_i \equiv r_i^e m \ mod \ n \ \ pour \ 1 \leq i \leq k \tag{IV.11}$$

B choisi un sous-ensemble de $k/2$ candidats $R = i_j 1 \leq i_j \leq k \ et \ 1 \leq j \leq k/2$, et l'envoie à A. A révèle les $r_i \in R$ et B vérifie ces candidats. B retourne ensuite la multiplication des candidats signés :

$$C \equiv \prod_{i \notin R} C_i^d \ mod \ n \tag{IV.12}$$

18. trad. Cut-and-choose.

A désaveugle ensuite les candidats signés :

$$M \equiv \frac{C}{\prod_{i \notin R} r_i} \equiv m^{kd} \; mod \; n \tag{IV.13}$$

IV.3 Étude des contributions

Les besoins de l'architecture ont été précisés dans la section IV.1. Nous faisons ici une étude des contributions majeures dans le domaine des systèmes à pseudonymes. Il s'agira donc de déterminer dans quelles mesures celles-ci répondent à nos besoins. Pour simplifier les explications, l'entité sujet des certificats sera appelée utilisateur.

IV.3.1 Contribution de Chaum

Les contributions de Chaum ont constitué la base des architectures à certificats ne permettant pas d'associer les identités sur le générateur et sur le consommateur. Il a notamment développé le paradigme entourant les certificats utilisables dans le cadre de la monnaie électronique (Chaum *et al.*, 1990). Nous allons donc reprendre ici les concepts et les mécanismes cryptographiques majeurs, et décrire les manques qui justifient l'utilisation de mécanismes différents ou complémentaires.

L'architecture repose sur le mécanisme de signature à l'aveugle basé sur RSA présenté à la section précédente. Dans le cas d'usage de cette contribution, un certificat représente une pièce de monnaie. Les mécanismes mis en place permettent de révoquer l'anonymat d'une entité si celle-ci présente deux fois un même certificat. La révocation, locale et synchrone, consiste à révéler un identifiant tel que le numéro de compte de l'individu auprès de la banque u, incrémenté d'un compteur v de certificats, et d'un incrément i par candidat. Le candidat est un terme qui désigne un élément soumis au procédé de sélection aléatoire. L'identifiant est placé dans le message aveuglé à faire signer par l'utilisateur. Pour s'assurer que l'utilisateur ne triche pas, le générateur, ici la banque, applique la méthode de la sélection aléatoire. L'utilisateur obtient donc un certificat qui a la forme suivante :

$$C = \prod_{1 \leq i \leq k/2} f(x_i,y_i)^d \ mod \ n \tag{IV.14}$$

avec f et g deux fonctions de hachage sans collision, et

$$x_i = g(a_i,c_i) \ et \ y_i = g(a_i \oplus (u \| (v+i)),di) \ avec \ a_i,c_i,d_i \in_{\mathrm{R}} [1,k] \tag{IV.15}$$

L'utilisateur présente ensuite ce certificat au commerçant. Celui-ci s'assure que le certificat est bien formé et que sa signature est valide. Il va pour cela reconstruire les candidats, et vérifier que le produit des candidats est bien égal au certificat chiffré avec la clé publique du signataire. Le commerçant envoie pour cela une valeur aléatoire z de taille $k/2$ à l'utilisateur. En prenant z bit à bit, si $z_i = 1$, celui-ci fournit a_i,c_i et y_i, le commerçant recalcule alors $C_i = f(g(a_i,c_i),y_i)$. Si $z_i = 0$, l'utilisateur fournit x_i, $a_i \oplus (u \| (v+i))$ et d_i

et le commerçant calcule $C_i = f(x_i,g(a_i \oplus (u\|(v+i)),di))$. Il vérifie ensuite que :,

$$C^e \equiv \prod_{1 \leq i \leq k/2} C_i \ mod\ n \tag{IV.16}$$

Chaum adresse notamment la problématique d'un utilisateur et d'un consommateur qui s'allieraient pour faire un transcrit avec le même z. Il propose pour cela d'avoir un identifiant du commerçant introduit dans z. Il adresse également la question de la double dépense du certificat. Il est sous-entendu que l'utilisateur est conscient qu'il ne doit pas présenter deux fois un même certificat. Tant qu'il ne le fait pas, son identité, u, n'est pas révélée. Lorsque l'utilisateur présente un certificat, le commerçant peut l'encaisser immédiatement ou le faire ultérieurement. L'idée est la suivante : le certificat est une valeur unique que le générateur peut lister dans une liste des certificats déjà présentés. Ainsi, un commerçant peut à l'encaissement vérifier directement avec la banque que le certificat n'a pas été déjà encaissé. L'intérêt de permettre de révéler un identifiant de l'utilisateur dans le cas de la double dépense est de permettre de sanctionner l'utilisateur. Or, il s'agit d'un principe de dissuasion qui permet de supposer que le commerçant n'est pas obligé de vérifier le certificat dès son encaissement. La terminologie suivante est souvent employée bien qu'elle porte à confusion : si la vérification est faite dès l'encaissement, la monnaie est dite *en ligne*, par opposition avec la monnaie *hors ligne* qui suppose un mécanisme de dissuasion permettant de ne pas avoir à procéder à la vérification du double encaissement dès la présentation d'un certificat.

S'il s'agit d'un commerçant qui essaie de tricher, il ne dispose que d'un transcrit avec un même z ce qui permet à la banque d'identifier que le tricheur est le commerçant. Si les transcrits des deux encaissements sont différents, le z diffère, cela implique que l'utilisateur a triché car il est le seul à pouvoir le faire. En ayant deux transcrits différents avec des z différents, la probabilité qu'un bit de chacun des deux z soit différent est grande, ce qui assure que l'identité u puisse être révélée grâce à un nouveau calcul en opérant un « ou exclusif » logique. Pour un même i, où $z_i \neq z'_i$, la banque possède a_i et $a_i \oplus (u\|(v+i))$, ce qui lui permet d'avoir $u\|(v+i)$ qui identifie l'utilisateur sur le générateur.

Chaum propose également un mécanisme de chéquier. L'utilisateur se voit attribuer un chéquier pour un certain montant qui lui est débité à la délivrance de celui-ci. L'utilisateur paye avec un nombre limité de chèques, de montants inconnus de la banque, mais dont la somme ne peut dépasser celle du chéquier. L'utilisateur peut retourner à la banque le chéquier s'il n'est pas épuisé afin d'être crédité du montant non dépensé. Enfin, Chaum présente un mécanisme où plusieurs certificats sont émis simultanément, et par lequel, dès lors qu'un des certificats vient à être dépensé deux fois, un identifiant de l'ensemble des certificats est révélé, permettant ainsi de les ajouter à une liste de révocation.

Enfin, il est proposé de coder une valeur dans l'exposant des candidats, potentiellement un attribut. Reprenons le schéma de signature de la section précédente. Supposons k candidats. Le signataire les ordonne et indique le nouvel ordre des candidats à l'utilisateur. La position du candidat est encodée dans son exposant et donc modifiable par l'utilisateur. Ainsi, l'utilisateur aveugle ses candidats :

$$C_i \equiv r_i^{e^k} m \ mod\ n \ \ pour\ 1 \leq i \leq k \tag{IV.17}$$

B choisi un sous-ensemble de $k/2$ candidats $R = i_j 1 \leq i_j \leq k$ et $1 \leq j \leq k/2$, et l'envoi à A. A révèle les $r_i \in R$ et B les vérifie. B retourne ensuite les candidats signés avec leur position encodée dans l'exposant :

$$C_{isigned} \equiv r_i^{e^k d^i} m^{d^i} \equiv r_i^{e^{k-i}} m^{d^i} \ mod\ n \ \ pour\ 1 \leq i \leq k/2 et i \notin R \tag{IV.18}$$

A désaveugle ensuite les candidats signés en divisant par $r_i^{e^{k-i}}$:

$$M_i \equiv m^{d^i} \ mod\ n \tag{IV.19}$$

Pour vérifier la signature, il faut vérifier que $m \equiv M_i^{e^i} \ mod\ n$.

Les contributions de Chaum ont initié les travaux du domaine, notamment concernant la non-associativité entre la génération et la présentation d'un certificat. Cependant, il est difficile de chiffrer de multiples attributs à moins de les concaténer dans l'exposant. Les fonctionnalités de présentation sélective du contenu n'est donc pas réalisable. La gestion du cycle de vie des certificats est limitée aux certificats à usage unique puisque les multiples présentations d'un même certificat sont associables. La révocation de l'anonymat ne permet qu'une révocation synchrone.

IV.3.2 Contribution de Brands

Brands (Brands, 1993, 1994, 2000) propose le schéma de signature suivant. L'utilisateur représente les attributs qu'il souhaite faire signer en RSA ou en DL et aveugle le résultat. Le principe est ici décrit pour des représentations en logarithmes discrets (DLREP)[19]. Soient les attributs $(x_1,...,x_l)$ et le secret α, aussi appelé facteur d'aveuglement, les représentations en bases $(g_1,...g_l,h_0) \in_R G_q$ de la clé publique du générateur, et h le contenu à signer :

$$h = (g_1^{x_1} ... g_l^{x_l} h_0)^{\alpha} \tag{IV.20}$$

19. cf. (Brands, 2000) pour RSAREP

Notons que la valeur h est présentée au consommateur lors de la vérification de la signature. Pour que le générateur et le consommateur ne puissent pas lier les transactions par le certificat, il est donc nécessaire que la signature sur h soit faite sans que le générateur n'apprenne h. Soient $(y_1,...,y_l,x_0)$ la clé privée de signature du générateur, et $(g_1 = g_0^{y_1},...,g_l = g_0^{y_l},h_0 = g_0^{x_0})$ sa clé publique. Soient A le générateur et B l'utilisateur. Voici le protocole de génération de la signature sur h :

$$
\begin{aligned}
&A \longrightarrow B : a_0 = g_0^{w_0}, w_0 \in \mathbb{Z}_q \\
&A \longleftarrow B : c_0 = c_0' - \alpha_2 \\
&avec\ h = (g_1^{x_1}...g_l^{x_l}h_0)^{\alpha_1},\ c_0' = \mathcal{H}(h,g_0^{\alpha_2}(g_1^{x_1}...g_l^{x_l}h_0)^{\alpha_3}a_0),\ \alpha_1 \in \mathbb{Z}_q^*\ et\ \alpha_2,\alpha_3 \in \mathbb{Z}_q \\
&A \longrightarrow B : r_0 = (w_0 - c_0)/(x_0 + x_1y_1 + ... + x_ly_l)\ mod\ q
\end{aligned}
$$

Pour générer r_0, le générateur doit connaître $(x_1,...,x_l)$. L'utilisateur accepte cela comme une signature valide sur h si $a_0 \stackrel{?}{=} g_0^{c_0}(g_1^{x_1}...g_l^{x_l}h_0)^{r_0}$, puis il calcule $r_0' = (r_0 + \alpha_3)/\alpha_1$. La vérification de la signature peut être justifiée ainsi :

$$
\begin{aligned}
r_0 = (w_0 - c_0)/(x_0 + x_1y_1 + ... + x_ly_l) &\Leftrightarrow r_0(x_0 + x_1y_1 + ... + x_ly_l) = (w_0 - c_0) \\
&\Leftrightarrow (g_0^{x_0}g_0^{x_1y_1}...g_0^{x_ly_l})^{r_0} = g_0^{w_0}g_0^{-c_0} \\
&\Leftrightarrow (h_0g_1^{x_1}...g_l^{x_l})^{r_0}g_0^{c_0} = a_0
\end{aligned}
\qquad \text{(IV.21)}
$$

La signature sur le certificat, nommée *certificat à clé secrète* par Brands, est composée des deux valeurs c_0' et r_0'. La vérification du certificat se fera par l'équation de vérification :

$$
c_0' \stackrel{?}{=} \mathcal{H}(h,g_0^{c_0'},h^{r_0'}) \qquad \text{(IV.22)}
$$

que l'on peut justifier ainsi :

$$
\begin{aligned}
&c_0' = \mathcal{H}(h,g_0^{\alpha_2}(g_1^{x_1}...g_l^{x_l}h_0)^{\alpha_3}a_0)\ or \\
&\qquad (h_0g_1^{x_1}...g_l^{x_l})^{r_0}g_0^{c_0} = a_0 \Leftrightarrow (h_0g_1^{x_1}...g_l^{x_l})^{r_0'\alpha_1-\alpha_3}g_0^{c_0'-\alpha_2} = a_0 \\
&\qquad\qquad \Leftrightarrow h^{r_0'}(h_0g_1^{x_1}...g_l^{x_l})^{-\alpha_3}g_0^{c_0'-\alpha_2} = a_0 \\
&\qquad\qquad \Leftrightarrow h^{r_0'}g_0^{c_0'} = a_0g_0^{\alpha_2}(h_0g_1^{x_1}...g_l^{x_l})^{\alpha_3} \\
&\qquad soit\ c_0' = \mathcal{H}(h,h^{r_0'}g_0^{c_0'})
\end{aligned}
\qquad \text{(IV.23)}
$$

Pour présenter le certificat, l'utilisateur donne (h,c_0',r_O') au consommateur. Le consommateur vérifie $c_0' = \mathcal{H}(h,h^{r_0'}g_0^{c_0'})$. L'utilisateur mène ensuite une preuve de connaissance :

$$
PK\{(\alpha_1,...,\alpha_{l+1}) : h = \prod_{i=1}^{l+1} g_i^{\alpha_i}\} \qquad \text{(IV.24)}
$$

La connaissance des attributs et du secret d'aveuglement permettent de prouver la possession d'un certificat. Si tous les attributs sont révélés, le secret d'aveuglement permet de garantir la preuve de possession. Cependant, tous les attributs sont aveuglés par α ce qui nécessite également que l'entité prouve le logarithme discret $z_i = x_i\alpha$. La preuve de connaissance utilisée par Brands est une variante de Shnorr. Il utilise comme réponse au challenge :

$$s_{\alpha_i} = cz_i + r_{\alpha_i} \tag{IV.25}$$

Cela conduit à faire une vérification de la preuve par :

$$t' = h^{-c} \prod_{i=1}^{l+1} g_i^{s_{\alpha_i}} \stackrel{?}{=} t \tag{IV.26}$$

Chacun des attributs peut ensuite être révélé indépendamment et prouvé comme étant contenu dans h. Supposons dans l'exemple précédent que x_1 est révélé, il suffit de prouver $hg_1^{-z_1} = \prod_{i=2}^{l+1} g_i^{s_{\alpha_i}}$, c'est-à-dire que $h = g_1^{z_1} \prod_{i=2}^{l+1} g_i^{s_{\alpha_i}}$, que l'on note :

$$PK\{(\alpha_1,...,\alpha_{l+1}) : h \equiv \prod_{i=1}^{l+1} g_i^{\alpha_i} \wedge h = g_1^{z_1} \equiv \prod_{i=2}^{l+1} g_i^{\alpha_i}\} \tag{IV.27}$$

Intéressons-nous maintenant à la limitation du nombre de fois où il est possible de présenter un même certificat. L'idée est la suivante : si un certificat est présenté plus de fois qu'il ne le devrait, les attributs contenus dans celui-ci peuvent être révélés au consommateur. Il s'agit de dissuasion si l'un des attributs est un identifiant de l'utilisateur. Il peut s'agir d'une révocation synchrone locale si l'identifiant est un lien vers l'identité sur le générateur, ou globale s'il s'agit d'un identifiant de l'identité réelle. Pour que ce système fonctionne, à l'instar du mécanisme de Chaum, les consommateurs de certificats déposent les transcrits sur le générateur ainsi que le certificat. Le générateur vérifie alors que ce certificat n'a pas déjà été présenté. Le cas échéant il est en mesure de révéler les attributs au consommateur. Le mécanisme suivant est utilisé pour révéler les attributs en cas de double dépense. Il est important de noter que l'on suppose pour l'instant que l'engagement utilisé par l'utilisateur est « figé ». Prenons $h = (g_1^{x_1} g_2^{x_2} g_3^{x_3} h_0)^{\alpha_1}$. Voici la première présentation :

$$t = h^{-c} g_1^{r_1} g_2^{r_2} g_3^{r_3} h_0^{r_4} \tag{IV.28}$$

et la seconde :

$$t^* = h^{-c^*} g_1^{r_1^*} g_2^{r_2^*} g_3^{r_3^*} h_0^{r_4^*} \tag{IV.29}$$

Le même engagement signifie $t = t^*$, donc

$$\begin{aligned} & h^{-c} g_1^{r_1} g_2^{r_2} g_3^{r_3} h_0^{r_4} = h^{-c^*} g_1^{r_1^*} g_2^{r_2^*} g_3^{r_3^*} h_0^{r_4^*} \\ \Leftrightarrow\ & h^{c-c^*} = g_1^{r_1-r_1^*} g_2^{r_2-r_2^*} g_3^{r_3-r_3^*} h_0^{r_4-r_4^*} \\ \Leftrightarrow\ & h = g_1^{r_1-r_1^*/c-c^*} g_2^{r_2-r_2^*/c-c^*} g_3^{r_3-r_3^*/c-c^*} h_0^{r_4-r_4^*/c-c^*} \end{aligned} \tag{IV.30}$$

On en déduit que :

$$\begin{aligned} \alpha_1 &= r_4 - r_4^*/c - c^* \\ x_1\alpha_1 &= r_1 - r_1^*/c - c^* \Leftrightarrow x_1 = r_1 - r_1^*/r_4 - r_4^* \\ x_2\alpha_1 &= r_2 - r_2^*/c - c^* \Leftrightarrow x_2 = r_2 - r_2^*/r_4 - r_4^* \\ x_3\alpha_1 &= r_3 - r_3^*/c - c^* \Leftrightarrow x_3 = r_3 - r_3^*/r_4 - r_4^* \end{aligned} \tag{IV.31}$$

Comme nous l'avons supposé, l'engagement doit être « figé ». Il est donc fixé « à l'avance » lors de la signature. L'utilisateur intègre l'engagement dans le certificat, ce qui a pour conséquence que la signature ne soit valable que pour celui-ci, ce qui fait de (h,a) un certificat à usage unique. La vérification de la signature sera $c_0' = \mathcal{H}(h,a,h^{r_0'} g_0^{c_0'})$. L'inconvénient de cela est que le témoin varie en fonction des attributs que l'utilisateur souhaite montrer aux consommateurs. Cependant, cela va dépendre de la présentation et donc ne peut être anticipé lors de la signature. Pour palier à cela, Brands utilise ce qu'il nomme des correcteurs. Ainsi, l'engagement peut être fixé à la signature mais être variable pour chacune des combinaisons d'attributs montrés à l'aide des correcteurs. Enfin, pour permettre de limiter l'utilisation d'un certificat à n présentations, il est possible de créer n engagements à la signature du certificat.

L'architecture de Brands répond à la majeure partie des besoins exprimés. Les certificats permettent l'inassociativité, la présentation sélective des attributs ainsi que les preuves de connaissance sur les attributs. Il propose une solution pour limiter le nombre de présentations d'un certificat. Cela s'accompagne d'une mesure de dissuasion pour un nombre de dépenses supérieur à celui autorisé. Il est important de préciser que prêter ou partager un certificat nécessite de céder l'ensemble des attributs et le secret nécessaires à la preuve de possession du certificat. La solution proposée pour lutter contre la non-transférabilité est que le générateur force un attribut dans le certificat que l'utilisateur ne souhaitera pas révéler. Pour que cela fonctionne il est nécessaire que chaque générateur soit à même de fournir une telle valeur. Cette solution doit être efficace sur tous les certificats employés pour éviter le partage. Ajoutons que Brands ne propose pas de système de révocation de l'anonymat asynchrone. Le problème majeur du système de certificats de Brands est que les multiples présentations d'un même certificat sont associables par h. Cela n'est pas présenté ici mais Brands propose un protocole de régénération de certificats simplifié.

IV.3.3 Contribution de Camenisch

Nous décrivons ici l'architecture de Camenisch et Lysyanskaya (Camenisch & Lysyanskaya, 2001 ; Camenisch & Herreweghen, 2002), notamment issue des précédents travaux de Lysyanskaya (Lysyanskaya *et al.*, 2000). Nous étudions spécifiquement le schéma de signature Camenisch-Lysyanskaya (CL-Signature Scheme) (Camenisch & Lysyanskaya, 2003) plus évolué que le schéma de signature initialement présenté dans (Camenisch & Lysyanskaya, 2001).

Soit $\mathbf{QR}_n$ l'ensemble des résidus quadratiques modulo n. Le signataire génère les paramètres de signatures : n le module RSA produit de p et q deux premiers sûrs[20] tels que $p = 2p' + 1$ et $q = 2q' + 1$, avec p' et q' sûrs. Sa clé publique est $(n,R_0,...,R_{L+1},S,Z)$ avec $R_0,...,R_{L+1},S,Z \in \mathbf{QR}_n$. Les facteurs de n sont sa clé privée. La taille binaire de n est l_n.

L'espace des messages, qui comprend notamment les attributs, est l'ensemble $\{(m_0,...,m_{L-1}) : m_i \in \pm\{0,1\}^{l_m}\}$ soit l'intervalle $[-2^{l_m}+1,2^{l_m}-1]$. Les attributs de l'utilisateur, les m_i, sont donc représentés avec les bases de la clé publique du générateur.

Le générateur choisit alors un nombre aléatoire premier e ($l_e > l_m + 2$). L'exposant e permet la vérification d'une signature reposant sur le problème RSA. Le calcul de l'inverse de l'exposant e public repose sur la décomposition en nombre premier de n. d, la clé privée de signature, est l'inverse de e module $\varphi(n)$, soit $ed \equiv 1 \ mod \ \varphi(n)$ et $\varphi(n) = \varphi(pq) = (p-1)(q-1)$.

Une signature sur un ensemble de messages se calcule de la manière suivante, avec v de longueur $l_v = l_n + l_m + l_r$, r un paramètre de sécurité :

$$A \equiv (\frac{Z}{R_0^{m_0}...R_{L+1}^{m_{L+1}}S^v})^{1/e} \ mod \ n \tag{IV.32}$$

La signature consiste en (A,e,v) et la vérification se fait par :

$$Z \stackrel{?}{\equiv} A^e R_0^{m_0}...R_{L+1}^{m_{L+1}}S^v \ mod \ n \tag{IV.33}$$

Ce schéma autorise le fait que certains messages soient inconnus du signataire. Il faut en contre partie en apporter la preuve de possession. Il faut pour cela utiliser la CL-signature amendée qui nécessite $R_0,...,R_{L+1},Z \in \langle S \rangle$. Si on considère que les messages $(m_0,....,m_{L'-1})$ ne seront pas connus du signataire, l'utilisateur choisit v' aléatoirement et

20. trad. Safe prime

calcule :

$$U = S^{v'} \prod_{i=0}^{L'-1} R_i^{m_i} \ mod\ n \tag{IV.34}$$

Il l'envoie au générateur et en fait ensuite la preuve de possession :

$$PK\{(\alpha_0,...,\alpha_{L'-1},\beta) : \pm U \equiv S^{\beta} \prod_{i=0}^{L'-1} R_i^{\alpha_i} \ mod\ n \wedge \alpha_0,...,\alpha_{L'-1} \in \pm\{0,1\}^{l_m}\} \tag{IV.35}$$

Le générateur choisit aléatoirement $\hat{v}$, calcule $v'' = \hat{v} + 2^{l_v - 1}$ et choisit e. Il calcule ensuite la signature :

$$A \equiv (\frac{Z}{US^{v''} \prod_{i=L'}^{L-1} R_i^{m_i}})^{1/e} \ mod\ n \tag{IV.36}$$

Puis prouve que A a été calculé correctement et que $A \in \langle S \rangle$:

$$PK\{(\delta) : A \equiv \pm(\frac{Z}{US^{v''} \prod_{i=L'}^{L-1} R_i^{m_i}})^{\delta}\} \tag{IV.37}$$

L'utilisateur dispose d'un certificat dont il va prouver la possession de la signature. Il va pour cela faire varier A sans pour autant altérer la signature. Il faut pour cela utiliser une valeur aléatoire r et que $A \in \langle S \rangle$. Ainsi, ce tuple est aussi une signature valide : $(A' = AS^{-r} \ mod\ n, e, v' = v + er)$ que l'on peut justifier ainsi :

$$\begin{aligned} A' \equiv (\frac{Z}{R_0^{m_0}...R_{L+1}^{m_{L+1}} S^{v'}})^{1/e} \ mod\ n &\Leftrightarrow AS^{-r} \equiv (\frac{Z}{R_0^{m_0}...R_{L+1}^{m_{L+1}} S^{v+er}})^{1/e} \ mod\ n \\ &\Leftrightarrow A \equiv (\frac{Z}{R_0^{m_0}...R_{L+1}^{m_{L+1}} S^{v+er-er}})^{1/e} \ mod\ n \\ &\Leftrightarrow A \equiv (\frac{Z}{R_0^{m_0}...R_{L+1}^{m_{L+1}} S^{v}})^{1/e} \ mod\ n \end{aligned} \tag{IV.38}$$

L'utilisateur peut donc révéler A' au consommateur puisqu'il n'est pas possible de lier A et A'. Il s'agit de la propriété la plus importante du schéma de signature *CL-Signature* qui assure la non-associativité de la génération et de la présentation de la signature.

Dans le cas où l'utilisateur ne mène qu'une preuve de possession d'un certificat de ce générateur, il ne révèle donc aucun attribut, l'utilisateur mène une preuve de connaissance de la représentation $(m_1,...,m_{L+1},e,v)$ de Z en base $(R_0,...,R_{L+1},A',S)$, soit :

$$PK\{(\alpha_0,...,\alpha_{L-1},\varepsilon,\nu') : Z \equiv \pm A'^{\varepsilon} S^{\nu'} \prod_{i=0}^{L+1} R_i^{\alpha_i} \ mod\ n \wedge \alpha_i \in \pm\{0,1\}^{l_m} \wedge \varepsilon \in [2^{l_e-1}+1, 2^{l_e}-1]\} \tag{IV.39}$$

Pour prouver que $\alpha_i \in \pm\{0,1\}l_m$ et $\varepsilon \in [2^{l_e-1}+1, 2^{l_e}-1]$, il est nécessaire que les m_i et e correspondants soient dans des intervalles plus petits. Après correction, la preuve à

apporter est :

$$PK\{(\alpha_0,...,\alpha_{L-1},\varepsilon,\nu') : ZA'^{-2^{l_e+1}} \equiv \pm A'^{\varepsilon} S^{\nu'} \prod_{i=0}^{L+1} R_i^{\alpha_i} \ mod\ n \\ \wedge\ \alpha_i \in \pm\{0,1\}^{l_m} \ \wedge\ \varepsilon \in \pm\{0,1\}^{l'_e+l_\varnothing+l_{\mathcal{H}}+2}\} \tag{IV.40}$$

L'utilisateur peut choisir de révéler les attributs qu'il souhaite. Il prouve ensuite le fait que ceux-ci appartiennent au certificat. On note I_r l'ensemble des indices des attributs révélés. L'utilisateur envoie au consommateur A' et les $\{m_i | i \in I_r\}$. Puis, mène la preuve de connaissance suivante :

$$PK\{(\{\alpha_i \ | i \notin I_r\},\varepsilon,\nu') : ZA'^{-2^{l_e+1}} \prod_{i\in I_c} R_i^{m_i} \equiv \pm A'^{\varepsilon} S^{\nu'} \prod_{i\notin I_r} R_i^{\alpha_i} \ mod\ n \\ \wedge\ \alpha_i \in \pm\{0,1\}^{l_m+l_\varnothing+l_{\mathcal{H}}+2} (i \notin I_r) \ \wedge\ \varepsilon \in \pm\{0,1\}^{l'_e+l_\varnothing+l_{\mathcal{H}}+2}\} \tag{IV.41}$$

Le système à pseudonymes décrit dans (Camenisch & Lysyanskaya, 2001) utilise un schéma de signature différent de celui-ci. Il est cependant tout à fait possible de l'utiliser, ce que nous faisons ici. Dans ce système, l'utilisateur établit un pseudonyme différent avec chaque organisation. Il établit également un secret avec celle-ci afin de prouver la possession de ce pseudonyme. Le secret est en fait un couple fait d'un secret maître que l'utilisateur devra dans certaines circonstances utiliser avec plusieurs organisations, et d'un secret spécifique à chaque organisation. Le pseudonyme est donc un couple $(N_{(U,O)},P_{(U,O)})$ où $N_{(U,O)}$ est l'identifiant du pseudonyme et $P_{(U,O)}$ le moyen de prouver sa possession. $P_{(U,O)}$ est représenté par le secret maître x_U et le secret spécifique $s_{(U,O)}$ en base (R_0,R_1) de la clé publique de l'organisation. L'utilisateur s'authentifie ensuite par une preuve de possession :

$$PK\{(\alpha,\beta) : P_{(U,O)} = R_0^{\alpha} R_1^{\beta}\} \tag{IV.42}$$

Un certificat contient le pseudonyme de l'utilisateur auprès de l'organisation génératrice. Lors des preuves de possession, le consommateur peut demander à l'utilisateur d'établir la preuve que le secret maître est le même dans le pseudonyme du certificat et dans le pseudonyme de l'utilisateur employé auprès du consommateur, et cela sans le révéler. En fait, le certificat contient $P_{(U,O)}$ avec $m_0 = x_U$ et $m_1 = s_{(U,O)}$. Pour prouver que le secret maître est le même au sein de plusieurs certificats et dans le pseudonyme employé auprès de l'organisation consommatrice, il suffit à l'utilisateur de faire une preuve de connaissance en apportant la preuve de l'égalité de logarithmes discrets dans des bases différentes. Ce système repose donc sur le fait que l'utilisateur doit utiliser le même secret maître sur toutes les organisations desquelles un consommateur peut requérir des certificats, avec le fait qu'il soit émis pour une seule et même identité. Le secret maître contribue donc

à lutter contre le partage de certificats étant attendu que deux utilisateurs distincts ne possèdent pas un même secret maître sur deux organisations distinctes. Cela implique un ensemble des secrets maîtres suffisamment grand pour que, sans tricherie, deux utilisateurs ne puissent pas générer un même secret.

Il est ensuite nécessaire de dissuader l'utilisateur de révéler son secret maître à un individu pour qu'il ne puisse pas partager ou céder ses certificats. Camenisch propose deux mécanismes de dissuasion. Ces mécanismes, visant à lutter contre le fait que l'utilisateur puisse révéler son secret maître, permettent de lutter à la fois contre le partage et contre la session de certificats. En effet, pour prouver la possession d'un certificat, la connaissance du secret maître est nécessaire.

La première méthode de dissuasion, nommée « tout-ou-rien »[21], consiste en la publication par les organisations d'une base contenant les pseudonymes associés à tous les certificats émis et qui sont souhaités utilisables dès lors que secret maître est connu. Ainsi, si l'utilisateur révèle son secret maître, il s'expose à la diffusion de tous ses certificats émis par le générateur où ce secret est employé. Cette solution de dissuasion suppose que l'utilisateur accepte de céder son secret maître et non un ensemble de certificats précédemment utilisés. L'implémentation apparaît en outre délicate puisqu'elle nécessite la mise en ligne d'une base de certificats ne révélant rien sur les entités tant que leur secret maître n'est pas connu.

La deuxième méthode de dissuasion est basée sur l'utilisation de clés publiques d'architectures externes. L'autorité de certificats de cette architecture publie les clés privées des utilisateurs chiffrées avec leur secret. Pour que cela ait un sens, il faut que la clé soit d'importance pour inciter les utilisateurs à ne pas révéler le secret maître.

Nativement, les certificats sont utilisables un nombre illimité de fois et cela avec de multiples présentations non-associables. Camenisch propose donc une méthode similaire à celles rencontrées jusqu'ici pour permettre l'usage unique. Il est pour cela introduit un identifiant de certificat dans l'un des attributs, établi conjointement avec le générateur, sans que celui-ci ne l'apprenne. En notant cet identifiant id, voici un exemple de signature le contenant :

$$A \equiv \left(\frac{Z}{R_0^{x_u} R_1^{s_{(U,O)}} R_2^{id} S^v}\right)^{1/e} \; mod \; n \tag{IV.43}$$

Notons que pour deux certificats différents, l'utilisateur ne doit pas utiliser deux fois le même id sur une même organisation. L'utilisateur prouve ensuite au consommateur la validité de ce certificat et il fournit l'identifiant $H_{(U,O)} = h_0^{id}$ de celui-ci qui est le loga-

21. trad. All-or-nothing.

rithme discret de l'identifiant utilisé à la génération avec une base h_0 du générateur (s'il le faisait avec une base du consommateur, l'identifiant du certificat changerait en fonction de celui-ci), et enfin, il doit prouver que l'identifiant dans $H_{(U,O)}$ est le même que dans le certificat. Cela va permettre l'identification par le générateur d'une double dépense de certificat.

Pour permettre une vérification « hors-ligne » ou simplement la sanction d'une double dépense, il est nécessaire de révoquer l'anonymat à la double dépense. Camenisch propose à la place un mécanisme de dissuasion qui consiste à révéler le secret maître. L'utilisateur doit donc également fournir $r = cx_u + s_{(U,O)}$ à chaque présentation de certificat, avec c un challenge du vérifieur, et il doit prouver que r est correctement formé. S'il est détecté qu'un certificat est présenté deux fois, deux r différents pourront être associés et le secret maître révélé :

$$x_u = (r - r')/(c - c') \tag{IV.44}$$

En résumé, l'utilisateur fournit au consommateur A',$H_{(U,O)}$,r et g_0^r et prouve :

$$\begin{aligned} PK\{(\alpha,\beta,\gamma,\varepsilon,\nu) : ZA'^{-2^{l_e+1}} \equiv \pm A'^{\varepsilon} S^{\nu} R_0^{\alpha} R_1^{\beta} R_2^{\gamma} \ mod\ n \ \wedge \ H_{(U,O)} = h_0^{\gamma} \\ \wedge\ g_0^r = (g_0^c)^{\alpha} g_0^{\beta} \ \wedge \ \alpha,\beta,\gamma \in \pm\{0,1\}^{l_m} \ \wedge \ \varepsilon \in \pm\{0,1\}^{l'_e+l_{\varnothing}+l_{\mathcal{H}}+2}\} \end{aligned} \tag{IV.45}$$

La révocation synchrone consistant à révéler x_U constitue une mesure de dissuasion portant sur la valeur de x_U. Il ne s'agit donc ni d'une révocation locale ni d'une révocation globale puisque cette valeur est seulement connue de l'utilisateur et ne peut donc être associée à aucune identité connue. Cette révocation est à coupler avec la mesure de dissuasion du « tout-ou-rien » par exemple.

Étudions maintenant le système de révocation de l'anonymat asynchrone par une autorité de révocation. Celle-ci pourra, à la vue du transcrit résultant de la présentation d'un certificat, révéler, soit le pseudonyme de l'utilisateur sur le générateur au consommateur (révocation locale), soit un identifiant de l'utilisateur sur une autorité possédant l'identité réelle de l'utilisateur (révocation globale). C'est à l'utilisateur et au consommateur de négocier quel type de révocation est employé. Il s'agit donc de prouver au consommateur qu'il lui est bien procuré un moyen de révoquer l'anonymat en cas de litige.

Pour la révocation de l'identité globale, cela revient à fournir une pièce d'identité anonyme d'une première autorité, révocable par une seconde, qui doivent être toutes deux de confiance pour le consommateur. La révocation locale a un sens si le consommateur intègre dans la confiance le fait que le générateur soit en mesure de prendre des mesures contre l'utilisateur en cas de litige entre celui-ci et le consommateur, le tout arbitré par l'autorité qui juge la validité de la demande de révocation.

Pour la révocation globale, chaque utilisateur enregistre sa clé publique $Y_U = g^{x_U}$ auprès de l'autorité possédant l'identité réelle :

$$PK\{(\alpha,\beta) : P_{(U,O)} = R_0^{\alpha} R_1^{\beta} \ \wedge \ Y_U = g^{\alpha}\} \tag{IV.46}$$

L'utilisateur va ensuite fournir au consommateur Y_U chiffré avec la clé publique de l'autorité de révocation et prouver que le secret maître est le même dans Y_U et dans les certificats. Celle-ci possède un groupe $G = \langle g \rangle = \langle h \rangle$ d'ordre q. Elle possède cinq secrets $(x_1,...,x_5) \in_{\mathcal{R}} \mathbb{Z}_q^*$ et publie sa clé publique $(y_1,y_2,y_3) = (g^{x_1}h^{x_2},g^{x_3}h^{x_4},g^{x_5})$. Remarquons que Y_U est encodé avec un de ses *générateurs*. L'utilisateur choisit $r \in_{\mathcal{R}} \mathbb{Z}_q^*$ et calcule $w_1 = g^r$, $w_2 = h^r$, $w_3 = y_3^r Y_U$ et $w_4 = (y_1 y_2^{\mathcal{H}(w_1,w_2,w_3)})^r$. L'utilisateur envoie ensuite $w_{(U,R)} = (w_1,w_2,w_3,w_4)$ et mène les preuves suivantes :

$$\begin{aligned} & PK\{(\alpha,\beta,\gamma,\varepsilon,\nu) : ZA'^{-2^{l_e+1}} \equiv \pm A'^{\varepsilon} S^{\nu} R_0^{\alpha} R_1^{\beta} \ mod \ n \\ \wedge \ w_1 = g^{\gamma} \ \wedge \ w_2 = h^{\gamma} \ \wedge \ w_3 = g^{\alpha} y_3^{\gamma} \ \wedge \ & w_4 = (y_1 y_2^{\mathcal{H}(w_1,w_2,w_3)})^{\gamma} \\ & \wedge \ \alpha,\beta \in \pm\{0,1\}^{l_m} \ \wedge \ \varepsilon \in \pm\{0,1\}^{l'_e+l_{\varnothing}+l_{\mathcal{H}}+2}\} \end{aligned} \tag{IV.47}$$

w_3 apporte au consommateur la preuve que l'utilisateur a bien chiffré sa clé publique Y_U avec la clé publique de l'autorité de révocation. L'autorité de révocation pourra révéler Y_U en opérant $w_3/w_1^{x_5}$.

Pour la révocation de l'identité locale, un identifiant de l'utilisateur sur le générateur est ajouté à son pseudonyme sur le générateur. Cet identifiant est chiffré de la même façon auprès de l'autorité de révocation puis fourni au consommateur. L'utilisateur prouve ensuite que cet identifiant chiffré est bien celui contenu dans le pseudonyme du certificat.

En résumé, le système de Camenisch est le plus complet. Il offre toutes les fonctionnalités des certificats attendues, exception faite de la limitation du nombre d'utilisation des certificats qui ne peut être que celle de l'usage unique. Cependant, à la différence de Brands, les multiples présentations d'un même certificat sont non-associables. Le système de non-transférabilité est le plus intuitif, les certificats sont liés par un secret maître, et le problème de la non-transférabilité est reporté sur celui-ci. Cependant, la difficulté repose dans les mesures de dissuasion employées. Révéler des certificats déjà employés ou le secret maître en cas de double dépense ne nous semblent pas être des mesures de dissuasion intéressantes. Révéler un identifiant pointant vers une identité civile, synonyme de possibilités de sanction, semble être une mesure plus pertinente.

IV.4 Bilan

L'anonymat fort qui résulte des protocoles de génération et de présentation de certificats sans possibilité d'associer les identités a pour conséquence la nécessité de coupler certaines mesures de dissuasion et de révocation de l'anonymat afin de pallier aux problématiques de transférabilité ou de dépassement du nombre de dépenses autorisées.

IV.4.1 Certificats

Rappelons une propriété souhaitée du système à pseudonymes : rendre les multiples présentations d'un même certificat non-associables. Si ces multiples présentations se font sous une même identité auprès d'une même entité, cette propriété n'a pas d'importance. Par contre, elle devient intéressante si celles-ci se font sous des identités différentes sur différents fournisseurs ou si aucune identité n'est établie. L'associativité des multiples présentations, qui impose l'emploi de certificats à usage unique ou leur renouvellement, est l'inconvénient majeur des contributions de Chaum et de Brands. La présentation d'un certificat modifié par Camenisch est une solution élégante et constitue l'avantage majeur de cette contribution.

La contribution de Chaum pour la génération de certificats n'offre pas assez de souplesse dans la gestion des attributs, à la différence des certificats de Brands ou de Camenisch. Les certificats sont pour les deux assez proches, notamment par le fait qu'il soit possible de représenter divers attributs par des logarithmes discrets, et de combiner cela avec des preuves de connaissance à divulgation nulle de connaissance sur les attributs. Cela offre la souplesse adéquate pour ne révéler que l'information souhaitée, c'est-à-dire ne choisir que les attributs que l'on souhaite révéler, et de ne prouver que des propriétés d'attributs si nécessaire.

Selon ces premières constatations, la « CL-Signature » (CL-Signature Scheme) (Camenisch & Lysyanskaya, 2003) pour les protocoles de génération et de vérification de certificats semble un choix pertinent. Cependant, l'architecture de Brands permet les présentations multiples de certificats limités en nombre de dépenses possibles. Néanmoins, le retrait de multiples certificats à usage unique lorsque l'on souhaite limiter le nombre d'utilisation d'un certificat est une méthode pertinente (Par exemple, le certificat limité à dix utilisations prend la forme de dix certificats à usage unique).

La sérialisation des certificats anonymes est délicate et nous reviendrons sur cette problématique au chapitre VIII. Notons cependant dès lors que nous considérons qu'un générateur de certificats publie les attributs qu'il peut fournir, et cela en indiquant à l'aide

de quel *générateur*. Cela permet d'éviter que le choix de *générateurs* pour représenter les attributs puisse être un canal caché entre le générateur et le consommateur. Cela permet également d'assurer au consommateur que l'attribut présenté est celui requis. Cette description, à laquelle s'ajoutent diverses déclarations sur les propriétés des attributs, notamment concernant les preuves, se fait dans des données publiques signées du générateur. Cela permet de déclarer les structures potentielles des certificats. Ainsi, les attributs dans les certificats ne contiennent plus que les valeurs des attributs, et non plus, des couples (nom,valeur) ou des tuples (nom, valeur, type) comme cela se pratique couramment. Le fait que les certificats ne contiennent que les valeurs des attributs apparaît dans un premier temps plus simple à gérer compte tenu du fait que la génération des preuves de propriétés reposent sur des opérations arithmétiques sur les attributs. La valeur numérique exacte de l'attribut est en outre requise pour mener des preuves de propriété. Dans le cas contraire, il n'est pas souhaité que des preuves de propriété soient menées, une valeur de hachage de l'attribut est suffisante pour permettre la présentation sélective. Nous reviendrons sur la structure des certificats et des données publiques des générateurs, couramment appelées *méta-données*, à la section VIII.4.

Les certificats qui ne sont pas limités en nombre d'utilisations doivent être contrôlés par une durée de validité. Celle-ci, si elle est assez courte, pallie à l'impossibilité de maintenir une liste de révocation.

Lorsqu'il est souhaité des certificats limités en nombre d'utilisations, nous avons précédemment indiqué que l'utilisation de certificats à usage unique simplifie la gestion de la problématique. Cela simplifie notamment les protocoles à mettre en œuvre issus de la proposition de Brands. Les certificats à usage unique peuvent avoir une durée de validité ou non, mais cela est fortement conseillé pour traiter la problématique de la révocation. Si durée de validité il y a, il est nécessaire de mettre en œuvre une procédure pour le « réencaissement » du certificat auprès du générateur. En effet, si les certificats représentent de l'argent, il n'est pas concevable que l'argent soit « perdu » au delà des durées de validité.

Les certificats à usage unique posent le problème d'être généralement générés et utilisés « quasiment simultanément », en considérant les temps de propagation à travers le réseau négligeables dans ce cas. Cela pose le problème de la corrélation temporelle de deux événements pouvant conduire à l'associativité des transactions. Dans la mesure du possible, il faudra que l'implémentation permette d'insérer un délai aléatoire entre la génération et la présentation d'un certificat.

La vérification de l'usage unique d'un certificat dès sa présentation semble la solution à privilégier même si la dissuasion semble justifier la possibilité de vérification à poste-

riori. Notons cependant que le mode « en ligne » de vérification auprès des générateurs est soumis à la même réserve concernant la corrélation temporelle de deux événements, et qui permettrait au générateur de suivre l'activité d'un utilisateur.

Le mode « hors ligne » nécessite d'introduire dans le certificat un identifiant de l'utilisateur révélé en cas de fraude et permettant l'application de sanctions (la dissuasion). Cette condition à l'existence du mode « hors-ligne », est également nécessaire pour le mode « en-ligne ». Il est intéressant de noter que l'implémentation d'un outil client de gestion des certificats doit permettre de supprimer un certificat à usage unique dès son emploi afin d'assister l'utilisateur dans la bonne utilisation de ses certificats (mais ce n'est pas un moyen de contrôle).

IV.4.2 Systèmes à pseudonymes

Il est attendu du système à pseudonymes des protocoles de génération de pseudonymes et d'établissement de l'identité sur les organisations. Il est également, et surtout, attendu des solutions pour les problèmes « architecturaux » que sont la révocation de l'anonymat, la non-transférabilité et la gestion du cycle de vie des pseudonymes et des certificats. Camenisch propose plusieurs solutions pour résoudre ces problèmes architecturaux. Il s'agit de la raison pour laquelle il peut être intéressant d'employer ces protocoles. Cependant, ce n'est pas une nécessité pour exploiter les propriétés des certificats, y compris ceux générés à l'aide de la CL-Signature. Une paire de cléfs RSA peut être un type de pseudonymes se justifiant pleinement.

IV.4.3 Révocation de l'anonymat

Nous avons indiqué à la section IV.1 que la révocation synchrone résultait d'une action spécifique, détectable par le système. Cette action se restreint à celles de dépenses de certificats. Ainsi, lors d'une double dépense, ou au-delà d'un nombre déterminé, la « libération » d'un identifiant permet la révocation locale ou globale. La révocation synchrone peut également être ni locale ni globale mais révéler une information liée à un mécanisme de dissuasion. Dans l'architecture de Camesnich, la révocation synchrone de ce type est à coupler avec la mesure de dissuasion du « tout-ou-rien ».

La révocation asynchrone est faite en dehors d'une action de dépense de certificat. Le schéma de révocation de Camenisch met en lumière la faisabilité d'un schéma de signature permettant l'intervention de deux tiers distincts pour la révocation. Cela permet d'assurer que la première est en charge de la révocation, et la seconde, de révéler l'identité. Ce découplage permet de séparer cette responsabilité, nécessité soulignée à la section IV.1.

Cela permet notamment d'éviter le suivi d'activité potentiel par la seconde autorité. Le fait de découpler les responsabilités a également un sens d'un point de vue de la mise en œuvre par des organismes indépendants. Dans le cas d'une architecture appliquée à la vie numérique civile, les révocations de l'identité réelle par l'état civil, et d'un pseudonyme pointant sur cette identité par un organisme affilié à la justice semble être un choix pertinent.

Techniquement, il suffit que l'autorité délivre des certificats à usage unique que l'utilisateur chiffre avec la clé publique de l'autorité de révocation (par exemple avec l'algorithme Cramer-Shoup employé par Camenisch) et qu'il donne au consommateur. Après révocation, le consommateur obtient le certificat qu'il peut échanger auprès de l'autorité pour obtenir l'identité réelle. Ainsi, avec l'exemple de Cramer-Shoup, l'utilisateur enregistre une clé publique auprès de l'état civil. Cette clé publique est formée à partir du secret maître de l'utilisateur. L'utilisateur n'obtient de certificats de l'état civil que s'il prouve que le secret maître est bien le même dans la clé publique et dans le certificat (équation IV.46). Dans l'équation IV.47, w_3 permet au consommateur de vérifier que l'utilisateur a bien chiffré sa clé publique avec la clé publique de l'autorité de révocation.

Notons au passage que le fait de présenter un tel certificat peut permettre de se passer, dans certains cas, de la révocation de l'anonymat synchrone liée à la dépense multiple. En effet, cela peut permettre d'utiliser des certificats cessibles qui ne contiennent aucune information d'identité. Cela n'empêche pas la détection de la sur-dépense. Ainsi, la responsabilité engagée est celle du porteur de certificat, et non celle de l'entité pour qui le certificat a été généré. Cela permet par ailleurs l'obtention de certificats par des organisations qui ne gèrent pas les identités, qui ne font que faire de l'échange de certificats, argent contre timbre par exemple. Comme nous l'avions soulevé, la cession de certificats est problématique du fait que le cédant reste en possession du certificat. Si l'on souhaite implémenter ce mécanisme, il est nécessaire d'y ajouter la notion de certificat attestant de la cession permettant d'attribuer la responsabilité.

IV.4.4 Non-transférabilité

Placer une clé nécessaire à prouver chacun des certificats et faire reposer dessus le poids de la non-transférabilité est une solution intuitive mais qui doit être employée avec soin. En effet, il faut aider l'utilisateur à protéger ce secret, permettre sa révocation et son renouvellement.

Comme nous l'avions souligné à la section IV.1.3.2, il est nécessaire de s'appuyer à la fois sur la technologie et sur la dissuasion pour éviter la cession. L'utilisation d'une plateforme

de confiance semble nécessaire pour aider l'utilisateur à protéger son secret. Cependant, cela ne garantit pas le fait que le secret ne soit pas cédé. Aujourd'hui, il est admis que lors de l'utilisation d'une carte bancaire, c'est un périphérique qui est authentifié, et que l'utilisateur est responsable du périphérique ainsi que de l'utilisation qui en est faite tant qu'il ne déclare pas sa perte. Cela est d'autant plus simple que son utilisation est synonyme d'une dépense. Qu'en est-il si une plateforme de confiance est employée comme support de la carte nationale d'identité ? Peut-on faire cette même considération, donc accepter que toutes les utilisations d'une carte d'identité soient la responsabilité de l'identité désignée par celle-ci ?

Il semble nécessaire en premier lieu de renforcer l'idée de l'emploi d'une plateforme de confiance avec des contrôles biométriques, rendant la cession plus difficile, mais également de dissuader celle-ci. La dissuasion ne permet pas d'empêcher un acte frauduleux, elle agit cependant directement sur le comportement. Autrement dit, il est possible de dissuader l'utilisateur de tricher même si aucune barrière technique ne l'en empêche. Si l'on opte pour une solution technique sans dissuasion, une fois la barrière technique franchie, l'utilisateur souhaitant tricher le fera. Si l'on opte pour une solution purement dissuasive, l'utilisateur peut être involontairement fautif. Il est donc nécessaire de combiner les mécanismes techniques et de dissuasion. Une plateforme de confiance pourra permettre une cession difficile du secret, et aura également l'avantage d'aider l'utilisateur à ne pas commettre involontairement une faute. Nous reviendrons sur l'utilisation de supports physiques à la section VIII.5.1.

Mettre un poids fort sur le secret consiste à rendre la possession de celui-ci synonyme de quelque chose de valeur (sanction pénale, somme d'argent, diffamation, etc.). Autrement dit, l'idée est qu'un utilisateur redoute une perte de valeur s'il venait à le révéler. Il faudra cependant prendre garde au fait que le poids sur le secret ne dissuade pas l'utilisateur d'une utilisation courante du système. L'idée de la dissuasion revient donc en quelque sorte à mettre quelque chose en gage et de conditionner l'accès à celui-ci par la connaissance du secret cible de la dissuasion[22].

L'approche du « tout-ou-rien » de Camenisch (Camenisch & Lysyanskaya, 2001) consiste à mettre en gage l'accès à tous les certificats déjà générés sur les générateurs où le secret est employé. Cela semble intéressant lorsque de multiples certificats sont demandés par un consommateur puisque cela impose d'avoir un même secret sur plusieurs générateurs, donc cela augmente la valeur du secret. Notons au passage que les générateurs doivent publier tous les identifiants de pseudonymes, et pour ceux-ci les signatures des certificats déjà

22. La « prise d'otage » est une métaphore qui semble fantaisiste au premier abord mais qui s'avère d'une pédagogie redoutable.

générés. Le second secret valable localement sur un générateur assure que la connaissance du secret maître ne suffise pas à obtenir un certificat sur le générateur. De même pour pouvoir le présenter. Il est donc également nécessaire que celui-ci soit connu sur chaque générateur pour que le « tout-ou-rien » représente une menace. Or, s'il est connu, ainsi que le secret maître, cela est synonyme de la possibilité d'obtenir l'accès sur le générateur, donc d'obtenir et de présenter n'importe quel certificat de celui-ci. Nous pensons donc que le « tout-ou-rien » ne représente pas une mesure de dissuasion intéressante.

La mesure de dissuasion « classique », nommée « basée sur la PKI »[23], fut introduite par (Dwork *et al.*, 1996). Il s'agit de mettre en gage un secret relatif à une architecture à clé publique tierce. Soit cette clé révèle en elle-même une information, soit elle est synonyme de droits d'accès. Dans ce dernier cas, l'idée est de dissuader l'usager du fait que la cession de son secret maître offre un moyen d'usurpation de son identité pour des accès importants. Or, cela va à l'encontre des objectifs initiaux de cette architecture, et fait peser un poids considérable sur le secret maître. Rappelons qu'il est souhaité prévenir l'usurpation d'identité ou la cession de droits d'accès. Il n'est donc pas envisageable d'utiliser ces problématiques comme mesures de dissuasion. En d'autres termes, il ne peut s'agir en aucun cas de mettre une identité en gage. Comment, même si l'acte de cession est volontaire, imposer juridiquement les conséquences des actes d'un tiers faits sous cette identité, notamment lorsque le risque de perte d'un secret est existant ? Il est en outre fort probable qu'il ne soit juridiquement pas acceptable de mettre en gage des accès.

Les solutions de dissuasion semblent donc nécessaires mais délicates à mettre en œuvre. Celles présentées jusqu'ici ne sont pas convaincantes du fait du manque de réalisme du gage. Le gage doit avoir de la valeur mais ne doit pas dissuader l'utilisateur d'utiliser le système, ni aller à l'encontre des principes de respect de la vie privée que cette architecture ambitionne. Il est donc nécessaire de pousser la réflexion quant à la notion de gage afin d'y introduire des notions réalistes. Rappelons en quelque sorte les règles du jeu de la cession et du prêt de certificats. Concernant la mise en commun de certificats, l'enjeu est l'obtention d'un accès qui n'aurait pas été obtenu avec les certificats de chacun. Lors de la cession de certificats, le gain peut être extérieur, une rétribution financière par exemple. Supposons donc que la cession du secret maître soit synonyme d'un gain pour l'utilisateur. L'idée du gage conditionné par le secret à protéger est donc que sa valeur soit supérieure à celle du gain. La difficulté est que parfois il n'y a pas réellement de gain, la cession peut être faite au profit d'un destinataire pour rendre un service par exemple. La valeur du gage est alors mise en balance avec la confiance. Il est alors utile de savoir si la confiance peut « s'acheter », c'est-à-dire s'il existe un seuil de valeur du gage à partir duquel la confiance n'a plus cours. Enfin, la notion de valeur est à mettre en correspondance avec ce que les

23. trad. PKI-based.

fournisseurs de services ont à perdre et la force de dissuasion du gage envers l'utilisation du système. Pour conclure, dans un premier temps, il semble judicieux de s'appuyer sur la détection de fraude qui peut être faite en dehors du système, la révocation de l'anonymat et la dissuasion par des sanctions judiciaires si le préjudice est avéré.

IV.4.5 Recouvrement et portabilité

Les pseudonymes, le secret maître et les certificats sont tous concernés par la portabilité et le recouvrement. La solution de l'utilisation d'une plateforme de confiance « duplicable » de manière sécurisée par l'utilisateur qui pourrait ainsi conserver le duplicata semble réaliste. Il est cependant également possible d'envisager un dépôt en ligne. Par exemple en chiffrant les données et en les répartissant dans deux dépôts indépendants de manière à ce qu'aucune donnée ne soit intelligible sans le « ré-assemblage » de celles-ci puis leur déchiffrement.

IV.4.6 Conclusion

Ce chapitre nous a permis d'illustrer les techniques cryptographiques répondant aux trois fonctionnalités des certificats suivantes :

- la non-associativité entre génération et présentation,
- la présentation sélective d'attributs,
- les preuves de possession et sur des propriétés d'attributs.

Nous avons également justifié l'emploi de pseudonymes indistinguables pour l'établissement d'identité pour permettre la non-associativité des identités. Nous avons ensuite relevé et étudié l'une des problématiques majeures de la gestion des identités qu'est la non-transférabilité des secrets. Nous avons enfin précisé la notion de dissuasion au regard des moyens technologiques de prévention du partage et de la cession des certificats.

IV.5 Mise en œuvre

Le schéma de signature CL-Signature a fait l'objet d'une implémentation en langage de programmation C. La librairie est disponible à l'adresse: *http://magnum.telecom-st-etienne.fr*.

IV.5.1 Librairie

Les deux composantes majeures de cette librairie sont l'implémentation du schéma de signature CL-Signature et des preuves de connaissance par le protocole de Shnorr.

L'implémentation du schéma de signature comprend les fonctionnalités :

- de génération des paramètres cryptographiques (clsig_gen.c),
- de signature (clsig_sign.c),
- de vérification de signature (clsig_vrf.c),
- de fonction d'aide à la représentation des messages (clsig_utl.c).

L'implémentation du protocole de Shnorr comprend les fonctionnalités :

- de preuves de connaissances (shnorr_pok_dlrep.c),
- de preuves de connaissances avancées telles que permettant de prouver l'égalité de deux logarithmes discrets (shnorr_pok_dlrep_advanced.c),

IV.5.2 Notes d'implémentation

IV.5.2.1 API OpenSSL

L'implémentation repose principalement sur la librairie mathématique d'OpenSSL[24], notamment concernant l'arithmétique modulaire (exponentiation, inversion, etc...).

Les fonctions *BN_generate_prime_ex()* et *BN_is_prime_ex()* sont employées pour la génération de nombres premiers

IV.5.2.2 Génération de résidus quadratiques

Le nombre premier p' est généré par les fonctions d'OpenSSL, puis il est testé si $p = 2p' + 1$ est un nombre premier. Si tel est cas, p est un premier sûre. q est généré de la même manière.

24. www.openssl.org

Le groupe multiplicatif $\mathbb{Z}_n^*$, avec $n = pq$ est d'ordre $\varphi(n) = \varphi(pq) = (p-1)(q-1)$. Nous recherchons des résidus quadratiques modulo n de ce groupe, soient des éléments du groupe QR_n. Les éléments de QR_n sont des éléments de QR_p et QR_q.

Nous commençons par rechercher un générateur α_p de $\mathbb{Z}_p^*$. Or $\alpha_p \in \mathbb{Z}_p^*$ est un générateur de $\mathbb{Z}_p^*$ si et seulement si $\alpha_p^{\frac{\varphi(p)}{p_i}} \not\equiv 1 \ (mod\ n)$ avec p_i les facteurs premiers de $\varphi(p)$. Or $p = 2p' + 1$ et $\varphi(p) = p - 1$ car p est premier, les facteurs premiers de $\varphi(p)$ sont donc p' et 2. Il est recherché un générateur de $\mathbb{Z}_p^*$ de la même manière.

Une des propriétés d'un générateur est $\mathbb{Z}_p^* = \{\alpha_p^i \ mod\ p \mid 0!i!\varphi(p) - 1\}$ et $a \in \mathbb{Z}_p^*$ est un résidu quadratique modulo p si et seulement si $a = \alpha_p^i mod\ p$ avec i paire. Nous obtenons donc, en prenant les puissance de deux d'un générateur, des résidus quadratiques appartenant à ce groupe. Notons qu'un élément sur deux de $\mathbb{Z}_p^*$ est dans QR_p. L'ordre de QR_p est donc $(p-1)/2$.

Il nous faut désormais déterminer des résidus quadratiques appartenant à $\mathbb{Z}_p^*$ et $\mathbb{Z}_q^*$. Nous employons pour cela le théorème des restes chinois (CRT) permettant de résoudre le système d'équation suivant:

$$\begin{aligned} x &\equiv \alpha_p^i \ mod\ p \\ x &\equiv \alpha_q^j \ mod\ q \end{aligned} \tag{IV.48}$$

Quelque soit (i,j) un couple d'entiers paires. La solution de ce système est donné par $x_{(i,j)} = \alpha_p^i * q * (1/q \ mod\ p) + \alpha_q^i * p * (1/p \ mod\ q) \ \ mod\ n$. Cette formule nous permet de générer des éléments de QR_n. Notons que les éléments devant appartenir à QR_p et QR_q, l'ordre de QR_n est $\frac{(p-1)(q-1)}{4}$. Or, $\varphi(n) = (p-1)(q-1) = 4p'q'$, l'ordre de QR_n est $p'q'$.

IV.5.2.3 Génération des paramètres RSA

Camenisch requière un exposant premier bien que cela ne soit pas obligatoire. Cela accélère cependant le test permettant de déterminer si e et $\varphi(n)$ sont co-premiers.

Pour un exposant quelconque, il suffit de tester que $coprime(e,\varphi(n))$ donc que $coprime(e,(p-1)(q-1))$. Ce qui revient à tester $coprime(e,(q-1))$ et $coprime(e,(p-1))$ plus efficace en espace.

Si e est premier, il suffit de tester que $(p \ mod\ e) \neq 1$ et $(q \ mod\ e) \neq 1$.

IV.5.2.4 Exponentiation RSA

Lors de la signature, nous nous contentons de faire une simple exponentiation. Il peut cependant être intéressant d'employer l'algorithme des restes chinois qui permet un calcul plus efficace. La clé secrète n'est alors plus d mais les éléments $dmp = d \ mod \ p$, $dmq = d \ mod \ q$ et $iqmp = 1/q \ mod \ p$ avec $p > q$.

Il peut tout de même être intéressant de générer ces paramètres qui permettent de renseigner l'ensemble des variables membres de la structure *RSA* de l'API OpenSSL ce qui permet notamment d'employer la fonction de test de l'API *RSA_check_key()*.

IV.5.3 Résultats

L'implémentation permet à ce jour de mener des preuves de possession d'une signature, de faire de la présentation sélective de contenu et de générer des certificats valables un nombre de fois limité avant de révéler un identifiant (révocation globale/locale synchrone). Il est également possible de prouver l'égalité de deux attributs contenus dans deux certificats différents. Les preuves sur les propriétés des attributs ne sont pas encore assez efficaces pour être mentionnées comme fonctionnelles.

CHAPITRE V

Négociation, Identité & Confidentialité

*Le **chapitre 5** précise les notions de connaissance et de reconnaissance d'un tiers, d'identité connue publiquement et de confiance acquise en dehors du système de négociation. La notion d'anonymat est discutée à la vue de ces concepts. L'apport des travaux du chapitre précédent permet notamment de discuter plusieurs considérations pratiques sur l'emploi de pseudonymes qu'il est possible d'envisager entre deux interlocuteurs. La confidentialité des échanges basée sur le pseudonyme employé comme clé publique permettant l'échange du secret de confidentialité est ensuite étudiée. Nous justifions la certification de la clé publique dans chacun des certificats, par une signature à l'aveugle si la non-associativité est requise. Il est alors justifié le concept de confiance croissante dans la confidentialité du canal de communication. Le pseudonyme étant une information sensible, il est supposé renouvelable d'un pseudonyme à usage unique vers un pseudonyme déjà employé. Cette étude est illustrée à l'aide du protocole TLS.*

Sommaire

“Le rêve est une seconde vie.”

Gérard de Nerval.

V.1 Identité et négociation

En première partie, nous avons mis en lumière le fait que l'association des identités numériques et des activités d'une entité pouvaient représenter une menace pesant sur sa vie privée. Au chapitre précédent, une architecture d'échange de certificats, permettant la non-associativité des identités lors de leur établissement par des pseudonymes ainsi que par des certificats dont la génération et les multiples présentations sont non-associables, a été présentée. Nous nous intéressons dans cette section à l'opportunité que la non-associativité des transactions offre pour les négociations. En outre, l'un des enjeux majeurs des négociations de confiance dans un environnement ouvert est l'établissement d'une relation de confiance avec un inconnu. Il est donc important de préciser ce qui est entendu par « inconnu » au regard des notions d'identité réelle et des statuts d'anonymat ou de « pseudonymat ». Nous nous intéressons notamment aux liens qui existent entre l'identité des interlocuteurs, leurs pseudonymes, l'établissement de canaux de communication sécurisés et la négociation. Pour cela, nous apportons une attention toute particulière à reprendre le sens des notions d'établissement d'une identité dans une communication. Nous essayons de replacer dans le contexte d'une communication, puis de la négociation, les conditions qui permettent de préserver l'anonymat au sens de la non-associativité et ce, en rappelant les contraintes intrinsèques de l'adressage d'une entité.

Lorsque l'initiateur débute une négociation avec un fournisseur, s'il possède une connaissance préalable de celui-ci, la négociation peut être différente d'une négociation avec un fournisseur inconnu, du fait qu'il puisse déjà lui accorder une certaine confiance. Il s'agit en quelque sorte d'une « confiance pré-existante ». Cette connaissance peut être issue de précédentes négociations, d'un système de réputation, ou d'une expérience passée dans le monde physique (par la publicité ou par le bouche à oreille par exemple). Si l'interlocuteur est reconnu par un pseudonyme prouvé et que ce pseudonyme est employé comme clé publique servant à l'échange d'un secret, il n'y a pas de difficultés particulières ni pour son autorisation si l'identité établie possède déjà les droits requis, ni pour établir un canal de négociation confidentiel. Par contre, si le pseudonyme est inconnu et la confiance pré-existante apportée par une expérience dans le monde physique, nous verrons que cela soulève diverses difficultés pour établir l'identité de ce tiers. Enfin, nous souhaitons traiter le cas où l'initiateur et le fournisseur sont totalement inconnus, cas pour lequel la confiance n'est établie qu'à partir des certificats présentés au cours d'une unique négociation. Nous verrons notamment ce que cela signifie pour l'établissement d'un canal de négociation confidentiel.

Rappelons en préambule les propriétés fondamentales issues du précédent chapitre. De multiples négociations d'une entité, avec une ou plusieurs entités, avec potentiellement

de multiples utilisations d'un même certificat, peuvent être non-associables si l'établissement d'une identité n'est pas requis. Si un établissement d'identité est requis, cela est supposé au travers d'un pseudonyme dédié indistinguable rendant ainsi les multiples identités d'une même entité non-associables par les pseudonymes et la signature des certificats. Une entité est ainsi anonyme au sens de la non-associativité de ses multiples négociations et identités.

V.1.1 Identité réelle et alias

Une expérience dans le monde physique (une campagne publicitaire par exemple) peut être source de confiance et il est possible de considérer que cette confiance est associée à un alias de l'entité sujet de l'expérience. Un alias est un identifiant relatif à l'identité réelle d'une entité, et une entité peut être connue par différents alias. Les alias se différencient des pseudonymes du fait que de multiples alias sont associables par les facultés intellectuelles d'un humain. A l'inverse, il est attendu qu'un pseudonyme soit un identifiant qu'il ne soit pas possible de lier à une identité réelle (Pfitzmann & Kohntopp, 2001), aussi bien par un humain que par une machine. Dans le monde numérique, il est également d'usage de décliner l'identité d'une entité à travers un alias, citons l'attribut DN d'un certificat X509 par exemple (Housley *et al.*, 1999). Ainsi, à travers les alias, il est possible qu'une entité connue dans le monde physique puisse être « reconnue » dans le monde numérique. Une organisation peut par exemple mener une campagne de publicité sous l'alias « OrgaXYZ », et présenter un certificat contenant l'alias « XYZ SARL ». L'organisation peut ainsi bénéficier par l'association de ces deux alias d'un certain niveau de confiance dans le monde numérique acquis lors d'une expérience dans le monde physique.

La cryptographie à clé publique fut introduite par (Diffie & Hellman, 1976b), ainsi que le concept d'association d'un alias[1] à une clé publique pour prouver une identité réelle. Les certificats à clés publiques (Kohnfelder, 1978) permettant de telles associations sont désormais couramment employés dans le monde numérique pour prouver une identité relative à une identité réelle. Les certificats à clés publiques sont signés de tiers de confiance, appelés autorités de certification (dès lors AC), qui sont les garants de cette association. Les AC ont donc deux rôles principaux pour lesquels la confiance leur est accordée :

- authentifier l'identité réelle d'une entité,
- délivrer des certificats dont les alias qu'ils contiennent ne portent pas à confusion sur l'identité réelle qu'ils désignent.

Nous avons déjà abordé la difficulté de réaliser le premier point. Le second est sûrement encore plus difficile. En effet, comme nous l'avons souligné, un alias est significatif dans

1. Aussi appelé nom.

un procédé d'interprétation par l'humain, sujet à défaillir. Deux organisations peuvent se voir délivrer des certificats avec des alias proches qui peuvent induire un individu en erreur. Les AC auraient donc la charge de vérifier, d'une part, que l'alias délivré est cohérent avec une dénomination publique d'une entité, mais également, que celui-ci ne porte à confusion avec aucun autre alias délivré à une autre entité. La multiplicité des AC dans un environnement ouvert, ainsi que de multiples entités pouvant se voir délivrer un certificat, semblent s'opposer à la faisabilité d'une telle tâche. Qui plus est, une AC aux procédures rigoureuses peut mener un tel procédé. Cependant, il suffit que n'importe quelle autre AC de confiance ne soit pas aussi rigoureuse pour qu'il existe une faille. Nous reviendrons sur le fait que cette architecture ait été pensée avec l'idée que les AC soient de confiance pour les consommateurs de leurs certificats.

Comme cela est souligné dans (Ellison *et al.*, 1999), espérer une telle architecture avait du sens au moment de sa publication. Mais dans un environnement ouvert tel que le Web, cela ne semble plus être le cas. L'emploi d'alias uniques et significatifs peut être considéré à une échelle locale, dans un espace de noms restreint, mais pas à une échelle globale. Une solution technique qui viserait une base de données globale des alias ne semble donc pas réalisable compte tenu des multiples entités qui ont des dénominations similaires. En outre, cela ne lève pas l'incertitude quant à l'association par l'humain d'un alias avec une entité connue.

Même si l'on considère que l'évolution du monde numérique pousse vers un nombre croissant de contacts initiés au sein du monde numérique, qu'une réputation, source de confiance, puisse être établie sur des pseudonymes ne portant donc pas à confusion, et que les alias soient propices aux erreurs, il est impossible de penser une architecture sans prendre en compte le concept de l'identité réelle déclinée par des alias. La consommation dans le monde physique existera toujours, et cette source de confiance pour les interactions dans le monde numérique doit être prise en compte. Il est donc nécessaire d'y apporter un soin particulier. Les travaux de cette thèse n'iront pas plus avant sur cette problématique, citons simplement que des travaux tels que (Zimmermann, 1995 ; Ellison *et al.*, 1999) peuvent y contribuer. L'utilisation d'alias dans le monde numérique est donc un challenge dont nous sommes conscients. Nous considérerons cependant pour le restant de ces travaux, en tenant compte des remarques précédentes, qu'un certificat à clé publique sera employé pour associer un alias à un pseudonyme afin d'apporter de la confiance, acquise en dehors du système de négociation, envers l'entité qui présente ce pseudonyme.

Ainsi, si les contacts sont menés dans le monde numérique avec une entité qui ne bénéficie d'aucune confiance pré-existante avec son interlocuteur acquise en dehors du système de négociations, aucun alias n'est requis. Le système de négociation inclut toutes les transac-

tions qu'il est possible de mener avec des identités déclinées par des pseudonymes auxquels peuvent être associés des historiques de négociation, de la confiance et de la réputation. Il est par exemple possible de considérer qu'un système de réputation soit basé sur les alias, ce qui justifierait leur emploi, ou sur les pseudonymes, ce qui supposerait le contraire. Outre la certification d'un alias, les certificats à clés publiques ont été utilisés parce qu'ils offraient une solution à la gestion des clés par la certification de celles-ci. Il s'agit du second rôle qui leur est donné et sur lequel nous revenons en détail dans la suite de cette section.

Pour conclure, en considérant une architecture de négociation globale, toute la confiance peut être bâtie autour des pseudonymes et leur être associée. Les certificats à clés publiques certifiant un alias peuvent être employés pour importer dans le système de négociation de la confiance acquise en dehors mais ceci est un procédé faillible. Un pseudonyme n'est lui pas soumis à l'interprétation humaine, donc uniquement soumis à des considérations techniques (taille de l'espace des clés et algorithmes cryptographiques). Prouver la possession d'un pseudonyme est le moyen de bénéficier d'un capital de confiance précédemment acquis dans le monde numérique. Un pseudonyme peut ainsi être utilisé de manière répétée, avec un même interlocuteur si la confiance n'est souhaitée être bâtie qu'avec celui-ci, ou avec plusieurs interlocuteurs si la confiance est souhaitée avoir une dimension publique, c'est-à-dire faisant l'objet d'échanges entre plusieurs entités (à l'aide de systèmes de réputation par exemple). Lorsqu'un pseudonyme est employé avec plusieurs interlocuteurs, nous appelons celui-ci « pseudonyme public » ou « pseudonyme de groupe », que nous différencions ainsi du pseudonyme dédié indistinguable nécessaire à la non-associativité. Respectivement, nous appelons ces deux états le « pseudonymat public » et le « pseudonymat ». Nous introduisons également le terme « domaine de réputation » comme l'ensemble des entités auprès duquel un pseudonyme est employé. Un pseudonyme dédié permet de maintenir une relation de confiance pour de multiples négociations avec un même interlocuteur. Le domaine de réputation d'un tel pseudonyme est donc restreint à une unique entité.

V.1.2 Anonymat et pseudonymat

A la section II.1.4, nous avions introduit la définition de l'anonymat (Pfitzmann & Kohntopp, 2001) comme le fait qu'un sujet ne soit pas distinguable des autres sujets dans un ensemble de sujets appelés l'ensemble d'anonymat. Nous avions également précisé que l'anonymat dépendait, en ce sens, de l'observateur de l'ensemble d'anonymat. Nous considérons dans cette section que toutes les communications liées à la négociation sont indistinguables du point de vue d'un observateur extérieur au système de négociation[2].

2. trad. Outsiders.

Cela suppose par exemple l'emploi de réseaux d'anonymat s'appuyant sur le « routage en oignon[3] ». Le but est de se focaliser sur le point de vue des acteurs du système de négociation[4].

Conduire une négociation anonymement, c'est-à-dire non-associable à aucune autre, est faisable à l'aide des certificats anonymes. Cela suppose qu'aucun pseudonyme connu n'est établi (aucune gestion de compte n'est souhaitée) et qu'il n'est donc pas souhaité bénéficier d'une confiance acquise par de multiples négociations. Une question intéressante est donc de savoir s'il est possible que deux parties puissent mener une négociation anonymement au sens de la non-associativité. Pour répondre à cette question, il est nécessaire de considérer la problématique de l'adressage du fournisseur. Un initiateur a besoin de connaître l'adresse d'un fournisseur susceptible de lui fournir l'objet qu'il requiert[5]. Or, si l'adressage est synonyme d'une adresse fixe, cela signifie un facteur d'association, donc que dans ces conditions le fournisseur ne peut être anonyme. Il est par conséquent nécessaire de supposer un mécanisme permettant de servir des adresses de fournisseurs en fonction d'un objet. Ces adresses seraient différentes et indistinguables à chaque négociation, ceci avec un même fournisseur, rendant ainsi possible le fait qu'un initiateur puisse conduire de multiples négociations avec un même fournisseur, sans qu'il ait de moyens de se rendre compte qu'il s'agisse d'un même fournisseur. Il est possible de supposer qu'un tel mécanisme existe sans en spécifier les pré-requis. Cette hypothèse, d'un mécanisme servant des adresses indistinguables pour les fournisseurs, est requise pour faire celle de deux parties pouvant négocier anonymement au sens de la non-associativité des négociations. Dans l'environnement ouvert qu'est le Web, la mise en œuvre de tels mécanismes apparaît complexe. Il est cependant intéressant d'étudier ce cas puisque d'autres environnements y semblent propices, notamment les environnements pervasifs et ubiquitaires. En outre, nous supposons l'adresse de l'initiateur comme un facteur non-associable compte-tenu de l'hypothèse de communications au travers d'un réseau d'anonymat.

Le pseudonymat permet de maintenir la confiance acquise pour de multiples négociations avec un même interlocuteur. Le pseudonymat suppose que l'entité qui l'emploie puisse établir l'identité de son interlocuteur afin de pouvoir établir le pseudonyme qui est dédié à celui-ci. Nous en déduisons qu'il n'est pas possible qu'une partie utilise le pseudonymat si l'autre partie est anonyme. Est-il alors possible que deux parties puissent être sous pseudonymat, en considérant que l'adresse du fournisseur puisse être fournie par le mécanisme précédent ? Pour établir un pseudonyme, il est nécessaire d'établir l'identité de l'interlocuteur qui lui aussi nécessite d'établir l'identité de son interlocuteur. Cela consti-

3. Le réseau TOR par exemple.
4. trad. Insiders.
5. En considérant l'adresse comme un point terminal applicatif (trad. Applicative endpoint) incluant l'adresse réseau.

tue donc une contradiction. L'une des parties pourrait s'appuyer sur un facteur extérieur pour supposer un pseudonyme. Cependant, cela signifierait un facteur permettant l'associativité et cela rendrait le pseudonymat employé pour la non-associativité obsolète. Il est donc possible de conclure qu'un pseudonymat n'est possible que face à un pseudonymat public établi en premier. Notons que le pseudonymat est indépendant du fait qu'un alias soit présenté. En revanche, en considérant les alias comme des facteurs d'association, le pseudonymat semble inutile lorsqu'un alias est présenté.

Les certificats anonymes sont employés pour la non-associativité des transactions de génération et de présentation. Les utiliser, sous pseudonymat si l'établissement d'une identité est requis, permet des négociations non-associables. En conséquence, la propriété de non-associativité des certificats anonymes est utile sous couvert de l'anonymat ou du pseudonymat. Cependant, il est possible qu'un fournisseur utilise un pseudonymat public auprès d'initiateurs, lui permettant par la même de bâtir son domaine de réputation, et un pseudonymat « dédié » avec ses générateurs afin de bénéficier de la propriété de non-associativité des certificats. Notons que même avec un pseudonymat public, le porteur peut bénéficier des autres propriétés des certificats anonymes que sont la présentation sélective et les preuves de connaissance.

V.2 Pseudonymat et Confidentialité

V.2.1 Confidentialité avec un inconnu

Il est convenu que les négociations devraient être conduites de manière confidentielle. Ainsi, il est attendu qu'une négociation ne soit intelligible que pour les deux interlocuteurs de la négociation, ce qu'il est coutume d'appeler un « canal de communication sécurisé ». Il est couramment entendu par « canal de communication sécurisé » l'authentification des points terminaux et l'échange d'un secret leur permettant de chiffrer les communications. Cependant, cela n'a plus court lorsqu'il s'agit d'échanger de manière confidentielle avec un tiers inconnu, impliquant l'impossibilité d'authentifier un tiers connu. Il est pourtant souhaité rendre confidentiels les échanges des règlements, des attributs et les objets de négociation, face aux observateurs extérieurs[6]. Ainsi, ce qui devrait être compris et réalisé pour les négociations de confiance est que la confidentialité est attendue pour un interlocuteur possesseur de certificats, quel qu'il soit puisqu'il pourrait être inconnu.

Si l'on considère qu'un pseudonyme est une clé publique qu'il est possible de prouver à l'aide d'une clé privée, et en supposant un crypto-système asymétrique où il est possible de chiffrer avec une clé publique, connaître un pseudonyme signifie la possibilité d'envoyer un secret à son possesseur. En supposant que la négociation débute par la fourniture d'un pseudonyme, celui-ci sera utilisé pour envoyer un secret employé pour un chiffrement symétrique des échanges de la négociation. Assurer la confidentialité de la négociation est donc trivial si le pseudonyme établi est déjà connu. Cela signifie simplement vérifier la possession du pseudonyme. La difficulté existe donc si le pseudonyme est inconnu, soit parce que les parties négociatrices n'ont jamais négocié ensemble, soit parce que les deux parties ont souhaité rester anonymes.

(Kohnfelder, 1978) établit qu'il est évident que l'échange direct de clés entre interlocuteurs est la meilleure solution en terme de gestion des échanges de clés, et que si cela n'est pas possible il est nécessaire de s'appuyer sur des tiers de confiance. L'échange direct de clés signifie l'emploi d'un moyen d'échange qui permet d'avoir la certitude que les clés détenues sont celles des entités avec lesquelles on souhaite échanger, or, la notion d'échange direct n'existe dans l'environnement ouvert de notre étude que pour l'ensemble réduit de générateurs que sont les tiers de confiance initiaux. Il est donc nécessaire de s'appuyer sur ces tiers de confiance, dont on possède déjà les clés supposées obtenues de manière sûre, pour découvrir les autres clés de nouveaux tiers de confiance et des interlocuteurs de négociation.

6. Qui pourraient être les nœuds du réseau utilisé pour l'anonymisation des communications.

En considérant que les deux parties de la négociation soient inconnues, la menace n'est évidemment pas l'usurpation de l'identité d'un des interlocuteurs. En d'autres termes, l'autorisation est basée sur les certificats présentés et non sur pas sur l'identité du porteur. En supposant que la possession de chaque certificat est prouvée de manière sûre, le but d'un attaquant se réduit à connaître le secret assurant la confidentialité. En supposant ensuite que les pseudonymes employés servent de clé publique pour l'échange du secret et que ce dernier ne peut être appris sans la connaissance de la clé privée associée, l'attaquant doit substituer le pseudonyme employé pour l'échange du secret par un pseudonyme dont il connaît la clé privée. Cette attaque est connue sous le nom d'interception ou d'attaque par l'« homme du milieu »[7]. Il est donc nécessaire de s'appuyer sur les tiers de confiance pour assurer l'intégrité des pseudonymes, c'est-à-dire pour les certifier, ce que (Kohnfelder, 1978) concrétisa par le certificat à clé publique d'après les travaux de (Diffie & Hellman, 1976b).

En résumé, ce qui est attendu est que le secret employé pour le chiffrement soit échangé au travers d'un pseudonyme employé comme clé publique signée de tiers de confiance, et que le pseudonyme employé pour échanger le secret soit celui du possesseur des certificats. Nous en déduisons que le pseudonyme doit être prouvé comme appartenant au possesseur des certificats ce qui nécessite de lier le pseudonyme aux certificats. Autrement dit, le pseudonyme devrait être certifié dans les certificats utilisés pour établir la confiance dans l'interlocuteur. Les générateurs de certificats se voient donc attribuer le rôle de la certification du pseudonyme jusque-là attribué aux autorités de certification des architectures à clés publiques. Autrement dit, lors d'une négociation entre tiers inconnus, si la clé publique employée pour la confidentialité n'est pas contenue dans les certificats sur lesquels s'établit la relation, il est possible que la confidentialité ne soit pas assurée avec le porteur des certificats.

Nous avons ici dissocié les deux rôles usuels de l'autorité de certification à savoir l'association d'un alias à une clé publique et la certification d'une clé publique. Comme nous l'avions évoqué, le premier rôle peut toujours être assuré par des AC afin d'apporter de la confiance « provenant de l'extérieur », le second rôle pouvant désormais être assuré par tout générateur de certificats. De plus, assigner ce rôle aux générateurs est pertinent avec le fait que les tiers de confiance assurant la certification de la clé publique doivent appartenir au domaine de confiance du consommateur de ces certificats. Cette solution est proche du modèle de Web de confiance[8] (Zimmermann, 1995), exception faite que les certificateurs sont les générateurs et que l'objectif n'est que l'intégrité du pseudonyme et non pas son association à un alias.

7. trad. Man In The Middle.
8. trad. Web of trust

Si le pseudonyme est appris du générateur durant sa certification, celui-ci devient à même de lier cette transaction avec le consommateur. Cependant, la confidentialité du canal de négociation est requis par les parties négociatrices et non pas par les générateurs. Lorsque la non-associativité est requise entre un générateur et un consommateur, la certification du pseudonyme peut donc être réalisée par une signature à l'aveugle. Notons qu'un alias pourrait être délivré au sein de certificats anonymes et non au sein d'un certificat à clé publique. En revanche, le rôle d'un alias étant d'identifier une identité connue, ce que l'on souhaite intrinsèquement un facteur d'associativité, les certificats anonymes pour leur propriété de non-associativité ne se justifient pas pour un certificat contenant un alias.

Revenons à l'implémentation de l'architecture à clé publique globale qui aujourd'hui régit de nombreux accès sécurisés à travers le Web. Les AC doivent être de confiance pour les consommateurs. Ce qui signifie en premier lieu l'approvisionnement sûr des clés publiques des AC[9]. Cependant, en pratique, la plupart des AC sont « inconnues » des utilisateurs et des organisations. Notons qu' il est difficile de considérer, au regard de ces considérations, que les AC soient sources de confiance transitive, donc qu'elles soient propices à l'établissement de relations de confiance entre inconnus.

En admettant que de la confiance leur soit tout-de-même accordée pour la certification d'un alias, cela ne signifie pas que la confiance puisse satisfaire les attentes décrites pour la négociation que sont la fourniture de certificats d'attributs satisfaisant, d'une part, le contrôle d'accès des organisations, et d'autre part, les besoins de contrôle et de confiance des usagers. Cela suppose donc l'emploi conjoint de certificats de générateurs satisfaisant ces attentes et de certificats à clés publiques issus de ces AC. Pour les raisons explicitées précédemment, la clé publique employée pour la confidentialité devrait être « re-certifiée » dans les certificats satisfaisant la négociation. Si l'organisation ne bénéficie pas d'une confiance pré-existante, l'alias n'apporte rien et les certificats à clé publique deviennent inutiles pour leur rôle d'association d'une clé publique à un alias.

Nous sommes donc dans l'idée soit que l'architecture de certificat que nous employons dans ces travaux se substitue à l'architecture de certificats existante en restreignant les AC à leur rôle de certification d'un alias, soit que l'architecture à clé publique aujourd'hui mise en œuvre soit utilisée conjointement à notre architecture. Notons alors que dans l'architecture à clé publique globale actuellement mise en œuvre, les schémas de signature employés pour la signature des certificats ne permettent pas la non-associativité. Ainsi, dans l'état actuel des choses, la clé publique est un pseudonyme prouvé associé à un alias et l'emploi de pseudonymes dédiés est rendu inutile par l'associativité des certificats à clé

9. Il est intégré dans cette notion, le jeu de certificats natif aux navigateurs et systèmes d'exploitation des AC Web racines.

publique. En considérant que l'alias n'apporte pas une confiance suffisante, ou que le tiers est préalablement inconnu et donc que l'alias n'apporte rien, l'autorisation se baserait alors sur les multiples certificats des générateurs de confiance, la clé publique du certificat à clé publique serait employée pour établir un canal confidentiel et elle serait re-certifiée par toutes les autorités afin d'avoir confiance dans le fait qu'une relation confidentielle est entretenue avec le porteur des certificats présentés. La clé publique n'a alors pas besoin d'être signée à l'aveugle puisque nous avons supposé un schéma de signature pour la génération des certificats à clé publiques n'assurant pas la non-associativité.

Certaines propositions ((Hess *et al.*, 2002) par exemple) ne proposent que d'employer de multiples certificats à clés publiques. Il s'agit bien d'un moyen d'augmenter la confiance dans l'association d'alias avec une entité si celle-ci est préalablement connue. C'est aussi le moyen d'augmenter la confiance dans la confidentialité du canal si tous les certificats certifient la même clé publique, mais aussi si les AC appartiennent au domaine de confiance du consommateur et permettent de satisfaire aux attentes de la négociation.

La solution présentée ici, consistant à faire signer par les générateurs le pseudonyme dédié employé comme clé publique permettant l'échange du secret de confidentialité est une solution plus générale. Elle peut s'appuyer sur l'architecture à clé publique existante mais elle semble plus pertinente lorsque les interlocuteurs d'une négociation sont inconnus, elle est donc plus générale.

Il est possible de conclure sur la dissociation des problématiques de confidentialité dans un canal de communication et de confiance pré-existante dans une entité. La première est traitée par la multiple certification du pseudonyme employé pour la confidentialité au sein des certificats servant la négociation. La seconde s'appuie sur de multiples AC en charge de vérifier l'identité réelle des entités et de délivrer un alias cohérent[10]. Ceux-ci peuvent être présentés n'importe quand durant la négociation dès lors que l'un des interlocuteurs souhaite bénéficier d'un niveau de confiance acquis extérieurement. La confiance dans la confidentialité du canal peut être fournie par un pseudonyme certifié, si nécessaire par une signature à l'aveugle, par les générateurs des certificats et utilisé pour échanger un secret de chiffrement. En admettant que chaque consommation d'un certificat apporte plus de confiance dans l'interlocuteur, il est possible de considérer que la confiance dans la confidentialité du canal de négociation est également croissante. Ainsi, chaque consommation de certificat augmente la confiance dans l'interlocuteur ainsi que la confiance dans la confidentialité du canal.

10. Il pourrait alors être judicieux que de telles AC soient des organismes justifiés, état civil et Chambres du Commerce et de l'Industrie par exemple

V.2.2 Flot applicatif

Il est possible que l'objet de la négociation soit simplement une information certifiée. Mais cela peut être également un accès à une application. Ce qui pourrait notamment induire un flot d'échange applicatif successif à une négociation menée avec succès. Il est également possible de penser que la consommation d'une application distante soit ponctuée de multiples négociations. Enfin, la consommation d'une application distante, la navigation Web par exemple, peut être source de confiance. Toutes ces finalités ont en commun un flot de données applicatif dépendant de la notion de confiance et des échanges des négociations de confiance. Les solutions d'environnements clients enrichis que nous évoquions au chapitre 3 supposent que, lorsqu'une négociation mène à une autorisation pour un accès applicatif, un canal de communication pour l'application soit ouvert. Il semble intuitif qu'il faille coupler les deux flots. Lorsqu'il s'agit d'un accès, la confiance dans la confidentialité du canal de communication est ainsi exploitée pour le flot applicatif. En outre, si la consommation d'une application est source de confiance, celle-ci peut être associée à un pseudonyme.

La secret employé pour la confidentialité du canal applicatif, s'il est indépendant, devrait être dérivé de paramètres négociés durant la négociation de confiance. Il est cependant envisageable d'« encapsuler » le flot applicatif dans la négociation de confiance, donc de n'avoir à sécuriser qu'un unique canal de communication. Cela implique et confirme la notion de couche attribuée à la gestion des identités dans les négociations de confiance. Cependant, cela n'est pas anodin puisque l'agent de négociation aura la charge de recevoir l'ensemble des flux, de traiter ceux de la négociation et de diriger les flux applicatifs vers les applications. Nous reviendrons plus précisément sur ces notions à la section VII.1.1.

V.3 Mise en œuvre

V.3.1 Considérations pratiques

Pour que l'une des parties puisse utiliser le pseudonymat, il faut que l'autre partie utilise un pseudonymat public. Seul l'un de ces deux pseudonymes est nécessaire pour échanger un secret. En supposant qu'un seul pseudonyme est utilisé à cette fin, son possesseur a la charge de le faire certifier dans ses certificats. L'autre partie a la charge de vérifier l'intégrité du pseudonyme à chaque consommation de certificat et de fournir le secret. Cette dernière voit en quelque sorte sa confiance augmenter dans la confidentialité de la négociation au fur et à mesure de sa consommation de certificats. La partie qui voit son pseudonyme employé pour échanger le secret peut requérir de son interlocuteur que le secret soit certifié de sorte qu'elle puisse elle-même vérifier la confidentialité du canal et qu'elle puisse elle aussi acquérir de la confiance dans la confidentialité des échanges avec le possesseur des certificats qu'elle consomme. Il est évident que si l'un des interlocuteurs est « malhonnête », la confidentialité n'est pas assurée, ce qui est cohérent avec l'idée d'une confiance croissante avec son interlocuteur et dans la confidentialité du canal. Il est également envisageable de générer un secret dans un mode « Diffie-Helmann » en s'appuyant sur les deux pseudonymes. Dans ce cas, les deux parties ont à certifier leur pseudonyme. Si l'on conçoit que deux parties puissent négocier anonymement avec les réserves émises précédemment, un pseudonyme à usage unique peut être employé par une ou les deux parties. Si la non-associativité est attendue entre la génération et la présentation de certificats, les pseudonymes et le secret doivent être signés à l'aveugle.

Nous avons identifié plusieurs combinaisons de statuts d'anonymat réalisables entre les interlocuteurs :

- de l'anonymat face à l'anonymat (en supposant des adresses indistinguables pour le fournisseur),
- de l'anonymat face à un pseudonymat public,
- du pseudonymat face à un pseudonymat public,
- du pseudonymat public face à un pseudonymat public.

Le cas le plus courant, et celui que nous adressons principalement, est celui d'utilisateurs dans le rôle des initiateurs utilisant un pseudonymat, et des organisations dans le rôle de fournisseurs utilisant un pseudonymat public. Cela est cohérent avec la préoccupation principale de chacun, s'il en est une : le respect de la vie privée pour les utilisateurs et la volonté de bâtir une réputation et de conserver la confiance acquise entre négociations pour les organisations. Cette supposition permet de résoudre certaines situations, potentiellement conflictuelles, comme deux interlocuteurs souhaitant être sous pseudonymat.

Cependant, si une telle situation se produisait, il suffirait de trouver un consensus général signifiant que la logique veut que les utilisateurs qui sont les plus souvent dans le rôle d'initiateur soient privilégiés. Un fournisseur peut évidemment être concerné par le respect de sa vie privée, et être intéressé par la non-associativité de ses transactions. Cependant, le cas à privilégier est un fournisseur employant un pseudonymat public avec les initiateurs et éventuellement un pseudonymat avec ses générateurs. Il est en revanche possible de supposer que le fournisseur puisse, s'il le souhaite, ne pas établir dès le début de la négociation un pseudonyme public mais un pseudonyme à usage unique qu'il renouvellera lorsqu'il aura obtenu un certain niveau de confiance.

V.3.2 Travaux similaires

Le rapprochement entre l'établissement d'un canal de communication sécurisé et les négociations de confiance fut initié par (Hess *et al.*, 2002). Il est proposé de modifier le protocole TLS (Dierks & Allen, 1999 ; Dierks & Rescorla, 2006) afin que celui-ci supporte les négociations de confiance automatisées. L'établissement du canal sécurisé est établie par le protocole *TLS Handshake* usuel, et les négociations sont effectuées au sein du protocole *TLS Rehanshake* amendé. Il n'est cependant pas précisé si la clé publique employée pour l'échange du secret est certifiée dans d'autres certificats que celui employé lors du protocole *TLS Handshake* initial. Il est simplement proposé d'employer de multiples certificats à clé publique ce qui ne solutionne pas la problématique de la confidentialité comme nous l'avons précédemment évoqué.

V.3.3 Gestion de l'établissement de l'identité

Nous supposons que le protocole *TLS Hanshake* initial peut être mené avec un pseudonyme du fournisseur certifié ou non, qui sera ensuite certifié dans les autres certificats présentés. Les certifications de pseudonymes et du secret de confidentialité sont déterminées au sein du protocole *TLS Hanshake* (comme l'est actuellement la version du protocole employé par exemple). Nous avons justifié le fait que les interlocuteurs peuvent avoir à négocier l'établissement d'un pseudonyme déjà employé puisqu'il signifie l'associativité des négociations et par conséquent représente un élément sensible. Nous pouvons donc supposer que l'un des interlocuteurs puisse initialement employer à des fins de confidentialité du canal un pseudonyme à usage unique. Puis qu'il le renouvelle avec un pseudonyme déja employé au cours de la négociation. Soit ce pseudonyme est simplement prouvé, soit il peut également servir à établir un nouveau canal en renouvelant le secret de confidentialité. Nous supposerons que le renouvellement peut se faire à l'aide du protocole *TLS Rehanshake*. L'idée est ici que le protocole *TLS Rehanshake* est mené sous le couvert des paramètres de sécurité du canal. Ainsi, le pseudonyme établit est automatiquement lié à

la négociation passée et donc à la confiance déja acquise.

Sur la figure V.1 est illustré un cas d'usage où le fournisseur établit un pseudonyme à usage unique en premier lieu. L'initiateur révèle ensuite l'objet de la négociation. Enfin, le fournisseur établit un pseudonyme public et permet ainsi la création d'un compte pour le pseudonyme présenté par l'initiateur. L'initiateur ne négocie pas l'établissement de son pseudonyme dans cet exemple. La fin de la négociation est ensuite résumée. Le pseudonyme P1 est utilisé pour sécuriser la négociation. Ainsi, P1 est confirmé dans les certificats jusqu'à ce que P2 soit établi. C'est ensuite P2 qui est certifié. Le renouvellement du pseudonyme étant fait au travers du canal sécurisé, la confiance précédemment acquise est préservée.

Pour rester proche du protocole TLS, on suppose que la possession du pseudonyme est prouvée à l'aide d'un challenge implicite[11]. On pourrait cependant utiliser un protocole d'établissement de pseudonymes utilisant une preuve de connaissance en remplaçant les messages *ServerKeyExchange*, ou *ClientKeyExchange*, et *CertificateVerify*. Le renouvellement de pseudonymes peut être fait au sein du protocole *TLS Rehanshake* avec pour opérande la re-planification des clés[12].

Notons cependant que les pseudonymes des architectures à pseudonymes présentées au chapitre 4 ne permettent pas de chiffrer avec leur partie publique. Il est donc nécessaire d'employer un pseudonyme qui serait par exemple une clé RSA (Rivest *et al.*, 1978) ou de lier une clé RSA à un autre pseudonyme. L'emploi d'une clé RSA nous ramène à un cas d'usage proche des implémentations actuelles. Les initiateurs peuvent ainsi utiliser les pseudonymes présentés dans l'architecture de Camenisch. Le fournisseur emploie quant à lui une clé RSA comme pseudonyme public. Il peut également employer le système à pseudonymes de l'architecture de Camenisch avec ses générateurs.

Il est ensuite possible de décrire les prémisses des agents assumant les rôles d'initiateur et de fournisseur au sein de la négociation par des machines d'état. Ces machines d'états nous permettent de présenter les statuts d'anonymat que les deux rôles, initiateur et fournisseur, peuvent percevoir de leur interlocuteur. Elles sont illustrées à la figure V.2 et la figure V.3. Les états atteignables sont restreints aux combinaisons précédemment décrites. Au sein de celles-ci, les messages envoyés à l'interlocuteur sont symbolisés par une flèche avec légende. Les états de l'agent, suite à la réception d'un message, sont les boîtes carrées aux angles arrondis. Les autres boîtes carrées sont les états finaux possibles d'une transaction. La négociation est ponctuée de sous-négociations qui sont vues comme des

11. trad. Implicit challenge.
12. trad. Replenishment of keying material.

boîtes noires. Autrement dit, ces machines d'états font apparaître les sous-négociations comme des « méta-états » qui passent à l'état suivant, ou à la sous-négociation suivante, en libérant leur objet. Ils sont représentés par des bulles. Ce sont en quelque sorte des sous-machines d'état qui ont pour états finaux la fourniture de l'objet de la sous-négociation qu'elles réalisent. Il est considéré les sous-négociations avec les objets suivants :

- la déclaration de l'objet de la négociation,
- l'établissement d'un pseudonyme,
- la fourniture d'informations supplémentaires requises pour la création d'un compte initiateur,
- l'objet de la négociation (c'est un ensemble de sous-négociation dont celles qui ne sont pas illustrées pour les objets précédemment cités sont rassemblées en une seule « bulle »).

Quelques remarques :

1. Lorsqu'un initiateur négocie avec un fournisseur pour la première fois, il ne peut déterminer si le pseudonyme présenté par le fournisseur est un pseudonyme à usage unique ou un pseudonyme public. Cependant, si la négociation conduit au fait que l'initiateur doit établir un pseudonyme, si le fournisseur emploie un pseudonyme à usage unique, il le renouvellera avec son pseudonyme public, et l'initiateur en déduira que le fournisseur utilisait un pseudonyme à usage unique. Si le fournisseur laisse l'initiateur établir un pseudonyme sans changer son pseudonyme, l'initiateur peut déduire que le fournisseur emploie un pseudonyme public.
2. Sur cette représentation, il est supposé que l'initiateur négocie toujours l'établissement d'un pseudonyme déjà employé, même si ce n'est pas obligatoirement le cas en pratique.
3. Il est considéré que l'espace des pseudonymes est suffisamment grand pour qu'il n'y ait pas de collisions. En pratique, cela signifie que si le fournisseur emploie un pseudonyme à usage unique, l'initiateur ne peut pas prétendre le reconnaître.
4. Il est considéré que si l'initiateur signifie le besoin d'établir une identité pour un compte existant, et que le fournisseur initie la négociation avec un pseudonyme à usage unique, l'initiateur n'est pas censé reconnaître le fournisseur, il doit donc indiquer à celui-ci qu'il attend un pseudonyme public. S'il ne le fait pas, il est considéré que l'initiateur ne peut pas ensuite établir un pseudonyme connu du fournisseur (sinon il y aurait collision).

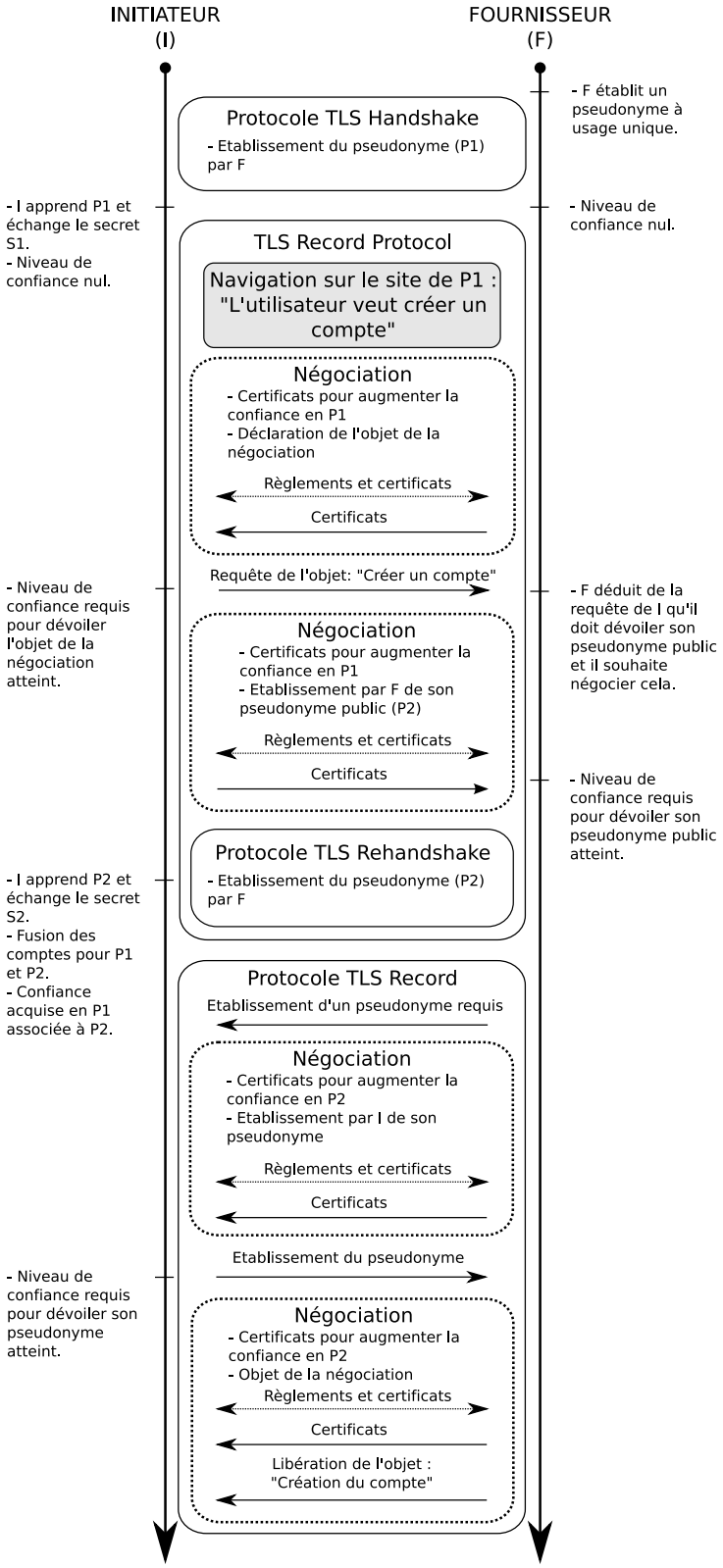

FIG. V.1 – *Exemple de négociation avec renouvellement du pseudonyme fournisseur.*

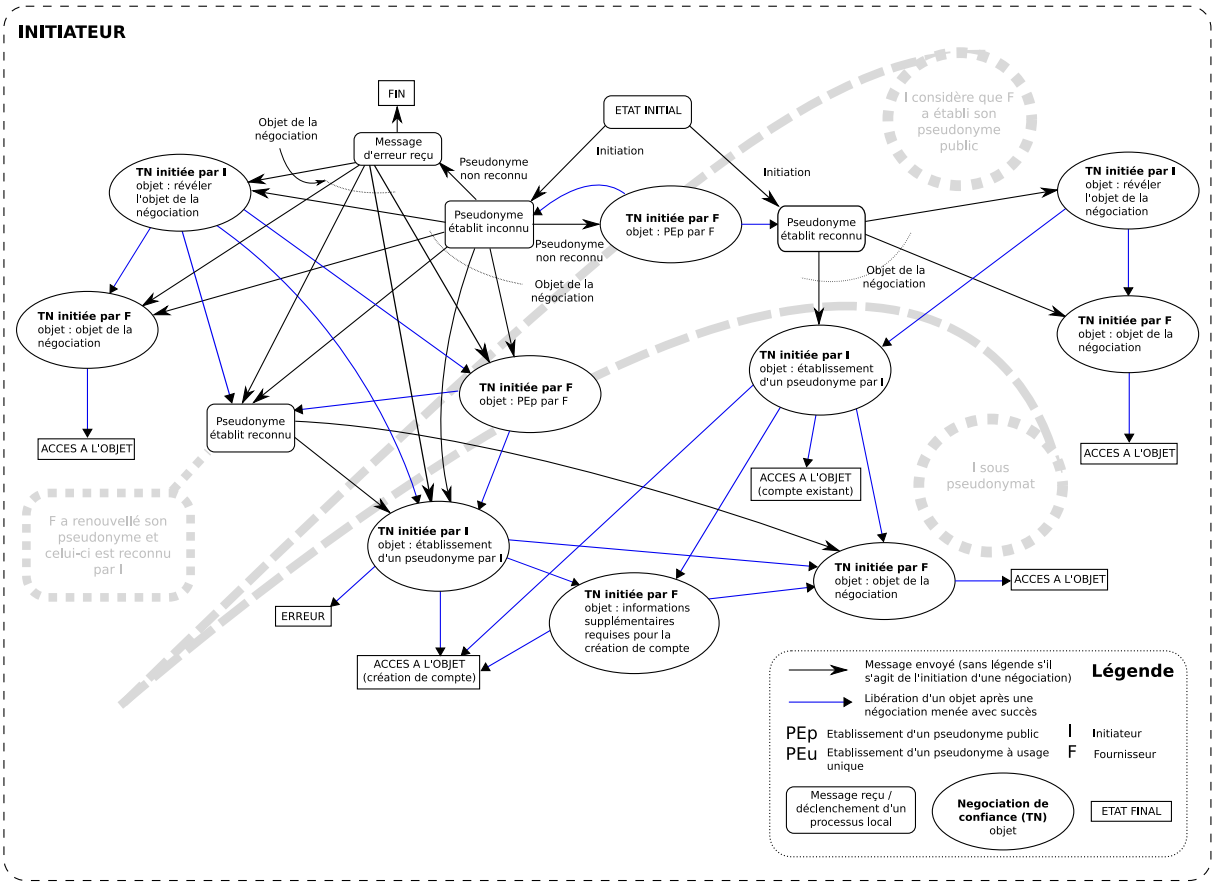

FIG. V.2 – *Machines d'états du rôle Initiateur.*

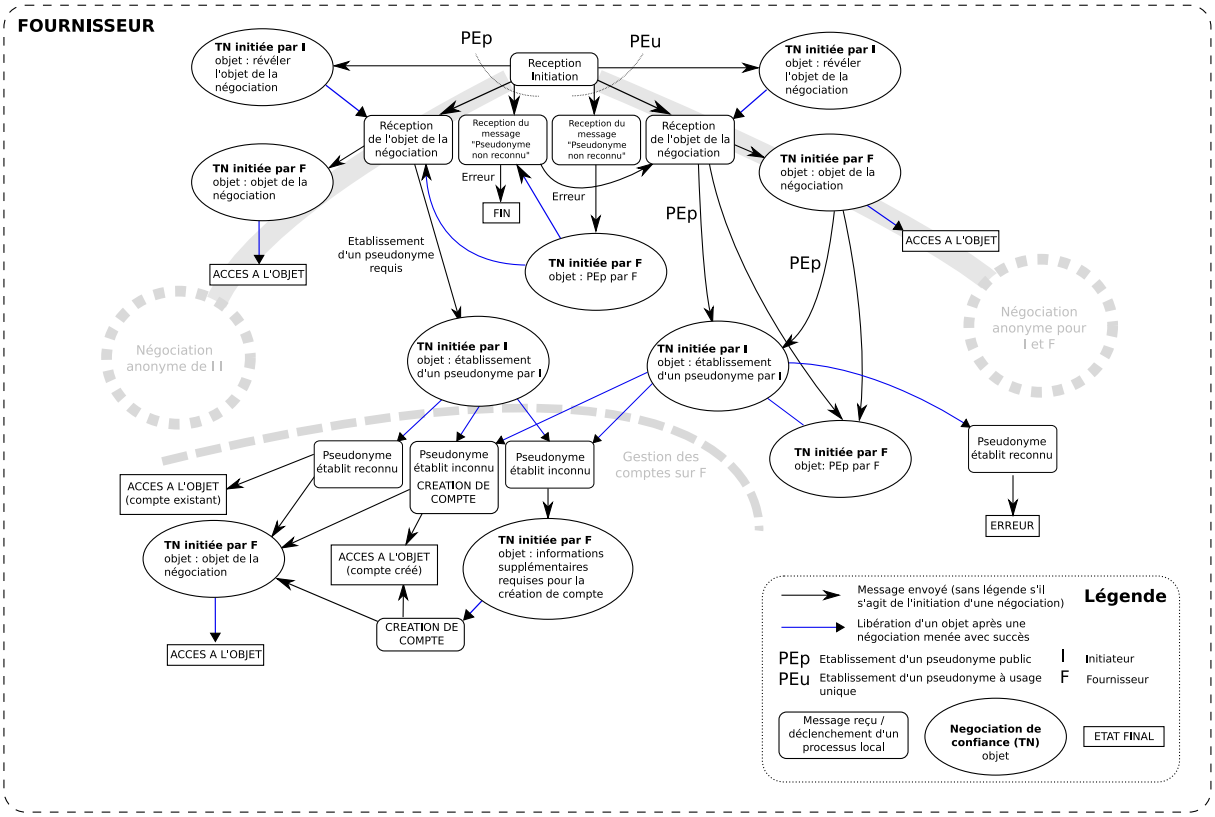

FIG. V.3 – *Machines d'états du rôle Fournisseur.*

V.3.4 Sketch cryptographique

Étudions le cas où un fournisseur utilise un pseudonyme public (une clé RSA) employé pour sécuriser les échanges. L'initiateur requiert deux certificats de deux générateurs différents de son domaine de confiance. L'organisation présente ces deux certificats qui sont obtenus selon le schéma CL-Signature présenté au chapitre précédent. Chacun d'eux va contenir la clé RSA signée à l'aveugle par les générateurs du fournisseur ainsi que le secret maître de l'organisation. Le secret maître est prouvé comme étant le même dans les deux certificats et il est supposé un mécanisme, non présenté ici, permettant à l'initiateur d'avoir confiance dans le fait que ce secret maître est non-transférable. La clé RSA est prouvée comme étant contenue dans les deux certificats.

Rappelons la phase de génération de la clé de signature des générateurs pour le schéma CL-Signature (Camenisch & Lysyanskaya, 2003 ; Camenisch, 2008). Par $\mathbf{QR}_n \subseteq Z_n^*$ est dénoté l'ensemble des résidus quadratiques module n, c'est-à-dire, les éléments $a \in Z_n^*$ tels que $\exists b \in Z_n^*$ et que $b^2 \equiv a \; mod \; n$.

Génération de clés : Entrée : l_n, choisir un modulo RSA n de $l_n - bit$ tel que $n = pq$, $p = 2p' + 1$, $q = 2q' + 1$, où p, q, p', et q' sont des premiers. Choisir, aléatoirement et uniformément, R_0,...,R_{L+1},S,$Z \in \mathbf{QR}_n$. Soient la clé publique (n,R_0,...,R_{L+1},S,Z) et la clé secrète p.

Le générateur choisit alors un nombre aléatoire premier e ($l_e > l_m + 2$). L'exposant e permet la vérification d'une signature reposant sur le problème RSA. Le calcul de l'inverse de l'exposant e public repose sur la décomposition en nombre premier de n. d, la clé privée de signature, est l'inverse de e module $\varphi(n)$, soit $ed \equiv 1 \; mod \; \varphi(n)$ et $\varphi(n) = \varphi(pq) = (p-1)(q-1)$.

Le pseudonyme public du fournisseur est une clé RSA notée (n_O,e_O). Une session du protocole *TLS Hanshake* est conduite : la possession de cette clé est prouvée à l'initiateur et un secret pour la confidentialité des échanges est généré. L'initiateur requiert deux certificats issus des générateurs I_A et I_B. La procédure d'obtention des certificats par le fournisseur est la même avec les deux organisations. Les clés publiques des générateurs sont connues et considérées comme sûres par le fournisseur. Cela permet au fournisseur de les authentifier et d'établir avec chacun d'eux un canal de communication sécurisé. Le fournisseur établit ensuite son identité auprès des générateurs avec un pseudonyme dédié. Traitons le cas du fournisseur noté O et du générateur I_A. Soient x_U le secret maître et s_{O,I_A} le secret local dédié à I_A qui sont respectivement les quantités α et β dans le preuve

suivante :

$$PK\{(\alpha,\beta) : P_{(O,I_A)} = R_{A_0}^{\alpha} R_{A_1}^{\beta}\}$$

O aveugle alors sa clé RSA et envoie le résultat à I_A (1) puis mène une preuve de connaissance (2) :

$$(1)\ U = S_A^{v'''} R_{A_2}^{n_0} R_{A_3}^{e_0} \ mod\ n_A$$
$$(2)\ PK\{(\alpha_0,\alpha_1,\alpha_2) : U \equiv \pm S_A^{\alpha_0} R_{A_2}^{\alpha_1} R_{A_3}^{\alpha_2} \ mod\ n_A \wedge \alpha_1,\alpha_2 \in \pm\{0,1\}^{l_m}\}$$

I_A choisit ensuite un nombre aléatoire v'', un nombre premier aléatoire e_A et délivre le certificat A_A à O :

$$A_A \equiv (\frac{Z_A}{U S_A^{v''} R_{A_0}^{x_U} R_{A_1}^{s_{O,I_A}}})^{1/e_A} \ mod\ n_A$$

Soit :

$$A_A \equiv (\frac{Z_A}{S_A^{v_A} R_{A_0}^{x_U} R_{A_1}^{s_{O,I_A}} R_{A_2}^{n_0} R_{A_3}^{e_0}})^{1/e_A} \ mod\ n_A$$

I_A prouve que le certificat A_A est calculé correctement. O vérifie que le tuple (A_A,e_A,v_A) est une signature valide :

$$Z_A \stackrel{?}{\equiv} A_A^{e_A} R_{A_0}^{x_U} R_{A_1}^{s_{O,I_A}} R_{A_2}^{n_0} R_{A_3}^{e_0} S_A^{v_A} \ mod\ n_A$$

O s'appuie alors sur la propriété de la CL-Signature pour modifier la signature et la rendre inassociable à celle de départ. Avec r_A un nombre aléatoire, $(A'_A = A_A S_A^{-r_A} \ mod\, n_A, e_A, v'_A = v_A + e_A r_A)$ est aussi un tuple valide d'une signature sur le certificat.

O obtient de la même façon un certificat de I_B, seule la valeur s_{O,I_B} diffère dans la procédure d'établissement de l'identité menée avec I_A. O prouve alors à l'initiateur qu'il possède les deux certificats de I_A et de I_B (il révèle pour cela A'_A et A'_B), que ces certificats contiennent la clé RSA employée pour sécuriser le canal (clé déjà connue de l'initiateur lors de la session initiale du protocole *TLS Hanshake*) et qu'ils contiennent tout deux un même secret maître (non révélé grâce à un engagement).

En d'autres termes, O commence par envoyer A'_A et A'_B à l'initiateur. Soient $g_0,...,g_L$ les éléments d'un groupe d'ordre premier. O choisit une valeur aléatoire r' et engage le

secret maître : $C := g_0^{r'} g_1^{x_U}$. Enfin, O mène la preuve suivante :

$$\begin{aligned} PK\{(\alpha_0,\alpha_{A_1},\alpha_{B_1},\varepsilon_A,\nu'_A,\varepsilon_B,\nu'_B,\rho) : \\ Z_A A_A'^{-2^{l_e+1}} R_{A_2}^{n_0} R_{A_3}^{e_0} \equiv \pm A_A'^{\varepsilon} S_A^{\nu'_A} R_{A_0}^{\alpha_0} R_{A_1}^{\alpha_{A_1}} \ mod\ n_A \\ \wedge\ Z_B A_B'^{-2^{l_e+1}} R_{B_2}^{n_0} R_{B_3}^{e_0} \equiv \pm A_B'^{\varepsilon} S_B^{\nu'_B} R_{B_0}^{\alpha_0} R_{B_1}^{\alpha_{B_1}} \ mod\ n_B \\ \wedge\ C \equiv g_0^{\rho} g_1^{\alpha_0} \\ \wedge\ \alpha_0,\alpha_{A_1},\alpha_{B_1} \in \pm\{0,1\}^{l_m+l_\varnothing+l_\mathcal{H}+2} \\ \wedge\ \varepsilon_A,\varepsilon_B \in \pm\{0,1\}^{l'_e+l_\varnothing+l_\mathcal{H}+2}\} \end{aligned}$$

L'initiateur vérifie avec cette preuve que :

- l'organisation possède deux certificats issus de I_A et de I_B,
- le couple (n_0,e_0) est contenu dans les deux certificats,
- le secret maître (x_U) est le même dans le deux certificats.

CHAPITRE VI

Négociation & Interactions

*Au **chapitre 6**, la négociation de confiance est dans un premier temps justifiée au regard des objectifs de l'architecture, notamment de la diffusion fine et contrôlée de l'information par les usagers. L'utilisateur est considéré comme étant au centre de l'architecture et « aux commandes » des échanges. Il est nécessaire de l'assister et d'améliorer son expérience par l'automatisation de ses choix. Nous nous appuyons sur les travaux scientifiques portant sur les négociations de confiance automatisées pour traiter ces problématiques d'utilisabilité. Une étude est faîte pour déterminer un langage de contrôle d'accès adapté à la négociation. Il est enfin présenté la faisabilité de ces objectifs par un cas d'étude. Outre la description de cet objectif de recherche sur l'utilisabilité, ce chapitre permet de présenter plusieurs considérations de mise en oeuvre, notamment la détermination des générateurs disponibles satisfaisant les conditions de contrôle d'accès d'un consommateur.*

Sommaire

"La limite de ce système n'est pas défini par la technologie mais par la rationalité limitée d'Alice, son inaptitude à contrôler ce qu'elle ne comprend pas. [1]"

Piotr Cofta, *Trust, complexity and control - Confidence in a convergent world.*

1. trad. "The limit of this scheme is defined not by technology but by Alice's bounded rationality, her inability to control what she does not understand."

VI.1 Desiderata

L'ambition de ces travaux est en partie d'adresser la vie relationnelle des usagers dans un univers numérique où il n'y a pas d'autorité centrale. Celle-ci dans cet environnement, souvent qualifié d'« ouvert », est sujet à l'établissement de contacts avec des inconnus. Il est donc déterminant de pouvoir s'appuyer sur la confiance pour établir des relations. Dans un univers fait de communications et d'interfaces, l'information collectée sur un interlocuteur est la source à partir de laquelle la décision de faire confiance peut être prise. Nous essayons donc ici de caractériser de manière informelle les pratiques actuelles afin de justifier le bien-fondé de l'emploi de la négociation de confiance en environnement ouvert.

La consommation de services sur le Web est ponctuée de créations de comptes. Celles-ci supposent, dans la majorité des cas, la fourniture d'informations personnelles. Cela soulève de multiples problématiques, notamment concernant le respect de la vie privée. Diverses solutions sont proposées. L'une d'entre elle consiste à avertir les utilisateurs de l'utilisation qui sera faite de ces informations, et plus précisément, sur leur conservation. Il est par exemple indiqué le fait que ces données font l'objet d'une réglementation, qu'elles ne seront pas divulguées, ou qu'elles ne seront conservées que pour une durée déterminée. Ces initiatives sont accompagnées de solutions technologiques de diffusion telles que le standard P3P [2] par exemple. Divers outils, souvent couplés au navigateur Web, permettent également à l'utilisateur de contrôler les informations qu'il diffuse, *privacy bird* par exemple [3]. Ces outils peuvent assurer diverses fonctionnalités, dont l'analyse des politiques P3P, ou faciliter la saisie d'informations [4]. Cependant, rien ne garantit à l'utilisateur le fait que les organisations respectent leurs engagements. Et même si les politiques diffusées peuvent être signées de tiers de confiance, l'utilisateur n'a plus de moyen de contrôle de ses informations une fois celles-ci diffusées. Nous préférons donc une approche privilégiant un contrôle fin de l'information diffusée.

Ajoutons à cela que les informations saisies par les utilisateurs servent généralement au processus de contrôle d'accès à une ressource ou un service, en y incluant la création de compte. Cependant, rares sont les informations qui ont réellement un sens dans la politique de contrôle d'accès telles que la majorité d'un utilisateur par exemple. Prenons le cas de la fourniture d'une adresse électronique « valide » lors de la création d'un compte. La syntaxe est vérifiée à la saisie. La validité de l'adresse est ensuite vérifiée par l'envoi d'un jeton à cette destination que l'utilisateur doit retourner pour permettre la

2. Platform for Privacy Preferences - http://www.w3.org/P3P/
3. http://www.privacybird.org/
4. Outils généralement appelés « form-fillers ».

création du compte. Cependant, l'adresse électronique n'a pas de nécessité particulière à être employée comme un élément de contrôle d'accès. Si l'objectif est de permettre le recouvrement d'un mot de passe perdu par l'utilisateur, sa saisie devrait être conseillée et permise à l'utilisateur après la création du compte. Il ne s'agit en aucun cas d'un moyen de contrôle sur l'utilisateur en cas de fraude, ou de limitation de la création de compte automatisée[5]. L'adresse électronique semble donc n'être collectée que pour permettre aux organisations hôtes des fournisseurs de services de constituer des listes de diffusion qui ont potentiellement une valeur marchande. Cela amène à penser que la majeure partie des informations collectées n'a d'autre intérêt que d'enrichir des bases de données, voire, que certains services ne seraient proposés que pour collecter des informations personnelles.

En outre, la fourniture d'informations personnelles n'est qu'une des possibilités pour collecter de l'information pertinente pour le contrôle d'accès. Pour une grande partie des informations requises, seule l'information que l'utilisateur les possède, ou le fait qu'elles aient certaines propriétés, peuvent être suffisants pour opérer le contrôle d'accès. Il s'agit donc de permettre à l'utilisateur de s'engager, et de prouver ses engagements. Parmi les informations utiles, il est donc possible de distinguer :

- les informations dont seule la preuve de possession est nécessaire (un numéro de sécurité sociale valide par exemple),
- les informations dont il est nécessaire de prouver certaines propriétés (une date de naissance pour prouver un âge)
- les informations qu'il est réellement nécessaire de dévoiler (le groupe sanguin par exemple).

En résumé, il est nécessaire de pousser les organisations à « consommer mieux ». L'idée est de donner un coût à l'obtention d'informations selon leur valeur estimée par l'utilisateur, et que ce coût soit la fourniture d'informations en échange. Outre l'obtention d'informations par l'usager afin de satisfaire ses besoins de confiance et de contrôle, nous faisons donc l'hypothèse d'un système où l'utilisateur est en capacité de requérir des informations en échange de ses propres informations afin d'« assainir » la consommation de ses informations personnelles par les organisations. Il s'agit de permettre une négociation où :

- l'utilisateur a le choix de diffuser ou non certaines informations, c'est-à-dire, que lui soient fournies des alternatives,
- les organisations ont des certificats qu'elles ne souhaitent pas diffuser sans aucune contre-partie afin de justifier la notion de coût.

Empreint des pratiques actuelles, il peut être difficile de concevoir que des informations puissent être demandées par des utilisateurs à des organisations. Dans un monde nu-

5. Seuls les tests de Turing et dérivés ont un sens, les captchas par exemple

mérique où ces transactions seraient possibles et « simples », il est possible d'admettre aisément qu'un usager demande un certificat attestant de la santé financière de l'organisation préalablement à son achat. L'organisation peut ne pas être encline à révéler le montant exact de sa trésorerie. Par contre, elle pourrait accepter de prouver, à l'aide d'un certificat fourni par sa banque, qu'elle est financièrement saine si cela lui permet d'augmenter ses ventes (par exemple par un certain ratio de son bénéfice sur son chiffre d'affaires).

Les utilisateurs sont, eux, parfois peu enclins à fournir des informations personnelles. En reprenant l'exemple de la création de compte, les informations nécessaires à l'obtention d'un service sont généralement fournies correctement lorsqu'elles sont jugées déterminantes pour l'obtention d'un objet (une adresse de livraison par exemple). Par contre, pour les informations jugées non déterminantes, ou trop « intrusives », l'utilisateur fournit généralement de fausses informations afin de dévoiler un minimum d'informations, mais également, pour terminer au plus tôt des procédures administratives souvent jugées longues et ennuyeuses. Cela implique que le contrôle d'accès ne sera dans ce cas pas pertinent s'il est basé sur le contenu de l'information. Les informations employées dans le contrôle d'accès ne doivent pourtant pas souffrir de leur inexactitude. Cela justifie le besoin de certification de l'information, par des tiers de confiance des consommateurs. Cela nous conduit à une architecture où les deux parties s'échangeraient mutuellement des informations dont certaines seraient certifiées. Ainsi, l'échange d'informations certifiées permet dans un premier temps aux organisations d'opérer leur contrôle d'accès et aux utilisateurs d'obtenir des moyens de contrôle et de confiance sur les organisation. Ensuite, il est possible qu'à terme les échanges bilatéraux contribuent à réduire la quantité d'information requise des utilisateurs.

En reprenant la terminologie introduite au premier chapitre, le fournisseur délivre un objet, une ressource ou un service, en fonction d'informations dont une partie est certifiée par des tiers de confiance. Il s'agit de la gestion de confiance[6] (Blaze *et al.*, 1996a). Le fait que des informations soient fournies en échange d'autres informations implique que ces informations soient des ressources auxquelles l'accès est contrôlé par d'autres informations, dont certaines sont certifiées. Il y a donc lieu à négociation pour déterminer une séquence d'échanges satisfaisant les règlements de contrôle d'accès de chacun. Il s'agit des négociations de confiance que nous évoquions au premier chapitre. Il est possible de distinguer trois rôles fondamentaux au sein de celles-ci :

- les initiateurs qui requièrent des objets,
- les fournisseurs qui fournissent des objets,

6. trad. Trust management.

– les fournisseurs de certificats.

L'initiateur demande un objet au fournisseur et ils négocient pour cela. Rappelons la vue générale d'une négociation à la figure VI.1 :

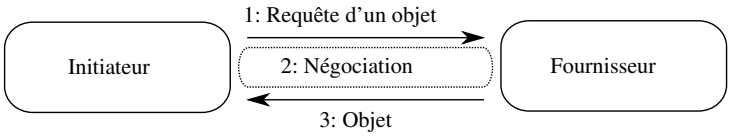

FIG. VI.1 – *Vue générale d'une négociation.*

Les négociations de confiance ont pour finalité la délivrance de l'objet initialement requis, et sont constituées de multiples « sous-négociations », ayant chacune leur propre objet, et pouvant se traduire par de multiples séquences d'échanges d'informations. La diffusion d'informations, certaines certifiées, est soumise à la présentation d'autres informations. L'objet même de la négociation, ainsi que les règlements qui expriment les certificats souhaités, peuvent être des éléments sensibles sujets à négociation. Ajoutons à cela que chacun des objets (dont l'objet initial) peut être renégocié. Il est par exemple imaginable que le fournisseur fasse une offre pour un nouvel objet si l'initiateur fournit des informations supplémentaires (s'il augmente la somme de son achat par exemple).

L'une des questions fondamentales posées en début de ce chapitre est de savoir s'il est possible de faire confiance à un inconnu[7]. La négociation de confiance est un moyen d'y parvenir grâce aux relations de confiance avec les tiers de confiance. Il est pour cela nécessaire de déterminer les tiers de confiance permettant une mise en relation comme cela est illustré à la figure VI.2.

La confiance est ensuite attribuée au porteur de certificats au travers du concept de confiance transitive. Nous pouvons préciser ces relations à l'aide de la terminologie employée dans (Jøsang *et al.*, 2006a,b) illustrée à la figure VI.3.

Ainsi, chaque échange de certificats permet en quelque sorte d'augmenter la confiance dans leur porteur, et ouvre la voie à la fourniture de nouveaux règlements et certificats. La confiance devrait ainsi croître avec la présentation de certificats. L'échange de certificats est donc un mécanisme cohérent d'implémentation du concept de négociation de confiance au sens d'un établissement graduel et dynamique d'une relation de confiance.

En résumé, la gestion de la confiance permet le contrôle d'accès en environnement ou-

7. L'idée est ici de dire que l'inconnu est initialement inconnu, et donc, nous ne débattons pas du fait que l'inconnu devient connu au fur et à mesure de la négociation, ce qui permet de lui faire confiance.

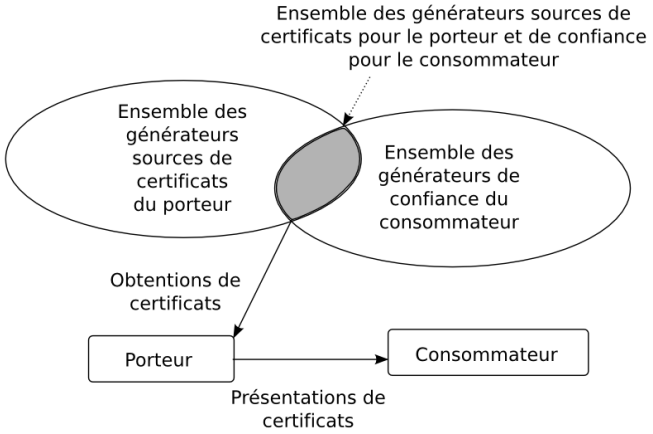

FIG. VI.2 – *Présentation de certificats issus du domaine de confiance du consommateur.*

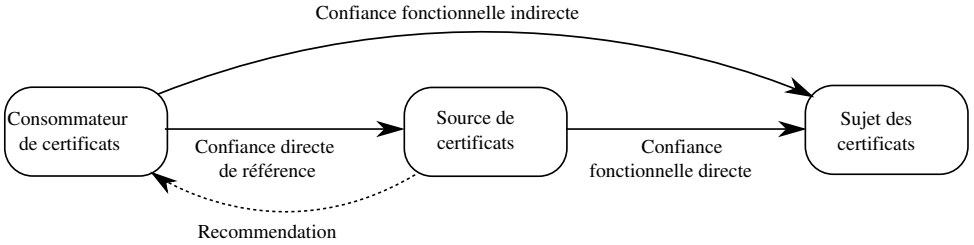

FIG. VI.3 – *Principe de la confiance transitive.*

vert et la confiance transitive est le moyen d'obtenir de la confiance dans un inconnu. Il s'agit pour les organisations de satisfaire aux conditions de contrôle d'accès aux ressources demandées. Pour les usagers, il s'agit d'accroître la confiance et le contrôle sur une organisation. Pour les deux, les échanges d'informations au cours de la négociation servent à satisfaire aux conditions de contrôle d'accès à d'autres informations. Il est en outre possible d'envisager que la négociation de confiance puisse concourir à l'assainissement de la consommation d'informations personnelles par les organisations. Enfin, les négociations de confiance apparaissent comme un mécanisme pertinent pour l'établissement de relations de confiance entre inconnus lorsque les interlocuteurs possèdent *a minima* un tiers de confiance commun.

VI.2 Interactions et négociation

Le système de négociation soulève plusieurs problématiques :

- les contrôles d'accès aux ressources et aux informations,
- la maîtrise des sources d'informations,
- la négociation proprement dite,
- les interactions utilisateurs.

En effet, nous souhaitons voir établir et entretenir des relations de confiance entre interlocuteurs au travers de négociations de confiance. Cette négociation permet en outre de satisfaire aux différents règlements de contrôle d'accès qui régissent la libération de ressources et d'informations. L'utilisateur est au cœur de ce processus et il s'agit d'un défi que de lui permettre de négocier : il doit contrôler l'information qu'il diffuse et demander des informations en échange. L'objectif est également qu'il retire de la confiance de cette négociation qui dans son esprit n'est pas assimilable à une fonction mathématique attribuant un niveau de confiance à chaque certificat obtenu.

Les négociations de confiance sont issues de la convergence de la gestion de la confiance et de la négociation. De nombreux travaux ont été menés afin d'étudier les algorithmes permettant à deux interlocuteurs d'accomplir une négociation reposant sur des informations certifiées. Ces études ont abouti à l'élaboration aussi bien d'algorithmes de négociation que de modèles et de langages de contrôle d'accès. À l'origine des travaux sur l'automatisation des négociations de confiance, citons (Winsborough *et al.*, 2000). De nombreux travaux ont ensuite visé à la fois les algorithmes, la sûreté de ceux-ci, notamment en traitant les règlements diffusés comme des ressources sensibles, mais également des architectures traitant l'ensemble de ces problématiques (Yu *et al.*, 2000 ; Seamons *et al.*, 2001 ; Li *et al.*, 2001 ; Winslett *et al.*, 2002 ; Li & Winsborough, 2002 ; Winsborough & Li, 2002 ; Yu & Winslett, 2003b ; Bertino *et al.*, 2004 ; Li *et al.*, 2005a ; Winsborough & Li, 2006).

Nous considérons que ces algorithmes peuvent être employés pour assister l'utilisateur dans ses négociations. La difficulté réside donc, non pas dans l'emploi de ces algorithmes, mais dans leur utilisation dans le cadre d'une négociation menée par l'utilisateur. L'utilisateur doit bénéficier de ces algorithmes pour qu'il soit assisté dans ses choix et dans sa pratique de la négociation. Il peut s'agir d'indications sur les informations à diffuser et disponibles, sur des éléments de confiance, et sur des choix. Il s'agit également de transformer ses choix et ses interactions en règles de contrôle d'accès qui pourront ensuite être exploitées par les algorithmes de négociation afin d'automatiser ou de conseiller l'utilisateur dans ses négociations suivantes. Nous considérons donc l'automatisation comme un

moyen de réduire le nombre d'interactions utilisateurs requises en cours de négociation, donc comme un moyen améliorer l'expérience de négociation pour l'utilisateur. Ainsi, l'automatisation peut signifier à la fois la sympathie, la prise de décision automatisée, ou l'empathie, l'assistance en lui demandant des acquittements ou de faire des choix simplifiés.

Il est d'ores et déjà intéressant de se poser la question de savoir quelles interactions de l'utilisateur il est possible d'espérer automatiser. L'établissement d'une identité, lorsque l'interlocuteur est « reconnu » et de confiance, en est un exemple. Par contre, lorsque le certificat à fournir est une somme d'argent, il devient difficile de concevoir qu'en pratique les paiements de l'utilisateur puissent être automatisés. Il est cependant possible de demander à l'utilisateur de désigner une source préférée et de lui demander ensuite simplement un acquittement. L'humain est en quelque sorte un algorithme non déterministe capable de choix qu'il est parfois possible de penser arbitraires, tout du moins par l'observation, mais que nous savons influencés par son sentiment de confiance. Ainsi, même si certains de ses choix peuvent être automatisés, la majeure partie doit rester soumise à son acquittement.

Le sentiment de confiance permettant le déclenchement d'une relation de confiance est une notion subjective qui ne peut être appréhendée en quelques phrases. Notons que l'impression de négociation donnée à l'utilisateur peut lui permettre de se sentir plus en confiance. Cette impression de négociation repose sur de nombreuses notions telles que le fait que l'interlocuteur puisse faire des concessions, notamment lorsqu'il requiert certaines informations que l'utilisateur ne souhaite pas diffuser. Il s'agit donc de permettre à l'utilisateur de proposer différentes solutions répondant à un même règlement, donc que les règlements proposés offrent des choix. Ces choix pourraient également ne pas être explicites afin de donner l'impression à l'utilisateur qu'il est force de propositions, propositions qui si elles aboutissent seraient source d'un sentiment de confiance. Il s'agit par exemple de permettre à l'utilisateur de proposer à l'interlocuteur une preuve de propriété d'une information certifiée plutôt que de la révéler. L'enjeu est donc de déterminer un langage d'expression des règlements offrant cette souplesse. Il s'agit aussi, et surtout, d'une question de politique de contrôle d'accès des fournisseurs qui doivent prendre ceci en considération.

La machine est-elle plus « simple » à appréhender ? Il s'agit d'un algorithme complexe mais parfaitement déterministe régi par les règles du contrôle d'accès et les algorithmes de négociation. Si l'humain se trouve face à une machine pour négocier, les marges de manœuvre sont faibles dans le sens où, même si sont intégrées des notions de contrôle d'accès réactif couplées à des systèmes cognitifs, il est peu probable que la machine soit propice à des choix irrationnels sur lesquels les relations de confiance peuvent reposer. C'est pour

cela que le terme *sentiment de confiance*, et l'idée qu'il est possible de *donner une impression de confiance* sont importants. Ce sujet pourrait donner lieu à des travaux bien plus conséquents que ceux présentés ici. Nous réduisons notre étude au fait que pour prétendre au sentiment de confiance par la négociation, les organisations doivent donner une impression de confiance en permettant à l'utilisateur de faire des choix. Par contre, nous ne considérons en aucun cas qu'il soit possible pour l'utilisateur d'influencer le « comportement d'une machine » pour qu'elle fasse des choix qui ne sont pas explicitement définis par son règlement de contrôle d'accès et l'algorithme de négociation qu'elle emploie. Le système de négociation est implémenté par un agent que l'on appelle un « gestionnaire de négociation[8] » ou simplement « agent de négociation ». Il a la charge de vérifier les signatures des certificats, leur possession et les preuves de connaissance. Ce module a également la charge de fournir au vérificateur de règlements les informations extraites des certificats ainsi que les informations de validité des certificats et des preuves. Enfin, il a la charge de l'automatisation de la négociation. Il est possible que pour cela il s'appuie sur des algorithmes de négociation automatisée. Ces algorithmes sont généralement appelés stratégie de négociation. L'algorithme de négociation s'appuie sur le règlement local de l'agent et sur les règlements fournis par l'interlocuteur en cours de négociation pour prendre ses décisions.

Les choix de l'utilisateur au cours d'une négociation représentent en quelque sorte sa propre stratégie de négociation et sa politique de contrôle d'accès à ses informations personnelles. L'emploi d'un gestionnaire de négociations utilisant un algorithme de négociation implémentant une stratégie de négociation est donc le moyen d'assister l'utilisateur dans ses choix. Il est possible d'envisager la mise en œuvre suivante. L'agent de négociation dont est muni l'utilisateur possède un algorithme de négociation et un règlement local vierge. Au fur et à mesure des négociations, les choix et les interactions de l'utilisateur sont analysés afin de renseigner le règlement local qui sera ainsi utilisé lors des négociations ultérieures par l'algorithme de négociation. Cela suppose que, lors des premières négociations, l'utilisateur puisse mener à bien des négociations sans une assistance personnalisée. Le gestionnaire de négociation analyse les règlements obtenus et présentent les choix à l'utilisateur. Cela implique que les choix offerts à l'utilisateur soit d'une complexité limitée. Il est ensuite nécessaire que l'utilisateur soit assisté pour transformer ses interactions et ses choix en règles de contrôle d'accès constituant le règlement local. Lors des négociations successives, lorsque l'agent de négociation détermine qu'une règle du règlement local peut être appliquée pour un règlement reçu, ou une partie de celui-ci, il s'appuie sur l'algorithme de négociation pour conduire la négociation. Lorsqu'aucune règle du règlement local n'est configurée pour satisfaire une règle du règlement reçu, l'utilisateur est sollicité.

8. trad. Negotiation manager.

Il est possible de découper en quatre points les principales fonctionnalités requises de l'environnement de négociation de l'utilisateur :

1. Mener une analyse pertinente des sources d'informations. Il est nécessaire de permettre à l'utilisateur d'ajouter ses sources potentielles d'informations et d'établir de nouvelles sources d'informations à partir de négociations de confiance. Il s'agit ensuite de déterminer quelles sont les informations fournies par ces sources et le type de certificat employé (donc ses propriétés).
2. Assister l'utilisateur dans la transformation de ses choix en un règlement formalisé en un langage interprétable par un module de négociation automatisé. Nous appellerons ce règlement, le « règlement local » de l'utilisateur.
3. Déterminer les sources du fournisseur qui font partie du domaine de confiance de l'utilisateur, c'est-à-dire déterminer les certificats que l'utilisateur peut obtenir. Il s'agit au cours d'une négociation de le conseiller sur la confiance qu'il peut avoir en son interlocuteur et sur les moyens d'augmenter celle-ci en requérant les certificats les plus pertinents. (Cela signifie également que l'utilisateur puisse évaluer la confiance qu'il a dans les générateurs de son domaine de confiance.)
4. Analyser les règlements fournis par les fournisseurs afin de déterminer quelles sont les sources qui peuvent y répondre par leur appartenance au domaine de confiance fournisseur, en tenant compte des choix de l'utilisateur et du règlement local enrichi lors des négociations précédentes.

Dans la suite de ce chapitre nous illustrons l'emploi des technologies de la négociation de confiance automatisée pour réaliser un cas d'étude de cette proposition.

VI.3 Détermination des outils

Au sein de cette section, nous étudions les travaux scientifiques des domaines du contrôle d'accès et des négociations de confiance automatisée afin de déterminer ceux qui vont nous servir à illustrer l'automatisation des choix de l'utilisateur.

VI.3.1 Contrôle d'accès

Nous avons jusque-là parlé à plusieurs reprises d'identité et d'établissement d'une identité. Il est cependant nécessaire de préciser à nouveau ces notions pour le contrôle d'accès. Le contrôle d'accès vise à attribuer des droits à un sujet sur un objet. Le *sujet* résulte de l'établissement d'une identité (Benantar, 2005). Or il est important de noter que même si un des interlocuteurs n'apporte pas la preuve d'une identité existante, ou qu'il ne présente pas un identifiant particulier, un pseudonyme par exemple, il se verra tout de même créer un *principal* le temps de la négociation. Le *principal* est un terme qui désigne la représentation temporaire d'une identité au sein du processus de contrôle d'accès (Benantar, 2005). Tout accès contrôlé donne donc lieu à l'établissement de cette identité temporaire, mais peut également se concrétiser par une identité durable par l'audit et l'enregistrement de ses actions auprès du système. Le *principal* est l'entité qui se voit attribuer le pouvoir de mise en œuvre des droits d'accès au sein du système.

Une architecture de contrôle d'accès repose en son cœur sur un moniteur de référence (Lampson, 1974), en charge de contrôler tous les accès. Il s'appuie pour cela sur des règles de contrôle d'accès issues de multiples règlements qui forment la politique de contrôle d'accès d'un domaine de sécurité représenté par l'ensemble des ressources à la charge du moniteur de référence. La politique de contrôle d'accès respecte généralement un modèle. Celui-ci, s'il est précis, voire formel, permet d'analyser et de raisonner sur le comportement de l'implémentation, et de vérifier de manière formelle les propriétés de cette politique. L'implémentation d'une politique de contrôle d'accès se fait au travers de mécanismes de contrôle d'accès.

Plusieurs types de contrôle d'accès ont été modélisés. Citons les modèles de contrôle d'accès initiaux : le modèle discrétionnaire[9] (DAC) et le modèle par mandat[10] (MAC). Le premier se base principalement sur la possession de ressources, donc sur les identités qui les possèdent. Le second repose sur la définition de niveaux de contrôle d'accès attribués aux ressources et aux sujets, donc sur l'autorisation d'accès lorsque les niveaux sont en correspondance avec la politique définie. Le troisième modèle, sans doute le plus connu et

9. trad. Discretionnary Access Control
10. trad. Mandatory Access Control

le plus répandu, est le contrôle d'accès basé sur les rôles[11] (RBAC) (Sandhu *et al.*, 1996), mais il ne peut être comparé aux deux premiers. Il consiste en l'attribution de droits par des règlements, non pas à des sujets mais à des rôles. Les sujets sont ensuite associés à un ou plusieurs rôles leur permettant ainsi d'acquérir des droits. RBAC est considéré d'un niveau d'abstraction supérieur à DAC et à MAC. Cela permet notamment de réaliser un contrôle d'accès RBAC en reposant sur un contrôle d'accès effectif par MAC ou par DAC (Osborn, 1997 ; Osborn *et al.*, 2000).

RBAC s'avère efficace lorsqu'il s'agit d'implémenter une politique de contrôle d'accès alors que les identités des sujets ne sont pas préalablement connues aux accès. En d'autres termes, il est possible de définir les règles de contrôle d'accès à des ressources en attribuant des droits à des rôles sans connaître les sujets qui les exploiteront. L'association des sujets à des rôles peut se faire dans un second temps, ce qui répond à notre besoin. En effet, il doit être possible d'attribuer des droits à des sujets qui ne sont connus du système que lors d'une requête d'accès, et éventuellement leur attribuer des droits qu'ils peuvent ne jamais ré-exploiter dans une nouvelle session. Notre étude suppose donc que les droits soient attribués en fonction des informations, notamment certifiées, présentées par une entité. Il s'agit donc d'associer des rôles à une entité selon ces informations, donc de lui attribuer des droits selon une politique de contrôle d'accès prédéfinie.

Les certificats présentés sont synonymes de l'attribution de droits. Il est possible de considérer que l'identité locale au moniteur de référence est « construite » par les multiples informations présentées. De multiples rôles peuvent ainsi être associés au porteur au fur et à mesure de la présentation de certificats. Inversement, les requêtes d'accès peuvent être retranscrites en droits requis pour obtenir ces accès, donc en certificats qu'il est nécessaire de fournir. Enfin, les informations présentées peuvent être des droits d'accès dans une organisation qui serait celle du générateur. Ces « droits certifiés » peuvent ainsi être pris en considération dans le contrôle d'accès du consommateur comme n'importe quel autre information certifiée. Cela soulève cependant la problématique d'interopérabilité des politiques de sécurité que nous n'adressons pas dans ces travaux. Notons simplement que nous préférerons, dans la mesure du possible, la fourniture d'informations certifiées permettant au consommateur d'attribuer des droits, à la présentation de droits que l'entité possède au sein d'organisations tierces de celle du consommateur. Nous faisons cette remarque du fait qu'il paraisse intuitif que la décision de contrôle d'accès revienne au consommateur, donc que l'obtention d'une autorisation certifiée ne soit qu'une application particulière de l'utilisation de certificat, l'application de délégation du contrôle d'accès.

Les travaux de Blaze (Blaze *et al.*, 1996a) introduisent le contrôle d'accès basé sur des

11. trad. Role-Based Access Control

informations provenant de tiers. La notion de domaines de sécurité distincts, permettant ainsi de traiter les problématiques inter-organisationnelles, est mise en lumière. Cela justifie l'idée que les informations sont issues de tiers de confiance, d'où l'introduction du terme « gestion de la confiance[12] ». Dans ce système, l'utilisateur présente au système hébergeant la ressource qu'il requiert une autorisation issue d'un domaine de sécurité distinct. Il s'agit donc plus d'une délégation du contrôle d'accès que d'un système permettant l'attribution de droits en fonction d'informations issues de tiers de confiance. PolicyMaker (Blaze *et al.*, 1996b) et Keynote (Blaze *et al.*, 1999) sont deux systèmes qui résultent de ces travaux et offrent un langage d'expression des certificats et des règlements ainsi qu'une architecture d'implémentation intégrant un vérificateur[13]. La différence principale entre les deux est que le second intègre la vérification des signatures des certificats dans l'architecture dédiée à la gestion de la confiance. Ces deux architectures reposent sur le fait que c'est l'application qui gère l'accès à la ressource, selon les recommandations émises par les implémentations de l'architecture de gestion de la confiance. Celles-ci n'ont donc pas la charge d'assurer l'application des règlements du contrôle d'accès. Le système de gestion de la confiance REFEREE offre des possibilités de contrôle plus riches en intégrant le contrôle par règlement, le contrôle des règlements et la vérification des certificats. En d'autres termes, toutes les informations évaluables peuvent être décrites et analysées par des règlements, de même que le fonctionnement du système.

Sont ensuite arrivés plusieurs systèmes proposant d'associer des rôles en fonction d'attributs présentés au sein de certificats. Or, comme il est possible de considérer toutes les informations présentées comme des attributs de l'identité locale au moniteur de référence, les systèmes de contrôles d'accès basés sur les attributs[14] (ABAC) se sont développés en se basant sur RBAC. Citons notamment SDSI (Ellison *et al.*, 1999) et la logique de délégation[15] (DL) (Li *et al.*, 2003) qui sont considérés comme de la délégation basée sur des attributs. Bien que la sensibilité des règlements et des attributs soit établie et traitée, il leur manque cependant la notion d'échanges mutuels d'informations où l'information présentée est une ressource dont l'accès est contrôlé par d'autres informations. La notion d'établissement graduel de la confiance n'est pas traitée ce qui justifie la distinction de ces systèmes avec ceux des négociations de confiance.

Pour conclure, il existe différents systèmes de gestion de la confiance avec leurs propres langages d'expression des règlements et des certificats. Ceux-ci permettent de réaliser un contrôle d'accès appelé ABAC reposant sur RBAC. Les concepts de gestion de la confiance vont constituer le socle sur lequel vont reposer les systèmes de négociations de confiance

12. trad. Trust Management
13. trad. Compliance checker.
14. trad. Attribute-Based Access Control
15. trad. Delegation Logic.

qui y ajoutent les dimensions de négociation et d'automatisation.

VI.3.2 Négociations de confiance

Les premières approches ont supposé que l'initiateur produisait une requête accompagnée des certificats nécessaires pour satisfaire les conditions du contrôle d'accès de cette requête. De nouvelles études ont intégré l'idée de règlements délivrés aux interlocuteurs au cours du processus de contrôle d'accès, faisant du processus de contrôle d'accès une négociation potentielle.

Le système de négociation s'apparente donc à une « sur-couche » au contrôle d'accès des ressources, des certificats, des informations personnelles et des règlements. Les négociations de confiance, avec l'introduction d'algorithmes pour leur automatisation, ont été introduites par (Winsborough *et al.*, 2000). Le sujet a ensuite été largement traité, aussi bien pour présenter de nouveaux algorithmes (Yu *et al.*, 2000 ; Li & Winsborough, 2002 ; Winsborough & Li, 2002) que pour prouver certaines de leurs propriétés (Seamons *et al.*, 2001 ; Winsborough & Li, 2006) ou bien encore pour définir des langages et des modèles de contrôle d'accès (Li *et al.*, 2001, 2002).

VI.3.2.1 Langages et systèmes de négociation

Un ensemble de propriétés attendues d'un langage employé dans un système de négociation de confiance a été défini (Seamons *et al.*, 2002 ; Bertino *et al.*, 2004). Nous reprenons ici les propriétés qui nous semblent les plus importantes et ajoutons celles requises à la vue de l'étude menée jusqu'ici.

1. **Une sémantique définie.** Cela induit que lorsque l'un des interlocuteurs détermine qu'une information satisfait à un règlement de l'autre partie, cette dernière accepte aussi cette information comme satisfaisante. Cela englobe la sémantique employée pour les certificats et leur contenu.
2. **Monotonicité.** Un langage doit être monotone, ce qui implique que l'apport de nouvelles informations satisfaisant des règles exprimées ne peut que se traduire par des droits octroyés supplémentaires. Cela implique que la non-présentation d'une information correspond à une propriété de cette information. Par exemple, ne pas montrer son certificat indiquant le nombre de points sur le permis est équivalent à ne plus avoir de points sur son permis.
3. **Combinaison de certificats.** Il faut pouvoir indiquer que plusieurs certificats de sources différentes doivent être présentés conjointement.
4. **Expression des attributs.** Exprimer l'information requise en considérant que les certificats sont des objets structurés dont les attributs sont définis par un nom et

une valeur. Chaque attribut possède également un type qui, à l'aide d'une ontologie commune, permet d'interpréter le sens et la syntaxe des attributs. Notons que cette ontologie peut également contribuer à bâtir un référentiel des propriétés prouvables sur des attributs.

5. **Chaînes de certifications.** (cette recommandation diffère de ce qui est indiqué dans les références dont ces propriétés sont extraites) Il s'agit de permettre à un consommateur d'indiquer des contraintes sur l'appartenance des sources à son domaine de confiance. Il peut indiquer directement un générateur. Il peut également indiquer une autorité dans une chaîne de certification permettant ainsi au porteur de pouvoir obtenir un certificat de n'importe quelle autorité de rang inférieure. Il s'agit par exemple d'indiquer que le certificat est accepté si le générateur, qui est une banque, fait partie d'une chaîne de certification dans laquelle est contenue l'autorité nationale des banques françaises. Il est en fait possible de concevoir deux types de chaîne de certifications : dans le style des infrastructures à clés publiques « classiques » ou par échange de certificats. La première solution repose sur le fait que le consommateur « remonte » la chaîne de certification par vérifications successives des certificats à clés publiques des autorités. La seconde suppose que le porteur obtienne des certificats par des échanges successifs tout au long de la chaîne jusqu'à l'obtention du certificat du générateur approprié. Ce mécanisme est appelé « découverte des chaînes de certificats » (Li *et al.*, 2001) et peut englober les chemins de certification des infrastructures à clés publiques.
6. **Fonctions externes.** Il existe dans les règlements plusieurs opérations logiques ou mathématiques. Il est donc nécessaire que les parties s'accordent sur celles-ci.
7. **Établissement de l'identité.** (cette recommandation diffère de ce qui est indiqué dans les références dont ces propriétés sont extraites) Il s'agit ici de pouvoir indiquer les conditions de l'établissement d'une identité ou que celui-ci est requis. Ces besoins sont les mêmes pour la présentation d'un alias. Enfin, il doit être possible d'indiquer si une pièce d'identité est requise, si elle doit être anonyme et donc révocable.
8. **Sources de certificats.** Il s'agit d'indiquer si certains certificats sont à obtenir d'un tiers autre que le tiers négociateur.
9. **Sensibilité des règlements diffusés.** Des fragments de règlements sont diffusés à l'interlocuteur pour lui indiquer les conditions qu'il doit satisfaire. Ces fragments peuvent être vus comme de multiples règlements dont certains sont sensibles. Il est donc nécessaire de pouvoir contrôler leur libération comme n'importe quelle ressource.
10. **Objet de la négociation.** (cette recommandation diffère de ce qui est indiqué dans les références dont ces propriétés sont extraites) Il doit être possible de retarder la déclaration de l'objet de la négociation en obtenant au préalable des certificats.

Nous appelons par la suite agent de négociation l'ensemble de l'environnement de négociation d'une entité. Cet agent possède ainsi un module de vérification des règlements[16] et peut également assumer le rôle de moniteur de référence. Il a la charge de vérifier :

- la syntaxe et la cohérence du règlement,
- le respect du règlement local par les certificats obtenus,
- le respect du règlement par les générateurs à disposition,
- la validité des certificats (vérification de la possession des certificats, exécution des protocoles de preuve de connaissance, donc vérification des conditions sur les attributs et vérification des conditions de date, du nombre d'utilisations et de la non-révocation),
- les conditions de non-transférabilité,
- les chaînes de certification.

L'agent a la charge éventuelle de gérer les divers algorithmes de négociation et les interactions de l'utilisateur pour que celui-ci prenne les décisions importantes de délivrance d'information.

Voici une revue non exhaustive des langages et systèmes de négociation majeurs :

1. Keynote (Blaze *et al.*, 1999) est le langage le plus connu pour la gestion de la confiance. Keynote se prête bien à la délégation d'autorisations. Cependant, il convient mal à la déclaration d'attributs, attributs sur lesquels on souhaite que les consommateurs basent les autorisations.
2. Le projet TE est un système de négociation reposant sur le langage TPL (Herzberg *et al.*, 2000). Le langage TPL exploite un contrôle d'accès basé sur les rôles attribués en fonction des certificats présentés. Ce langage répond à la majeure partie des conditions énoncées précédemment. Cependant, il n'adresse ni la sensibilité des certificats, ni celle des règlements. La délivrance des certificats est supposée automatique dès que ceux-ci sont requis. Il existe une fonctionnalité appelée « collecteur de certificats », couplée au vérificateur, qui a d'une part la charge de remonter les chemins de confiance et d'autre part celle de collecter l'ensemble des certificats d'une entité. Il suffit à celle-ci de donner un premier certificat qui indique un « dépôt » de certificats en ligne. Ce composant est au cœur du système ce qui diffère donc totalement de la vision « centrée sur l'utilisateur » en allant à l'encontre des principes de la non-associativité des transactions.
3. Le langage PSPL introduit par (Bonatti & Samarati, 2002b) ne traite pas des chaînes de certificats mais permet de gérer la sensibilité des règlements et de les traiter comme des ressources.

16. trad. Compliance checker.

4. (Yu & Winslett, 2003b) présente un méta-langage visant à satisfaire le besoin de contrôler les règlements comme des ressources sensibles. L'appellation méta-langage vient du fait qu'il sert à formaliser certaines propriétés en adaptant les règlements écrits à l'aide d'autres langages.
5. ATNL (Li *et al.*, 2005a) est un langage basé sur le langage RT (Li *et al.*, 2001), lui-même issu de la logique de délégation (Li *et al.*, 2003). Le langage ATNL offre les fonctionnalités du langage RT et y ajoute le traitement de certaines propriétés attendues des certificats anonymes. Le langage ATNL permet notamment de décrire un contrôle d'accès indépendamment sur chacun des attributs contenus dans un même certificat, ainsi que le fait de pouvoir exprimer les contraintes sur les attributs afin de mener des preuves. Le langage RT est conçu pour faire un contrôle d'accès par rôles attribués en fonction d'attributs certifiés. En outre, il répond à une grande partie des pré-requis précédemment énoncés.

Des comparatifs de ces langages sont présentés dans (Seamons *et al.*, 2002) et (Bertino *et al.*, 2004). Le langage ATNL semble un bon candidat puisque le langage RT répond à chacune des propriétés (hormis celles que nous avons introduites). De plus, ce langage est simple d'accès. En outre, il est présenté en syntaxe BNF, ce qui rend possible une sérialisation simple en XML. Notons cependant qu'aucun langage ne satisfait actuellement toutes les propriétés énoncées. Le critère de choix de langage que nous considérons comme le plus important est celui relatif aux propriétés d'établissement d'une identité et de non-transférabilité. Il doit par exemple être possible d'exprimer :

- la nécessité de présenter un alias, un pseudonyme et une pièce d'identité,
- la reconnaissance d'un pseudonyme,
- que les certificats doivent être liés par un secret maître régi par un gage.

Il s'avère donc que le langage ANTL possède l'expressivité suffisante pour poursuivre notre étude.

VI.3.2.2 Algorithmes

De nombreux travaux ont été menés pour mettre en œuvre des systèmes de négociation efficace et sûre entre deux agents de négociation autonomes. Il existe des travaux traitant des probabilités de succès d'une négociation pour deux stratégies de négociation identiques ou lorsque les stratégies de négociation diffèrent, alors classées en familles (Yu *et al.*, 2003). Cependant, les interactions de l'utilisateur avec le système sont toujours traitées en préalable à la négociation pour la configuration des règles de contrôle d'accès de son règlement local. En d'autres termes, rien ne stipule l'analyse des choix et des interactions de l'utilisateur dont découlerait la configuration de règles de contrôle d'accès. (Seamons *et al.*, 2002) stipule pourtant la nécessité d'une interface homme machine

conviviale pour la capture et la maintenance des règlements comme l'un des pré-requis à un système de protection de ressources. Il résulte de ces travaux la volonté d'établir un langage simple qui pourrait être implémenté à partir d'une interface d'administration, et la possibilité de définir un règlement écrit avec un autre langage à l'aide de celui-ci. Il est cependant possible de supposer que les négociations restent menées par un agent de négociation qui ne tient pas compte des interactions utilisateurs. Les interactions utilisateurs en cours de négociation de confiance pour l'approvisionnement d'un règlement local ne sont donc traitées, à notre connaissance et à ce jour, dans aucune publication. Nous proposons donc d'utiliser les règles de contrôle d'accès du règlement local de l'utilisateur comme des règles d'automatisation.

L'humain est en quelque sorte un algorithme de négociation non-déterministe qui doit interopérer avec les algorithmes déterministes employés par les machines. Un algorithme de négociation peut avoir diverses propriétés. Certaines d'entre elles ont été étudiées et formalisées, par exemple dans (Yu *et al.*, 2003). Les négociations de confiance ont notamment été modélisées pour étudier leur propriété de complétude. Cette propriété implique que si une négociation peut être menée avec succès, les algorithmes employés sont complets et interopérables, si la négociation est toujours conduite avec succès. Or, l'utilisateur fait des choix non-déterministes. Il peut décider à n'importe quel moment, sans raison apparente, de ne pas mener à terme la négociation, donc de ne pas satisfaire à cette propriété. Il est donc difficile de travailler sur le choix d'un algorithme de négociation qui pourrait s'allier à l'utilisateur et ensuite de définir les propriétés d'un tel système. Ceci étant dit, nous présentons ici brièvement les algorithmes de négociation les plus connus afin d'en sélectionner un pour l'étude de la prochaine section. Notons que l'algorithme de négociation représente par nature les échanges entre les parties négociatrices et constitue donc le protocole de la négociation. La formalisation du protocole de négociation et de ses propriétés peut donc s'appuyer sur celle de l'algorithme duquel il est issu. Pour permettre la mise en œuvre d'une négociation, il sera nécessaire de retranscrire l'algorithme en messages protocolaires et ensuite de sérialiser ces messages comme cela est présenté au chapitre 8.

(Winsborough *et al.*, 2000) présente deux stratégies de négociation relativement simples intitulées EAGER et PARSIMONIOUS. (Yu *et al.*, 2000) propose la stratégie PRUNES. Ont ensuite été présentées les stratégies tenant compte de la sensibilité des règlements. Citons PolicyGraph (Seamons *et al.*, 2001) qui consiste à créer un graphe dont le sommet d'arrivée est unique : il s'agit de l'objet de la négociation. Les nœuds du graphe sont des règlements, ce qui fait de la racine du graphe un règlement non sensible. Les liens représentent la satisfaction d'un règlement. (Li & Winsborough, 2002 ; Winsborough & Li, 2002, 2006) présentent TrustTargetGraph (TTG) bâti sur le même principe. Enfin, TTG a été étendu en ETTG afin de fonctionner avec le langage ATNL (Li *et al.*, 2005a).

Nous considérons cette dernière stratégie comme la plus aboutie, bien que simple d'accès par sa représentation en graphes. Elle est en outre suffisamment riche pour pouvoir étudier le comportement possible de l'utilisateur face à cet algorithme.

VI.4 Mise en œuvre

VI.4.1 Système de négociation

Nous proposons la représentation fonctionnelle de l'environnement utilisateur dédié à la négociation illustrée à la figure VI.4. Il s'agit ici de mettre en lumière un module central dédié à la stimulation de l'utilisateur pour obtenir des décisions, les analyser et les traduire en règles de contrôle d'accès. Ce module prend la place centrale qu'occupe habituellement le module d'analyse des règlements et d'application de stratégie. La charge d'analyse du règlement local est désormais attribuée au module d'analyse des décisions utilisateurs. Ces deux modules pourraient être vus comme un seul, mais la distinction permet d'illustrer les fonctionnalités supplémentaires nécessaires pour gérer les interactions utilisateurs. Ces deux modules ont donc la charge de l'automatisation grâce à l'analyse et à la mise en œuvre des décisions de l'utilisateur.

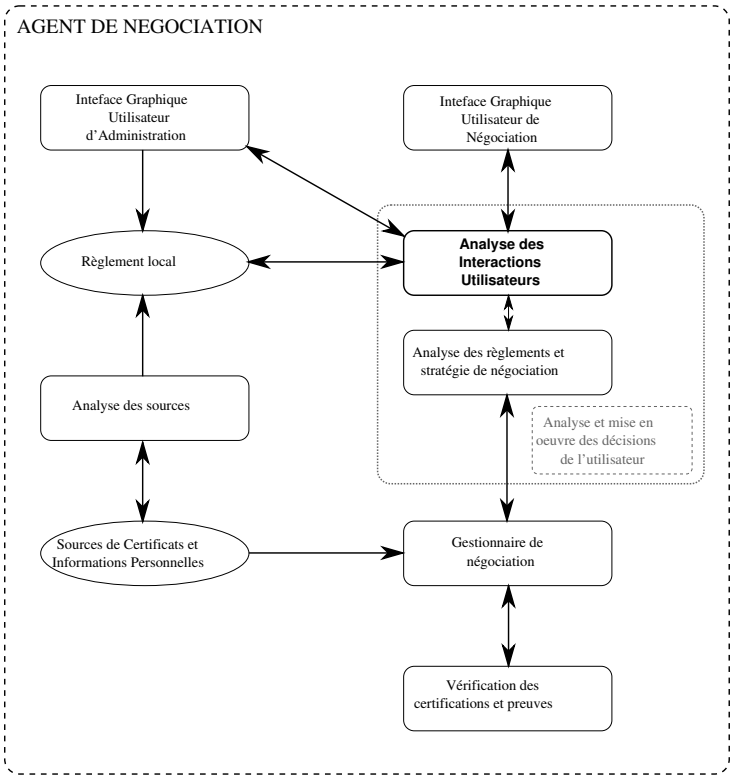

FIG. VI.4 – *Représentation fonctionnelle de l'agent de négociation centré sur les interactions utilisateurs.*

VI.4.2 Analyse des sources

Chacun des négociateurs a ses propres sources de certificats. Il est nécessaire que chaque partie puisse déterminer qu'elles sont les générateurs qui vont lui permettre d'obtenir les

certificats satisfaisant aux règlements de son interlocuteur. Un générateur source peut être approprié selon les informations qu'il fournit et selon le fait qu'il appartienne au domaine de confiance du consommateur.

Une part de la tâche consiste donc en l'analyse de ce que les générateurs fournissent. Pour cela, il est supposé une phase de déclaration d'une source d'information où le générateur indique, au sein d'un règlement, le détail de ce qu'il est à même de fournir. Ce règlement peut également contenir le règlement de contrôle d'accès aux certificats. L'obtention des certificats peut également être sujet à négociation. Dans ce cas, cela implique que les conditions du contrôle d'accès ne sont pas connues à l'avance par le porteur éventuel. Il est cependant possible de supposer que dans la grande majorité des cas, un générateur nécessite uniquement l'établissement de l'identité du porteur pour lui délivrer des certificats.

Un ensemble de tiers de confiance peut être publiquement connu (l'État, les banques, les notaires, les employeurs, etc.). Un générateur peut également être déclaré comme source suite à une négociation de confiance avec celui-ci.

Un générateur doit indiquer les informations qu'il est à même de fournir dans un certificat. Le règlement indiquant cela peut être considéré comme l'ensemble des méta-données des certificats, c'est-à-dire décrivant le contenu potentiel des certificats. Les méta-données indiquent le type de certificat (par exemple X509 ou CL-Signature) et ses attributs (par exemple le nom du générateur, la durée de validité, le nombre d'utilisation, le format, l'encodage, etc.). Elles indiquent également les attributs d'identité (dénomination, format, etc.). Il est possible de considérer, sauf restriction particulière, qu'un certificat peut être obtenu sur n'importe quel sous-ensemble d'attributs de l'ensemble d'attributs offerts par un générateur. La problématique des méta-données des générateurs et de la sérialisation des certificats sera précisée section VIII.4.2.2.

Il est notamment important de déterminer quels générateurs fournissent des certificats anonymes et quels sont les engagements possibles. L'analyse des sources comprend donc une phase importante qui consiste à déterminer, sur un attribut, quelles propriétés il est possible de prouver. Notons alors deux possibilités, utilisables indépendamment ou conjointement, envisageables afin de déterminer quels engagements il est possible de mener pour prouver des propriétés sur les attributs. Notons qu'il doit pour cela être possible de bâtir un référentiel des propriétés prouvables sur des attributs sur lequel s'appuyer.

Précisons quelques rudiments du langage ATNL (Li *et al.*, 2005a). Au sein d'un règlement en langage ATNL, la déclaration des sources constitue la première partie d'un tel

règlement. Un ensemble de « principaux » est représenté par un « rôle »[17]. Ainsi, de l'analyse des sources de certificats résulte un ensemble de rôles exprimés sous la forme d'un générateur suivi du rôle que le certificat permet d'obtenir sur les consommateurs :

$$Generateur.Role \tag{VI.1}$$

Cela suppose que dès l'analyse des sources, il soit possible de présumer des rôles qu'un certificat permette d'obtenir sur les éventuels consommateurs. Il est aussi possible d'interpréter cela comme la dénomination locale du certificat pour une utilisation dans les règles du règlement. Nous préférerons cette deuxième approche même si dans ce cas d'étude nous nous prêtons au jeu de l'attribution de rôle à la lecture des sources qui permet une étude de cas plus explicite. En outre, la première approche ne met pas en lumière un générateur comme une source de multiples certificats de types différents. Voici l'exemple d'un certificat issu du générateur $TelecomSaintEtienne$ qu'il est possible d'interpréter comme une « carte d'étudiant » ou le rôle « étudiant » qu'il est possible d'établir sur les consommateurs :

$$TelecomSaintEtienne.etudiant \tag{VI.2}$$

L'entité pour laquelle les sources sont déclarées est représentée par un alias la désignant localement. Elle est ainsi déclarée comme pouvant obtenir ces rôles par des « relations d'appartenance » :

$$TelecomSaintEtienne.etudiant \longleftarrow Mikael \tag{VI.3}$$

Il est également possible de représenter une chaîne de certification par une « une relation de délégation » ou un « certificat de délégation[18] » (qui peut être employé pour la délégation de tâches administratives) :

$$\begin{aligned} InstitutTelecom.etudiant &\longleftarrow TelecomSaintEtienne.etudiant \\ TelecomSaintEtienne.etudiant &\longleftarrow Mikael \end{aligned} \tag{VI.4}$$

VI.4.3 Automatisation de l'établissement d'identité

Nous considérons un utilisateur dans le rôle de l'initiateur. Étudions dans un premier temps ce qu'il est possible d'automatiser concernant l'établissement d'une identité.

Lorsque l'initiateur reconnaît le pseudonyme du fournisseur, il est possible d'établir automatiquement un pseudonyme déjà employé auprès du fournisseur ou de demander un acquittement à l'utilisateur. S'il s'agit d'une génération de pseudonyme, il n'y a pas lieu de

17. Terminologie de la contribution.
18. trad. Delegation credential

demander l'aval de l'utilisateur car cela ne constitue pas une information sensible puisque le pseudonyme est inassociable donc ne révèle aucune information.

En d'autres termes, lorsqu'un pseudonyme est réutilisé il s'agit de révéler une information sensible, donc cela peut exiger des conditions de contrôle d'accès et par conséquent de négocier. Ainsi, lorsqu'un pseudonyme doit être fourni à un fournisseur pour la première fois, il est possible de demander à l'utilisateur s'il veut en créer un nouveau ou s'il souhaite utiliser un pseudonyme déjà utilisé par ailleurs. Rappelons que nous avions qualifié l'emploi d'un même pseudonyme avec plusieurs interlocuteurs de pseudonymat public, cela afin de bâtir un domaine de réputation. La négociation de l'établissement d'un pseudonyme suppose l'obtention de certificats. Il est donc possible d'automatiser cette demande de certificat, par exemple en demandant automatiquement toujours les mêmes certificats à ce fournisseur. Si les certificats demandés peuvent être « généralisés », par exemple au type « certificats quelconques », cette règle peut toujours être appliquée, quel que soit le fournisseur. Ainsi, à chacune des demandes de certificats à un fournisseur, il est possible d'automatiser cette demande, soit spécifiquement pour ce fournisseur, soit en généralisant à plusieurs ou à tous les fournisseurs. La généralisation suppose que l'agent soit susceptible de pouvoir généraliser une demande d'information.

Lorsque l'utilisateur prend une décision, il est intéressant de savoir sur quels éléments, pouvant entrer dans sa décision, nous pouvons influer. Il est envisageable de présenter à l'utilisateur des « indicateurs de confiance », c'est-à-dire des indications sur l'état de la négociation. Par exemple, si le pseudonyme du fournisseur n'est pas reconnu et que l'utilisateur veut utiliser un pseudonyme déjà employé ailleurs, il s'agit d'une situation sensible. Il s'agira donc de signaler à l'utilisateur cela et qu'il est important de demander des certificats au fournisseur pour confirmer la confidentialité du canal et augmenter la confiance en ce tiers. Il est possible d'automatiser ce comportement s'il est possible de généraliser les certificats requis. Si le pseudonyme du fournisseur est reconnu, la confidentialité n'est plus un problème, il s'agit donc de demander des certificats pour augmenter la confiance en ce tiers, ou de satisfaire à des conditions de contrôle d'accès pré-existantes. De manière générale, si l'utilisateur établit un nouveau pseudonyme, ce n'est pas une opération sensible dans le sens où aucune information associable n'est révélée. La négociation doit apporter la confiance nécessaire dans l'interlocuteur, et par conséquent se traduire par une réutilisation éventuelle du pseudonyme. Si la négociation n'aboutissait pas sur une relation de confiance, le pseudonyme ne serait pas réutilisé.

Intéressons-nous maintenant à la transcription en langage ATNL des principales règles précédemment présentées. Au sein d'un règlement en ATNL, les règles de contrôle d'accès sont déclarées après la déclaration des sources.

L'objet d'une règle, c'est-à-dire l'accès permis lorsque cette règle est satisfaite, peut être l'obtention d'un rôle ou la délivrance de ressources. L'alias de l'entité désigne le *principal* du rôle et l'instruction de libération d'une ressource est notée *disclose*. Ce prédicat prend en argument le type de délivrance et l'objet. Par exemple, pour un pseudonyme, le type de délivrance sera $full$. Vient ensuite la règle séparée par une flèche. La règle est une combinaison de rôles, représentée par une intersection d'ensembles. Autrement dit, c'est une combinaison d'informations à présenter pour satisfaire la règle de contrôle d'accès. Une règle pouvant être sensible, il est possible d'appliquer une règle régissant sa présentation. Cette règle est appelée « pré-condition [19] ». La règle et sa pré-condition sont séparées par un point d'exclamation. Voici la syntaxe d'une règle pour l'attribution d'une relation d'appartenance, soit l'attribution d'un rôle à l'interlocuteur, avec un rôle noté $G.R$ et $\bigcap_{i=0}^{n} G_i.R_i$ l'intersection de plusieurs rôles :

$$G.R \longleftarrow \bigcap_{i=0}^{n} G_i.R_i \ ! \ \bigcap_{j=0}^{n} G_j.R_j \tag{VI.5}$$

Lorsque des conditions sont appliquées sur les certificats et les attributs d'une règle, une seconde règle, séparée par un point-virgule, est indiquée afin de préciser ces conditions; elle peut elle-aussi être sujette à une pré-condition :

$$\begin{aligned} G.R \longleftarrow & \bigcap_{i=0}^{n} G_i.R_i \ ! \ \bigcap_{j=0}^{n} G_j.R_j \ ; \\ & \bigcap_{i=0}^{n} G_i.R_i \ ! \ \psi(x_1,...,x_n) \end{aligned} \tag{VI.6}$$

Pour exprimer que le pseudonyme du fournisseur est reconnu, nous utilisons un rôle qui est attribué par une primitive externe qui s'appuie sur l'historique des négociations. Nous supposons dans cet exemple que l'automatisation de l'établissement d'un pseudonyme déjà utilisé avec un même fournisseur puisse être requise. La règle pour indiquer cela sans autre condition est :

$$\begin{aligned} disclose(full, dernierPseudonyme) \longleftarrow \ & Initiateur.estPseudoReconnu(val = x); \\ & x = true \end{aligned} \tag{VI.7}$$

19. trad. Pre-conditions

S'il est possible de généraliser la demande d'un certificat, ou d'un ensemble de certificats pour cet établissement, la règle peut être modifiée en :

$$disclose(full,dernierPseudonyme) \longleftarrow \bigcap_{i=0}^{n} G_i.R_i \; ! \; Initiateur.estPseudoReconnu(val = x); \\ x = true \tag{VI.8}$$

Cette règle peut aussi être restreinte à certains fournisseurs dont les pseudonymes sont déclarés au sein du règlement :

$$disclose(full,dernierPseudonyme) \longleftarrow Initiateur.estFournisseur(val = y); \\ y ='' \; pseudonymeFournisseur \; '' \tag{VI.9}$$

Notons que le moteur d'analyse du règlement ne devrait pas appliquer cette règle si celle d'automatisation de l'établissement d'un pseudonyme s'appliquant de manière générale est configurée.

Cette même règle avec la requête d'un ensemble de certificats en préalable :

$$disclose(full,dernierPseudonyme) \longleftarrow \bigcap_{i=0}^{n} G_i.R_i \; ! \; Initiateur.estFournisseur(val = y); \\ y ='' \; pseudonymeFournisseur \; '' \tag{VI.10}$$

Si un fournisseur n'est pas reconnu, il est possible d'automatiser l'utilisation d'un nouveau pseudonyme :

$$disclose(full,nouveauPseudonyme) \longleftarrow Initiateur.estPseudoReconnu(val = x); \\ x = false \tag{VI.11}$$

Pour le fournisseur, les besoins sont similaires. Si l'établissement de son pseudonyme public est sensible, il est conditionné par un ensemble de règles et le fournisseur commence en diffusant un pseudonyme à usage unique. Cependant, l'établissement d'un pseudonyme public n'est généralement pas déclaré dans une requête de l'initiateur. L'utilisateur requiert plutôt un objet qui nécessite un établissement de compte, ce qui signifie implicitement l'établissement d'un pseudonyme public par le fournisseur. Les conditions de l'établissement d'un pseudonyme public se retrouvent donc au sein de règlements d'autres ressources contrôlées. Elles doivent cependant indiquer lorsqu'il doit être établi un pseudonyme public. La problématique est similaire pour la création de compte. Il ne s'agit pas d'une requête particulière de l'utilisateur. Simplement, le fournisseur peut déduire de la requête qu'il peut personnaliser les négociations dès lors que cet accès est donné. Il demande alors un pseudonyme à l'utilisateur pour lui associer cette négociation. Il peut

également requérir des informations supplémentaires pour accepter de délivrer ce premier accès. Ainsi, certaines règles de contrôle d'accès dépendent du fait qu'un pseudonyme initiateur soit reconnu ou non. C'est notamment le cas de la requête d'accès à un compte explicite de la part de l'utilisateur. Notons que, d'une requête d'accès à un compte suivie de l'établissement d'un pseudonyme par l'initiateur qui n'est pas reconnu, le fournisseur peut déduire un objet « création de compte ». Voici par exemple les conditions pour établir un compte :

- si le pseudonyme initiateur est reconnu :

$$Fournisseur.CompteEtabli \longleftarrow Fournisseur.estPseudoReconnu(val = x); \quad x = true \tag{VI.12}$$

- si le pseudonyme initiateur n'est pas reconnu :

$$Fournisseur.CompteEtabli \longleftarrow Fournisseur.estPseudoReconnu(val = x) \cap \bigcap_{i=0}^{n} G_i.R_i; \quad x = false \tag{VI.13}$$

VI.4.4 Automatisation d'une négociation : cas d'usage

Le langage ATNL permet la prise en considération des certificats dits cryptographiques[20]. Entre autre, cela permet d'exprimer les présentations sélectives d'attributs et leurs propriétés. Comme nous l'avions préalablement précisé, nous considérons dans un premier temps qu'un certificat peut être obtenu sur n'importe quel sous-ensemble d'attributs d'identités parmi ceux proposés par un générateur, outre les attributs propres au certificat. Ainsi, dans la partie du règlement dédiée aux sources, nous déclarons des générateurs et les nommons de manière à les désigner localement.

Il est possible que des générateurs ne délivrent qu'un ensemble d'attributs au sein d'un certificat dont l'ensemble a un sens reconnu. Ainsi, en employant la terminologie ATNL, les générateurs peuvent émettre plusieurs types de certificats, donc de rôles. Par exemple, une école d'ingénieurs peut être en charge d'émettre deux types de certificats : les cartes d'étudiants et les diplômes d'ingénieurs. Ces certificats peuvent alors contenir des informations redondantes telles que le nom et le prénom.

La primitive du langage ATNL utilisée pour montrer un certificat sans montrer son contenu est : « commit ». Nous dirons que les attributs contenu dans le certificat sont « engagés ». Il est nécessaire de retranscrire les certificats en langage ATNL selon le schéma de signature employé. Ainsi, un certificat selon le schéma CL-Signature possède à la base tous ses attributs en « engagements ». Il est cependant possible d'envisager que

20. trad. Cryptographic credentials.

l'un des attributs soit toujours montré au consommateur dès que son certificat est montré. Cet attribut n'est alors pas en engagement. A l'inverse, un certificat d'attributs X509 reposant sur un schéma de signature RSA ne voit aucun de ses attributs en engagement.

En outre, montrer un certificat revient à révéler l'information d'« appartenance » du porteur au générateur dans le sens où le porteur possède un certificat de ce générateur. Si ce générateur est associé à un type de certificat, le permis de conduire par exemple, présenter ce certificat signifie être titulaire du permis de conduire. La présentation des attributs et de leur propriétés se trouvent dans une section distincte du règlement.

Les informations personnelles non certifiées peuvent être stockées dans le règlement et être protégées par les mêmes mécanismes ce qui est un moyen de faire du « remplissage automatisé de formulaire ». Prenons l'exemple de certificats délivrés par une école d'ingénieurs où chacun des attributs peut être montré indépendamment ainsi que de l'automatisation de la fourniture d'une adresse électronique non certifiée. Notons que selon la syntaxe ATNL, chaque attribut qui peut être révélé sans contrôle d'accès est noté avec le mot clé « non-sensitive », sinon il est noté avec le mot clé« sensitive », et si aucune règle de contrôle d'accès correspondante n'est stipulée, il n'est jamais diffusé. Nous modifions cette propriété d'interprétation du langage pour que l'absence de règle signifie le besoin d'une interaction requise de la part de l'utilisateur.

Certificates:

InstitutTelecom.etudiant	⟵	TelecomSaintEtienne.etudiant
TelecomSaintEtienne.etudiant(nom=commit('Ates'),annee='2004')	⟵	Initiateur
TelecomSaintEtienne.diplomeIngenieur(nom=commit('Ates'))	⟵	Initiateur

Attributes:

nom	= 'Ates'	:: TelecomSaintEtienne.etudiant	:: sensitive
nom	= 'Ates'	:: TelecomSaintEtienne.diplome	:: sensitive
annee	= '2004'	:: TelecomSaintEtienne.etudiant	:: sensitive
email	= 'abc@xyz.org'	::	:: non-sensitive

L'utilisateur a deux sources potentielles pour diffuser son nom certifié. Lorsque le nom est requis par le fournisseur, il est nécessaire de demander à l'utilisateur son choix, puis s'il souhaite choisir une source par défaut pour automatiser la présentation du nom, et le cas échéant s'il souhaite donner son acquittement.

Supposons maintenant un cas d'usage qui mette en valeur l'automatisation de choix de l'utilisateur. Nous supposons un utilisateur appelé « Alice » et un fournisseur, un loueur de voitures nommé « Loueuraleur ». Ce dernier établit toujours un pseudonyme public.

L'utilisateur n'établit pas de pseudonyme. Il est supposé qu'Alice navigue sur le site Web du commerçant, puis qu'elle indique le souhait de louer une voiture en précisant son modèle. Pour faire le devis, le fournisseur lui demande de prouver qu'elle possède le permis de conduire depuis plus de 3 ans et qu'il lui reste des points. Il lui demande également un certificat de gage, de prouver que les certificats sont liés ainsi que les dates et les lieux de départ et d'arrivée. Pour cela, Alice requiert, par l'intermédiaire de son interface de négociation, un alias certifié au fournisseur ainsi qu'une évaluation de la part de l'« association française des loueurs de voitures » appelée « AssociationBonLoueur ». Cela traduit ce qu'Alice souhaite pour avoir confiance dans son interlocuteur et dans la confidentialité de leurs échanges. L'organisation indique que pour divulguer ces informations il lui faut au moins la preuve d'un permis de conduire français. Pour cela, Alice indique qu'il lui faut au moins une preuve de possession du certificat d'évaluation. Le fournisseur accepte, la succession d'échanges s'opère et le commerçant fournit le devis à Alice en indiquant un montant et en précisant qu'une pièce d'identité anonyme révocable est requise pour la location. Alice indique qu'elle souhaite l'adresse du loueur ainsi qu'un alias certifié par la « Chambre du Commerce et de l'Industrie » du point d'arrivée ou du point de départ. L'organisation fournit ces informations qui ont un contrôle d'accès d'ores et déjà satisfait.

Pour exprimer l'ensemble de ces conditions, nous étendons la proposition de (Li *et al.*, 2005a) pour y inclure le symbole « $\cup$ » permettant d'indiquer le choix. En l'occurrence, cela nous permet d'indiquer que, si la règle pour le devis est satisfaite, il n'est pas nécessaire de ré-appliquer une règle. Cependant, le choix sert, dans notre exemple, plus à résoudre un besoin d'expression du règlement qu'à offrir un choix à l'utilisateur. Au sein de cette négociation, les seuls choix que peut faire l'utilisateur sont de pouvoir requérir des certificats avant de révéler les siens.

Pour l'organisation, dont les négociations sont supposées entièrement automatisées, toutes les règles sont contenues dans le règlement en annexe C à la section B.1. Il est supposé que le montant du paiment est paramétré par une application métier.

Il est supposé que le règlement de l'utilisateur est initialement vierge, exception faite des déclarations des sources. Nous avons supposé que lorsque l'utilisateur reçoit le règlement pour le devis, il n'est pas enclin à diffuser des informations, ce qui permet de supposer qu'il n'a pas encore confiance dans la confidentialité du canal. De plus, il souhaite associer son expérience de navigation avec son interlocuteur. Il s'appuie pour cela sur le « Groupement des Bonnes Associations de France ». Ainsi, par son interface de navigation, il peut consulter les antennes existantes dans son département relatives aux loueurs de voiture. Il requiert donc des informations de cette association : certificat de membre, un alias et une évaluation. Il est possible de produire une première automatisation de cette interaction

initiale, donc de demander à l'utilisateur s'il souhaite automatiser la demande d'un certificat issu d'un chemin de certification du Groupement des Bonnes Associations de France dès qu'un certificat lui est demandé et qu'il ne connaît pas le pseudonyme du fournisseur. S'il accepte, cela se traduit au sein de son règlement par :

$$Initiateur.Any \longleftarrow GBAF.Evaluation \cap Initiateur.estPseudoReconnu(val = x); \quad x = false \tag{VI.14}$$

Nous avons ici introduit l'opérateur « Any » qui nous permet d'indiquer une règle qu'il est souhaité voir s'appliquer à toutes les autres règles. Nous qualifions celle-ci de « précondition générique ».

Il est également possible de demander à l'utilisateur s'il souhaite automatiser la diffusion d'une preuve de possession de son permis de conduire dès qu'il reçoit un certificat quel qu'il soit. Ceci se traduit par :

$$disclose(ac, Initiateur.PermisConduire) \longleftarrow Any \tag{VI.15}$$

Nous réutilisons ici l'opérateur « Any » de manière informelle. De la façon dont il est est employé, on peut cependant déduire que l'interprétation devrait être plutôt « Dès que n'importe quel rôle est acquis ». Il s'agirait donc ici d'introduire un formalisme permettant de préciser que le rôle acquis doit être issu de la présentation d'un certificat.

Lorsqu'une pièce d'identité anonyme et révocable ainsi qu'une somme d'argent lui sont demandés, nous avons supposé que l'utilisateur requiert un contrôle plus fort que celui qu'il a retiré des informations déjà reçues. Ainsi, il demande une pièce d'identité de l'entreprise émise par une CCI. Il n'est en aucun cas possible d'automatiser la fourniture d'argent. Par contre, il est possible d'indiquer les banques par ordre de préférence de l'utilisateur. Rappelons qu'aucune règle sur les attributs n'est initialement définie. Or, l'interprétation par le langage ATNL de l'absence de l'attribut de contrôle des attributs signifie que l'attribut ne doit jamais être diffusé, par exemple :

Attributes:
montant = 'undefined' :: BanqueA.argent ::
montant = 'undefined' :: BanqueB.argent ::

Il s'agit de la raison pour laquelle nous avons précédemment indiqué qu'il est nécessaire de modifier cette interprétation pour que l'absence de règle signifie qu'une intervention de l'usager est requise. Ainsi, l'exemple précédent signifie qu'il est nécessaire de demander à

l'utilisateur le choix de sa banque même si la « BanqueA » est indiquée comme sa banque préférée en interprétant l'ordre d'apparition.

Il est possible d'automatiser la fourniture d'une pièce d'identité anonyme en échange de l'obtention d'une pièce d'identité de l'entreprise issue de l'ACFCI comme suit :

$$Initiateur.PieceIdentityAnonRevoc \longleftarrow ACFCI.Identite(nom = x_1, adresse = x_2) \tag{VI.16}$$

Le règlement d'Alice après l'ajout à celui-ci de ces quelques règles d'automatisation est présenté en annexes C à la section B.2.

Une partie de la négociation peut désormais être automatisée. Il est supposé un scénario similaire pour une seconde négociation d'Alice mais avec un loueur différent. Alice est cependant munie d'un règlement local enrichi des règles précédemment définies.

Alice reçoit un pseudonyme que son agent ne reconnaît pas. Elle navigue sur le site Web du loueur et requiert un devis. Un règlement lui est retourné. L'agent demande une preuve de possession d'un certificat d'évaluation. Il s'agit de la pré-condition générique qui s'applique ici dès le début de la négociation, ce qui diffère par rapport au cas précédent où cet échange résultait de plusieurs tractations. Après analyse du règlement, l'agent déduit que les informations demandées requièrent une intervention utilisateur. Alice demande un alias et une évaluation, et indique que, si elle les obtient, son agent peut satisfaire le règlement du devis. Pour cela, Alice pré-remplit les informations concernant son trajet. L'organisation demande le permis, l'agent le fournit automatiquement et obtient l'alias et l'évaluation, et enfin, répond au règlement. Le devis est reçu par l'agent avec la demande des certificats *argent* et *pièce d'identité anonyme révocable*. L'agent de négociation de l'initiateur automatise la demande d'une pièce d'identité du loueur et se voit satisfait. L'agent montre à l'utilisateur le devis en lui indiquant les attributs nom et adresse du loueur ainsi que le prix en lui demandant d'acquitter le paiement pour sa banque par défaut. L'utilisateur valide et reçoit une facture.

Le module de gestion des interactions utilisateurs bascule entre automatisation de la transaction à l'aide d'un algorithme de négociation et sollicitation de l'utilisateur via l'interface graphique. Nous introduisons l'algorithme ETTG adapté pour se coupler au langage ATNL, notamment pour le traitement des certificats cryptographiques. L'algorithme peut être représenté sous la forme d'un graphe orienté dont le sommet d'arrivée est l'objet de la négociation (dans notre exemple la location). Le principe est le suivant : chaque interlocuteur ajoute un maximum de sommets en essayant de satisfaire un maxi-

mum de conditions représentées par les sommets entrants du graphe. Ainsi, le graphe est construit tour à tour par chacun des interlocuteurs. Le graphe de cette négociation est représenté sur la figure VI.5. Les sommets de l'utilisateur sont en fond blanc et ceux du loueur en fond gris. L'utilisateur est noté M et le loueur L.

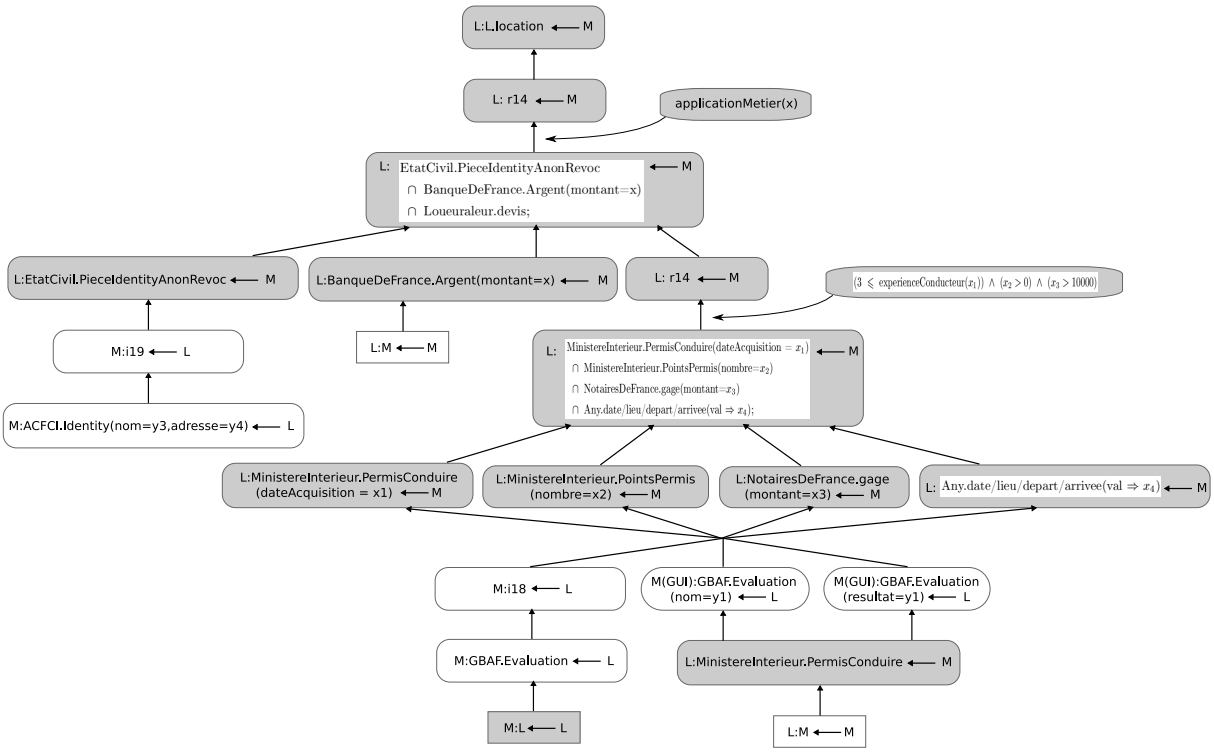

FIG. VI.5 – *Exemple de graphe de confiance.*

L'échange du graphe de négociation et son élaboration durant la négociation constitue le protocole de négociation. S'il est souhaité employer l'algorithme ETTG comme protocole de négociation, il suffit de construire les trames protocolaires permettant l'échange du graphe de négociation et que les deux interlocuteurs supportent l'algorithme ETTG leur permettant d'interpréter le graphe. La détermination des trames protocolaires requises et leur sérialisation, notamment en XML, peuvent être des tâches relativement simple comme nous le verrons au chapitre 8.

Notons que le règlement local de l'utilisateur est un élément extrêmement sensible pour de nombreuses raisons. Le règlement représente, par certaines règles, un moyen de lier les multiples identités d'une entité. Le règlement contient également des informations personnelles. Enfin, il est au cœur du processus de décision des présentations d'informations. Il est par exemple envisageable qu'un attaquant souhaite automatiser un paiement. Il lui suffirait de corrompre le règlement en faisait apparaître « non-sensitive » ou « sensitive » avec une règle d'accès triviale comme attribut de contrôle de l'attribut *montant*.

Le « choix » est facteur du sentiment de confiance dont nous disions qu'il est fondamental pour donner à l'utilisateur le sentiment de négocier. Les choix qui sont offerts à l'utilisateur dans notre cas d'étude ont été restreints au fait que l'utilisateur puisse requérir des informations en contre-partie des siennes. Il faut ajouter la possibilité pour l'utilisateur de choisir un générateur parmi plusieurs. Enfin, nous avions soulevé l'idée que l'utilisateur pourrait être force de proposition pour des attributs. Il est par exemple possible de supposer que le fournisseur requiert l'âge de l'utilisateur et que ce dernier ne propose que de fournir l'information de sa majorité. Cet exemple est trivial mais illustre le fait que l'on entre dans des considérations subjectives. En effet, en supposant que le fournisseur autorise l'accès sur deux rôles « âge » et « majorité », cela signifie que l'organisation soumet à l'utilisateur une règle plus forte que ce qu'elle nécessite. Autrement dit, elle demande en premier à l'utilisateur de révéler son âge que l'on considère comme un rôle plus fort sur un plan du contrôle d'accès que la majorité et qui nécessite de révéler plus d'information, cela alors qu'elle se satisfait en fait de la majorité. Il est discutable de savoir si la proposition couronnée de succès de l'utilisateur lui apporte plus de confiance parce qu'il a été force de proposition, ou au contraire, qu'il en retire moins de confiance en se disant que l'organisation essaie de glaner un maximum d'informations. De plus, l'expression de ces règles se complexifie du fait que plusieurs règles peuvent s'appliquer pour une même ressource.

VI.5 Conclusion

Nous avons présenté dans ce chapitre le principe de l'automatisation des interactions de l'utilisateur à l'aide des principes de la négociation automatisée. Lors de l'étude, nous avons pu mettre en avant diverses limitations du langage ATNL mais pour lesquelles nous n'avons pas formalisé les améliorations. En effet, les propriétés du langage attendues nous ont poussé à proposer des extensions à ce langage sans que l'ambition de ces travaux ne soit une extension formalisée de ce langage mais simplement l'illustration de la faisabilité de l'automatisation des choix de l'utilisateur par les outils de la négociation de confiance automatisée. Cependant, l'implémentation de l'agent négociation, non effectuée à ce jour, rendra ce travail nécessaire si le langage ATNL est choisit.

La problématique de détermination des automatisations possibles à partir des choix et des interactions de l'utilisateur est primordiale. Il semble dans un premier temps que l'indexation dans une base de ces connaissances soit nécessaire en considérant que les situation rencontrée, comme la reconnaissance d'un fournisseur, puisse être identifiées et indexées. En outre, la conception d'un mécanisme permettant d'interpréter les choix et les interactions de l'utilisateur pour les traduire en règles de contrôle d'accès à ses informations personnelles semble ainsi une voie de recherche intéressante. Il est par exemple concevable de prédéfinir un ensemble de règles modélisant les comportements possibles de l'usager et les règles applicables, puis d'employer un système de déduction qui aurait pour rôle d'associer les interactions de l'utilisateur à un comportement reconnu afin de lui proposer des règles d'automatisation.

Enfin, l'utilisabilité et la pertinence de notre approche mériteraient d'être évalués par des tests d'utilisabilité en présence d'un utilisateur afin d'évaluer la complexité de la tâche et sa faisabilité. Le chapitre 9 précise les notions d'ergonomie, d'utilisabilité et de tests d'utilisabilité, et initie l'expérimentation à mener.

Partie III: Concrétisation

CHAPITRE VII

Un agent pour la négociation

*Le **chapitre 7** explore l'idée d'une couche de gestion des identités dédiée au contrôle d'accès des applications. L'objectif est de soulever les enjeux et les problématiques majeurs d'une telle ambition. Une description fonctionnelle de l'agent de négociation est ensuite donnée de manière à ce qu'il soit adapté à l'environnement des utilisateurs comme outil de gestion des identités numériques et aux organisations comme outil de contrôle d'accès aux applications.*

Sommaire

"La Matrice est partout - elle est tout autour de nous - même maintenant, dans cette pièce. Tu peux la voir quand tu regardes par la fenêtre ou quand tu allumes la télévision. Tu peux la sentir quand tu vas travailler; quand tu vas à l'église; quand tu paies tes impôts. C'est le monde qui a été plaqué sur tes yeux pour te rendre aveugle à la vérité – que tu es esclave. Comme tout le monde, tu es né en captivité – né dans une prison que tu ne peux ni sentir, ni toucher – une prison pour ton esprit."

Morpheus à Neo, *The Matrix*.

VII.1 Intégration

Lorsque l'objet de la négociation est la fourniture d'un ensemble d'informations, éventuellement de certificats, l'agent initiateur suffit à la consommation de ce service. Cependant, lorsque l'objet de la négociation est la consommation d'une « ressource applicative », la négociation de confiance devient une composante importante du procédé de contrôle d'accès aux applications. Cela introduit une notion de couplage entre les agents de négociation et les applications, donc la problématique d'intégration.

Employer la négociation de confiance pour mener le contrôle d'accès aux applications, afin notamment de répondre à la problématique de gestion des identités numériques, peut donner à cette technologie la dimension de couche sous-jacente aux applications. L'idée d'une couche de gestion des identités est pertinente mais ambitieuse. Elle est pertinente du fait qu'il peut être souhaité de voir les applications existantes déléguer leur gestion des identités à une application unique. Cette idée se justifie également du fait qu'il est souhaité une solution adressant la problématique de la gestion de la vie numérique des usagers, en y incluant les authentifications multiples et la fourniture d'informations. Elle est cependant ambitieuse car elle pose des problèmes d'intégration, c'est-à-dire de modification des applications existantes. Vouloir faire de la négociation de confiance la couche de gestion des identités, sur laquelle le contrôle d'accès aux applications serveurs va reposer, est lourd de conséquences et constitue un défi dont nous relevons ici les principales problématiques.

VII.1.1 Gestion des identités côté utilisateurs et notion de couche

Intéressons-nous dans un premier temps à l'environnement utilisateur. Nous décrivons ici trois « étapes » dans la perspective du déploiement d'un module client pour opérer la couche de gestion des identités. Il s'agit d'une approche informelle et intuitive qui nous aidera à mettre en avant l'enjeu de l'universalité.

La première étape d'intégration est l'« intégration nulle ». Quelques outils logiciels sont déployés au sein de l'environnement de l'utilisateur pour faciliter sa vie numérique (outils d'aide à l'auto-saisie de formulaires et portefeuille de mots de passe). Les échanges de certificats se font directement entre organisations ou au travers du navigateur Web standard employé comme relais de manière à gérer les interactions de l'utilisateur (la fédération d'identités par exemple).

La seconde étape suppose le déploiement d'un « environnement client enrichi ». Cela nécessite un environnement client et la modification des applications existantes côtés

« client/initiateur » et « serveur/fournisseur ». Les flux liés à la gestion des identités et aux applications sont faiblement couplés et sont conduits à travers des canaux de communication distincts. Il s'agit d'une étape intermédiaire qui implique les deux faits suivants :

- les applications délèguent leur gestion des identités,
- il doit exister un protocole de communication entre couches.

L'étape ultime est celle de l'intégration par un « module client de la couche de gestion des identités ». L'idée derrière la notion de couche implique le fait suivant supplémentaire :

- les flux de chaque couche sont « encapsulés » dans les flux de la couche sous-jacente. Autrement dit, les flux applicatifs sont encapsulés dans les flux de la négociation et circulent à travers un même canal de communication.

Ces termes sont par la suite employés afin de distinguer le fait que les flux applicatifs sont encapsulés ou non dans les flux de la négociation.

VII.1.2 Objets de la négociation et applications

Pour déterminer les difficultés d'intégration, il est utile de revoir quels sont les types d'objets sujets à négociation et les moyens de leur obtention. Les objets peuvent être :

- des accès applicatifs, ce qui signifie que l'obtention de l'objet se traduit par un flux applicatif consécutif à une négociation menée avec succès,
- des informations éventuellement certifiées (de l'argent par exemple),
- soumis à la fourniture d'informations en ligne mais sont délivrés par des voies physiques (déclaration d'impôts, achat/livraison).

L'aboutissement de la négociation pour le second type d'objet se traduit par l'obtention de l'information certifiée dans un message de la négociation. L'aboutissement de la négociation pour le troisième type d'objet se traduit par un acquittement de succès de la négociation par exemple. Il est possible de considérer que les applications sont dédiées à la négociation donc qu'il n'y pas réellement de problématique d'intégration.

Cependant, les négociations de ces deux types d'objets peuvent être menées couplées à des flux applicatifs (une navigation Web par exemple). Ces flux peuvent alors être relatifs à ceux de la négociation pour :

- permettre de déterminer l'adresse d'un fournisseur à même de fournir un objet,
- permettre au fournisseur de présenter à l'utilisateur des interfaces graphiques lui permettant de l'informer sur la négociation si l'interface graphique de l'agent initiateur n'est pas à même de représenter toutes les informations d'une négociation,
- rendre la consommation de l'application, la navigation Web par exemple, source de confiance.

Ainsi, le premier type d'objets précédemment présenté, et les deuxième et troisième types s'ils sont liés à des flux applicatifs, sont soumis à des problèmes d'intégration avec des applications tierces. Cela signifie que les échanges applicatifs :

- peuvent être soumis à des accès en partie contrôlés par la négociation,
- peuvent voir leur confidentialité reposer sur des paramètres de sécurité issus de la négociation,
- sont issus d'une entité dont la confiance devrait être principalement obtenue de la négociation.

VII.1.3 Donner un sens à la notion de couche de gestion des identités

Nous nous intéressons ici aux problèmes d'intégration des applications. Cela suppose que les accès aux applications soient en partie soumis à négociation. Cela implique, d'une part, que l'environnement du serveur applicatif soit muni d'un agent de négociation pouvant assumer le rôle de fournisseur, et d'autre part, que l'environnement du client applicatif, celui de l'utilisateur, soit muni d'un agent de négociation pouvant assumer le rôle d'initiateur. Ceci est illustré à la figure VII.1.

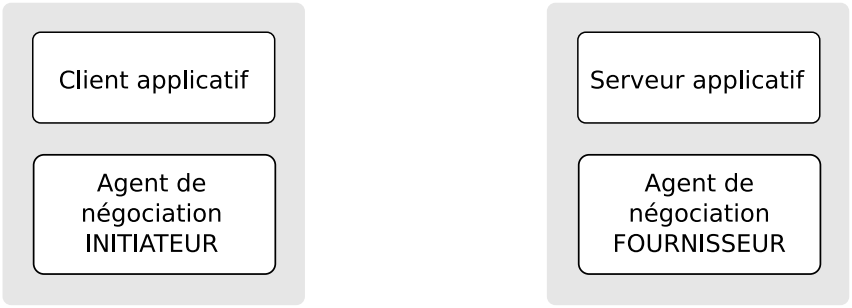

Fig. VII.1 – *Terminologie de la négociation pour des accès aux applications.*

Nous avons souligné à la section III.3.5 que le fournisseur peut être amené à déclencher une négociation lorsque l'initiateur requiert un objet sujet à négociation. La terminologie employée se justifie tout de même dans le sens où c'est une requête d'accès de l'initiateur qui déclenche la négociation. Ceci dit, l'initiateur doit être en capacité de détecter l'initiation par le fournisseur. Dans un environnement possédant un client enrichi, nous avons indiqué qu'il est nécessaire que le client applicatif soit modifié afin de pouvoir détecter cet événement, et ensuite, de déléguer la négociation à l'agent de négociation initiateur. Il s'agit du choix fait au sein de la technologie CardSpace (Nanda & Jones, 2008) : le navigateur Web est modifié pour détecter une initiation sous la forme d'une balise dans

l'entête d'un document XHTML ainsi que pour déléguer la transaction à l'agent Cardspace. Notons que, lorsque le fournisseur initie, il est toujours question d'un flux applicatif et que cette initiation fait suite à une requête d'accès de l'initiateur au niveau applicatif. A l'inverse, il doit être possible que l'agent client de l'application permette de déclencher une négociation en déléguant l'initiation à l'agent de négociation initiateur en indiquant l'objet qu'il souhaite négocier.

Dans un modèle d'intégration avec un environnement client enrichi, l'initiateur adresse le point d'entrée applicatif de l'agent de négociation fournisseur lorsqu'il initie une négociation. Lorsque la négociation aboutit avec succès, ouvrant droit à un accès applicatif, le client adresse un second point d'entrée applicatif, celui du serveur applicatif, et établit un nouveau tunnel de communication. Il est donc nécessaire qu'une information issue de la négociation et portant sur le contrôle d'accès, que nous appelons pour l'instant autorisation d'accès, puisse être délivrée de l'agent de négociation fournisseur au serveur applicatif. Ce modèle suppose l'ouverture d'un canal de communication applicatif, distinct de celui de la négociation et par lequel cette autorisation est présentée et l'application est consommée. Les paramètres de sécurité de ce canal, que nous appelons canal applicatif, devraient être dérivés de ceux du canal de négociation pour que la confiance établie durant la négociation soit bénéfique pour la communication avec l'application. Dans le cas contraire, cela peut conduire au fait que la consommation d'application soit difficilement associable à une entité « connue » *via* la négociation. Il s'agit de la problématique que nous avons soulevé à la section V.2.2 en prenant l'exemple d'une navigation Web qui n'est dans ce cas associable à un tiers que par un alias. Ainsi, il est recommandé, pour ce modèle, que les flux applicatifs consécutifs à une négociation, menée avec succès, transitent sur un canal applicatif dont les paramètres de sécurité sont obtenus de la négociation. Concrètement, cela peut signifier que le canal applicatif soit établi avec le même pseudonyme que le fournisseur a présenté pour la négociation et que l'autorisation soit véhiculée au sein d'un jeton signé permettant ainsi à l'application de reconnaître son agent de négociation.

La figure VII.2 présente le schéma d'une initiation fournisseur avec un environnement client enrichi. Le lien « 1 » indique une requête d'accès applicatif que le serveur détecte comme sujet à négociation. L'application détermine qu'il s'agit d'un accès contrôlé pour lequel l'accès n'est pas autorisé (Il pourrait ici y avoir un échange entre l'application et l'agent de négociation). Le fournisseur retourne l'initiation de la négociation dans le flux applicatif en indiquant l'objet de la requête (lien « 2 »). Le client applicatif le détecte et fait appel à son agent de négociation (lien « 3 »). La négociation se fait au sein d'un canal différent (lien « 4 ») et se termine par un jeton d'autorisation envoyé à l'agent de négociation initiateur (lien « 5 »). Ce dernier le retourne au client applicatif (lien « 6 ») qui renouvelle sa requête d'accès avec celui-ci (lien « 7 »). L'accès est alors offert (lien

« 8 »).

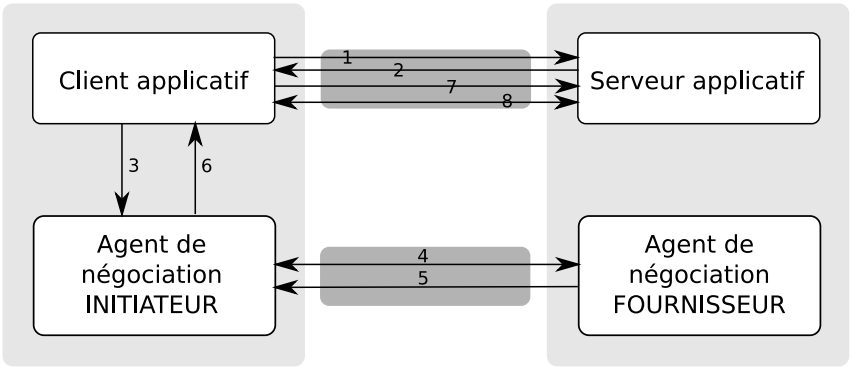

FIG. VII.2 – *Initiation fournisseur avec un environnement utilisateur enrichi.*

Le « modèle en couches », implique que les flux applicatifs transitent par les agents de négociation au sein du protocole de négociation. Les flux applicatifs sont encapsulés dans les flux de négociation. L'agent de négociation a donc également la charge de « décapsuler » les flux applicatifs pour les transmettre aux applications. Autrement dit, les flux applicatifs et de négociation transitent au travers d'un même canal de communication. Selon les recommandations émises au chapitre 5, tout accès applicatif débute par l'établissement d'un pseudonyme par le fournisseur, puis par l'établissement d'un canal sécurisé. Les flux applicatifs sont ainsi directement associés à ce pseudonyme, donc aux négociations sur ce canal.

La figure VII.3 présente le schéma d'une initiation fournisseur avec un modèle en couches. Le lien « 1 » indique une requête d'accès applicatif qui transite à travers les agents de négociation. L'agent de négociation fournisseur n'est pas à même de détecter qu'il s'agit d'une requête nécessitant une négociation. Le serveur applicatif le détecte et retourne à son agent de négociation une demande de négociation en lui indiquant l'objet de la négociation (lien « 2 »). L'agent de négociation fournisseur retourne une demande d'initiation de négociation à l'agent de négociation initiateur et une négociation a lieu (lien « 3 »). Suite à cette négociation menée avec succès, l'agent de négociation fournisseur retourne au serveur applicatif une autorisation (lien « 4 ») et celle-ci retourne l'accès applicatif (lien « 5 »).

Considérons des objets de négociation qui sont des accès applicatifs, l'initiation peut être faite par l'initiateur ou le fournisseur. Dans le cas du modèle d'intégration avec un environnement client enrichi et lors d'une initiation par le fournisseur, le client applicatif reçoit cette initiation au sein du flux applicatif. Il doit donc être capable de le détecter, puis de déléguer à l'agent de négociation en indiquant l'objet. Dans le cas du modèle en

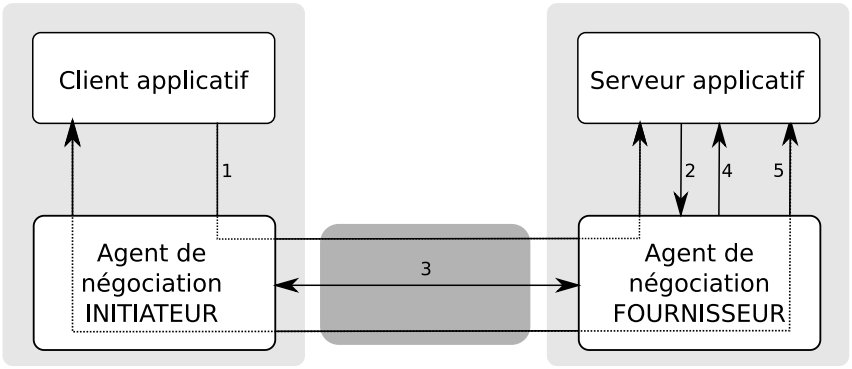

FIG. VII.3 – *Initiation fournisseur avec un modèle en couches.*

couches et lors d'une initiation par le fournisseur, c'est l'agent de négociation initiateur qui reçoit la trame d'initiation de la négociation. Il conduit donc la négociation jusqu'à l'obtention de l'accès et fait ensuite suivre les flux applicatifs à l'application.

Une initiation par l'initiateur dans le cas du modèle en couches suppose un client applicatif capable de déterminer quels accès applicatifs font l'objet d'une négociation afin de les déléguer à l'agent en indiquant leur objet. Cela signifie en quelque sorte que le client applicatif connaît une partie du règlement de contrôle d'accès de l'application du fournisseur.

Enfin, lorsque l'accès est obtenu par l'initiateur, dans un modèle en couches, le client applicatif n'est pas sollicité pour porter l'autorisation issue de la négociation par opposition au modèle d'intégration avec un environnement client enrichi. Le flux applicatif issu de l'initiateur est envoyé par l'agent fournisseur « accompagné » de l'autorisation à l'application serveur.

En résumé, en appliquant le modèle en couches, un seul canal de communication est nécessaire permettant d'associer tout flux applicatif à un même tiers. En outre, les deux modèles impliquent un protocole de communication entre applications et agents de négociation. Le modèle en couches évite cependant un dialogue à travers deux canaux de communication distincts et attribue à l'agent de négociation une fonction de « relais ». Côté fournisseur, l'agent est sollicité pour tout accès applicatif. Les applications conservent leurs adresses mais c'est l'agent de négociation qui « répond » en ayant la charge de router les flux aux applications. Autrement dit, l'agent de négociation, dans un modèle en couches, a la charge de gérer toutes les connexions applicatives entrantes. C'est en quelque sorte un « pare-feu applicatif ». Côté initiateur, tous les flux applicatifs transitent par l'agent de négociation local qui a la charge d'établir les connexions applicatives. Les applications clientes doivent donc indiquer à leur agent les points d'entrées des applications serveurs

cibles.

VII.1.4 Protocoles de négociation

Nous avons vu, au précédent chapitre, le protocole de négociation entre deux agents au travers de l'algorithme de négociation automatisé ETTG. Les échanges de l'arbre de négociation peuvent être retranscrits en messages protocolaires d'échanges des règlements. Lorsque la négociation aboutit, un consensus est atteint et les messages contenant les informations sont échangés. À ce protocole basique de négociation, il faut ajouter les messages d'initiation. Cette initiation peut être faite par l'initiateur dans un message indiquant la requête d'un objet, ou par le fournisseur dans un message contenant un règlement en indiquant éventuellement le sujet de la négociation. Notons que l'initiation par le fournisseur est consécutive à un accès applicatif, elle est donc indiquée dans un message dont l'agent de négociation initiateur pourrait s'attendre à ce que ce soit un message applicatif. Enfin, il doit exister un message du protocole de négociation qui soit un message d'encapsulation et qui serve au transport des flux applicatifs. Au chapitre suivant, nous revenons sur la sérialisation de ce protocole de négociation.

Il est également nécessaire de préciser les protocoles de communication entre les agents et les applications qu'ils régissent. Nous considérons que chaque application a la charge soit de déterminer les rôles requis pour chacun de ses objets (un service, une tâche, une méthode d'une classe, etc.), soit que l'agent de négociation est capable de déduire les rôles requis en fonction de l'objet indiqué par l'application. Dans le cas où l'agent de négociation fournisseur déduit les rôles en fonction d'un objet, ce qu'il délivre à l'application est bien une autorisation que l'application met en œuvre. Les applications ont alors la charge de vérifier que les flux sont porteurs des autorisations. Notons qu'au chapitre précédent nous avons fait le choix de déclarer au sein du règlement de l'agent fournisseur des règles précisant les rôles nécessaires pour certains objets de l'application (un devis par exemple) afin d'illustrer ce besoin. Dans le cas où l'application indique les rôles dont elle a besoin, le terme autorisation est abusif, il s'agit plus précisément de l'affirmation des rôles de l'usager par l'agent de négociation. Cela suppose que les applications et l'agent de négociation partage un espace de noms commun pour décrire les rôles. Les applications ont alors la charge de vérifier que les flux sont porteurs des rôles requis.

Quel que soit ce choix, l'agent de négociation fournisseur a la charge d'interagir avec l'initiateur pour qu'il puisse apporter les preuves qu'il possède les rôles requis. Il est possible que des rôles ou des autorisations obtenus pour un accès auprès d'une application soient utilisables pour d'autres applications, et cela sans que l'utilisateur n'ait à fournir à nouveau les preuves correspondant à ces rôles. Notons que lorsque ces applications sont

hébergées par une organisation, il s'agit de certifier les rôles ou les autorisations, ce qui est une solution de délégation d'autorisations entre organisations liées de confiance.

La délégation par les applications nécessite une conception applicative « saine » où, dès la conception, les objets et les règles de contrôle d'accès sont déterminés. Ensuite, l'association entre objets et rôles peut être faite au niveau de l'application ou de l'agent de négociation. L'application met en œuvre le contrôle d'accès, ce qui pour certains la légitime pour cette tâche. Pour d'autres, l'agent de négociation est l'opportunité de centraliser le contrôle d'accès. Notons alors que, dans ce cas, le besoin d'expressivité est fort envers le langage de contrôle d'accès qui doit permettre d'exprimer les contraintes de toutes les applications. Au chapitre précédent, nous avons donné un exemple avec le langage ATNL dont l'instruction *disclose* permet d'indiquer les règles de libération d'un objet. Cette instruction peut donc servir à indiquer que le fournisseur accepte de diffuser une information en fonction de l'application qui est sollicitée, mais également pour exprimer les conditions d'accès sur des objets de l'application. Il faut pour cela que le module de l'agent de négociation en charge d'interpréter le règlement puisse faire la distinction entre ces deux utilisations de l'instruction *disclose*.

Que l'agent de négociation ait la charge ou non d'associer les rôles nécessaires aux objets requis, c'est au niveau de l'application qu'est déterminé le fait qu'un objet soit sujet à un contrôle d'accès. Il pourrait sembler plus simple que l'agent de négociation détermine de lui-même, à la vue des flux applicatifs, les objets des requêtes applicatives, et par conséquent s'ils sont sujets à négociation. Cependant, cela supposerait que l'agent de négociation fournisseur soit à même d'interpréter les flux applicatifs, ce qui n'est pas son rôle.

La délégation de la gestion des identités implique que les applications puissent traduire le fait qu'elles requièrent des informations d'identité, par exemple un pseudonyme ou d'autres attributs d'identité, donc qu'elles soient capables de formuler cela auprès de leur agent de négociation. Elles peuvent également avoir à disposition leur propre base de données d'identités, leur servant par exemple à personnaliser un service ou à auditer les activités. Elles peuvent donc ne requérir qu'un identifiant connu, ce qui se traduirait par la requête de l'objet *établissement d'identité* et de l'information *pseudonyme* à leur agent de négociation.

En résumé, entre le client applicatif et l'agent de négociation initiateur, le protocole, que nous appelons « protocole de négociation inter-couches », doit permettre d'indiquer, du client vers l'agent :

- un flux applicatif destiné à un fournisseur (en indiquant un point d'entrée applicatif, une URL par exemple),

– une initiation en indiquant son objet.

De l'agent de négociation initiateur vers le client applicatif, il doit permettre de signaliser :

– les flux applicatifs,
– les résultats des négociations si l'application en était à l'origine, et notamment des informations sur le fournisseur.

Entre l'agent de négociation fournisseur et le serveur applicatif, le protocole de négociation inter-couches doit permettre d'indiquer, du serveur vers l'agent :

– un flux applicatif destiné à l'initiateur,
– une initiation en indiquant des rôles ou un objet.

De l'agent de négociation fournisseur vers le serveur applicatif, il doit permettre de signaliser :

– les flux applicatifs,
– une initiation en indiquant l'objet.
– des rôles obtenus par l'initiateur pour l'autoriser ou une autorisation pour un objet.
– des informations d'identité sur l'initiateur de manière à personnaliser la ressource.

À titre d'exemple, supposons un client Web qui redirige son flux vers son agent. Ce dernier établit un tunnel SSL avec le pseudonyme délivré par l'agent fournisseur. L'agent fournisseur redirige ensuite le flux à l'application. L'encapsulation du flux applicatif, le protocole HTTP dans cet exemple, est représentée à la figure VII.4 .

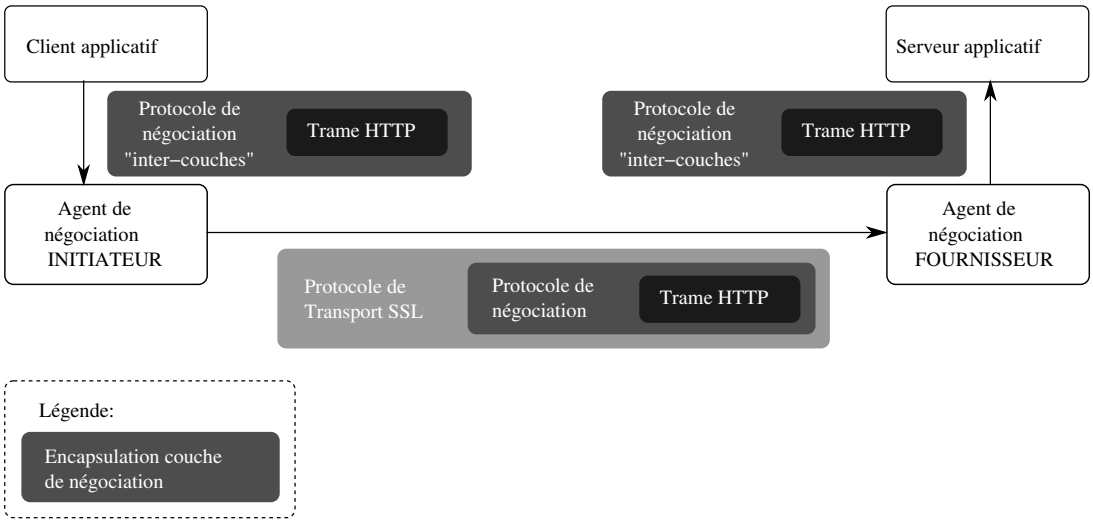

FIG. VII.4 – *Encapsulation du flux applicatif HTTP.*

Supposons que le flux applicatif soit sujet à un accès contrôlé, ce que le serveur Web détecte. Il indique à son agent qu'une négociation doit être conduite en indiquant son objet. L'agent de négociation fournisseur retourne à l'agent de négociation initiateur un

règlement (le fournisseur a déduit les rôles nécessaire de l'objet). Cela est illustré à la figure VII.5.

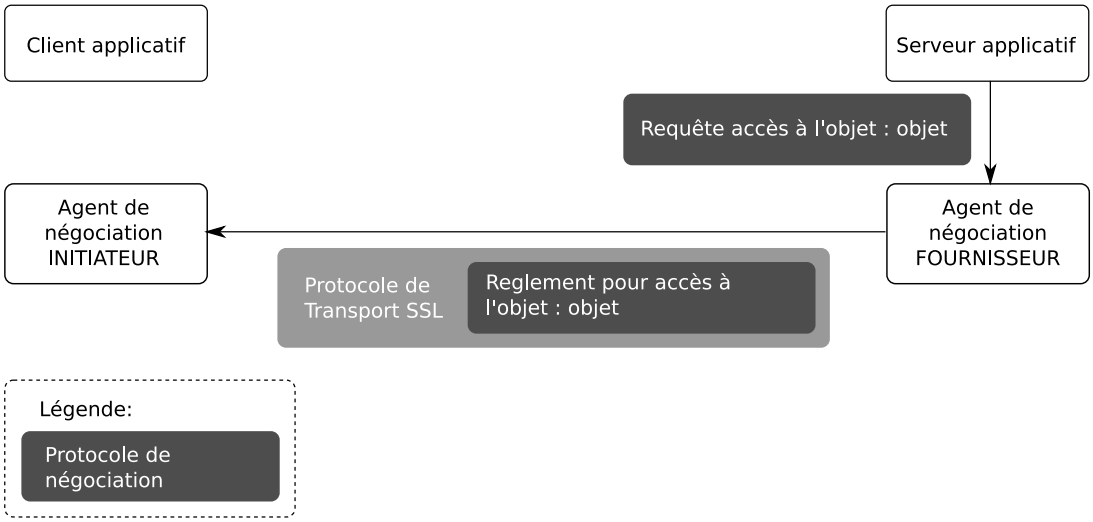

FIG. VII.5 – *Exemple de messages protocolaires pour une initiation par le fournisseur.*

VII.2 Fonctionnalités

Jusque-là, nous avons soulevé le besoin de nombreuses fonctionnalités pour enrichir l'environnement utilisateur afin que les usagers puissent gérer leurs identités, leurs relations et leurs négociations numériques. Dans cette section, nous nous efforçons de regrouper les fonctionnalités en modules afin de déterminer l'architecture fonctionnelle de l'agent de négociation, notamment pour qu'il soit adapté à l'environnement des utilisateurs comme outil de gestion des identités numériques et aux organisations comme outil de contrôle d'accès aux applications. L'agent de négociation constitue donc un module unique que l'on souhaite universel quels que soient les rôles empruntés par le système hôte au sein de la négociation : initiateur, fournisseur, organisation ou utilisateur.

Les modules principaux de l'agent de négociation sont présentés à la figure VII.6. Sur cette figure, il est également mis en valeur la distinction entre la partie logicielle, qui a trait à être commune à chaque environnement, et les données variables portant sur les entités qui exploitent l'agent. S'il s'agit d'un agent gérant l'accès à de multiples applications, il est possible que l'espace de données regroupe des informations de multiples entités, pour chacune des applications serveurs par exemple. Si l'agent de négociation est utilisé dans le rôle d'initiateur par un utilisateur, l'espace des données constitue en quelque sorte la matérialisation de sa vie numérique. En outre, cette distinction permet de mettre en valeur les questions de portabilité et de recouvrement.

Notons tout de même que certains modules peuvent être inutilisés, ou utilisés différemment, selon que l'environnement est celui d'un initiateur ou d'un fournisseur. Ce schéma ne fait pas apparaître tous les modules, notamment ceux de plus bas niveau tels que les modules de sérialisation (en XML par exemple), de communication réseau (pile TCP/IP par exemple), de primitives cryptographiques, ou bien encore de stockage.

Notons que la partie *Administration* permet à l'utilisateur, ou à l'administrateur (dans le cas d'un fournisseur), de configurer l'environnement de négociation en dehors des négociations. Cependant, ces fonctions sont disponibles et sollicitées durant les négociations.

Voici en quelques lignes la fonction de chacun des modules :

1. **Encapsulation des flux applicatifs et protocole de négociation.** Ce module a la charge d'assurer les échanges applicatifs et de négociation. Il a notamment la charge du protocole de négociation et assure par conséquent la détection de l'initiation des négociations. Il s'agit du module d'entrée/sortie qui interface avec l'application locale et l'agent de négociation de l'interlocuteur.

2. **Interface graphique.** Ce module gère l'interfaçage avec l'utilisateur pour la saisie de ses choix et le paramétrage de l'agent. Il permet l'affichage de l'état des négociations et des transactions au cours des négociations. Ce module peut avoir la charge des affichages faits en « sur-impression » des interfaces des applications clientes. Pour l'agent fournisseur, ce module se limite à l'interface d'administration.
3. **Analyse des choix et interactions utilisateurs.** Ce module obtient les choix de l'utilisateur *via* ses interactions avec l'interface graphique. Il permet de proposer, au travers du module d'affichage, des choix pour l'automatisation de la négociation et alimente le règlement local en conséquence. Ce module est dédié à l'agent de négociation initiateur.
4. **Analyse des règlements des interlocuteurs et du règlement local - Stratégie de négociation.** Ce module a la charge de l'analyse des règlements de l'interlocuteur et des sources disponibles au sein du règlement local. Il analyse ensuite les règles d'automatisation du règlement local. Puis, suivant les besoins, il propose à l'utilisateur au travers de l'interface graphique : de faire des choix parmi les sources disponibles, d'ajouter des sources, d'acquitter une diffusion, de faire la proposition de preuves ou d'obtenir des informations en échange. Ce module est autonome pour le fournisseur. Enfin, ce module s'appuie sur le module de communication pour dialoguer avec les générateurs et les consommateurs.
5. **Obtention de certificats et d'attributs.** Obtention des certificats et d'informations stockées en ligne. Ces obtentions peuvent être soumises à des établissements d'identité qui constituent des négociations *a minima*. Ce module s'appuie donc sur le module d'*analyse des règlements et de stratégie de négociation*.
6. **Fourniture d'attributs, de certificats, de preuves et établissement d'identités.** Ce module a la charge de bâtir les messages visant à la diffusion d'informations, notamment des preuves. Ce module est appelé par le module d'*analyse des règlements et de stratégie de négociation*, notamment pour les établissements d'identité, et fournit les données à envoyer au module de communication.
7. **Vérification des certificats, des chemins de confiance et des preuves.** Ce module a la charge de vérifier les signatures, les chemins de confiance et les preuves. Il a également la charge de déterminer si une source disponible est dans un chemin de confiance d'une source requise par un règlement de l'interlocuteur.
8. **Enregistrement des négociations.** Module d'audit et de journalisation des activités.
9. **Gestion des attributs d'identités.** Ce module permet au travers de l'interface graphique de renseigner une base des informations d'identité non certifiées.
10. **Gestion des sources.** Ce module permet d'ajouter des sources en intégrant leurs points d'entrées applicatifs et leurs certificats. Il a la charge de l'analyse des certifi-

cats qu'elles sont à même de fournir pour renseigner le règlement local. Ce module peut être sollicité au travers de l'interface d'administration, notamment en cours de négociation pour l'initiateur.

11. **Configuration du règlement local et de l'automatisation.** Ce module permet de modifier « manuellement », par une interface graphique d'administration, les paramètres d'automatisation. Ce module est également sollicité par le module d'*analyse des règlements et de stratégie de négociation* pour l'agent initiateur.
12. **Consultation du journal des négociations.** Enregistrement et consultation des activités de négociation.
13. **Configuration générale.** Paramétrage générique du logiciel agent (la langue par exemple).

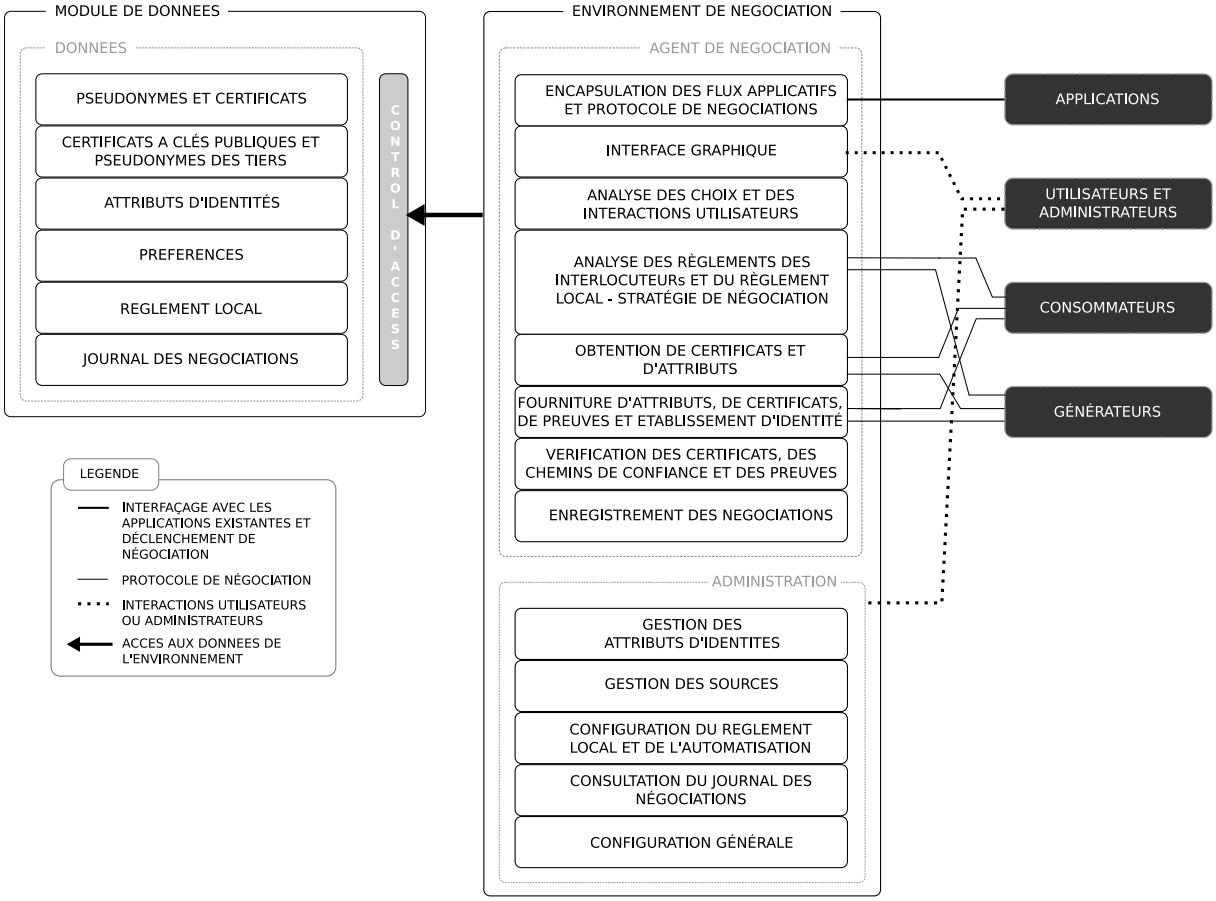

FIG. VII.6 – *Modules logiciels principaux d'un environnement pour la négociation.*

VII.3 Conclusion

Préalablement à ce chapitre, nous avions décrit un modèle de négociation entre le fournisseur et l'initiateur relativement « dissymétrique ». Nous avons notamment accentué cette « dissymétrie » en défendant un modèle centré sur l'utilisateur. Cela nous a permis de mettre en lumière des mécanismes de diffusion des informations orchestrés par les sujets et les possesseurs des certificats, donc d'introduire la notion de porteur. Puis, la négociation de confiance et l'automatisation des interactions de l'utilisateur en un règlement de contrôle d'accès ont permis, en quelque sorte, de rendre ce modèle plus « symétrique ». Ce chapitre, grâce à l'étude d'un modèle en couche sorte d'idéal de l'intégration, permet de rendre concret l'idée d'un module universel permettant d'emprunter les multiples rôles de la négociation de confiance. Au chapitre suivant nous étudions les problématiques de l'universalité d'un tel module ainsi que la question de l'interopérabilité.

CHAPITRE VIII

Vers la pervasivité

*Le **chapitre 8** constitue la synthèse des besoins affiliés à la notion d'universalité en vue de parvenir à la pervasivité. Il est donné un sens pratique à la notion de confiance entre organisations. Les notions d'interopérabilité, d'espaces de noms communs et de standardisation, notamment par les standards du Web, sont présentées. Il est proposé une solution pour la sérialisation des certificats anonymes basée sur des données publiques des générateurs de certificats. La réalisation d'une application XML de ces données implémentée en langage C à l'aide des librairies libxml2 et xmlsec1 est présentée. Une solution de sérialisation du protocole de négociation basée sur l'enrichissement de documents XML est ensuite présentée. La mobilité des usagers est un paradigme pour lequel des propositions sont faites, notamment basées sur une plateforme de confiance. Enfin, l'emploi de la négociation de confiance dans les environnements pervasifs et ubiquitaires et la notion d'« identité en tout lieu*[1] *» sont discutés.*

1. trad. Identity Everywhere.

Sommaire

"La question n'est pas de savoir comment seront les machines dans le futur mais comment serons nous. [2]"

Sherry Turkle, *The Second Self.*

2. trad. "That question is not what will the computer be like in the future but what will we be like."

VIII.1 Introduction

Toute communication suppose des interlocuteurs qui puissent se comprendre. Définir des espaces de noms et des protocoles sont donc une condition pour permettre des échanges entre parties négociatrices, potentiellement inconnues préalablement aux négociations, et de manière à véhiculer des informations entre générateurs et consommateurs. Ces problématiques sont celles associées à la notion d'interopérabilité concernant notre architecture. Dans la section suivante, sont présentés des standards, notamment basés sur les technologies du Web, qui se prêtent à plusieurs de nos besoins de sérialisation. Dans l'idéal d'un système universel, le fait qu'il soit basé sur d'autres normes et standards semble une condition *sine qua non*.

Nous avons abordé la question de l'universalité, en supposant qu'elle repose sur l'interopérabilité, le déploiement d'un agent de négociation nativement à tout système et l'intégration traitée au chapitre précédent. Ces problématiques sont celles des organisations, en tant que « décideurs », et reposent sur le choix de technologies et leur déploiement.

Les utilisateurs sont eux plutôt concernés par les questions de protection de la vie privée comme nous l'avons déjà abordé. Ils sont également sensibles à la disponibilité de leurs données. Nous rattachons cette problématique aux notions de mobilité et de nomadisme. Il s'agit de permettre à l'utilisateur de disposer, sur tout terminal, de ses informations d'identité, celles que nous avons distinguées sur la figure VI.4. Cela suppose également que l'environnement de négociation soit conçu pour une utilisation optimale, ce que nous nommons l'utilisabilité, et notamment qu'il soit adapté à différents types de terminaux utilisateurs et différents environnements de consommation. Adresser l'ensemble de ces problématiques (l'interopérabilité, l'universalité, la mobilité et l'utilisabilité) est la condition à l'ubiquité de l'environnement de négociation.

VIII.2 Confiance

Avant de poursuivre plus avant sur la concrétisation de ces travaux, il est nécessaire de revenir sur la condition fondamentale de cette architecture, la confiance. Nous avons évoqué la possibilité d'établir des conditions de contrôle d'accès et des relations entre inconnus au travers du principe de confiance. Nous avons évoqué au chapitre 2 les notions de confiance et de contrôle, puis de confiance transitive et de chemins de confiance au chapitre 6. Cependant, il est nécessaire de donner une dimension plus concrète à la confiance pour mesurer les enjeux de cette architecture.

Les organisations, dans le rôle de fournisseurs, s'appuient principalement sur des informations certifiées par des organisations tierces. Nous avons donc relevé que la confiance peut être issue de partenariats, comportant des engagements, formalisés et officialisés dans un contrat. Nous avons également relevé que la confiance peut naître de notions plus subjectives telles que le fait qu'une organisation soit considérée de confiance pour fournir une information dès lors qu'elle accorde elle-même de l'importance à cette information.

Les liens de confiance peuvent être unidirectionnels : des consommateurs vers les fournisseurs. Un consommateur fait ainsi confiance à un générateur sans que celui-ci n'ait besoin d'avoir conscience de son existence. Les liens de confiance peuvent également être bidirectionnels. Citons par exemple un partenariat entre deux opérateurs de téléphonie mobile. Un abonné du premier pourra se connecter à l'infrastructure du second s'il peut apporter un certificat issu du premier, et réciproquement. Enfin, il existe les fédérations bâties sur des liens bidirectionnels et au sein desquelles des organisations se font mutuellement confiance. Citons par exemple la fédération des universités européennes qui permet en particulier à un étudiant d'une université membre de la fédération de se connecter à l'infrastructure réseau sans fil (Wifi) de n'importe quelle université membre[3]. L'étude suivante du *projet Concordia* (projectconcordia.org, 2009) est une illustration de ces divers types de relations mises en œuvre avec les technologies de la fédération d'identités. Notons que la nécessité d'une infrastructure de confiance globale est la même, quels que soient les moyens technologiques de mise en œuvre de l'architecture de certificats. Dans cette étude apparaît le rôle d'« opérateur de fédération » que nous n'avons pas évoqué en première partie. L'opérateur de fédération joue en quelque sorte un rôle d'« entremetteur » assimilable à un système de réputation en émettant des recommandations sur les partenaires ou peut être vu comme une autorité de certification racine dans un chemin de confiance.

Le terme architecture de confiance et l'emploi courant de termes tels que « cercles de

3. Projet EduROAM

confiance » pour désigner des organisations ainsi liées ne rendent pas précisément compte de la nature des liens entre organisations. Le terme confiance se justifie du fait que les organisations représentent des domaines de sécurité distincts, donc que le contrôle ne peut être total. Il est tout de même attendu que ces liens soient synonymes de contrôle, le plus fort possible dans certains cas, pour des flux financiers par exemple. Les partenariats sont ainsi synonymes de contrats et d'engagements définissant les responsabilités de chacun. Lors de l'établissement d'une relation, les risques et les gains sont mis en balance et les termes du contrat peuvent inclure des recours légaux en cas de préjudice. Il est notamment pris en considération le fait qu'une relation de confiance puisse être préjudiciable. Une organisation peut ainsi mettre fin à cette relation en limitant les préjudices à des niveaux de pertes acceptés, pris en compte lors des calculs de risques initiaux, dès lors que divers indicateurs témoignent de préjudices potentiels.

Notons que la confiance peut être accordée pour la fourniture de certaines informations et non pour d'autres, ce qui transparaîtra dans le règlement de contrôle d'accès du consommateur.

Enfin, notons l'émergence de relations de confiance entre organisations qui seraient plus « spontanées ». Il s'agit d'établir des relations de confiance dynamiques entre générateurs et consommateurs. Aujourd'hui, ces pratiques sont marginales même si certaines technologies s'y prêtent (Cantor *et al.*, 2005 ; Ballinger, 2006), et en particulier les négociations de confiance.

Ainsi, la relation de confiance entre organisations peut également prendre en compte des informations portant sur des procédés d'assurance et d'évaluation tels que les critères communs pour les systèmes distribués (Mayfield *et al.*, 1995). Ces critères sont plutôt orientés vers les procédés métiers de développement. On trouve cependant également des consensus sur des problématiques plus proches. Citons par exemple la recommandation (Burr *et al.*, 2006) qui décrit des niveaux d'assurance suivant les types d'authentification[4]. Ces niveaux sont par exemple utilisés pour définir des moyens d'intéropérabilité entre technologies concurrentes de délégation de l'authentification, par exemple la démonstration « Proxying Assurance Between OpenID and SAML »[5]. Ce type de travaux s'avère très intéressant dans notre cas même si nous avons explicité le fait que nous ne souhaitons pas déléguer l'authentification auprès d'une organisation tierce. Par contre, un consommateur peut tout de même requérir de connaître les moyens que le générateur emploie pour établir l'identité des entités auxquelles il délivre des certificats. Nous avons notam-

4. trad. Level Of Assurance (LOA).

5. *http : //projectconcordia.org/index.php/Planned_Scenarios_for_RSA_2009# Proxying_Assurance_Between_OpenID_and_SAML*

ment vu qu'une architecture à pseudonymes est indépendante du schéma de signature, donc qu'il est possible d'utiliser différents types de pseudonymes et de moyens de prouver leur possession tout en utilisant des certificats anonymes. Ainsi, il est concevable que les générateurs emploient différents moyens d'établissement de l'identité. L'établissement de l'identité réelle d'une entité auprès d'une organisation « générateur » peut également être pris en compte, notamment lorsqu'il est attendu des recours légaux envers l'entité en cas de préjudice. En effet, il est courant que l'identité réelle ne soit pas la seule responsabilité d'un organisme d'état, et ainsi, que d'autres organisations aient à disposition l'identité réelle d'une entité. Le consommateur peut alors accepter ces diverses information comme des informations certifiées entrant dans son règlement de contrôle d'accès. Les règlements de contrôle d'accès doivent permettre l'expression de telles contraintes. Cela peut se traduire par la retranscription de ces critères comme n'importe quel autre rôle. Dans les technologies de délégation de l'authentification et de fédération, le consommateur peut par exemple soumettre une requête de délégation de l'authentification au générateur en indiquant des recommandations sur les moyens d'authentification qu'il attend. Citons notamment la spécification PAPE[6] qui permet d'exprimer des recommandations sur les moyens d'authentification employés. Selon la même idée, différents types d'informations portant sur les pratiques du générateur peuvent être certifiées et prises en compte dans le procédé de contrôle d'accès du consommateur des certificats et donc faire partie de la négociation.

Pour conclure sur la confiance entre organisations, nous pouvons constater que la confiance est « binaire ». Une fois la confiance accordée pour la consommation d'une information certifiée, celle-ci n'est pas nuancée, même si un ensemble de critères peuvent être pris en considération dans le contrôle d'accès afin de permettre la décision d'acceptation d'une information certifiée. Cela est cohérent avec l'idée de confiance reposant sur des mécanismes de contrôle d'accès. Une fois une règle de contrôle d'accès satisfaite, le moniteur de référence ne mitige par l'accès accordé par cette règle. Nous jugeons cette mise en œuvre de la confiance dans un environnement global, et visant potentiellement diverses opérations sensibles, comme la plus pertinente. Il nous apparaît en effet peut réalisable dans la majorité des cas d'usage de faire des estimations numériques graduées des relations de confiance puis de calculer le risque d'une relation et d'accepter de consommer une information certifiées si l'estimation atteint un seuil prédéfini. Cela reste cependant envisageable dans des cas particuliers.

L'usager est lui plus éloigné de ces préoccupations. Comme nous l'avons évoqué, sa confiance est plus subjective. Cependant, il peut être supposé que la confiance de l'utilisateur peut être acquise envers quelques grands acteurs de la vie numérique, l'État ou

6. http://openid.net/pipermail/specs-pape/2008-October/000150.html

les banques par exemple. Cela peut paraître paradoxal puisque ceux-ci représentent parfois des menaces pour l'utilisateur. Cependant, dans diverses situations, notamment où interviennent des tiers inconnus, pouvoir se rattacher à une entité connue est un moyen d'obtenir de la confiance. Pour des inscriptions en ligne à des services à la personne par exemple, les collectivités locales pourraient être amenées à indexer les prestataires, éventuellement à les évaluer, agissant ainsi en systèmes de réputation, de confiance pour les usagers.

Notons également une source de confiance non négligeable que représente l'ensemble des usagers. Il est possible de mesurer la puissance de ce facteur sur des sites bien connus qui implémentent des mécanismes d'indexation des objets de fournisseurs et qui permettent aux usagers d'évaluer les fournisseurs. Ces sites prennent parfois également en charge la mise en contact des interlocuteurs ainsi que les transactions bancaires. Il pourrait être espéré la multiplication d'organisations de ce type, centralisant ces multiples tâches, et cela pour chaque type d'objets afin d'éclater les profils de consommation des initiateurs et des fournisseurs. Cependant, nous pensons qu'il s'avère trop risqué de concevoir une architecture basée sur de multiples points d'associativité, aisément associables entre eux. Ainsi, ces fonctionnalités devraient être segmentées :

- les systèmes de réputation sur lesquels les utilisateurs pourraient évaluer des fournisseurs (sur des alias ou des pseudonymes) et qui émettent des certificats contenant les évaluations (les systèmes de réputation peuvent eux-mêmes faire l'objet d'évaluations),
- l'indexation des objets des fournisseurs,
- la mise en relation du fournisseur et de l'initiateur doit pouvoir se faire sans passer par un tiers (un point d'entrée applicatif devrait être obtenu de l'entité qui assume le rôle précédent).

Le besoin en systèmes de réputation peut notamment déclencher la mise en ligne d'organismes d'évaluation pour des pans de métiers. Ces organismes, supposés indépendants, pourraient également jouer le rôle d'autorités de certification en assurant des certifications d'alias. En outre, il semble intuitif que le fait de multiplier les autorités de certification, dédiées à des ensembles particuliers d'organisations, soit un moyen de réduire la confusion des alias. Enfin, il est possible d'inclure les recommandations émises par des associations de consommateurs et de « labélisation » dans les systèmes de réputation.

Il existe de nombreux travaux scientifiques autour des systèmes de réputation, notamment en ce qui concerne l'évaluation de la confiance lorsque les recommandations font appel à de la confiance transitive (Jøsang *et al.*, 2006a ; Saadi, 2009). Sans s'étendre sur le sujet, nous avons adopté le principe de la confiance transitive pour établir une relation

de confiance en un tiers. Cependant, nous concevons difficilement la prise en considération des multiples liens de confiance indirects. Ainsi, prenons l'exemple suivant, un tiers A fait confiance à un tiers B parce qu'il a reçu une recommandation de C, que ce dernier a fondé sur une recommandation reçue de D. Nombre de travaux scientifiques visent à intégrer dans l'évaluation les liens de confiance indirects comme celui qui lie A à D par C. Or, nous considérons que A ne retire sa confiance en B que de C et non de D s'il ne reçoit de recommandation que de C, peu importe comment C a établi sa confiance en B. En effet, si on considère que A peut retirer de la confiance en B par D, c'est qu'il connaît D et lui fait confiance pour cela, auquel cas, on considère que A doit recevoir une recommandation sur B de C et de D, et non plus seulement de C. Cela rejoint la notion de confiance « binaire » précédemment introduite. Nous n'intégrons dans les règles de contrôle d'accès que les générateurs qui sont dans le domaine de confiance du consommateur, ou d'un ensemble de générateurs par l'indication d'un chemin de confiance. Cela se traduit par la consommation de certificats issus de générateurs de confiance. Il est ainsi difficilement concevable, selon les travaux menés jusqu'ici, d'accepter de définir un règlement de contrôle d'accès en indiquant des informations certifiées issues de générateurs qui ne sont pas de confiance, et ainsi, d'indiquer qu'un certificat puisse être issu d'un générateur de confiance en tenant compte d'autres générateurs, qui ne sont pas de confiance du consommateur, mais en lesquels ce générateur a confiance et desquels il a potentiellement obtenu des informations. A l'inverse, si l'ensemble des générateurs sont de confiance, et qu'il est souhaité les prendre en considération dans le contrôle d'accès, cela signifie le besoin d'obtenir directement des certificats de ceux-ci.

Essayons maintenant de répondre à la question qui est de savoir quelles informations certifiées un utilisateur peut obtenir des organisations. Il est donc supposé que des générateurs connus des utilisateurs sont disponibles dès la première utilisation du système, et que d'autres sont ajoutés au fil de l'utilisation du système. Il est possible de supposer, dans un premier temps, que les certificats à clés publiques de l'ensemble des acteurs que nous avons cités précédemment sont connus de manière sûre. Ces acteurs sont alors aisément sélectionnables par l'interface de négociation de l'utilisateur. Celui-ci peut ensuite étendre son domaine de confiance en établissant de nouvelles relations de confiance envers d'autres générateurs. Ceux-ci sont alors déclarés auprès de l'environnement de négociation de l'usager.

Revenons brièvement sur les enjeux soulevés à la section II.4. Nous avions alors indiqué que :

> "Dans l'ensemble, les enjeux pour les organisations et les usagers se rejoignent. Il y a tout de même une distinction à faire, les organisations ayant un facteur économique majeur. Elles ne dépenseront, au maximum, pas plus que ce

> qu'elles peuvent y gagner. Le facteur économique est en balance avec le respect de la vie privée, critère qui influe fortement sur le coût et la complexité de l'architecture."

L'acceptabilité des acteurs est une problématique incertaine. Nous avions mentionné, pour les utilisateurs, la confiance et l'utilisabilité. Nous préciserons à nouveau cela par la suite.

Concernant les organisations, l'acceptabilité varie selon leur type. Les organisations commerciales ont pour objectif d'augmenter la consommation de services. L'évolution des applications disponibles au travers d'interfaces Web offertes par les « hébergeurs d'applications[7] » vers des applications pensées pour le Web que l'on nomme désormais « applications comme des services[8] » a fait de ces applications un vecteur d'adoption des architectures dédiées à l"échange d'informations certifiées entre organisations et un moteur pour la constitution d'une architecture de confiance globale. Les services à la demande[9](Schechter, 1999) sur le Web sont donc une voie privilégiée pour l'adoption par les entreprises des technologies de gestion des identités pensées pour un environnement ouvert.

Les administrations ont pour ambition de développer des services en ligne, ambition qui prend généralement la forme de projet intitulé « e-administration » et qui vise à réduire les coûts des démarches administratives notamment par la dématérialisation des documents administratifs. Lorsque les démarches sont réalisées en ligne, les frais de personnel administratif sont moindres, notamment du fait de l'automatisation des tâches. Cela fait des administrations des moteurs de la vie numérique, potentiellement sources de générateurs et de consommateurs de certificats. Notons également que tout document administratif dématérialisé peut être un certificat utilisable dans une négociation, donc que l'architecture définie se prête particulièrement bien à la conduite de démarches administratives et la constitution de dossiers administratifs.

Les moteurs pour une architecture de confiance globale sont donc réels. En outre, il semble que nous soyons à l'aube d'une telle architecture si l'on prend les projets du domaine comme indicateurs : FederID[10], FC^{2}[11], PRIME[12], Kantara Initiative[13], Concordia[14], Li-

7. trad. Application Service Provider (ASP)
8. trad. Software As A Service (SAAS).
9. trad. On Demand Services.
10. www.federid.org
11. www.fc2.org
12. https://www.prime-project.eu
13. kantarainitiative.org
14. projectconcordia.org

berty Alliance[15], Mon service Public[16], Internet2[17], etc. Cependant, cela n'implique pas qu'une architecture basée sur des mécanismes respectueux de la vie privée des usagers sera déployée. Il peut être mis en avant un argument déjà présenté en première partie, que l'adoption par les utilisateurs d'une telle architecture soit plus forte si elle est comprise comme un plus grand respect de leur vie privée. De plus, sur un plan architectural, les offres de services sont amenées à se multiplier, et la puissance de leur combinaisons est à découvrir au gré des mises en œuvre. Il est donc possible de supposer des problématiques d'orchestration. Or, penser une architecture centrée sur l'utilisateur est un premier pas vers l'idée de créer des applications distribuées dont les bouquets de services seraient composés par l'utilisateur au gré de ses besoins. L'utilisateur serait alors pensé comme le chef d'orchestre des architectures orientées services[18] et son agent de négociation comme une base pour produire un agent permettant cette orchestration en assurant les problématiques de contrôle d'accès.

15. projectliberty.org
16. www.service-public.fr/monservicepublic
17. www.internet2.edu/
18. trad. Service Oriented Architecture (SOA).

VIII.3 Vocabulaire et sémantique

Le paradigme de la communication dans le monde numérique pourrait se résumer à la nécessité qu'êtres humains et machines se comprennent. Il est possible de disserter longuement sur la notion de compréhension. Nous nous contenterons de l'idée qu'un but consécutif à une communication puisse être atteint si les interlocuteurs se comprennent. Cela soulève des problématiques de vocabulaire et de sémantique. Les besoins pour les échanges inter-organisationnels sont multiples, il est cependant possible de les regrouper en trois domaines :

- les informations d'identités,
- les règlements,
- les messages protocolaires.

Les divers interlocuteurs doivent pouvoir s'appuyer sur un vocabulaire commun et il faut qu'il y est consensus sur le sens de chacun des termes. Il est en effet nécessaire que de multiples organisations de toutes nationalités puissent s'échanger des informations, d'une part, et qu'un utilisateur de n'importe quel pays puisse interagir au sein du système d'autre part.

Il existe de nombreux travaux dans le monde informatique qui présentent des terminologies nous concernant : la gestion des identités (MacGregor *et al.*, 2006a), l'anonymat (Pfitzmann & Kohntopp, 2001), la confiance (McKnight & Chervany, 1996), etc. Il est donc possible de concevoir un thésaurus global commun des domaines cités précédemment, et ensuite, de s'appuyer sur des solutions technologiques pour internationaliser ce vocabulaire. Cela conduirait à l'emploi de multiples espaces de noms concordants.

Cependant, le sens des termes est primordial pour la compréhension entre interlocuteurs. Ainsi, les définitions de termes sont nécessaires, puis il est important d'adopter une démarche descriptive du domaine dans lequel ces termes sont signifiés afin de préciser ces définitions. Il s'agit notamment de décrire les relations qu'il peut exister entre les termes. Dans (MacGregor *et al.*, 2006a), il est par exemple donné de multiples relations liant les fournisseurs et les consommateurs de certificats, les sujets de ceux-ci, etc. En outre, une description de domaine, bien qu'enrichissant les définitions d'un vocabulaire, peut être une interprétation subjective (d'ordre culturel par exemple) des définitions et des relations liant les termes. L'utilisation d'un langage formel pour la description d'un domaine semble alors se justifier pour contribuer à réduire la subjectivité de l'interprétation. Il peut donc être intéressant de s'appuyer sur un vocabulaire et des définitions faisant référence dans le domaine, puis de les décrire de manière formelle. Une définition formelle n'écarte cependant pas toute subjectivité introduite par les concepteurs de la description, même

si elle contribue à la réduire. Outre la synthèse des termes existants, décrire de manière objective un domaine relève plus du consensus que d'une question technologique et par conséquent nécessite des moyens humains importants.

En admettant qu'une telle initiative soit conduite avec succès cela permettrait de définir un langage commun pour un système de négociation universel. En outre, cela ouvre la voie à des applications intéressantes, notamment du fait que la formalisation permette l'interprétation par un algorithme. Il devient donc possible, dans notre cas d'étude, de constituer des bases de connaissances compréhensibles de moteur d'inférence, donc de permettre des déductions sur les données produites des multiples négociations. Plusieurs applications semblent alors intéressantes au regard des problématiques soulevées jusqu'ici, citons par exemple le fait de déduire des propriétés prouvables sur les attributs d'identités ou le fait de déduire des règles d'automatisation à partir des choix de l'utilisateur.

Toute la difficulté réside dans la représentation de la connaissance. Plusieurs moyens ont été proposés avec divers niveaux d'expressivité. L'« hypothèse cognitiviste », ou le « cognitivisme », suppose que la cognition est, selon (Varela, 1988), la manipulation de symboles par un traitement computationnel. Les symboles sont des éléments qui représentent ce à quoi ils correspondent, ce que (Searle, 1985) nomme l'intentionnalité. De ce mouvement scientifique naît l'intelligence artificielle. Celle-ci repose initialement sur les réseaux sémantiques (Quillian, 1967) permettant de modéliser le mécanisme d'association d'idées. Divers autres formalismes lui ont ensuite succédé, par exemple les « frames » (Minsky, 1975) et les « scripts » (Shank & Abelson, 1977). La logique est aussi une dimension fondamentale de la description. La logique du premier ordre fut d'abord reconnue comme le moyen de donner du sens aux frames (Hayes, 1979). Furent ensuite employées la logique des propositions et la logique des prédicats, toutes deux sujettes à des difficultés computationnelles. Ce fut grâce à la logique de description que la logique pris une place importante dans la description de la connaissance (Brachman & Schmolze, 1985). Cela permit notamment au domaine de l'ontologie d'être perçu et employé comme support à l'inférence. Rappelons alors la définition de l'ontologie la plus couramment employée (Gruber *et al.*, 2007) :

> "Dans le cadre des sciences informatiques, une ontologie est une spécification d'une conceptualisation. Cela signifie qu'elle spécifie les concepts, les idées, les relations, les abstractions et davantage de manière objective. L'objectif est de clarifier le sens en permettant de partager la connaissance.[19]"

19. trad. "In the context of computer and information sciences, an ontology is a specification of a conceptualization. That is, it specifies the concepts, ideas, relations, abstractions, and so forth in an objective form. The intent is to clarify the meaning, enabling shared understanding."

Il s'agit donc de décrire un domaine en prenant attention à la subjectivité appelée biais ontologique. La seconde difficulté est celle de restriction du domaine. Plus il est large, plus il est difficile de le définir de manière exhaustive. En outre, la conception d'une ontologie se fait généralement en connaissance de l'existant et des possibilités d'extension. Ainsi, une ontologie peut être de haut-niveau, de domaine, de tâche ou d'application. Il est dans un premier temps possible de décrire une ontologie de manière graphique, en faisant apparaître les termes appelés concepts ainsi que leurs relations. On parle de « conceptualiser un domaine ». La logique descriptive, et les langages de description dérivés (par exemple OWL, SWRL, etc.), permettent ensuite de décrire de manière formelle l'ontologie. Il est ainsi possible de créer ce que l'on nomme couramment un système à base de connaissance dont le principe est de permettre de déduire des conséquences implicites d'une connaissance représentée explicitement (McGuinness *et al.*, 2003).

Le domaine est ainsi décrit par les définitions des termes et par un modèle, appelé « TBox », constitué d'un ensemble de règles qui régissent le domaine. Ce modèle représente la base de connaissances. Ce modèle est ensuite instancié lors d'une phase d'exploitation, il est alors évoqué le « peuplement de la base de connaissances d'individus ». L'ensemble de ces données est appelé « ABox ». Il est ainsi possible de déduire des connaissances sur la population des règles de la base de connaissances.

Nous pouvons tracer une esquisse de la constitution d'une base de connaissances de la négociation et donner un exemple d'application. Ainsi, la base de connaissances peut décrire ce qu'est une règle et une information d'identité de manière à extraire d'une règle les informations requises. Des règles peuvent ensuite être ajoutées de manière à déduire que, par exemple, lorsqu'une date de naissance est requise, un âge peut être prouvé. On peut également bâtir des règles plus riches. Il serait par exemple possible de définir une règle indiquant qu'une coordonnée est dans une zone géographique. Puis, en indiquant qu'un lieu de naissance est une coordonnée, et un pays une zone, il est possible de prouver que l'on est né dans un certain pays, et si le droit du sol s'applique dans ce pays, qu'un individu est né avec la nationalité correspondante. Ainsi, lorsqu'il est demandé à un individu son lieu de naissance, le système de déduction doit lui indiquer qu'il peut proposer à son interlocuteur de lui prouver qu'il est d'une certaine nationalité. Si la proposition est acceptée par le fournisseur, la preuve serait par exemple basée sur un calcul à partir du lieu de naissance contenu dans le certificat « pièce d'identité » (en supposant une base de données associant le nom d'une ville à ses coordonnées géographiques) et d'un certificat contenant les coordonnées du pays en question. Notons que cette règle peut ensuite être répertoriée et être proposée sans nécessiter d'inférence. Il est ainsi envisageable de constituer une base des propriétés connues, éventuellement de l'inférence, et de permettre ce procédé en complément en cours de négociation.

Au fur et à mesure des négociations, il est ainsi possible de faire appel à la base de connaissance pour essayer de déduire des preuves possibles. Il est important de distinguer le peuplement de la base de connaissances, pour faire ce type de déduction, d'une seconde application qui peut être la création d'une base de données formalisées des informations de négociations, suivant les règles de la base de connaissance utilisées pour structurer l'information. Cette base peut être employée pour extraire des données comme on le ferait d'un journal d'activité. Il est également possible d'exploiter cette base *a posteriori* pour faire des études statistiques ou comportementales.

L'utilisation d'une base de connaissances pour faire de la déduction sur des faits est la base des « systèmes experts ». La difficulté de tels systèmes est que les experts doivent représenter leurs connaissances et la maintenir, soit créer la base de connaissances de la négociation. Il est également envisageable que les utilisateurs puissent être ces « experts ». En d'autres termes, en supposant que les utilisateurs proposent d'eux-mêmes des preuves à leur interlocuteur, et qu'il soit possible de les formaliser, il serait possible que les interactions de l'utilisateur soient un moyen d'« instruire » le système en approvisionnant la base de connaissances.

De la même manière, le système pourrait être muni de quelques règles d'automatisation connues sur les interactions des utilisateurs, comme nous avons pu en décrire à la section VI.4. Puis, en faisant les mêmes suppositions que précédemment, une application pourrait être de déduire à partir des choix de l'utilisateur des règles d'automatisation.

VIII.4 Concrétisation et standardisation

L'ambition de cette section est de mettre en avant les technologies du système de négociation qui doivent être soumises à l'effort de standardisation. Il s'agit d'identifier toute technologie sujette à entrer dans une problématique d'interopérabilité et d'y répondre par un standard existant si cela est possible.

Il ne s'agit pas de vouloir ré-employer des standards à tout prix dans un élan d'altruisme. Nous justifions cela par le fait que la réutilisation de standards publiquement identifiés pour leurs fonctionnalités permet de rendre lisible un projet s'appuyant sur de multiples standards. Ainsi, la « modularisation », soit les diverses fonctionnalités d'un agent, peut être rendue plus compréhensible par l'utilisation de standards. La réutilisation des standards permet également de rationaliser les procédés de développement. Les standards sont par nature éprouvés. En outre, ils ont pour certains fait l'objet de développements logiciels, ce qui permet d'envisager la réutilisation de briques logicielles existantes. Ceci peut également stimuler l'adoption de la technologie. En résumé, s'appuyer sur des standards peut permettre une adoption des briques du projet qui n'ont pu faire l'objet de la réutilisation d'un standard.

Cette démarche nous permet en outre de concrétiser ces travaux. En effet, l'interopérabilité touche deux domaines bien distincts : les algorithmes et la sérialisation. Ainsi, cette section est l'opportunité de faire correspondre des technologies aux concepts et aux fonctionnalités exposés précédemment.

VIII.4.1 Standards sur les algorithmes

Dans cette section, nous entendons par algorithme sujet à l'interopérabilité tout processus dont la finalité est dépendante d'un processus complémentaire sur un tiers distinct. On distingue ici volontairement la finalité de l'objet. Par exemple, le processus complémentaire du chiffrement est celui de déchiffrement. L'objet du chiffrement est de rendre un message inintelligible. La finalité du procédé est de transmettre un message confidentiel. Notons au passage que l'on fait abstraction des procédés sous-jacents qui sont dans ce cas le transport, l'encapsulation, etc. Nous concernant, les algorithmes principaux sujets à l'interopérabilité sont :

- les algorithmes de chiffrement,
- les algorithmes de négociation qui constituent l'essentiel du protocole de négociation.

VIII.4.1.1 Les algorithmes de chiffrement

Le standard de chiffrement asymétrique RSA (Rivest *et al.*, 1978) peut être employé pour générer le pseudonyme fournisseur, échanger le secret assurant la confidentialité des échanges et permettre l'authentification du fournisseur. Pour la réalisation de la confidentialité du canal de communication, le standard TLS (Dierks & Allen, 1999 ; Dierks & Rescorla, 2006) est exploitable comme nous l'avons précisé à la section V.3.2. Les algorithmes de chiffrement symétriques sont alors ceux définies dans les spécifications de TLS.

Aucun standard n'est établi pour les algorithmes de chiffrement des pseudonymes initiateurs présentés dans le système à pseudonymes (Camenisch & Lysyanskaya, 2001). Il est cependant possible d'employer des pseudonymes qui sont des clés RSA. Le schéma de signature CL-Signature (Camenisch & Lysyanskaya, 2003) employé pour les certificats n'est pas non plus un standard. Par ailleurs, il existe d'autres schémas de signature qui pourraient satisfaire certaines propriétés attendues comme nous avons pu le voir. Enfin, les preuves de connaissances peuvent s'appuyer sur les algorithmes dérivés du protocole de Shnorr (Schnorr, 1990) qui sont aujourd'hui couramment employés.

VIII.4.1.2 Les algorithmes de négociation

Les algorithmes de négociation ont deux dimensions soumises aux problématiques de l'interopérabilité, celle algorithmique et celle de sérialisation qui est traitée par la suite. L'interopérabilité des algorithmes de négociation a fait l'objet de travaux scientifiques dont le principale est celui proposé par Li *et al.* (Li *et al.*, 2002). Par exemple, l'algorithme de négociation ETTG appartient à une famille d'algorithmes de négociation interopérables entre eux. Cependant, comme nous l'avons souligné, l'utilisateur est en quelque sorte un algorithme non-déterministe, ce qui ne permet pas de prétendre à l'interopérabilité des algorithmes de négociation ayant pour finalité des critères tels que la diffusion minimale d'information ou la complétude.

Il est également possible d'inclure dans l'agent de négociation le support d'autres technologies de certificats. Il s'agit donc de supporter d'autres algorithmes d'obtention, de signature et de présentation avec leurs limitations en terme de non-associativité notamment. Il est par exemple tout à fait concevable d'accepter des sources de certificats issues des spécifications CardSpace (Nanda & Jones, 2008), SAML2 (Maler, 2006) ou ID-WSF (Tourzan & Koga, 2007) qui pourront être présentés à des consommateurs supportant ces mêmes spécifications. Lorsque les spécifications ne diffèrent que par leur sérialisation, et non pas par l'algorithme de chiffrement, l'interopérabilité des diverses spécifications est possible, par exemple entre SAML2 et WS-Federation1.1b (Ates *et al.*, 2007). Il est en outre concevable concevable de combiner diverses spécifications. Par exemple, il est pos-

sible d'employer des assertions SAML, ne permettant pas la propriété de non-associativité, contenant des données issues d'un schéma de signature différent de celui de signature de l'assertion et permettant de mener des preuves de connaissance sur certains attributs (qui ne seraient donc pas « en clair » dans l'assertion).

VIII.4.1.3 Autres sujets à l'interopérabilité

Il y a d'autres sujets qui se rapportent à l'interopérabilité en terme de processus, même s'ils diffèrent de la définition de cette notion exprimée précédemment. En effet, il est possible d'y inclure les procédés pris en compte dans les contrats d'assurance que nous avons présenté dans ce chapitre à la section VIII.2. De tels contrats portent souvent sur l'emploi de procédés, par exemple les mécanismes d'authentification et les logiciels employés. Il s'agit donc bien d'accords sur les procédés même s'il n'y a pas réellement d'interopérabilité au sens pratique. Il y a par contre interopérabilité dans le sens où deux organisations acceptent une relation si les engagements d'un contrat, portant sur des procédés, sont respectés. Citons les mêmes références que précédemment pour les exemples donnés : (Burr *et al.*, 2006) pour les mécanismes d'authentification et (Mayfield *et al.*, 1995) pour des pratiques de sécurité plus générales, incluant notamment les pratiques de développement logiciel.

VIII.4.2 Standards pour la sérialisation

A de nombreuses reprises nous avons employé le terme « sérialisation ». Le terme sérialisation est employé comme un procédé permettant de transformer une information en une donnée qu'une machine puisse traiter. Cela justifie le fait que nous employons le terme de sérialisation pour décrire par exemple le procédé permettant de retranscrire en documents XML (Bray *et al.*, 2008) les données du système de négociation qui sont échangées. Ce procédé permet de passer d'une description fonctionnelle à des données structurées de manière à permettre à un algorithme l'extraction et le traitement de ces données. Ce procédé peut s'appuyer sur un ou plusieurs espaces de noms faisant éventuellement l'objet d'un travail ontologique. Il est possible de représenter les données en « ensembles cohérents », soit le fait qu'un ensemble de données ait un sens à être ainsi regroupées, par exemple une information d'identité, un certificat, une règle, un règlement, un message protocolaire, etc. Ainsi, nous définissons le terme « format des données » comme un ensemble de choix technologiques incluant la sérialisation mais également d'autres procédés visant le traitement des données tels que l'encodage (en UTF8 par exemple) ou la compression.

La première intuition est de retranscrire les ontologies des domaines qui nous concernent en des espaces de noms standards. Il est ensuite nécessaire de structurer ces données

à l'aide d'une « syntaxe » standard. Avant de décrire les sérialisations nous concernant, il est nécessaire de donner un aperçu des technologies du Web, riches en standards et couramment employées pour la sérialisation.

VIII.4.2.1 Les technologies du Web

Les technologies du Web sont à la sérialisation de documents et à leur transport ce que la pile TCP/IP est aux couches *transport* et *réseaux* du modèle OSI.

Le protocole applicatif HTTP (IETFWorkingGroup, 2009) est employé comme un protocole permettant principalement le transport de documents. Il peut donc être employé comme un protocole de transport pour des flux applicatifs si ceux-ci prennent la forme de documents. C'est par exemple le cas des architectures de fédération.

Les URL[20] (Berners-Lee, 1998) sont des identifiants employés comme le moyen de désigner un document sur un hôte ou un point d'entrée applicatif, application qui peut être servie par le protocole HTTP.

Enfin, les documents sont sérialisés au format XML (Bray *et al.*, 2008). XML est un métalangage qui définit un ensemble de règles orthographiques, abusivement dites « syntaxiques », permettant une structuration par arborescence d'un document. Pour permettre la sérialisation d'un document XML, il est possible de s'appuyer sur un espace de noms, le vocabulaire, éventuellement exprimé au sein des documents à l'aide du standard XML Namespaces (Bray *et al.*, 2006), et une grammaire définie à l'aide d'un schéma de document, dont les standards les plus courants sont les schémas DTD (Bray *et al.*, 2008) et les schémas W3C XML Schema (Gao *et al.*, 2009 ; Peterson *et al.*, 2009). Il est ainsi possible de définir des langages XML, aussi appelés des applications de XML, qui permettent de bâtir des documents respectant la syntaxe XML, un espace de noms et une grammaire. Une application XML permet donc de sérialiser un ensemble cohérent de données, à la condition de définir l'espace de noms et le schéma correspondant.

XML et ontologie

Il est possible de retranscrire une ontologie en de multiples espaces de noms. Les diverses dénominations sont alors synonymes d'un unique terme de l'ontologie afin de conserver le travail ontologique. Les documents XML permettent par leur structure arborescente de faire aisément un travail de changement d'espace de nom, ce qui peut être une aide pour l'internationalisation des applications. Cela permet en outre de pouvoir éventuellement sérialiser les ensembles de données dont nous avons besoin avec plusieurs

20. Unique Ressource Location

sérialisations standards concurrentes.

L'ontologie peut servir la sérialisation en servant de base à la constitution des espaces de noms. Inversement, l'emploi de XML pour la sérialisation peut également servir à un travail ontologique. Nous avons exposé à la section précédente qu'une ontologie pouvait être à la fois un thésaurus et un ensemble de concepts liés par des relations logiques. L'emploi de XML peut par exemple être le moyen d'identifier au sein de documents XML les concepts décrits par l'ontologie et faciliter le peuplement d'une base de connaissances. La base de connaissances d'une ontologie peut elle-même être sérialisée à l'aide d'une application XML. Cette application doit permettre de représenter les concepts et les relations qui les lient. L'application XML RDF (Beckett, 2004) permet de décrire des concepts. L'application XML OWL (Motik *et al.*, 2009) étend RDF en permettant une expressivité plus forte satisfaisant celle requise pour l'expression d'une base de connaissances. Il est d'une part important de distinguer le travail ontologique servant la sérialisation de la sérialisation servant le travail ontologique. Il est d'autre part important de distinguer au sein d'un travail ontologique les deux emplois de XML donnés précédemment : l'utilisation de documents XML pour peupler une base de connaissances et la notion de sérialisation de l'ontologie au format XML. En effet, le terme « Web sémantique » introduit parfois une confusion entre ces deux applications, notamment du fait qu'il est courant de « tagger » les documents XML existants pour y ajouter du sens. Cette pratique consiste à analyser des documents XML et à les enrichir d'éléments signifiants pour permettre une analyse ultérieure. Cette pratique peut notamment être employée pour faciliter le peuplement d'une base de connaissances. Enfin, le célèbre schéma du Web sémantique (cf. figure VIII.1) tel qu'il est donnée par le W3C (Berners-Lee, 2000) porte lui-même à confusion. En effet, il décrit un empilement de « couches technologiques » avec les applications XML à la base, puis en remontant, la description de domaines comprenant l'aspect ontologique, les relations entre termes, et enfin, la notion de confiance. Nous traduisons de ce schéma l'idée que l'ensemble des données pouvant exister à travers le Web peuvent être formalisées sous la forme d'ontologies et celles-ci sérialisées en XML. Les documents XML peuvent également être utilisés à la fois pour le peuplement de bases de connaissances ou pour exprimer les bases de connaissances. Ils peuvent ensuite être signés à l'aide des technologies de signature XML et permettre ainsi l'authentification et donc la gestion de la confiance.

XML et protocoles de communication

Les documents XML peuvent jouer le rôle de messages protocolaires. XML permet une structure arborescente des documents, propice à la notion d'encapsulation. Il est ainsi possible de concevoir des documents XML valides pour un schéma « parent », et intégrant des documents respectant d'autres schémas. Cela confère parfois à XML un rôle d'encapsulation utile pour les applications distribuées. En effet, les échanges des applications

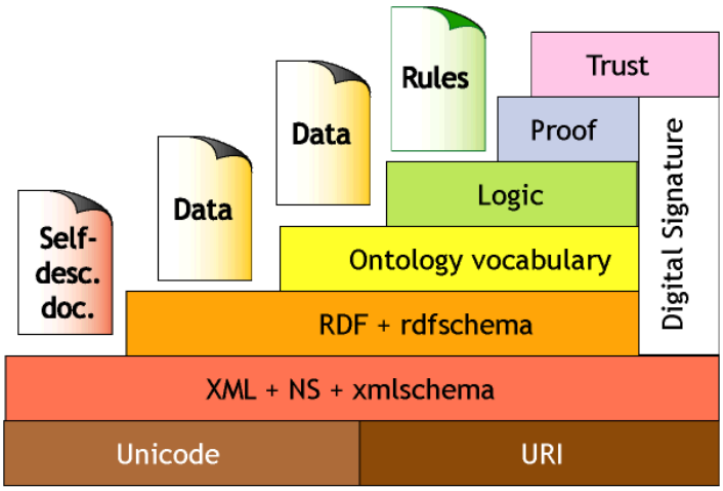

FIG. VIII.1 – *« Pile » du Web sémantique.*

distribuées peuvent reposer sur des messages XML, ce qui permet le fait que chaque agent puisse, en fonction de ses aptitudes, n'analyser que des sous-parties de documents XML. En utilisant les standards W3C XML Encryption (Imamura *et al.*, 2002) et W3C XML signature (Bartel *et al.*, 2008) par exemple, cela prend tout son sens puisque des sous-parties d'un document peuvent être rendues intelligibles à certains relais du message, et chaque relais peut être amener à signer ou à vérifier les signatures de plusieurs ensembles de données d'un même document.

L'utilisation de XML et la réutilisation d'applications de XML existantes semblent donc être une voie à privilégier pour la sérialisation. Posons-nous maintenant la question de l'exploitation de HTTP. HTTP est un protocole applicatif simple permettant le transport de documents. Il est donc possible de réaliser un protocole applicatif en employant HTTP et XML. Il s'agit notamment du mécanisme employé lors d'une délégation de l'authentification en SAML. La requête de délégation de l'authentification et sa réponse contenant l'assertion SAML sont des messages XML qui peuvent être chiffrés et signés par le fournisseur de services et le fournisseur d'identités. Le transport de ces messages est assuré au travers du navigateur de l'utilisateur employé comme relais. Ainsi, il y a deux échanges protocolaires de transport des messages, entre le fournisseur de services et le navigateur d'une part, et entre le navigateur et le fournisseur d'identité d'autre part. Il n'y a cependant qu'un seul échange protocolaire au niveau applicatif entre le fournisseur de services et le fournisseur d'identités.

Cependant, le protocole HTTP présente une particularité qui peut être considérée comme une limitation. Il ne permet de requête que du client vers le serveur. Or, comme nous l'avons constaté, le serveur peut être amené à produire des requêtes au niveau applicatif,

celles d'initiation de négociations. Cela suppose que le protocole applicatif de négociation transporté par le protocole HTTP puisse contenir des requêtes au sein de réponses HTTP. Il s'agit du cas du protocole de fédération où les requêtes des fournisseurs de services apparaissent dans les réponses HTTP. Notons cependant que l'initiation d'un fournisseur fait toujours suite à une requête d'une ressource qui ne peut être satisfaite. Il est donc possible de considérer qu'il y a des requêtes de l'utilisateur jusqu'à l'obtention de la ressource, ce qui permet au fournisseur de soumettre autant de requêtes du protocole de négociation qu'il le souhaite.

Nous supposerons donc que le protocole applicatif, celui de négociation, peut être conduit au travers de documents XML transportés ou non par le protocole HTTP. Cela n'a, en fait, que peu d'importance puisque l'expressivité des messages protocolaires n'est pas dépendante du protocole de transport. Notons enfin que, du point de vue du transport des messages protocolaires, nous considérons le niveau applicatif comme celui du protocole de négociation, le protocole de transport étant par exemple le protocole HTTP. Au chapitre précédent, nous avons étudié les messages protocolaires au niveau du protocole de négociation et nous avons considéré le niveau applicatif simplement comme celui du flux applicatif, le protocole de transport pouvant alors être le protocole de négociation si celui-ci encapsule les flux applicatifs.

VIII.4.2.2 Certificats, méta-données de certificats et règlements des générateurs

La sérialisation des certificats issus d'un schéma de signature assurant la propriété de non-associativité n'a pas fait l'objet de spécifications publiques connues à ce jour. Nous faisons ici une telle proposition.

Principe

La première nécessité est celle de définition des espaces de noms pour les informations d'identité et les certificats. L'espace de noms des informations d'identité peut être par exemple celui de LDAP, de SAML, ou de CardSpace. Celui des certificats peut être en parti basé sur des termes issus des certificats X509. Nous employons donc des espaces de noms standards mais qui peuvent être substitués par d'autres espaces de noms. A cela, nous ajoutons un espace de nom permettant de décrire les notions introduites par les certificats anonymes et décrites dans la suite de cette section.

Il est ensuite nécessaire de structurer les ensembles de données : les informations d'identité, les certificats et les règlements de générateurs stipulant notamment les informations certifiées fournies. Nous avons découpé ces informations en plusieurs types de documents

XML :

- les métadonnées publiques de générateur,
- les métadonnées privées de générateur,
- les métadonnées de certificats

Nous employons le terme « métadonnées » de certificat pour désigner les données qui décrivent les données signées. Le terme « métadonnées » publiques de générateur est emprunté à la spécifications SAML pour désigner un ensemble de données publiques qui permettent l'obtention du service de génération de certificats. Le terme « métadonnées » privées de générateur est employé par analogie.

Nous justifions ainsi le choix de ces différents types de documents. Les certificats rassemblent habituellement les métadonnées et les données, l'ensemble sous le couvert d'une même signature. Nous avons indiqué que les preuves sur les attributs pouvaient nécessiter des opérations mathématiques sur les valeurs des attributs contenues dans la signature. Cela nous a conduit à recommander que les attributs pris en compte dans le calcul de la valeur de signature ne contiennent que les valeurs des attributs, et non plus, des couples (nom,valeur) ou des tuples (nom, valeur, type) comme cela se pratique couramment. Le fait que les certificats ne contiennent que les valeurs des attributs apparaît dans un premier temps plus simple à gérer compte tenu du fait que la génération des preuves de propriétés reposent sur des opérations arithmétiques sur les attributs. La valeur numérique exacte de l'attribut est en outre requise pour mener des preuves de propriété. Dans le cas contraire, c'est-à-dire qu'il n'est pas souhaité que des preuves de propriété soient menées sur l'attribut concerné, une valeur de hachage de l'attribut suffit pour permettre la présentation sélective. Les métadonnées d'un attribut (sa désignation, son type, etc...) peuvent alors être incluses dans cette même valeur de signature en employant un *générateur*[21] différent. En outre, ces métadonnées peuvent également être contenue dans un document tiers décrivant la signature et son contenu, lui-même signé du générateur.

Les attributs sont représentés lors d'un calcul de signature par un *générateur*. Or, à la section IV.4.1 nous avons précisé que le choix d'un *générateur* pour représenter un attribut devait connu publiquement, c'est- à-dire que ce choix soit valable quel que soit le porteur qui obtienne un certificat, afin d'éviter que le choix de *générateurs* par le générateur ne représente un risque de canal caché.

Ces deux constatations nous ont poussées à proposer que la description du contenu des certificats se fasse dans des méta-données publiques signées du générateur, appelées « méta-données du générateur ». Ces métadonnées contiennent l'ensemble des informa-

21. Rappelons que lorsque le mot générateur suppose l'élément mathématique il est noté en italique.

tions relatives au contenu des certificat à savoir la désignation des *générateurs* employés pour représenter les attributs ainsi que la désignation des attributs, leur type et éventuellement les propriétés qu'ils peuvent permettre de prouver. Elles décrivent également les attributs des certificats (durée de validité, nombre d'utilisation, mécanisme d'authentification, identifiant de certificat, etc.). Elles peuvent également indiquer si plusieurs types de certificats sont délivrés. Ces méta-données sont publiques et valables pour toutes les identités ce qui n'en fait pas un facteur d'association lors d'une présentation d'information signées. Ainsi, un certificat est composé des métadonnées du générateur, des données contenues dans la valeur de signature et présentées au gré du porteur, et la valeur de signature.

Notons que lors de la conduite de preuve, le porteur et le consommateur doivent convenir des générateurs qui sont employés pour conduire la preuve. Cela implique que conduire une preuve de possession d'une signature valide d'un générateur peut revenir au fait que l'utilisateur indique quels attributs sont contenus dans le certificat s'il restreint l'emploi de générateur dans sa preuve à ceux pris en compte dans le calcul de la signature. Cependant, la possession d'une signature peut être prouvée avec des générateurs qui n'ont pas été pris en compte lors du calcul de la signature et cela sans que la preuve ne soit pas valide et donc sans que le consommateur ne sache si l'attribut représenté par ce générateur est inclus ou non dans la valeur de signature. Ce qui est requis lors de la conduite d'une preuve est que l'utilisateur connaisse les valeurs des attributs contenus dans le calcul de la signature. Il est ainsi possible de conclure que le consommateur ne sait pas quels attributs sont contenus dans une valeur de signature si le porteur ne le lui indique pas, donc, que par défaut, le consommateur et le porteur devrait conduire une preuve avec tous les générateurs contenus dans les métadonnées publiques du générateur afin d'éviter que l'utilisateur n'ait à fournir ce renseignement qui peut ne pas être valide.

Les métadonnées privées du générateur sont principalement les valeurs de sa clé privé, qui peuvent se réduire à l'un des facteurs premiers du module. Nous présentons un moyen de les sérialiser au sein d'un document XML. Il est bien sûr nécessaire, si l'emploi d'un tel document est choisi, de le sécuriser de manière approprié.

Les métadonnées publiques du générateur servent à un porteur potentiel à déterminer les moyens de parvenir à l'obtention du service de génération, en indiquant les points d'entrée applicatif par exemple, et à déterminer quels attributs certifiés un générateur est à même de fournir. Elles vont également servir de référence des valeurs de la clé publique du générateur lors de la conduite de preuve. Lorsque le porteur prouve la possession d'une signature sur des attributs, il présente les méta-données du générateur au consommateur, si celui-ci ne les a pas déjà en sa possession, en même temps que la valeur de signature et

les attributs. Il prouve ensuite que ces attributs ont été pris en paramètre lors du calcul de valeur de signature.

Les métadonnées du générateur servent au consommateur lors de la phase de conduite des preuves. Elles garantissent aux consommateurs les *générateurs* avec lesquels sont représentés les attributs, ce qui empêche le porteur de présenter un attribut pour un autre. Elles servent également pour réaliser les protocoles de preuves comme document de référence pour les valeurs de la clé publique du générateur. Enfin, il s'agit d'une référence pour déterminer les propriétés prouvables sur les attributs.

Il est nécessaire que le porteur connaisse les attributs et leurs valeurs contenues dans la valeur de signature. Lors de l'obtention d'un certificat, l'utilisateur peut de lui-même créer un document rassemblant ces informations, ou le générateur peut lui délivrer un récapitulatif de ces informations. Nous avons appelé ces informations les « métadonnées du certificat » bien que ce terme puisse porter à confusion. En effet, ces données sont employées par le porteur lors de la présentation d'informations certifiées mais ne sont jamais présentées au consommateur, qui, rappelons le, ne se base que sur les métadonnées publiques du générateur, la valeur de signature et éventuellement les données contenues dans la valeur de signature que le porteur révèle.

Le porteur, lorsqu'il obtient une valeur de signature du générateur, ne connait le contenu signé que de ce que le générateur lui indique. L'utilisateur peut alors vérifier que la valeur de signature contient bien chacune des informations censé être contenu. La délivrance de métadonnées de certificats signées du générateur semble donc être un mécanisme redondant mais permettant à l'utilisateur d'éviter une vérification fastidieuse de la valeur de signature et apportant une preuve, déjà sérialisée, du contenu du certificat obtenu.

Réalisation

La réalisation de la sérialisation des métadonnées de générateurs et de certificats inclue la définition de schémas XML ainsi que l'implémentation d'un outil de génération de documents XML respectant ces schémas. Nous avons choisi de donner le nom « x23 » à cette sérialisation [22]. L'ensemble des documents XML présentés dans cette section et en annexes sont des documents valides issus d'un cas d'usage et peuvent donc être employés tels quels à des fins de tests. Il en est de même pour les valeurs cryptographiques et les certificats X509 inclus dans les signatures W3C XML Signature (Bartel *et al.*, 2008).

22. Le choix de cette appellation se base sur la lettre « x » indiquant une sérialisation en XML et le nombre 23 pour l'appréciation de ce nombre premier par l'auteur. A ce propos, notons que 2 et 3 sont également des nombres premiers dont la somme est un nombre premier.

Il a été choisit de créer un document de schéma décrivant un espace de nom et permettant de créer les trois types de documents XML souhaité valide pour ce même schéma. Ce schéma est au format W3C XML Schema (Gao *et al.*, 2009 ; Peterson *et al.*, 2009). Il est reporté en *annexes C* et est disponible en ligne à l'adresse *http://magnum.telecom-st-etienne.fr*. Nous présentons ici des extraits de ce schéma.

Voici l'extrait du schéma relatif aux documents contenant les métadonnées publiques du générateur :

```
<xsd:element name="CLSIGPublicKey" type="CLSIGPublicKeyType"/>
<xsd:complexType name="CLSIGPublicKeyType">
  <xsd:sequence>
    <xsd:element name="modulus" type="xsd:string" minOccurs="1" maxOccurs="1"/>
    <xsd:element name="generators" type="generatorsType" minOccurs="1"
maxOccurs="1"/>
    <xsd:element name="exponent" type="xsd:string" minOccurs="1" maxOccurs="1"/>
  </xsd:sequence>
</xsd:complexType>


<xsd:element name="providerPublicMD" type="providerPublicMDType"/>
<xsd:complexType name="providerPublicMDType">
  <xsd:sequence>
    <xsd:element name="alias" type="xsd:string" minOccurs="1" maxOccurs="1"/>
    <xsd:element ref="ds:KeyInfo" minOccurs="1" maxOccurs="1"/>
    <xsd:element name="iis" type="iisType" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="certAttrs" type="certAttrsType" minOccurs="0" maxOccurs="1"
/>
    <xsd:element ref="ds:Signature" minOccurs="0" maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>
```

L'élément obligatoire *CLSIGPublicKey* contient les paramètres cryptographiques. L'élément *providerPublicMD* est l'élément racine du document. L'élément obligatoire *alias* décrit le nom du générateur et l'élément obligatoire *KeyInfo*, inclus du schéma W3C XML Signature, vise à contenir l'élément *CLSIGPublicKey*. L'élément facultatif *iis* contient un nombre indéfini d'élément *ii* indiquant les informations d'identités fournies par le générateur ainsi que les *générateurs* utilisés pour les représenter au travers de l'attribut *geneID* :

```
<xsd:complexType name="iiType" mixed="true">
  <xsd:sequence>
    <xsd:any minOccurs="0" maxOccurs="unbounded" namespace="##other"
processContents="lax"/>
  </xsd:sequence>
  <xsd:attribute name="name" type="xsd:string" use="required"/>
  <xsd:attribute name="geneID" type="xsd:string" use="required"/>
  <xsd:anyAttribute namespace="##any" processContents="lax"/>
</xsd:complexType>
```

De la même manière, l'élément facultatif *certAttrs* décrit les attributs des certificats générés. Enfin, l'élément *Signature* a pour objet la signature d'un document de ce type selon le schéma W3C XML Signature.

Voici une instance d'un document de ce type. Il s'agit d'un document auto-signée incluant un certificat X509 contenant une clé publique RSA signé d'une autorité de certification[23] :

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<negotiation:providerPublicMD xmlns="http://www.w3.org/2000/09/xmldsig#"
  xmlns:negotiation="urn:fr:univ-st-etienne:tse:satin:ates:negociation">
 <negotiation:alias>Provider_TSE</negotiation:alias>
 <KeyInfo>
  <KeyName>CLSIG</KeyName>
  <KeyValue>
   <negotiation:CLSIGPublicKey>
    <negotiation:modulus>...</negotiation:modulus>
    <negotiation:generators nb="3">
     <negotiation:generator id="0">...</negotiation:generator>
     <negotiation:generator id="1">...</negotiation:generator>
     <negotiation:generator id="2">...</negotiation:generator>
     <!--S-->
     <negotiation:geneblind>...</negotiation:geneblind>
     <!--Z-->
     <negotiation:genecheck>...</negotiation:genecheck>
    </negotiation:generators>
    <negotiation:exponent>...</negotiation:exponent>
   </negotiation:CLSIGPublicKey>
  </KeyValue>
 </KeyInfo>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">...</Signature>
</negotiation:providerPublicMD>
```

23. Document complet en *annexes C*.

Voici l'extrait du schéma relatif aux documents contenant les métadonnées privées du générateur :

```
<xsd:element name="CLSIGPrivateKey" type="CLSIGPrivateKeyType"/>
<xsd:complexType name="CLSIGPrivateKeyType">
    <xsd:sequence>
        <xsd:element name="firstPrimeFactor" type="xsd:string" minOccurs="1" maxOccurs=
"1"/>
        <xsd:element name="secondPrimeFactor" type="xsd:string" minOccurs="0"
maxOccurs="1"/>
        <xsd:element name="firstSafePrime" type="xsd:string" minOccurs="0" maxOccurs=
"1"/>
        <xsd:element name="secondSafePrime" type="xsd:string" minOccurs="0"
maxOccurs="1"/>
        <xsd:element name="order" type="xsd:string" minOccurs="0" maxOccurs="1"/>
        <xsd:element name="phi" type="xsd:string" minOccurs="0" maxOccurs="1"/>
        <xsd:element name="invExponent" type="xsd:string" minOccurs="0" maxOccurs="1"
/>
    </xsd:sequence>
</xsd:complexType>

<xsd:element name="providerPrivateMD" type="providerPrivateMDType"/>
<xsd:complexType name="providerPrivateMDType">
    <xsd:sequence>
        <xsd:element ref="ds:KeyInfo" minOccurs="1" maxOccurs="1"/>
        <xsd:element ref="ds:Signature" minOccurs="0" maxOccurs="unbounded"/>
    </xsd:sequence>
</xsd:complexType>
```

L'élément obligatoire *CLSIGPrivateKey* contient les paramètres cryptographiques. Un seul des facteurs premier est nécessaire pour reconstituer l'ensemble des paramètres privés. Les autres paramètres sont donc donc facultatifs. L'élément *providerPrivateMD* est l'élément racine du document. L'élément obligatoire *KeyInfo*, inclus du schéma W3C XML Signature, vise à contenir l'élément *CLSIGPrivateKey*. Enfin, l'élément *Signature* a pour objet la signature d'un document de ce type selon le schéma W3C XML Signature.

Voici une instance d'un document de ce type :

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<negotiation:providerPrivateMD xmlns="http://www.w3.org/2000/09/xmldsig#"
  xmlns:negotiation="urn:fr:univ-st-etienne:tse:satin:ates:negociation">
 <KeyInfo>
  <KeyName>CLSIG</KeyName>
  <KeyValue>
   <negotiation:CLSIGPrivateKey>
    <negotiation:firstPrimeFactor>
     E09BC59E0870CBC59282687BCAC27CDE6ED2608304D5D81B00A29AD1C5F7BD09
     </negotiation:firstPrimeFactor>
    <negotiation:secondPrimeFactor>
     DA3BFB753D82CB0E9302A4EA705356F7F5B2B02F45C9F880C7CBA1BA5DC5B527
     </negotiation:secondPrimeFactor>
    <negotiation:firstSafePrime>
     01C1378B3C10E1978B2504D0F79584F9BCDDA4C10609ABB036014535A38BEF7A13
     </negotiation:firstSafePrime>
    <negotiation:secondSafePrime>
     01B477F6EA7B05961D260549D4E0A6ADEFEB65605E8B93F1018F974374BB8B6A4F
     </negotiation:secondSafePrime>
    <negotiation:order>
     BF7946CEB687225EFA1BB6878CD8BDA6A39C969292B9F1C52261905C5002BE15B3D14020
     A24921A9483E0A83CE40EAF8811A5F896D2FC8BEF1993FC80E52295F</negotiation:order>
    <negotiation:phi>
     02FDE51B3ADA1C897BE86EDA1E3362F69A8E725A4A4AE7C71489864171400AF856CF4500
     82892486A520F82A0F3903ABE204697E25B4BF22FBC664FF203948A57C</negotiation:phi>
    <negotiation:invExponent>
     02DC60D3A5E697328ADB30AA877A0DFC822156C70D7A3AC5562457DBCCD82250DBFBA5
     FF45DF27FC655D4232151C5B8CCF3E34EFEB27F986095C62929B8558CF61
     </negotiation:invExponent>
   </negotiation:CLSIGPrivateKey>
  </KeyValue>
 </KeyInfo>
</negotiation:providerPrivateMD>
```

Voici l'extrait du schéma relatif aux documents contenant les métadonnées de certificat :

```
<xsd:element name="CLSIGSignatureValues" type="CLSIGSignatureValuesType"/>
<xsd:complexType name="CLSIGSignatureValuesType">
  <xsd:sequence>
    <xsd:element name="signatureValue" type="xsd:string" minOccurs="1" maxOccurs=
"1"/>
    <xsd:element name="blindFactor" type="xsd:string" minOccurs="1" maxOccurs="1"/>
    <xsd:element name="quantities" type="quantitiesType" minOccurs="0" maxOccurs=
"1"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:element name="certificateMD" type="certificateMDType"/>
<xsd:complexType name="certificateMDType">
  <xsd:sequence>
    <xsd:element name="issuer" type="xsd:string" minOccurs="1" maxOccurs="1"/>
    <xsd:element name="dateOfIssuing" type="xsd:string" minOccurs="0" maxOccurs=
"1"/>
    <xsd:element ref="CLSIGSignatureValues" minOccurs="1" maxOccurs="1"/>
    <xsd:element ref="ds:Signature" minOccurs="0" maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>
```

L'élément obligatoire *CLSIGPrivateKey* contient la valeur de signature et l'ensemble des quantités ayant été représentées lors du calcul de la valeur de signature. Les quantités autre que celles servant à l'aveuglement sont décrites à l'aide d'un élément *quantity* indiquant l'identifiant du générateur ayant été utilisé lors de la représentation :

```
<xsd:complexType name="quantityType" mixed="true">
  <xsd:sequence>
    <xsd:any minOccurs="0" maxOccurs="unbounded" namespace="##other"
 processContents="lax"/>
  </xsd:sequence>
  <xsd:attribute name="geneID" type="xsd:string" use="required"/>
  <xsd:anyAttribute namespace="##any" processContents="lax"/>
</xsd:complexType>
```

Voici une instance d'un document de ce type :

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<negotiation:certificateMD xmlns="http://www.w3.org/2000/09/xmldsig#" xmlns:negotiation=
  "urn:fr:univ-st-etienne:tse:satin:ates:negociation">
 <negotiation:issuer>Provider_TSE</negotiation:issuer>
 <negotiation:CLSIGSignatureValues>
  <negotiation:signatureValue>
  018F4D3E4548E477F833716AF66C1A40E425CDCD3D65CFBAA97706B42A719EF161295FBE
  4825E51AC1BDC2B95DF002B4220E5A1F62E8C4B7B85C865660DB6F10A2
  </negotiation:signatureValue>
  <negotiation:blindFactor>
  01E8688C1D6B69FBE9C95B7DA5BC30060C1C50F79BA102C3567AAE737DEA3CBD9C9D58E
  211AFC591B77155D29CB2028E15790523145219FA449F5087CBF126E99EC42734C5B691BD
  EBB4F3180F825C62B8722F0C970E4D5655C2E19C9AA02E32C504AFFE3A46E1F94F1E722D0
  68DA5F37BA261F5025AB9F5E482FC674C90504A284715CFBD3951A4FE2063
  </negotiation:blindFactor>
  <negotiation:quantities nb="2">
   <negotiation:quantity geneID="0" name="name">4D696B61C3AB6C</negotiation:quantity>
   <negotiation:quantity geneID="1" name="firstname">41746573</negotiation:quantity>
  </negotiation:quantities>
 </negotiation:CLSIGSignatureValues>
</negotiation:certificateMD>
```

L'implémentation servant à la génération et à la validation de tels documents a été réalisé en langage C. Elle repose sur les librairies *libxml2* [24] et *xmlsec1* [25]. Elle est disponible à l'adresse *http://magnum.telecom-st-etienne.fr*. Elle est composée de deux fichiers : $x23\_gen.c$ et $x23\_load.c$.

Ajoutons quelques remarques :

- la déclaration des quantités, des informations d'identités et des informations relatives aux certificats dans les métadonnées publiques du générateur et de certificat peut être basée sur des schémas XML tiers.
- les documents présentés ne donne pas d'informations relatives à l'encodage des attributs mais il est possible d'ajouter de telles informations,
- il est possible de signer des valeurs de hachage des valeurs d'attributs s'il n'est pas attendu que des preuves de propriétés soient menées sur ces attributs. L'algorithme de hachage et ses paramètres doivent alors figurer dans les méta-données,
- un attribut peut être un fragment XML, par exemple la déclaration d'un contexte d'authentification, ce qui nécessite d'indiquer les traitements appliqués. Il s'agit donc par exemple d'indiquer les algorithmes de canonisation (C14N par exemple) et de hachage.

Ces besoins justifient que les éléments *ii*, *certAttr* et *quantity* aient un contenu régit par un schéma « laxiste ».

24. http://xmlsoft.org
25. www.aleksey.com/xmlsec

VIII.4.2.3 Règlements et protocole de négociation

À la section VI.4.4 nous avons présenté des exemples de règlements locaux d'un fournisseur et d'un initiateur. La création d'un espace de noms et d'un schéma permettant de sérialiser en XML ce type de documents ne lève pas de difficultés particulières. Il est cependant intéressant d'étudier la sérialisation d'une règle. Une règle, assimilable à une expression logique, se prête bien à une structuration arborescente, donc au format XML. Le protocole de négociation (l'exemple du chapitre précédent était basé sur ETTG) peut également faire l'objet d'une représentation en arborescence des divers règlements et des informations les satisfaisant. Le protocole de négociation peut donc être représenté par un document XML échangé entre les interlocuteurs et enrichi par l'ajout d'éléments au fur et à mesure de la négociation. Nous appelons ce document l'« arbre de négociation ».

Le protocole de négociation, représenté par ce document, permet la détermination d'une séquence d'échanges d'informations satisfaisant aux règles de contrôle d'accès de chacun. Il s'agit de ce que nous appelons la « phase de négociation ». Il est cependant également nécessaire d'employer un protocole de négociation plus riche permettant l'échange de ce document ainsi que des messages d'initiations, de fourniture d'informations, de délivrance de certificats, de présentation de certificats et de preuves, ainsi que potentiellement des messages d'encapsulation de flux applicatifs.

Chacun de ces messages peut être retranscrit sous la forme d'un document XML. Ce protocole consiste donc principalement en l'encapsulation de documents XML au sein d'autres documents XML. Le document représentant l'arbre de négociation échangé durant la phase de négociation est par exemple encapsulé dans des messages protocolaires de négociation indiquant qu'il s'agit de la phase de négociation. Ces derniers sont ensuite transportés via un protocole applicatif d'échange de documents tel que le protocole HTTP, qui peut lui-même être encapsulé par le protocole de transport de TLS.

Prenons l'exemple d'une requête d'accès qui conduit à la fourniture d'un règlement par le fournisseur indiquant que l'initiateur doit établir un pseudonyme et qu'il doit fournir une somme d'argent de 100€[26] :

$$\begin{aligned} disclose(full, Ressource) \longleftarrow\ & Fournisseur.estInitiateur(val = x) \\ & \cap\ BanqueDeFrance.Argent(montant = y); \\ & x =''\ pseudonymeInitiateur''\ \wedge\ y = 100 \end{aligned}$$

26. Les exemples de documents XML de cette section sont présentés pour illustrer nos propos et ainsi donner les premiers éléments nécessaires à la description d'un schéma et à la réalisation d'une implémentation. Cependant, ces travaux n'ont pas été réalisés à ce jour.

Voici un exemple possible de sérialisation en XML de cette règle :

```
<neg:regle source="Fournisseur">
    <neg:objet type="initRequest">
        <neg:objectType>discloseRule</neg:objectType>
        <neg:accessType>Full</neg:accessType>
        <neg:nomObjet>Ressource</neg:nomObjet>
        <neg:descrObjet>Description de l'objet</neg:descrObjet>
        <neg:conditions>
            <neg:operateur type="And">
                <neg:role>
                    <neg:source>Self<neg:source>
                    <neg:type>IdentityEstablishment<neg:type>
                </neg:role>
                <neg:role>
                    <neg:source>Banque-de-France<neg:source>
                    <neg:type>eCash<neg:type>
                    <neg:variables>
                        <neg:variable>Amount</neg:variable>
                    </neg:variables>
                </neg:role>
            </neg:operateur>
        </neg:conditions>
        <neg:conditionsAttr>
                <neg:condition on="Amount">
                    <neg:operateur type="equal">
                        <neg:value>100</neg:value>
                    </neg:operateur>
                </neg:condition>
        </neg:conditionsAttr>
    </neg:objet>
</neg:regle>
```

Cette règle est ensuite insérée dans un message d'encapsulation pour indiquer qu'il s'agit de la phase de négociation :

```
<neg:negoMsg type="negoPhase">
    <neg:Content>
        ...
    </neg:Content>
</neg:negoMsg>
```

Avec un message du même type, l'initiateur répond en étendant l'arbre de négociation et en indiquant qu'il souhaite un certificat. Notons que chacun des nœuds est marqué par un attribut « source » permettant d'identifier l'interlocuteur qui a ajouté le nœud :

```
<neg:role>
    <neg:source>Banque-de-France<neg:source>
    <neg:type>eCash<neg:type>
    <neg:variables>
        <neg:variable>Amount</neg:variable>
    </neg:variables>
    <neg:regle source="Initiateur">
        <neg:objet>
            <neg:objectType>role</neg:objectType>
            <neg:conditions>
                <neg:role>
                    <neg:source>ACFCI<neg:source>
                    <neg:type>IdentityCertificate<neg:type>
                    <neg:variables>
                        <neg:variable>Alias</neg:variable>
                    </neg:variables>
                </neg:role>
            </neg:conditions>
        </neg:objet>
    </neg:regle>
</neg:role>
```

Le protocole employé pour l'obtention de certificats auprès d'un générateur peut être le même protocole que celui de négociation entre un consommateur et un générateur. Le sujet qui souhaite obtenir des certificats initie une négociation en indiquant pour objet le certificat qu'il souhaite obtenir. Si le générateur ne nécessite qu'une authentification, le règlement envoyé en retour indique le besoin d'un établissement d'identité. Le générateur fournit le certificat dans un message protocolaire indiquant la fourniture d'informations. Ce type de messages protocolaires peut être le même que celui employé par le porteur d'un certificat lors de la présentation d'une signature, d'attributs ou lors d'une conduite de preuve de propriété d'un attribut :

```
<neg:negoMsg type="negoPresentation">
    <neg:Content>
        ...
    </neg:Content>
</neg:negoMsg>
```

Traitons l'exemple de l'échange de messages permettant de présenter un attribut et de prouver qu'il est contenu dans une signature valide. Nous supposons que cet attribut est une date de naissance notée x. La signature est :

$$A \equiv (\frac{Z}{R_0^x S^v})^{1/e} \ mod \ n$$

Le porteur modifie la signature et obtient le tuple (A',e,v'). Il doit mener la preuve :

$$PK\{(\varepsilon,\nu') : ZA'^{-2l_e+1}R_0^{-x} \equiv \pm A'^{\varepsilon}S^{\nu'} \ mod \ n \ \wedge \ \varepsilon \in \pm\{0,1\}^{l'_e+l_\varnothing+l_\mathcal{H}+2}\}$$

Dans un message protocolaire indiquant la fourniture d'informations il mène une preuve à laquelle il attribut un identifiant :

```
<neg:negoMsg type="negoPresentation">
    <neg:Content>
        <neg:presentation>
            <neg:inResponseTo>
                <neg:regle>
                    <!--Présenter date de naissance certifiée-->
                    <neg:regleRefID>58039459<neg:regleRefID>
                </neg:regle>
                <saml:Issuer>Provida</saml:Issuer>
                <neg:proof id="794238443">
                    <neg:Signature>
                        <!-- A' -->
                        <ds:SignatureValue>dbR76...iuo45</ds:SignatureValue>
                    </neg:Signature>
                    <neg:iis>
                        <neg:ii name="dateOfBirth" type="UnixTime" geneid="0">
                            <neg:value>381578600<neg:value>
                        </neg:ii>
                    </neg:iis>
                    <neg:commitments>
                        <!--La signature ne contient aucun attribut en engagement excepté
                        l'exposant et le facteur d'aveuglement qui sont forcément engagés-->
                        <neg:listGenerators/>
                        <!-- t = A'^r1 S^r2 -->
                        <neg:commitment>QVMJoi...X5HVT</neg:commitment>
                    </neg:commitments>
                </neg:proof>
            </neg:inResponseTo>
        </neg:presentation>
    </neg:Content>
</neg:negoMsg>
```

En supposant que chacune des règles de la négociation ait été déclarée avec un identifiant, la règle à laquelle répond cette preuve est indiquée par son identifiant. Ainsi, chaque fourniture d'information décline pour qu'elle règle elle s'applique. Dans cet exemple, il est supposé qu'une telle règle le besoin de présenter une date de naissance certifiée. L'élément preuve contient ensuite le nom du générateur, la signature A', l'attribut date de naissance x, et l'engagement $t = A'^{r_1} S^{r_2}$, dont r_1 et r_2 sont des valeurs aléatoires. Le consommateur répond en indiquant la preuve à laquelle se rapporte le message et indique le challenge c :

```
<neg:negoMsg type="negoPresentation">
    <neg:Content>
        <neg:presentation>
            <neg:inResponseTo>
                <neg:proof>
                    <neg:proofRefID>794238443<neg:proofRefID>
                </neg:proof>
                <neg:challenge>54352323423424<neg:challenge>
            </neg:inResponseTo>
        </neg:presentation>
    </neg:Content>
</neg:negoMsg>
```

Le porteur répond alors en indiquant la preuve à laquelle se rapporte le message, et indique les réponses $s_1 = r_1 - ce$ et $s_2 = r_2 - cv'$:

```
<neg:negoMsg type="negoPresentation">
    <neg:Content>
        <neg:presentation>
            <neg:inResponseTo>
                <neg:proof>
                    <neg:proofRefID>794238443<neg:proofRefID>
                </neg:proof>
                <neg:responses>
                    <neg:response idGene="signature">623462345634</neg:response>
                    <neg:response idGene="geneblind">678678678678</neg:response>
                </neg:responses>
            </neg:inResponseTo>
        </neg:presentation>
    </neg:Content>
</neg:negoMsg>
```

Le consommateur vérifie alors la preuve $t' = (ZA'^{-2l_e+1}R_0^{-x})^c A'^{s_1} S^{s_2} \stackrel{?}{=} t$ et que s_1,$s_2 \in \{0,1\}^{l'_e+l_\varnothing+l_\mathcal{H}+1}$.

Enfin, notons que les spécifications WS-SecurityPolicy (Lawrence & Kaler, 2009a) et WS-Trust (Lawrence & Kaler, 2009c) peuvent répondre en partie à la sérialisation faite pour les règlements et les échanges de règlements et d'informations. Bien que cela aurait apporté du crédit à cette section, l'application XML faite ici suffit à expliquer de manière concise les principes.

En conclusion, nous avons présenté l'utilité de l'emploi de standards, notamment des technologies du Web. Nous avons également présenté une solution pour la sérialisation des certificats anonymes basée sur les méta-données publiques des générateurs et une solution pour le protocole de négociation basée sur l'enrichissement d'un document XML.

VIII.5 Pervasivité et plateforme de confiance

Nous avons jusqu'ici soutenu l'idée que les négociations de confiance étaient une voie intéressante pour l'établissement de relations dans un environnement ouvert, pour l'obtention de ressources et de services, notamment en introduisant le fait que cette solution pouvait se justifier en tant que couche pervasive de gestion des identités. Nous avons pour cela introduit les besoins d'universalité de l'agent de négociation, d'interopérabilité des algorithmes et d'espaces de noms communs. Pour compléter cette idée, il est nécessaire d'introduire la notion de mobilité des usagers. Il est possible de faire l'hypothèse que les fournisseurs et les générateurs ne soient pas soumis à cette contrainte, qui est d'ordre physique, pour ne pas complexifier l'explication de cette problématique.

Introduire l'idée de mobilité consiste en la prise en considération du fait que l'utilisateur puisse se déplacer et être en capacité de se connecter *via* de multiples réseaux d'opérateurs. Il est possible de supposer que l'usager accède de manière transparente au réseau d'un opérateur dès lors qu'il en a obtenu l'autorisation et cela même en changeant de point d'accès physique au réseau[27]. Il est souhaité que les utilisateurs puissent se connecter aussi bien à leur domicile qu'au travers de tous les réseaux, notamment sans fils, qui leurs sont « physiquement » accessibles[28] (GSM, UMTS, WIFI, etc.). Il est possible de considérer qu'un utilisateur possède des droits d'accès à un sous-ensemble des réseaux d'opérateurs. Il s'agit donc de permettre aux utilisateurs d'obtenir des autorisations d'un opérateur de ce sous-ensemble lorsqu'aucun de ceux-ci n'est physiquement accessible alors que d'autres le sont. Outre les problématiques de partenariats entre opérateurs, il s'agit de permettre l'obtention de ces autorisations en respectant les contraintes de respect de la vie privée que nous avons fixées. Il s'agit également de pouvoir établir directement une relation de confiance avec l'opérateur de réseau en menant par exemple auprès de l'opérateur de réseau une « souscription flash » permettant à l'usager de créer un compte, voire même de payer directement sa consommation avec de la monnaie électronique. Il est par exemple possible de supposer des « hotspots » de retrait d'argent similaires aux distributeurs automatiques où l'utilisateur ne se connecterait que pour retirer de la monnaie électronique.

La seconde problématique est le fait que l'usager puisse être amené à employer de multiples terminaux d'accès. Il s'agit donc de permettre à l'utilisateur de disposer de ses données de négociation, que nous avions qualifiées de matérialisation de sa vie numérique et illustrées à la section VII.2, et ce, sur chaque terminal d'accès. Il s'agit d'une notion que nous appelons « identité en tout lieu » et qui a trait à la problématique de « portabilité ».

27. Nous considérons comme acquises les solutions techniques de basculement entre points d'accès physique (trad. Handover).
28. Si tant est que l'on puisse concevoir qu'un signal radio puisse être physiquement accessible.

Nous avions soulevé deux types de solutions à la section IV.4.5, l'emploi d'une plateforme de confiance (dès lors PdC) et l'emploi d'un dépôt en ligne. Notons que les solutions de portabilité peuvent être adaptées pour servir de moyens technologiques de recouvrement (sous-entendu que ce qui est recouvert n'est pas révoqué).

La solution d'un dépôt en ligne n'est pas adaptée pour permettre un accès mobile aux infrastructures réseaux puisque pour révéler un minimum d'informations au point d'accès, les deux possibilités sont :

- un dépôt accessible sur le segment réseau disponible (qui peut être extrêmement restreint),
- employer des certificats déjà en possession de l'usager.

La solution de la PdC semble donc à privilégier pour permettre un accès mobile et pour permettre à l'usager de disposer de ses informations d'identité sur tout terminal.

VIII.5.1 Plateforme de confiance

Comme nous l'avons mentionné à la section IV.4.4, la PdC permet de lutter contre la perte, le vol, l'extorsion, le prêt et la copie des secrets.

Les systèmes pouvant être considérés comme des PdC sont multiples. Ces systèmes ont vocation à être des environnements sécurisés au regard de critères d'assurance. Cela implique par exemple que la modélisation formelle d'algorithmes soit employée pour prouver les propriétés de tels systèmes. Le recours à de telles techniques implique que ces environnements soient parfois limités en performances et en capacités de stockage, notamment pour répondre à des contraintes de coûts. Les PdC ont également vocation à des utilisations qui requièrent parfois un encombrement physique minimal. Les cartes à puce[29] sont un exemple de PdC très répandues.

Ces pré-requis impliquent que les PdC disposent d'interfaces d'accès limitées afin de pouvoir garantir leur sûreté et ne sont prévues pour n'être accessibles qu'au travers de protocoles sûrs. Les pré-requis impliquent également que des fonctions de contrôle d'accès soient implémentées. Ces fonctions sont généralement basiques et peuvent même restreindre l'accès à une unique identité. Ils sont conçus pour résister à diverses attaques notamment physiques (la capture d'ondes électromagnétiques par exemple). Cela leur attribut le qualificatif de plateforme résistante aux altérations[30]. Ces environnements sont également conçus pour empêcher les canaux cachés (par l'absence de réponse, par les délais dans les réponses, par les messages d'erreur) par exemple au regard du risque que

29. trad. Smartcard.
30. trad. Tamper resistant.

représente la génération par la PdC de valeurs aléatoires. Les PdC sont alors également parfois conçues pour faciliter la détection de canaux cachés. L'emploi de procédés de fabrication ou d'algorithmes soumis à des critères d'assurance justifie le terme de *plateforme de confiance*. Le terme *confiance* a trait au comportement attendu pour qu'une PdC réalise, « sans fuite d'informations », les tâches qui lui sont attribuées (stockage de données et primitives cryptographiques par exemple). La confiance se rapporte également à celle attribuée aux tiers qui mettent en œuvre les PdC, les fabricants et les responsables de l'infrastructure par exemple.

Les PdC s'appuient notamment sur des sécurités « physiques » à la place de protections logicielles. Cela se traduit par le fait que certains composants physiques de la PdC, des co-processeurs par exemple, soient dédiés à des tâches spécifiques : chiffrement, moniteur de référence, espace de stockage blindés, etc. Il peut également s'agir d'implémenter des mesures de détection d'attaques et de contre-mesures. L'implémentation de mesures de sécurité sur des mécanismes physiques est également un critère de distinction des PdC des autres systèmes. Les systèmes intégrant des protections physiques peuvent être extrêmement fastidieux à concevoir et à mettre en œuvre, ce qui vient s'ajouter à la charge des preuves formelles de certaines propriétés.

Enfin, les PdC sont parfois employées par des usagers non-spécialistes, ce qui doit être pris en compte lors de leur conception. En résumé, les coûts et les difficultés techniques d'implémentation contribuent généralement à l'emploi de PdC aux fonctionnalités, performances et capacités de stockage limitées.

Pour certaines fonctionnalités, les PdC sont couplées à un agent logiciel sur un système distinct. Celui-ci peut notamment ajouter des fonctions de protection contre les canaux cachés entrants et sortants de la PdC (Chaum & Pedersen, 1993). Par exemple, la PdC peut contenir une clé de signature et l'agent logiciel peut permettre à l'utilisateur de s'authentifier en s'appuyant sur la PdC. En d'autres termes, l'agent sollicite la PdC pour produire la signature.

La première question à laquelle il faut répondre est la répartition des tâches entre l'agent de négociation et la PdC. Dans notre cas, il y a de multiples fonctionnalités pour lesquelles l'agent de négociation pourrait s'appuyer sur une PdC. Les PdC les plus répandues sont limitées à des fonctionnalités basiques telles que le stockage et la signature. Il est donc possible, dans un premier temps, de prévoir une délégation de tâches minimale, en se servant par exemple d'une PdC comme d'un espace de stockage sécurisé, ce qui offrirait les fonctionnalités de recouvrement et de portabilité. Il est possible de s'appuyer sur les protocoles de communication standards des PdC pour que l'agent puisse y stocker les don-

nées d'identité. Les données peuvent adopter un format connu des agents leur permettant de ne rapatrier que les données nécessaires afin de limiter les temps d'opération.
Dans un second temps, il est possible d'anticiper sur les fonctionnalités qu'une PdC pourraient supporter prioritairement pour améliorer la sécurité des données de négociations de l'usager.

1. Il est ainsi possible de concevoir une PdC à même de gérer une base de données des informations d'identités afin d'enrichir les possibilités de gestion des données qu'elle contient. Cela suppose l'utilisation d'un protocole conçu pour l'interrogation de la base de données de la PdC. Il serait ainsi par exemple possible d'interroger la base pour déterminer si le pseudonyme d'un fournisseur est reconnu.
2. Une fonctionnalité qui semble des plus intéressantes est celle de la gestion des pseudonymes de l'usager. La PdC serait ainsi conçue pour générer les pseudonymes et empêcher leur extraction. L'agent de négociation emploierait un protocole adapté pour obtenir les signatures de la PdC et mener les établissements d'identité.
3. Le traitement du règlement local de l'usager par la PdC semble aussi intéressant. Il nécessite cependant que la PdC soit en capacité de mener son analyse et que le protocole entre la PdC et l'agent soit adapté.
4. Enfin, les certificats peuvent être stockés dans la PdC et celle-ci avoir la charge de mener les preuves.

A terme, il est donc envisageable de définir une PdC implémentant toutes les fonctionnalités sensibles de l'agent de négociation et liées à la problématique de portabilité. Il est même envisageable de faire de la PdC le terminal d'accès de l'utilisateur permettant la consommation de services. Cependant, tant que ce ne sera pas le cas, il est nécessaire que la PdC puisse s'interfacer avec le terminal d'accès employé par l'usager. En outre, il reste le besoin d'interfaçage avec les applications clientes, même s'il est envisageable que certaines applications clientes soient intégrées à la PdC.

Nous avons précédemment indiqué que la PdC peut contribuer à empêcher l'utilisateur de commettre de mauvaises utilisations, par exemple partager un secret maître ou utiliser un certificat plus de fois qu'il ne devrait l'être. Cela soulève la problématique de la génération des preuves par la PdC. La PdC a ainsi la charge de vérifier que les conditions sont respectées. Les PdC doivent donc être capables d'interpréter les propriétés des certificats, notamment afin de contrôler leur nombre d'utilisations et leur durée de validité par exemple, puis elles doivent être capable de générer des preuves. Lorsqu'un certificat à usage unique est obtenu au cours d'une négociation, il ne semble pas y avoir de raison autre que celle-ci que de « stocker temporairement » le certificat dans la PdC afin que celle-ci mène la preuve. Le stockage peut se justifier pleinement pour des certificats à usages multiples souhaités portables. Il est concevable que l'utilisateur agisse de lui-même

pour permettre cela, si cela lui apporte un bénéfice. Cependant, pour lutter contre les usagers souhaitant tricher, en considérant la PdC comme un moyen de lutte, il est nécessaire de « forcer » la réalisation des preuves par la PdC, y compris pour les certificats à usage unique générés durant une négociation.

Il semble pour cela intéressant de reprendre le concept du secret maître décrit au chapitre 4. Ainsi, il est possible d'envisager que le secret maître soit généré par la PdC, qu'il n'en soit pas extractible et que tous les certificats ne soient exploitables qu'en connaissance du secret maître. Considérons que les PdC soient distribuées par des organisations qui seraient de confiance pour les consommateurs pour produire des PdC capables de générer un secret maître à la première utilisation et que celui-ci soit unique, non-modifiable et non-extractible.

La procédure d'établissement d'un pseudonyme avec une organisation présentée dans (Camenisch & Lysyanskaya, 2001) offre l'opportunité d'inclure le secret maître dans le pseudonyme et de prouver que le secret maître est issu d'un tiers de confiance sans avoir à le divulguer. L'utilisateur n'est pas en capacité de choisir son secret maître. Celui-ci n'est ainsi connu de personne, excepté de la plateforme de confiance. Cela suppose que les PdC supportent ce protocole d'établissement de pseudonyme.

Les générateurs ont alors la charge de vérifier que pour une même entité, le secret maître soit toujours le même. Pour que cela fonctionne, un utilisateur ne doit pas pouvoir renouveler aisément son pseudonyme auprès d'un générateur. Il doit notamment ne pas lui être possible de réinitialiser son pseudonyme avec un secret maître déjà employé. La réutilisation d'un même secret maître ne doit d'ailleurs pas être possible qu'elle que soit l'identité sur un même générateur. Cette mesure permet de limiter le partage en rendant très probable (à la mesure de renouvellement près), le fait que si un utilisateur cède son secret (en supposant qu'il ait réussi à l'extraire), il perde l'emploi du générateur où ce secret est employé. Si un utilisateur initie son compte sur le générateur avec le secret maître d'un tiers, et qu'il ne s'agit pas d'une première initialisation, alors, s'il souhaite le réinitialiser, ce ne peut pas être avec le même secret maître. Il doit donc employer une nouvelle PdC et changer son pseudonyme sur tous ses comptes dont les consommateurs peuvent nécessiter que le secret maître employé soit le même. Ce mécanisme suppose également le changement de PdC soumis à un contrôle physique fort.

Notons que nous supposons la ré-initialisation du secret maître sur un générateur par la preuve de deux pseudonymes, l'ancien et le nouveau, ce qui pose le problème du recouvrement en cas de perte. Cependant, la génération du secret aléatoire est souhaitée aléatoire, non contrôlé des constructeurs de cartes, et que le secret ne soit pas extractible.

Cela suppose donc une mesure de recouvrement devant s'appuyer sur un procédé tiers permettant d'établir l'identité du sujet et se substituant à la preuve par le pseudonyme, ce que nous nommions au chapitre 4 « un mécanisme d'établissement d'identité « de secours » prenant l'ascendant sur celui fait à l'aide des pseudonymes ».

Enfin, ce mécanisme suppose que la PdC soit capable de générer ses propres certificats signés avec une clé appartenant à un chemin de confiance d'une organisation reconnue pour émettre de telles PdC. Cela permet de prouver que le secret maître est issue d'une plateforme de confiance et qu'il est le même que dans les autres certificats présentés. Cela permettra en outre aux consommateurs de vérifier que le secret maître est issu d'une PdC de confiance. Il faut pour cela que les constructeurs de PdC appartiennent au domaine de confiance des consommateurs, et que les clés de signature des PdC appartiennent au chemin de confiance des constructeurs. Les certificats produits par les PdC doivent donc également s'appuyer sur un schéma de signature offrant la propriété de non-associativité et permettant les engagements. Citons par exemple la proposition (Smyth *et al.*, 2007) répondant à cette problématique.

Cet exemple permet d'illustrer le fait qu'une PdC puisse aider l'utilisateur dans la protection de ses secrets, mais puisse aussi aider à renforcer les mécanismes de vérification de la bonne utilisation des certificats. Il reste cependant le fait que rien n'empêche l'utilisateur de céder sa PdC à un tiers. Il est possible de renforcer ce mécanisme par le déblocage de la PdC par des contrôles biométriques, ce qui, à l'instar d'un secret (un code PIN avec une carte à puce par exemple) permet également d'éviter (retarder) l'usage en cas de perte. Néanmoins, l'utilisateur pourrait être présent au moment du déblocage de la PdC, puis laisser un tiers disposer de ses données. Les mesures de dissuasion sont donc complémentaires.

VIII.5.2 L'identité numérique dans un environnement pervasif et ubiquitaire

Nous avons jusque-là employé les termes de pervasivité et d'ubiquité en les réduisant aux aspects pertinents pour notre exposé, à savoir, la disponibilité d'un environnement de négociation universel. En d'autres termes, il s'agit que tout système impliqué dans les négociations de confiance dispose d'un tel environnement, en supposant que les problématiques d'intégration et d'interopérabilité soient résolues. Cela introduit également l'idée que les informations d'identité des utilisateurs soient disponibles même lorsque ceux-ci sont mobiles. Cependant, les concepts des environnements pervasifs et ubiquitaires forment un domaine d'étude plus riches et pour lequel il est intéressant d'introduire nos problématiques. Nous essayons donc de décrire ici brièvement ces notions et les enjeux

que ces environnements suscitent au regard d'une architecture globale de négociations de confiance.

Le terme « informatique pervasive[31] » est généralement attribué aux travaux de la compagnie IBM[32] dans la deuxième moitié des années 90. Ce terme définit alors la notion de services accessibles n'importe quand, n'importe où, et à la demande[33] (Schechter, 1999). Les combinaisons de services[34], et notamment ce qu'il est désormais nommé des applications comme des services[35], en sont le prolongement. Au-delà des notions d'architecture applicative (architectures orientées services, combinaisons de services, etc.) et d'ouverture des systèmes d'information, la notion sous-jacente est celle de la mobilité. Notons que les solutions de mobilité servent le nomadisme puisqu'elles contribuent à permettre la consommation de services pour des usagers itinérants. Le nomadisme est une problématique souvent attachée aux organisations souhaitant offrir l'accès à des ressources internes à leurs membres de l'extérieur. Cependant, la nomadisme est la condition de n'importe quel usager dans l'idée qu'il puisse lui être offert des services en tout lieu.

Au regard de notre problématique, il s'agit de permettre à un utilisateur de se connecter au travers de multiples opérateurs de réseaux, et par conséquent, de concevoir un système où les opérateurs de réseaux seraient des fournisseurs du service d'accès au réseau et des générateurs de certificats d'autorisation. Pour cela, l'usager s'appuie soit sur les générateurs disponibles sur les segments réseaux librement accessibles, soit sur des certificats déjà en sa possession. En effet, en considérant qu'un segment réseau soit disponible jusqu'au point d'accès réseau (que l'on considère comme le fournisseur) et que l'objet de la négociation soit l'accès à un segment réseau différent de celui disponible, cela suppose, soit que des générateurs de certificats soient accessibles sur le segment disponible, soit que l'usager utilise des certificats déjà en sa possession. Le client de connexion au réseau (par exemple le client WPA pour une connexion Wifi) peut alors déléguer à l'agent initiateur la négociation visant l'accès au réseau ou l'agent de négociation peut être le client de connexion au réseau s'il supporte les protocoles impliqués. Le succès de la négociation conduit le serveur applicatif (le point d'accès) à autoriser l'accès réseau. Si l'initiateur ne peut revêtir d'identité connue au sein du réseau disponible, la négociation est employée pour obtenir l'accès au réseau ce qui implique d'utiliser le protocole de négociation. Par contre, si l'usager peut établir une identité lui permettant d'obtenir l'accès au réseau au sein de réseaux physiquement accessibles, les moyens d'établissement de l'identité actuellement employés (802.11x, EAP, etc...) peuvent continués à l'être. Si l'on souhaite que

31. trad. Pervasive Computing
32. www.ibm.com
33. trad. On demand
34. trad. Mesh-up
35. trad. Software As A Service (SAAS).

l'agent de négociation gère la reconnaissance des réseaux disponibles avec les technologies actuelles, il est nécessaire qu'il supporte les protocoles de connexion au réseau. Autrement dit, l'agent de négociation doit être dans ce cas le client de connexion au réseau.

Il est parfois évoqué l'idée que l'utilisateur devrait avoir confiance en l'opérateur de réseau. L'emploi du système de négociation pour traiter l'accès au réseau permettrait de résoudre ce besoin de confiance en ne révélant que peu d'informations aux couches sous-jacentes à celles du canal de transport sécurisé de la négociation. Les informations révélées à l'opérateur de réseaux se réduisant à celles de la négociation, révélées au consommateur de ce réseau, et ce pour l'établissement d'une relation de confiance permettant l'accès au réseau.

La notion de mobilité soulève aussi la problématique de la confiance dans le terminal d'accès (ordinateur personnel, téléphone mobile, STB [36], etc.). En effet, l'utilisateur peut employer de multiples terminaux d'accès dans lesquels sa confiance varie. Il est évident que sa confiance n'est pas la même en son ordinateur personnel et en celui d'un cyber-café. Il est possible que l'utilisateur modifie de lui-même son comportement en fonction de son environnement, caractérisé par le terminal d'accès, et de l'agent de négociation qu'il a à sa disposition (un utilisateur peut le faire inconsciemment dans un cyber-café en se refusant à accéder à son compte bancaire en ligne par exemple). Notons que la PdC, en étant de confiance pour l'usager, réduit son besoin de confiance dans un environnement tiers pour chacune des fonctionnalités qu'elle implémente. Cependant, le besoin d'interface d'un agent logiciel et d'une PdC implique la notion de confiance dans l'agent. En effet, l'utilisateur doit autoriser l'agent logiciel à accéder à la PdC. Il délègue en quelque sorte ses droits. C'est le cas notamment lorsqu'un usager retire de l'argent à un distributeur automatique. Il saisit son code d'accès auprès de l'agent logiciel et non de sa PdC. Il fait alors confiance à l'agent pour faire bon usage de cet accès, sous-entendu qu'il ait un comportement attendu. En d'autres termes, l'utilisateur a confiance dans le fait que l'agent logiciel, qui lui permet de retirer de l'argent, ne débite que la somme qu'il obtient.

Considérons pour l'instant que cela constitue un ensemble de paramètres que l'utilisateur perçoit de son environnement et qu'il adapte son comportement en conséquence. Dans le cas du système de négociation, il est possible d'en déduire que le règlement local de l'usager, traduisant les règles d'automatisation de ses choix, doit tenir compte de cela. Ce besoin est d'autant plus important qu'il est attendu pour certaines applications de l'informatique pervasive que les interactions de l'utilisateur soient restreintes au minimum, voire que la diffusion d'informations permettant l'obtention du service soit transparente pour lui. Autrement dit, la PdC, permettant la mobilité et délivrant les informations, doit pouvoir interpréter l'environnement et s'appuyer sur le règlement local afin de délivrer

36. Set-Top Box : « Modem opérateur Internet enrichi ».

automatiquement des informations sur l'utilisateur.

L'ubiquité, dans son sens premier, a trait à « ce qui est partout ». Sans aucune intention de prosélytisme, l'ubiquité est le propre du concept de « Dieu ». En rapprochant cette notion de son aspect fonctionnel et technologique dans les sciences de l'information et de la communication, son domaine d'étude est l'informatique ubiquitaire[37] (Weiser, 1991). L'informatique ubiquitaire se distingue de l'informatique pervasive du fait qu'elle adresse initialement les domaines des interactions homme-machine, l'ambition de départ étant celle de la transparence. L'informatique ubiquitaire et l'informatique pervasive ont cependant récemment convergé comme l'explique Robinson (Philip Robinson, 2005) en nous livrant la figure VIII.2.

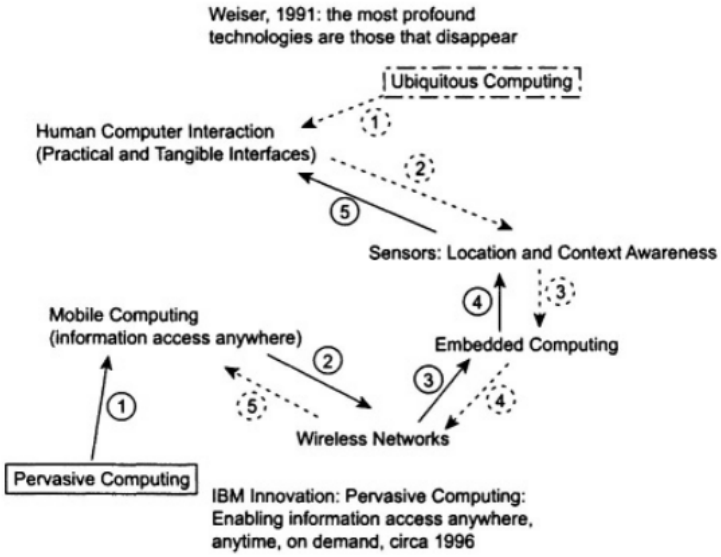

FIG. VIII.2 – *Convergence de l'informatique pervasive et ubiquitaire.*

Jusqu'ici nous n'avons principalement considéré comme informations issues de l'environnement physique de l'usager sa position géographique livrée par le point d'accès réseau employé. Grâce aux réseaux de capteurs, il est possible d'enrichir les informations perçues de l'environnement, généralement nommées « contexte ». Outre l'influence que le contexte a sur le comportement de l'utilisateur, celui-ci peut directement modifier la consommation du service ainsi que les négociations de confiance. Les informations relevées peuvent par exemple permettre de déterminer une position spatiale ou une vitesse de déplacement permettant d'adapter le service en conséquence.

Certaines de ces informations peuvent permettre de faciliter les interactions de l'utilisateur, ce qui rejoint l'ambition initiale de ce domaine. La consommation d'un service pour-

37. trad. Ubiquitous Computing

rait notamment être déclenchée par l'obtention d'informations contextuelles. Par exemple, en supposant que le service soit un appel à des secours, lorsqu'une personne reste trop longtemps immobile, ou qu'une chute violente est détectée, l'appel pourrait être automatiquement déclenché, autorisé et accompagné d'informations personnelles portant sur l'usager pour lequel les secours sont requis.

L'informatique ubiquitaire représente donc un défi encore plus grand que l'informatique pervasive. Le contexte peut enrichir la personnalisation du service mais peut également entrer dans le processus de contrôle d'accès, au service du fournisseur et aux données personnelles de l'usager. Cela passe par le fait que les réseaux de capteurs puissent jouer le rôle de générateurs en fournissant des informations certifiées sur le contexte. Ensuite, le contrôle de la diffusion d'informations contextuelles pourraient être centralisé par l'agent de négociation qui aurait la charge de les employer et de les diffuser. Il serait par exemple possible d'envisager qu'un réseau de capteurs soit un générateur du domaine de confiance des usagers et que, s'il génère un certain type de messages, cela satisfasse aux règles de contrôle d'accès du règlement local de l'usager pour diffuser des informations personnelles et pour mener des preuves. Cela fait de l'agent de négociation un outil ayant la charge d'analyser le contexte. Le règlement local doit alors incorporer ces informations et l'agent de négociation être à même de les analyser pour baser le contrôle d'accès dessus. En jouant le rôle de contrôleur de diffusion des informations des réseaux de capteurs, l'agent de négociation peut limiter la menace que représente de tels réseaux sur le respect de la vie privée.

Il doit être possible, d'une part, que l'usager puisse administrer ces règles d'automatisation (par exemple à partir de son ordinateur personnel), et d'autre part, qu'il lui soit proposé des pré-configurations correspondantes à des cas d'usage. Ainsi, cela permettrait la diffusion automatisée d'informations personnelles permettant la consommation de services dans des cas où l'utilisateur ne dispose par d'interface pour interagir avec son agent de négociation.

Les besoins d'établissement de relations de confiance avec des inconnus dans les environnements pervasifs et ubiquitaires ne sont pas différents de ceux que nous avons traités jusqu'ici, à l'exception du fait qu'il faille pouvoir établir des relations avec des inconnus sans interactions de l'utilisateur. Il serait par exemple concevable que l'environnement de l'utilisateur soit configuré pour que dans le cas d'usage précédemment introduit, l'agent de négociation puisse prendre la décision de se connecter automatiquement au premier réseau disponible, de contacter les services de secours les plus proches, et au travers d'une négociation, d'indiquer le nom et le dossier médical de la personne concernée. Il est également envisageable que le réseaux de capteurs soit un générateur de confiance de l'opérateur de réseau, et que celui-ci interprète l'obtention de ce certificat comme une urgence et autorise

en conséquence l'accès au réseaux. L'appel au secours peut également être déclenché directement par l'organisation en charge du réseau de capteur, et l'agent de négociation de l'usager ne fournir que le dossier médical. Notons que ce cas d'usage lève de nombreuses difficultés technologiques, notamment le fait qu'un agent de négociation puisse déterminer qu'un message d'alerte porte sur l'entité pour laquelle cet agent opère.

L'étude des supports physique et de la mobilité nous a permis de concrétiser le concept d'« identité en tout lieu ». Ainsi, dans les environnements de l'informatique pervasive et de l'informatique ubiquitaire, la négociation de confiance est pertinente, notamment dans sa dimension de couche sous-jacente aux services et comme moyen d'établir des relations entre inconnus et de contrôler la diffusion d'informations personnelles.

CHAPITRE IX

Une interface graphique pour l'utilisateur

*Le **chapitre 9** vise à « donner un visage » à l'environnement client. Cela permet notamment de comprendre en quoi il est possible que celui-ci soit une source de confiance pour l'utilisateur. Les questions d'ergonomie et d'acceptation utilisateur sont abordées afin d'introduire les tests utilisateurs permettant d'initier l'expérimentation nécessaire pour évaluer la proposition faite au chapitre 6.*

Sommaire

"Le seul véritable voyage ne serait pas d'aller vers de nouveaux paysages, mais d'avoir d'autres yeux."

Marcel Proust, *A la recherche du temps perdu.*

IX.1 Interactions et interfaces

L'acceptation du système de négociation est liée au paradigme de l'ergonomie. L'I.E.A.[1] (Association, n.d.) livre la définition suivante :

> "L'ergonomie[2] est la discipline scientifique qui vise la compréhension fondamentale des interactions entre les humains et les autres composantes d'un système, et la profession qui applique principes théoriques, données et méthodes en vue d'optimiser le bien-être des personnes et la performance globale des systèmes."

L'approche adoptée pour étudier les échanges de certificats inter-organisationnels nous a permis de dégager les enjeux principaux de l'architecture contribuant à en faire une application ergonomique :

- mettre l'utilisateur au centre des échanges,
- lui permettre de les comprendre,
- contrôler l'information diffusée,
- établir des relations

Nous considérons donc le système de négociation comme un système ergonomique pour la gestion des identités et le contrôle d'accès en environnement ouvert en vue de permettre la consommation de services. Plusieurs autres éléments permettent de prétendre à l'ergonomie du système de négociation, notamment :

- l'obtention de la confiance de l'utilisateur, au travers de ses interactions et de la perception de son environnement, et plus particulièrement grâce aux informations qu'il obtient de son interlocuteur,
- l'automatisation des transactions, de manière à les rendre accessibles et compréhensibles à de simples usagers sans compétence informatique particulière.

Le pendant de l'ergonomie est celui de l'utilisabilité du système par l'utilisateur. L'utilisabilité, ou usabilité, est définie par la norme ISO 9241 (Organisation, n.d.a) comme :

> "Le degré selon lequel un produit peut être utilisé, par des utilisateurs identifiés, pour atteindre des buts définis avec efficacité, efficience et satisfaction, dans un contexte d'utilisation spécifié."

(Nielsen, n.d.) livre cinq critères de l'utilisabilité d'un système: l'efficience, la satisfaction, la facilité d'apprentissage, la facilité d'appropriation et la fiabilité, que l'on peut résumer ainsi :

- l'efficacité : permettre aux utilisateurs du système d'atteindre le résultat prévu,

1. International Ergonomics Association
2. trad. Human Factors.

- l'efficience : permettre aux utilisateurs du système d'atteindre le résultat prévu avec des efforts et des temps réduits au minimum,
- la satisfaction : le confort lors des interactions.

Ainsi, il s'agit de permettre à l'utilisateur d'interagir avec le système de manière à satisfaire ces critères. Les moyens d'interagir avec le système sont basés sur des interfaces hommes-machines. Ces systèmes sont les « points d'entrées/sorties » de l'application avec l'utilisateur. Nous concernant, il s'agit pour l'utilisateur de lui permettre de négocier, d'ajouter des sources, de faire des choix, de mener des preuves, etc. Il s'agit également de lui permettre de l'aider à configurer ses règles d'automatisation afin que ses interactions se voient simplifiées lors de certaines utilisations du système.

Nous aboutissons donc aux moyens de faire interagir l'utilisateur avec le système. Cela se fait dans notre cas en grande partie au travers d'interfaces graphiques offertes par l'agent de négociation sur les terminaux d'accès. Dans un environnement pervasif et ubiquitaire, où l'on recherche la transparence, ce que nous supposons réalisable au travers de l'automatisation, il s'agira également de permettre à l'utilisateur d'obtenir des moyens de contrôle des transactions par des moyens de signalisation offerts par l'environnement pervasif et ubiquitaire et permettant ainsi de mener certaines négociations sans interface graphique autre que ces indicateurs.

Nous nous focalisons principalement dans ces travaux sur l'interface graphique de l'agent de négociation dédié à l'usager. Le défi est ici de satisfaire aux conditions de l'utilisabilité de l'agent de négociation, et du système au travers de l'agent, et cela sur de multiples terminaux d'accès offrant des interfaces de restitution et d'acquisition aux caractéristiques diverses. Il est alors possible de distinguer deux types de terminaux principaux :

- les terminaux « fixes » dans le sens où ils ne seront pas l'objet de déplacements physiques *en cours de négociation* : ordinateur de bureau, de salon, portable, STB, console de jeu, etc,
- les terminaux « mobiles » : téléphones mobiles, PDA, etc.

Il est possible de faire une distinction plus fine mais celle-ci est suffisante pour mettre en lumière les enjeux. La première catégorie symbolise un environnement où les interfaces d'acquisition et de restitution sont riches et maîtrisées du grand public. Concernant l'interface de restitution, on considère qu'elle ne représente pas de limitation (écran avec une résolution minimale de 1024 par 800 par exemple). Concernant l'interface d'acquisition, il faut distinguer l'environnement avec clavier et souris d'un environnement munie d'une télécommande ou d'une manette de console de jeu.

La seconde catégorie représente les terminaux dont les interfaces de restitution sont ré-

duites. Même si certaines générations de terminaux offrent des fonctionnalités de zoom, il est important de prendre en considération le fait que ces environnements doivent offrir une visualisation simple et épurée. Leurs interfaces d'acquisition sont également limitées. Les claviers doivent être considérés comme peu pratique et donc être sollicités au minimum. Certains de ces environnements ne disposent pas de souris. Cependant, compte tenu de la généralisation des écrans tactiles, nous les considérons comme l'interface d'acquisition principale.

(Cooper, 1995) relève trois paradigmes liés à l'interface homme-machine :

1. Le paradigme technologique : l'interface reflète le fonctionnement d'un mécanisme. Les interfaces peuvent ainsi être riches et précises mais sont plutôt destinées à des spécialistes.
2. Le paradigme de la métaphore : Il est attendu que l'interface se base sur le comportement d'un objet de la vie courante dont le fonctionnement est déjà largement appréhendé.
3. Le paradigme idiomatique : Il s'agit d'employer des éléments que l'utilisateur peut facilement associer à une idée traduisant une interaction.

Cela nous éclaire sur les moyens pour parvenir à satisfaire aux contraintes d'utilisabilité de l'agent de négociation, que l'on peut considérer comme une application complexe pour un usager sans compétence informatique, et cela dans des environnements parfois limités en termes d'interfaces d'acquisition et de restitution. Dans un premier temps, il peut s'agir de déterminer s'il est nécessaire d'employer de nouvelles métaphores propres à la négociation. Par exemple, CardSpace (Nanda & Jones, 2008) fait le choix des cartes pour désigner les sources d'informations et permettre le choix. Il s'agit ensuite d'identifier les idiomes les plus répandus que nous pouvons réemployer. Citons par exemple le code des couleurs pour indiquer un niveau de confiance, un triangle vert pour lancer une transaction, un point rouge pour lancer un enregistrement, une loupe pour voir les détails, un point d'interrogation pour accéder à l'aide, etc.

Enfin, il est nécessaire de pouvoir évaluer si les attentes de l'utilisabilité et de l'ergonomie sont satisfaites. Dans notre cas, il est possible d'envisager des tests de perception afin d'évaluer la compréhension de l'interface par les usagers et réalisables sur des « esquisses papiers ». Ceux-ci visent la compréhension globale du logiciel et notamment le vocabulaire employé. Ensuite, il est possible de mener des tests d'utilisabilité en mettant l'usager en situation. Cela permet d'observer l'utilisateur afin de cibler les difficultés qu'il rencontre à mener les divers scenarii employés.

IX.2 Esquisses de l'interface graphique

Nous présentons ici un aperçu de ce que pourrait être l'interface graphique d'un agent de négociation pour un environnement utilisateur. Nous n'employons pas de métaphore comparable à celle de CardSpace bien qu'elle soit intéressante et semble pouvoir s'imposer pour représenter des sources d'identités. Nous préférons pour l'instant mettre l'accent sur les interactions et les éléments des interfaces graphiques que les négociations peuvent nécessiter.

Supposons une négociation pour obtenir un devis. Lors d'une phase initiale, le loueur a présenté un pseudonyme ayant servi à établir le canal sécurisé, ainsi que deux certificats certifiant ce pseudonyme, dont le certificat du générateur « CCI42 » contenant également un alias. Lorsque l'utilisateur requiert un devis lors de sa navigation, il reçoit un règlement du fournisseur stipulant le besoin de présentation d'un pseudonyme (pour établir une identité lors des négociations suivantes), une adresse non certifiée, un certificat d'assurance, une somme de trente euros et une pièce d'identité anonyme. Notre exemple d'interface graphique pour l'agent de négociation est présenté à la figure IX.1.

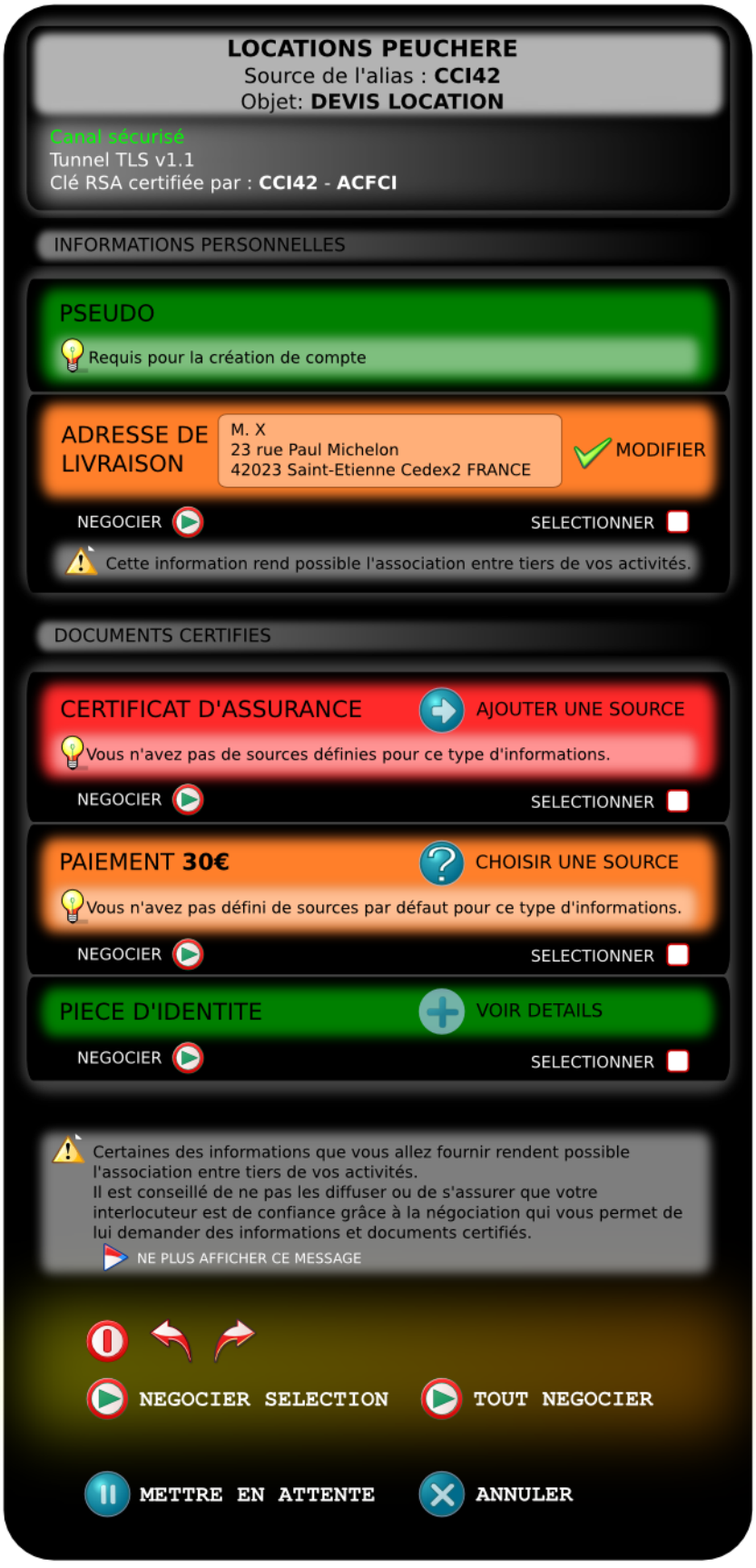

FIG. IX.1 – *Interface graphique de l'agent de négociation suite à la réception d'un règlement fournisseur.*

La disponibilité de sources d'informations certifiées est indiquée à l'utilisateur par un code de couleurs :

- *Vert*, une source définie par défaut est disponible (Sur cette interface, il est supposé une unique source disponible. Il aurait sinon été possible pour l'utilisateur de choisir une autre source.),
- *Orange*, plusieurs sources sont disponibles mais aucune n'est définie par défaut, il est proposé à l'utilisateur de choisir,
- *Rouge*, l'agent n'a pas pu déterminer une source répondant à l'information requise, il est proposé à l'utilisateur d'ajouter une source.

Dans l'état d'une négociation que représente cette interface, l'utilisateur a le choix de mettre cette négociation en attente. Cela signifie que l'agent enregistre les paramètres de cette négociation, ainsi que les moyens de parvenir, si possible, dans ce même état de négociation lorsque l'utilisateur souhaitera relancer cette négociation ultérieurement. Il est possible d'envisager qu'au lancement du terminal d'accès, ou à intervalles périodiques, un rappel des négociations en attente soit fait à l'utilisateur. Les négociations en attente font également l'objet d'une rubrique de l'interface d'administration.

Le bouton « Définir une source » de la figure IX.1 renvoit à l'interface d'administration comme cela est illustré à la figure IX.2.

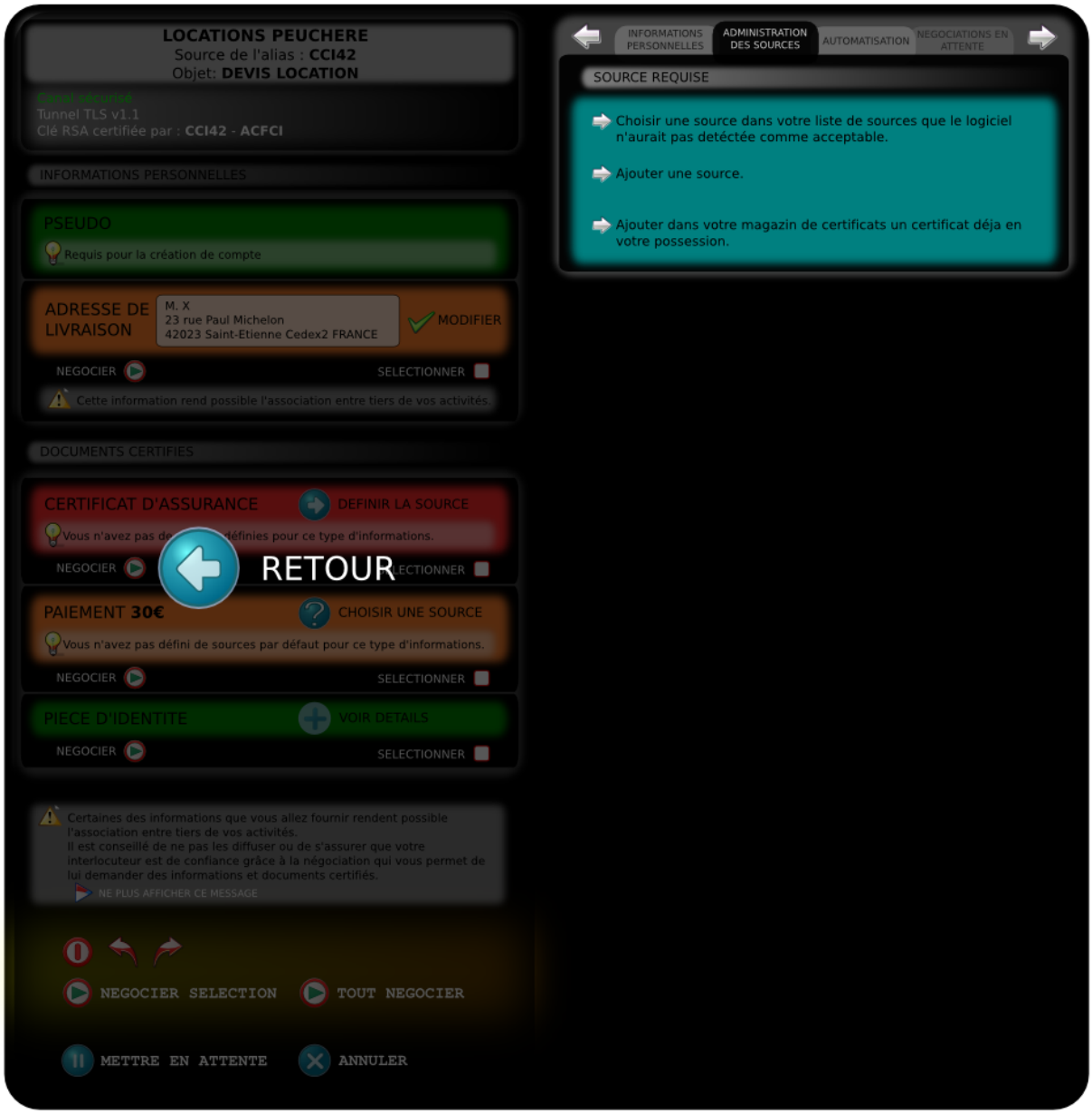

FIG. IX.2 – *Interface graphique de l'agent de négociation pour définir une source.*

L'utilisateur peut alors choisir d'indiquer une source dans la liste de sources disponibles, d'ajouter une nouvelle source ou d'ajouter un certificat qu'il posséderait déjà. Si l'utilisateur choisit d'ajouter une source comme cela est illustré à la figure IX.3, il est soumis à la même interface que lorsqu'il lance le logiciel en dehors d'une négociation et accède à la rubrique d'ajout de sources.

FIG. IX.3 – *Interface graphique de l'agent de négociation pour l'ajout d'une source.*

Il est ici supposé que l'utilisateur emploi un fichier de méta-données contenant un point d'entrée applicatif de la source. L'agent de négociation indique au générateur que l'usager souhaite obtenir un certificat d'assurance. Le générateur indique alors à l'agent qu'une liaison de compte est nécessaire en indiquant les informations requises. L'interface avertit alors l'utilisateur qu'il doit procéder à une liaison de compte comme cela est illustré à la figure IX.4. Si l'utilisateur accepte, une nouvelle interface de négociation est ouverte en indiquant les informations requises.

FIG. IX.4 – *Nouvelle négociation pour une liaison de compte.*

Le bouton « Choisir une source » ouvre une boîte de dialogue avec une « liste déroulante » des générateurs sources disponibles. L'utilisateur peut notamment y stipuler que dorénavant ce choix est son choix par défaut.

Le bouton « Négocier » sur chaque encart de certificat permet à l'utilisateur d'indiquer qu'il souhaite des informations en échange d'une information particulière. Le bouton « Tout négocier » lui permet de demander des informations en échange de l'ensemble des informations présentées dans cette interface. Comme cela est indiqué à la figure IX.1, lorsqu'une information permet une association, l'utilisateur en est averti. L'interface graphique montrée est présentée à la figure IX.5.

FIG. IX.5 – *Interface de négociation.*

Il s'agit ici de négocier la présentation de l'adresse. L'utilisateur peut alors parcourir son domaine de confiance pour demander un certificat. Il peut également enrichir son domaine de confiance sur cette interface. Lorsqu'il a choisi une source, il peut vérifier auprès du fournisseur que celui-ci fait partie de ses générateurs et qu'il peut accepter de fournir une information de celui-ci s'il obtient l'adresse comme cela est illustré à la figure IX.6.

FIG. IX.6 – *Interface de négociation.*

Il peut alors choisir l'information certifiée qu'il souhaite obtenir et s'il souhaite obtenir cette information, une preuve sur celle-ci ou une preuve de possession. Il peut alors vérifier que le générateur accepte de fournir cette information comme cela est illustré à la figure IX.7. Si le fournisseur accepte, l'utilisateur peut alors appuyer sur le bouton « Automatiser » et il accède ainsi à l'interface d'automatisation. L'utilisateur peut également demander d'autres informations ou accepter en appuyant sur le bouton « Action » et ainsi revenir à l'interface de négociation.

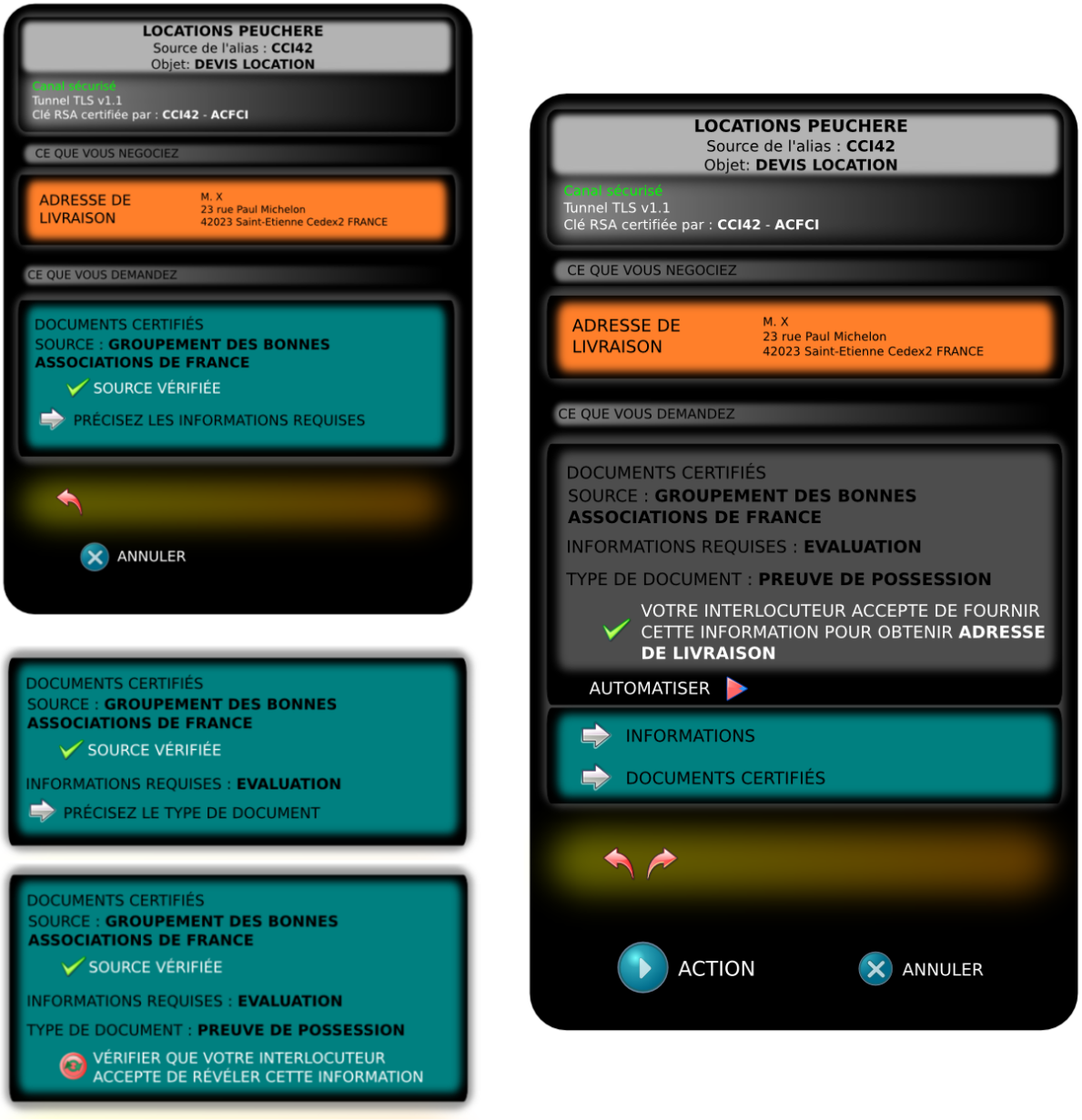

FIG. IX.7 – *Interface de négociation.*

Nous supposons que l'utilisateur a interagi de manière à définir une source pour le certificat d'assurance et de manière à choisir une source pour le paiement. L'interface lui permet alors de procéder à l'échange des informations dans le but d'obtenir le devis qui faisait l'objet de la négociation comme cela est illustré à la figure IX.8.

FIG. IX.8 – *Interface suite à la réception d'un réglement prêt à être satisfait.*

Lorsque l'agent de négociation est intégré à des applications, il peut être nécessaire de faire apparaître des composants de l'interface graphique de l'agent de négociation au sein de l'interface graphique de l'application cliente. Ce peut être par exemple un bouton « Identifiez-vous » lors d'une navigation Web. Dans un modèle d'« intégration en couches » (Cf. section VII.1.1), ce bouton dans l'interface de l'application cliente déclenchera directement l'appel à l'agent de négociation en indiquant comme objet l'établissement d'une identité. Dans ce mode d'intégration, le canal applicatif est sécurisé par le canal de négociation. Il est ainsi possible que l'agent de négociation fasse un affichage au sein de l'application cliente pour lui indiquer l'état de confidentialité du canal de communication comme cela est illustré à la figure IX.9

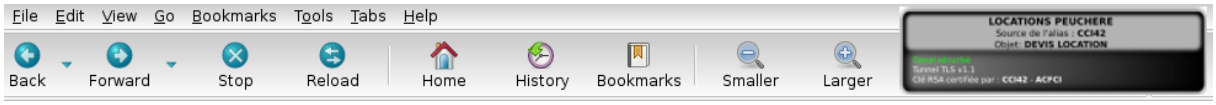

FIG. IX.9 – *Affichage sur une application cliente.*

Il serait trop fastidieux de montrer toutes les interfaces que le simple cas d'usage précédent suscite. Celles montrées ici illustrent cependant un exemple d'interface qui permet de mettre en lumière la faisabilité d'un tel environnement ainsi que diverses interactions auxquelles l'utilisateur est soumis au travers de l'interface graphique. D'ores et déjà, cela peut éventuellement permettre de mener un test de perception pour déterminer si un utilisateur est capable de comprendre les indications données à partir d'une explication du fonctionnement global. En complétant avec les interfaces manquantes, il est possible de construire un scénario permettant de mener un test d'utilisabilité et ainsi d'évaluer la proposition faite au chapitre 6.

CHAPITRE X

Conclusion

"La vie est l'art de tirer des conclusions suffisantes de prémisses insuffisantes."

Samuel Butler

Dans le monde physique, établir une relation avec un tiers en se basant sur la confiance se fait par le langage, la gestuelle et tout ce qui peut influer sur le sentiment de confiance de ce tiers. Dans le monde numérique, les modes de communications sont restreints aux protocoles mis en œuvre. Ainsi, dans le monde physique, il est possible d'exister par l'établissement de relations sans nécessiter d'autre moyen que sa personne. A l'inverse, dans le monde numérique, il est bien souvent nécessaire d'user d'informations issues du monde physique et de s'appuyer sur des tiers connus de son interlocuteur afin de certifier l'information et d'initier une relation de confiance.

En première partie, nous avons introduit la problématique générale de l'usage des certificats et des relations de confiance ainsi qu'un modèle et une terminologie employés tout au long de la thèse. Nous avons ensuite relevé et décrit les concepts principaux. Cela nous a permis de mettre en avant la confiance et le respect de la vie privée comme les notions fondatrices de ces travaux et les technologies de la sécurité informatique comme les moyens de parvenir à mettre en œuvre une telle architecture. Nous avons également pu mettre en relief le fait que nous adressions la problématique de la gestion de l'identité numérique, et en partie celle de la gestion de l'identité civile. Nous avons ensuite étudié quelques technologies et standards établis ou en devenir. Nous avons ainsi dégagé les manques concernant notamment le respect de la vie privée, les négociations de confiance et l'ergonomie de l'architecture. Nous avons ensuite mis en lumière la pauvreté de l'environnement utilisateur, donc la nécessité de l'enrichir. Cela nous a conduit à conclure cette première partie sur la vision de la gestion des identités centrée sur l'usager se concrétisant par l'ajout d'outils logiciels universels côté client.

En seconde partie, nous nous sommes efforcés de justifier l'opportunité que représente le déploiement d'un environnement utilisateur enrichi pour la gestion des identités et pour l'échange de certificats. Cela permet, en premier lieu, d'envisager un contrôle fin de la diffusion d'informations à l'aide d'outils cryptographiques. Nous avons illustré ce propos en présentant quelques outils cryptographiques permettant d'élaborer des certificats offrant les fonctionnalités de preuves de possession, de présentation sélective et de preuves de propriétés. Les problématiques majeures de la gestion des identités, que sont l'usurpation d'identité et la transférabilité, furent ensuite exposées, mettant en avant le besoin d'une solution à la fois technologique, psychologique et faisant appel à des procédés de la vie civile, impliquant notamment des tiers ayant un pouvoir judiciaire.

En troisième partie, nous avons fait une revue des enjeux et des difficultés majeurs de la mise en œuvre. Nous avons débuté par décrire l'enjeu d'une telle architecture lorsqu'elle est perçue pour son application la plus ambitieuse, c'est-à-dire pour en faire le support du contrôle d'accès aux applications. Il s'agit de faire de l'architecture de gestion

de la confiance une couche sous-jacente à la couche applicative responsable de la gestion des identités et du contrôle d'accès. Cela implique de fortes difficultés d'intégration. Il s'agit de modifier ou de concevoir les applications pour qu'elles opèrent avec la couche sous-jacente. Les fonctionnalités principales attendues pour l'agent logiciel ont ensuite été décrites. Cela nous a conduit à présenter un agent de négociation à la fois adapté à l'environnement des utilisateurs comme outil de gestion des identités numériques et aux organisations comme outil de contrôle d'accès aux applications. Nous sommes ainsi passés d'une vision « dissymétrique » de la consommation de service avec l'accent porté sur l'utilisateur comme chef d'orchestre de la diffusion de ses informations, à un modèle d'échanges plus « symétrique ». La possibilité de concevoir un agent logiciel universel nous a alors poussé à traiter des conditions *sine qua non* d'existence de cette architecture, à savoir, l'interopérabilité, l'universalité des logiciels, une architecture de confiance globale, un espace de noms commun ainsi que la résolution des problèmes architecturaux majeurs que sont la portabilité et le recouvrement. Nous avons pour cela réalisé une sérialisation en XML, appelée « x23 », des certificats basés sur le schéma de signature CL-Signature. Cela se traduit par un schéma de données selon la spécifications W3C XML Schema. Le principe de métadonnées publiques, employées lors de la présentation de certificats, décrit dans ces travaux, est en outre applicable à tout type de certificats que l'on souhaite non-associables. Nous avons ensuite élargi la discussion aux environnements pervasifs et ubiquitaires en essayant de donner un sens au concept d'« identité en tout lieu ». Il s'avère alors que, dans de tels environnements, la négociation de confiance, notamment comme moyen d'établir des relations entre inconnus, est pertinente. Nous avons enfin « donné un visage » à l'environnement utilisateur de manière à renforcer notre discours de faisabilité d'une telle architecture. En effet, nous avons illustré, du fait que l'acceptation utilisateur soit soumise au levier d'une mise en œuvre ergonomique, le fait que l'environnement graphique pouvait être décorrélé d'une éventuelle complexité architecturale. Ce dernier chapitre fut également l'opportunité d'introduire la notion de tests d'utilisabilité qui pourraient être conduits à l'aide des interfaces graphiques présentées, cela afin de valider la proposition faite au chapitre 6.

L'étude des enjeux principaux et des technologies existantes nous a conduit à dégager au chapitre 3 des critères d'évaluation. Si nous reprenions cette évaluation nous pourrions dire que nous avons traité l'ensemble des points en proposant des voies de résolution en nous appuyant sur des travaux scientifiques existants et sur les nôtres. Nous avons fait le choix de technologies ambitieuses, celles que nous pensions les plus pertinentes, et nous avons étudié et tiré partie de leurs combinaisons. Il est par conséquent évident qu'il est possible d'utiliser d'autres technologies avec des combinaisons différentes. En outre, l'évaluation du chapitre 3 ne reflétait pas toute la richesse des enjeux et des problématiques de la discipline de gestion des identités en environnement ouvert. Nous avons ainsi soulevé

de nouveaux enjeux et de nouvelles problématiques, puis nous avons fait des propositions pour certaines d'entre elles. Nos travaux ont permis l'élaboration d'outils logiciels mettant en œuvre le schéma de signature CL-Signature, les preuves de connaissances à l'aide du protocole de Shnorr ainsi que la sérialisations des certificats selon le schéma x23. Ces implémentations ont été réalisées en langage C et sont disponibles à l'adresse *http://magnum.telecom-st-etienne.fr*.

Enfin, nous avons dégagé des axes de recherche potentiels :

1. Les ontologies comme moyen d'inférence (ce pourrait être l'emploi de réseau neuronaux ou d'une autre technologie) dans le but de déduire des preuves sur les attributs d'identités en fonction des règlements, ou dans le but de déduire des règles d'automatisation en fonction du comportement (les choix et les interactions) de l'utilisateur.
2. Un système de contrôle d'accès unique pour un système, dont une partie serait basée sur la gestion de la confiance et sur les négociations. Il est pour cela nécessaire de dégager les modèles de contrôle d'accès qui sont à même de répondre le plus justement à cette problématique.
3. Les automatisations dans des environnements pervasifs et ubiquitaires, notamment lorsque les interfaces avec les utilisateurs prennent des formes restreintes ou inhabituelles.
4. Des tests de performance afin de valider l'hypothèse de faisabilité d'un agent de négociation au sein d'une plateforme de confiance.
5. L'orchestration de services par l'usager. Il est nécessaire d'approfondir ce sujet pour déterminer la faisabilité de rapatrier les échanges des applications distribuées entre organisations au premier plan afin de permettre une orchestration par l'utilisateur et de préciser ainsi les bénéfices concernant le respect de sa vie privée et l'utilisabilité.
6. Des tests d'utilisabilité validant l'automatisation des choix de l'utilisateur.

Vouloir faire du monde numérique, parfois abusivement appelé virtuel, un monde bien réel, c'est rendre concrètes les relations d'un usager avec ses interlocuteurs. La présentation de certificats de tiers de confiance est un des moyens qui permet de « se rattacher à quelque chose de connu » et qui permet de concrétiser cette notion. Les échanges multiples et les interactions sont ensuite le moyen de donner une dimension dynamique aux relations. Cependant, dans la majorité des cas d'usage, l'établissement de la relation est un moyen et non une fin. Et pour des questions d'utilisabilité, il semblerait préférable que cette phase soit transparente et non « concrète ». Il s'agit d'un dilemme qui nécessite un choix partisan. Nous l'avons fait en choisissant l'*interaction* par les négociations de confiance tout en prêtant attention à l'utilisabilité. Ceci nous a conduit à introduire la voie d'une automatisation des interactions. Cette automatisation est significative du fait que c'est l'utilisateur qui la construit au fur et à mesure de ses négociations. L'utilisateur

est ainsi initialement soumis à de multiples interactions. Il est ensuite possible d'envisager des négociations totalement transparentes, mais contrôlées, avec des tiers connus ou reconnus, voire avec des inconnus, éventuellement en tenant compte du contexte issu d'un environnement ubiquitaire. A l'inverse, il est possible d'explorer plus avant l'idée de négociation pour pouvoir négocier dans le monde numérique tout ce qu'il serait possible de négocier dans le monde physique. Notons qu'au chapitre 5, nous avions indiqué que :

> "Nous ne considérons en aucun cas qu'il soit possible pour l'utilisateur d'influencer le « comportement d'une machine » pour qu'elle fasse des choix qui ne sont pas explicitement définis par son règlement de contrôle d'accès et l'algorithme de négociation qu'elle emploie [la machine]."

Cela est cohérent avec le fait que la négociation se traduise dans les faits par la possibilité de faire des choix qui sont prédéterminés par les règlements de contrôle d'accès et la possibilité de requérir des informations. Il est évident qu'une négociation « humaine » est beaucoup plus riche. Il apparaît donc nécessaire de caractériser de manière plus fine la négociation de manière à déterminer ce qu'une implémentation logicielle permettrait d'envisager pour intégrer de nouvelles interactions. Enfin, notons que l'implémentation d'une négociation de confiance par l'échange de certificats est cohérente avec le modèle décrivant l'établissement d'une relation de confiance graduelle. Les points de concordance sont nombreux, par exemple le fait que chaque consommation de certificat contribue à établir la relation en satisfaisant une règle de contrôle d'accès à l'objet ou à une autre information, ou bien encore le fait que les relations de confiance puissent évoluer avec le temps si les règles de contrôle d'accès évoluent. Cependant, il est important de préciser que la négociation de confiance est une notion conceptuelle implémentée au travers de l'échange de certificats, donc qu'il est possible que d'autres formes d'implémentations existent.

Intéressons-nous un instant au concept de « vie numérique » et à son lien avec les négociations de confiance. Les relations issues des négociations de confiance peuvent paraître moins « authentiques » qu'au sein de réseaux sociaux par exemple. D'une part, parce que les interactions se font bien souvent entre hommes et machines et non pas entre hommes au travers des machines, et d'autre part, parce que le protocole de négociation limite l'expressivité des échanges. Cependant, la convergence des problématiques de gestion des identités numériques et civiles témoigne de l'existence d'une « vie civile numérique », et l'introduction dans le monde numérique de tiers ayant un pouvoir judiciaire illustre cette convergence. La constitution de domaines de confiance et de réputation est un indicateur de la constitution d'une « vie sociale numérique » et cela justifie le fait que l'associativité ait été au cœur de nos travaux. En effet, nous avons considéré et illustré le fait que l'associativité est l'élément le plus significatif lorsque l'on parle de respect de la vie privée

puisque l'association des activités et des identités numériques d'une même entité par des tiers distincts est une menace importante. Paradoxalement, permettre l'association de deux négociations avec un même tiers est nécessaire pour espérer entretenir une relation.

Pour conclure, posons-nous la question de l'émergence d'une architecture globale d'échange de certificats. Cette question se résume à déterminer si les technologies présentées ici, et leurs combinaisons, peuvent être envisagées comme une discipline qui soit porteuse d'activités économiques. Ce positionnement ambitieux de la gestion des identités au cœur des questions économiques est le seul à pouvoir justifier un déploiement global soumis à deux ré-agencements fondamentaux :

- Un ré-agencement institutionnel visant à définir les nouveaux acteurs de la vie civile dans le monde numérique,
- Un ré-agencement social visant à modifier les comportements des organisations et des usagers dans le monde numérique.

Annexes

ANNEXE A

Descriptions, analyses et évaluations des architectures existantes

A.1 Kerberos

A.1.1 Description et analyse

Kerberos (Kohl & Neuman, 1993 ; Neuman *et al.*, 2005) est issu d'un des premiers protocoles intégrant un tiers de confiance, le protocole Needham-Shroeder à clés partagées (Needham & Schroeder, 1978) amendé par (Denning & Sacco, 1981). Il permet l'authentification mutuelle de deux parties, en s'appuyant sur un tiers de confiance, et le partage d'un secret, appelé clé de session. Le tiers de confiance est appelé centre de distribution de clés (KDC), avec deux fonctionnalités qui peuvent être scindées en deux rôles, le serveur d'authentification (AS) et le serveur de tickets (TGS). Le principe est le suivant : un client s'authentifie à l'aide d'un secret auprès d'un KDC, et obtient un ticket qu'il fait valoir auprès de l'application pour laquelle il requiert un accès. Un KDC est généralement employé pour gérer l'ensemble des accès au sein d'un domaine administratif, appelé royaume[1]. Le ticket peut ainsi également servir de média d'autorisation puisque le KDC peut effectuer un contrôle d'accès centralisé. Autrement, l'utilisateur emprunnte une identité connue de l'AS afin d'exercer ses droits dans un royaume.

Il est possible d'interconnecter les royaumes au travers d'échanges de tickets entres KDC. Un KDC qui échange un ticket emprunte alors le rôle de centre de translation de clés (KTC). En considérant les royaumes Kerberos comme des domaines de sécurité différents, les KDC sont liés de confiance. Ils vérifient ainsi la validité des tickets comme provenant de KDC de confiance. L'échange de tickets entre KDC peut être fait au travers des méca-

1. trad. "Realm."

nismes Kerberos mais il existe également d'autres propositions, qui utilisent par exemple le chiffrement asymétrique (Zrelli *et al.*, 2007). Même si ce n'est pas l'usage habituel, il est possible qu'une application accepte des tickets de plusieurs KDC. Avec notre terminologie, le consommateur pourrait donc consommer des certificats de plusieurs générateurs.

Kerberos est un exemple intéressant car il s'agit d'une technologie mature et qui intègre la notion d'interconnexion de domaines administratifs, l'inter-royaume (cross-realm), au travers de tiers de confiance. Kerberos permet ainsi l'implémentation d'une architecture d'authentification unique mais également la possibilité de véhiculer au sein des certificats, ici les tickets, des informations personnelles ou d'autorisation, et cela en syntaxe ASN.1 [2].

A.1.2 Évaluation

2. Abstract Syntax Notation 1

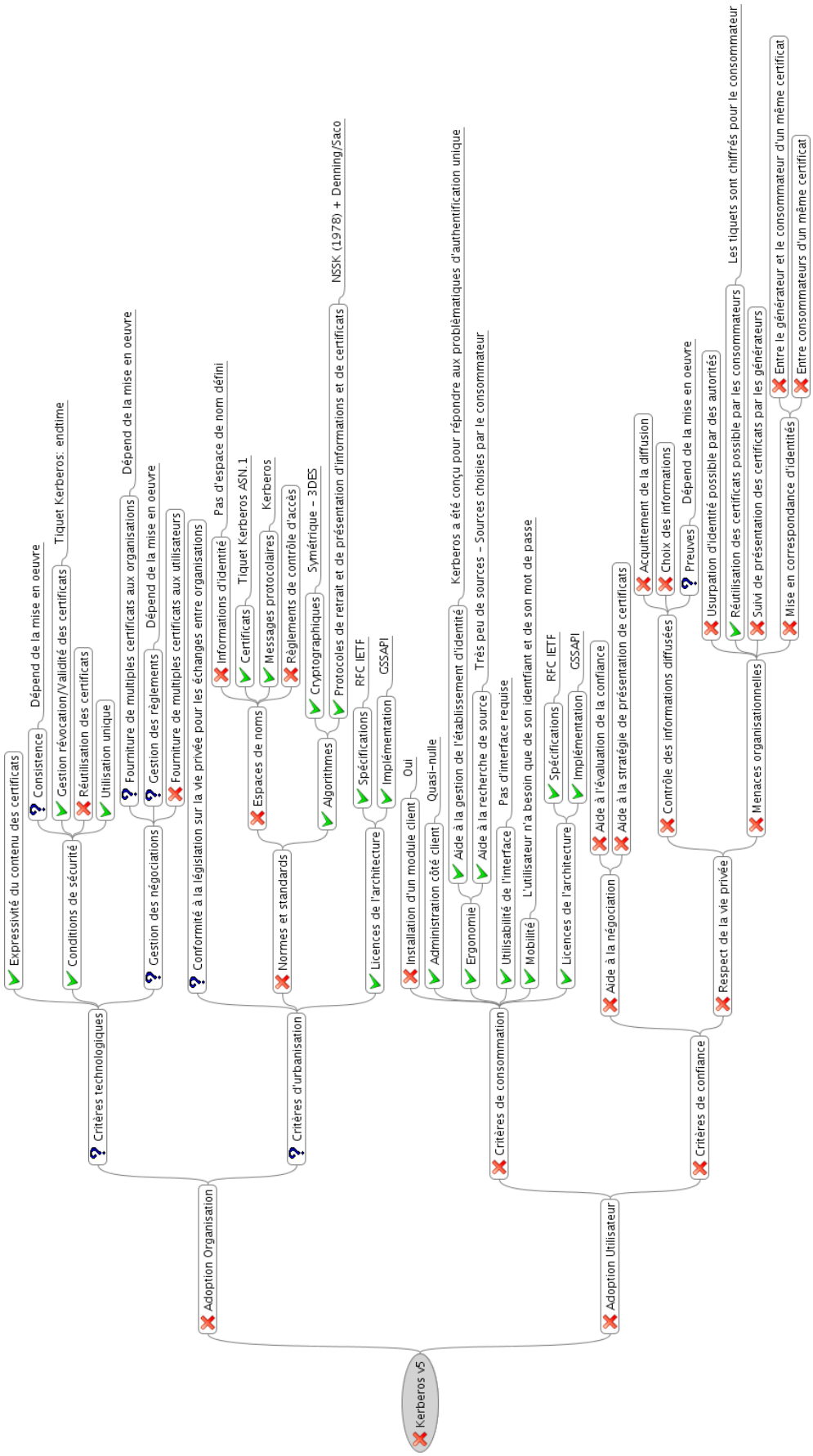

FIG. A.1 – *Evaluation de l'architecture Kerberos.*

A.2 RADIUS

A.2.1 Description et analyse

L'architecture RADIUS[3] (Rigney *et al.*, 2000b,a) est très utilisée au sein des architectures de télécommunications pour l'authentification, l'autorisation et le contrôle d'accès. Son successeur, DIAMETER, bien que représentant une évolution, se base sur les mêmes principes nous concernant.

Le principe est le suivant : l'usager n'est généralement pas muni d'un client RADIUS, il échange avec un point d'accès (NAS), qui est le client RADIUS, à l'aide d'un client CHAP, PAP ou EAP. Puis, le NAS authentifie le client auprès d'un serveur RADIUS. A l'instar de Kerberos, l'identifiant d'une identité indique le domaine organisationnel auquel l'identité est rattachée. Ainsi, si le serveur n'est pas une autorité de ce domaine, il se comporte en relai pour interroger le serveur RADIUS du domaine concerné. Les communications inter-domaines se font directement entre les serveurs RADIUS.

A.3 Infrastructures à clés publiques X509 couplées à TLS

A.3.1 Description et analyse

Les infrastructures à clés publiques ont été standardisées par l'IETF[4]. Le standard X.509 (PKIX) (Housley *et al.*, 1999 ; Housley & Hoffman, 1999) est issu de ces travaux. Il y est défini un format de certificat[5]. Dans les certificats X509, le sujet du certificat est décliné par l'attribut DN (Distinguished Name) issu des recommandations pour annuaires X.500. Le certificat possède une durée de validité et est lié à une liste de révocation (CRL) délivrée et signée par l'autorité de certification. Le certificat contient un numéro de série, soit l'identifiant du certificat, qui permet de vérifier s'il est listé dans une CRL. Les CRL pouvant être volumineuses, le protocole OCSP[6] permet d'interroger directement l'autorité pour connaître la validité d'un certificat. Les infrastructures X.509 introduisent également les autorités d'attributs à même de délivrer des certificats contenant des attributs sur un sujet. Ces attributs peuvent être de tout type (descriptif d'une entité, appartenance à des rôles utilisés pour du contrôle d'accès, attributions, permis, etc...). Ces certificats respectent également la syntaxe ASN.1. Un espace de nom générique et extensible des

3. Remote Access Dialin User Service
4. Internet Engineering Task Force
5. X.509 version 3
6. Online Check Status Protocol

informations a été défini.

X509 définit certaines bases de l'architecture attendue. Les consommateurs font confiance aux générateurs au travers des Infrastructures de Gestion de Clés Publiques (dès lors IGCP). Il faut ensuite que les initiateurs puissent établir une identité auprès des autorités de certification pour obtenir des certificats d'attributs dynamiquement au cours des négociations. Les initiateurs généreraient leurs propres clés pour établir leur identité au travers du protocole SSL[7] version 3 (Freier *et al.*, 1996) ou TLS[8] version 1.x (Dierks & Allen, 1999 ; Dierks & Rescorla, 2006), avec une authentification mutuelle en RSA[9] (Rivest *et al.*, 1978) adaptée pour l'exploitation des certificats X509. La négociation de confiance serait basée par l'échange de certificats d'attributs. Enfin, pour éviter qu'un consommateur utilise un certificat d'attributs auprès d'un autre consommateur, il faudrait par exemple que l'initiateur signe les certificats avec le nom du consommateur attendu.

A.3.2 Évaluation

7. Secure Socket Layer.
8. Transport Layer Security.
9. Crypto-système Rivest Shamir Adleman.

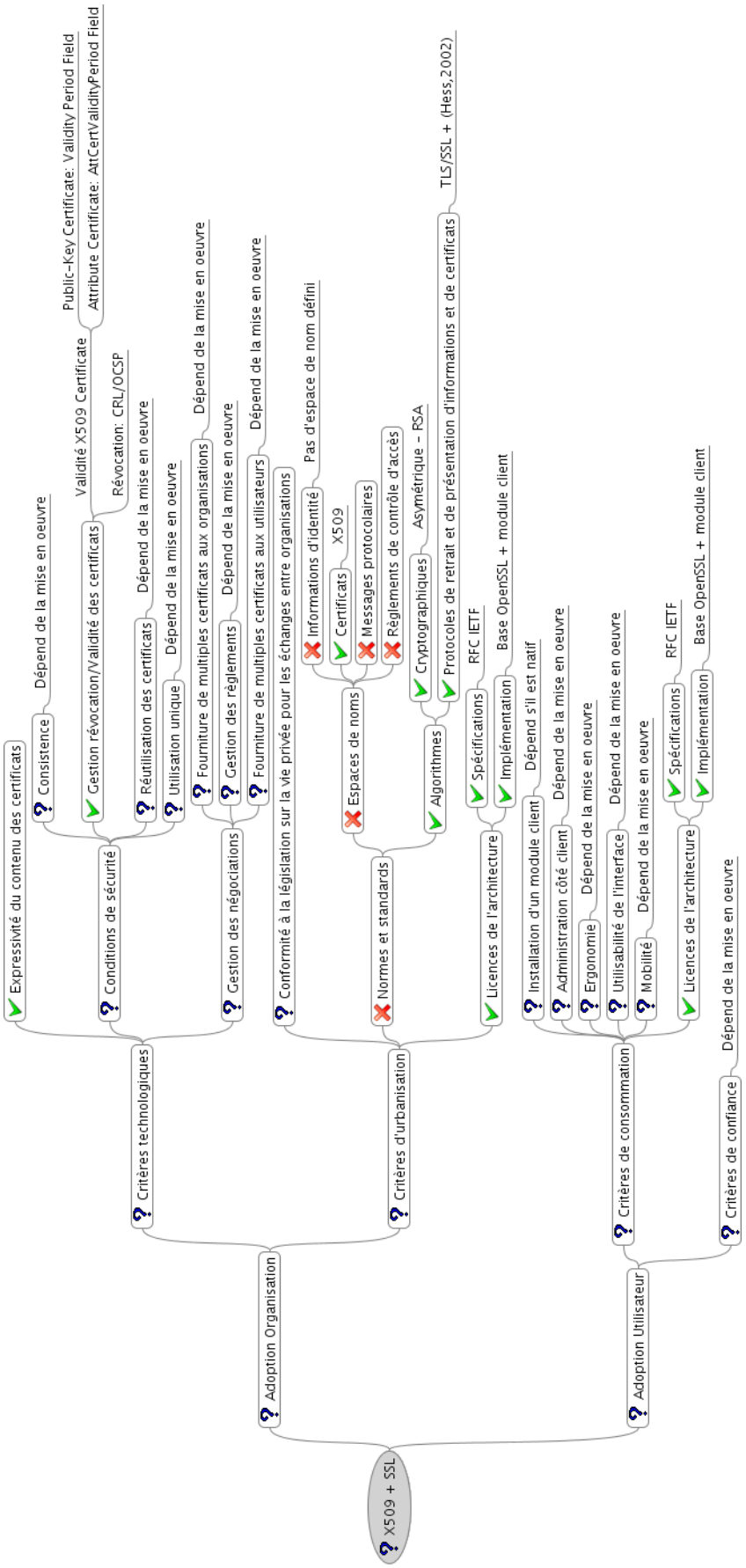

FIG. A.2 – *Evaluation d'une architecture combinant X509 et TLS.*

A.4 La fédération d'identités

A.4.1 Description et analyse

Les architectures de fédération d'identités sont essentiellement définies pour des implémentations reposant sur les technologies du Web, HTTP pour le transport applicatif et une sérialisation en XML. Il est nécessaire de distinguer les architectures de fédérations destinées à des implémentations reposant sur le client HTTP1.1, appelé navigateur Web standard, et celles reposant sur l'utilisation d'un environnement initiateur enrichi pour supporter des fonctionnalités liées aux négociations de confiance. La description des principes de la fédération pour navigateur Web standard faite ici se base principalement sur les spécifications SAML2 (Maler, 2006) et WS-Federation1.1b (Lockhart, 2006) qui partagent les concepts fondamentaux. Notre contribution (Ates *et al.*, 2007) propose une comparaison détaillée de ces spécifications et présente les bases de l'interopérabilité de ces deux architectures. Compte tenu de la prédominance des spécifications SAML2 pour cette technologie, nous nous y réfèrerons sauf mention contraire. Lorsque l'on souhaite traiter des fonctionnalités avancées de génération de certificats, nous nous appuierons sur les spécifications ID-WSF2.0 (Tourzan & Koga, 2007) conçues pour se coupler à celles de SAML2, et cela toujours pour des navigateurs Web standards. Pour la description de la fédération pour des environnements initiateurs enrichis, le standard majeur est à ce jour IDWSF2.0 Advanced Client (Cahill, 2007) qui repose également sur les spécifications SAML2 et que nous décrirons à la section suivante.

Les spécifications SAML et WS-Federation définissent leurs propres espaces de noms pour les certificats, les messages protocolaires et les méta-données des entités organisationnelles. Ils sont formalisés en schémas de données au format W3C XML Schema. Les méta-données permettent de décrire les points d'entrée applicatifs des services de fédération d'une entité, et contiennent généralement sa clé publique. Les spécifications SAML incluent toutes les sérialisations requises et s'appuient pour certaines fonctionnalités sur des schémas externes, par exemple WS-Addressing, XML Signature et XML Encryption. Les spécifications WS-Federation décrivent une imbrication logique de plusieurs spécifications existantes connues sous le nom de « pile WS-* » (principalement WS-Security (Lawrence, 2006), WS-SecurityPolicy (Lawrence & Kaler, 2009b), WS-Trust (Lawrence & Kaler, 2009d) et WS-MetadataExchange (Ballinger, 2006)) afin de définir une architecture de fédération.

La *fédération d'identités* repose sur le principe de l'*identité fédérée*. Ce concept se base sur un tiers de confiance, appelé *fournisseur d'identités (IdP - Identity Provider)* qui génère des certificats permettant aux consommateurs, appelés *fournisseurs de service (SP*

- *Service Provider)*, d'établir l'identité d'un initiateur. Le certificat délivré contient un identifiant (appelé nameID) de l'initiateur destiné à établir son identité sur le consommateur. Le consommateur recevant le certificat peut procéder à l'association de cet identifiant à une identité locale ou en créer une nouvelle. Si l'identité locale est existante, le consommateur doit donc procéder à une liaison de compte en utilisant par exemple un mécanisme d'authentification précédemment utilisé, ou en requérant des informations du sujet afin d'établir la preuve de possession d'une identité locale. L'association d'un identifiant généré aléatoirement par le générateur avec une identité, locale au consommateur, est appelée *fédération d'identités*. Ce procédé, nécessitant le consentement de l'utilisateur, est utilisé par chacun des consommateurs afin d'établir l'identité de l'initiateur à partir des certificats du générateur, les identifiants étant différents pour chacun des consommateurs. Une table des identifiants employés est ainsi définie pour chacune des identités sur le générateur qui peut être considérée comme l'*identité fédérée*. Ceci est illustré figure A.3.

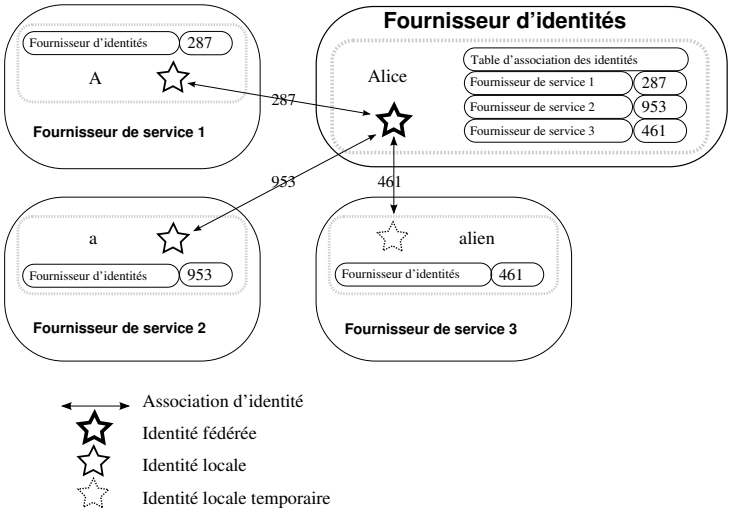

FIG. A.3 – *Identité fédérée*

La fédération d'identités repose donc sur le principe d'associations des identités entre générateurs et consommateurs. Par contre les identités sont non-associables, au travers de la fédération, entre consommateurs. Le terme *fédération d'identités* désigne également les partenariats qui permettent aux organisations d'établir des liens de confiance et donc d'accepter mutuellement leurs certificats.

Établir l'identité de l'initiateur à partir d'un identifiant contenu dans le certificat est une délégation de l'authentification. Ainsi, au sein d'une architecture de fédération, le consommateur émettra une requête au générateur lui spécifiant qu'il s'agit d'une délé-

gation de l'authentification et donc, qu'il attend en retour un certificat contenant un identifiant. L'initiateur apporte la preuve de son identité sur le générateur qui ensuite délivre la preuve nécessaire à l'établissement de son identité sur le consommateur. Ce principe permet à plusieurs consommateurs de baser l'établissement de l'identité sur un même générateur, ce qui justifie le terme de fournisseur d'identités. On considère cela comme une architecture d'authentification unique (Clercq, 2002 ; Pashalidis & Mitchell, 2003) puisque l'utilisateur ne fournit de preuve de son identité qu'à un générateur pour établir son identité sur plusieurs consommateurs. L'utilité d'une telle architecture est la réduction des tâches administratives de gestion des mécanismes d'authentification, et surtout, de rendre la consommation de services plus aisée en réduisant les interactions d'un initiateur visant à l'établissement de son identité. En effet, si le mécanisme d'authentification requiert une interaction de la part de l'utilisateur nécessitant un effort, la répétition de celui-ci peut conduire à une utilisation inconfortable et susciter des comportements à risque. Si la preuve utilisée est par exemple un mot de passe, l'utilisateur peut avoir tendance à choisir des mots de passe simples, ou a les inscrire sur un support physique ou numérique non protégé. La délégation auprès d'un tiers peut ainsi réduire les interactions de l'utilisateur pour la fourniture de preuves, interactions limitées à celles auprès du générateur. La fédération repose généralement sur une authentification par mot de passe sur les fournisseurs d'identités. Lorsque le fournisseur d'identités maintient une session, généralement à l'aide d'un « cookie HTTP », le mot de passe utilisateur n'est pas redemandé durant la période de validité de la session. Les délégations de plusieurs consommateurs peuvent avoir lieu auprès du même générateur sans que celui-ci ne requiert une nouvelle interaction de la part de l'utilisateur, la saisie du mot de passe par exemple.

Lors d'une délégation, la requête de certificats est faite par le consommateur au générateur. En effet, l'initiateur est supposé n'être muni que d'un navigateur Web standard, ce qui ne lui permet pas de bâtir ses propres requêtes de certificats. Ainsi, le consommateur émet généralement sa requête au générateur à l'aide d'une redirection HTTP. La réponse à cette requête, contenant le certificat, est délivrée par le générateur au consommateur par le même mécanisme. Le terme redirection a entrainé l'usage du terme « requêteur passif » pour désigner le navigateur Web standard. A l'inverse, on utilise le terme requêteur actif pour désigner un agent utilisé par l'initiateur lui permettant d'effectuer ses propres requêtes, et de présenter ses certificats de lui-même. Avec un requêteur passif, l'initiateur peut être considéré comme un porteur « passif » puisqu'il l'est au travers de redirections déclenchées par les consommateurs et par les générateurs. Cependant, il serait tout aussi justifié de penser que les consommateurs et les générateurs dialoguent directement au travers du navigateur Web utilisé comme un simple relais de messages.

Le mécanisme que nous venons de décrire soulève plusieurs éléments qui sont considé-

rés comme irrespectueux de la vie privée des usagers si le générateur et le consommateur sont des organisations distinctes :

- le premier vient de la délégation de l'authentification qui permet aux générateurs d'usurper l'identité des initiateurs auprès des consommateurs des preuves de l'identité,
- le générateur peut suivre la consommation d'un initiateur,
- les générateurs et les consommateurs peuvent lier les transactions, et donc mettre leurs identités respectives d'un même initiateur en correspondance ; il s'agit du principe même de l'identité fédérée.

Cependant, on peut tout de même noter que l'utilisation d'un identifiant différent avec chacun des consommateurs empêche ceux-ci de pouvoir mettre leurs identités respectives d'une même entité en correspondance. Le fait que les architectures basées sur des clients Web standards ne puissent pas complètement adresser les problématiques de la vie privée a déjà été souligné par Pfitzmann (Pfitzmann & Waidner, 2004 ; Ates *et al.*, 2008b).

Les spécifications SAML décrivent la possibilité que le consommateur puisse également ajouter au sein de sa requête celles de plusieurs attributs. Le consommateur étant avisé de ce que le générateur est à même de lui fournir. Le générateur demande à l'utilisateur son consentement pour la diffusion des attributs, puis retourne un certificat les contenant. Le consommateur peut ainsi obtenir des certificats de plusieurs générateurs. Il est également concevable que certains générateurs soient dédiés à la fourniture d'attributs et qu'ils délèguent l'authentification aux fournisseurs d'identités. Bien que la délégation de l'authentification soit une application majeure de la fédération, il est possible d'imaginer n'utiliser les mécanismes de fédération que pour l'obtention de certificats d'attributs auprès des générateurs. Ainsi les consommateurs pourraient obtenir des certificats issus de plusieurs générateurs afin de satisfaire la requête de l'initiateur.

Il se pose également la problématique de la résolution des sources multiples de certificats pour un utilisateur. Il existe des cas où cette question ne se pose pas, si le consommateur souhaite obtenir une pièce de l'état civil par exemple. Il y a cependant nombre de situations où c'est à l'utilisateur d'indiquer la source des certificats (par exemple pour choisir sa banque). Le consommateur dispose d'une liste prédéfinie de générateurs appartenant à son domaine de confiance et parmi lesquels il peut donner le choix à l'initiateur. Si celui-ci n'y trouve pas un générateur adéquat, le consommateur peut permettre à l'initiateur d'indiquer explicitement un générateur. Le consommateur peut alors dynamiquement s'y lier de confiance en faisant un échange dynamique des méta-données de fédération. Cela lui permet d'obtenir un certificat de ce générateur ainsi que les entrées applicatives pour y destiner ses requêtes. Cela est traité dans (Cantor *et al.*, 2005) pour les spécifications

SAML2 et (Ballinger, 2006) pour les spécifications WS-Federation. On peut cependant penser qu'il faut pour cela que la signature apposée sur le certificat soit celle d'un tiers de confiance, ou appartenant à un chemin de confiance du consommateur. Cela est concevable si l'utilisateur est à même de fournir une information, comme un URI[10] (Berners-Lee, 1998), ou de laquelle il est possible de déduire un URI. Cette problématique est traitée par les spécifications SAML2 sous la dénomination « publication et résolution des métadonnées »[11] (Cantor *et al.*, 2005). Pour répondre à la problématique de résolution des sources de certificats, les spécifications ID-WSF présentent un mécanisme d'enregistrement des sources d'attributs (Tourzan & Koga, 2007). Le rôle de résolution des sources est attribué à une autorité appelée *service de découverte (DS - Discovery Service)*. Celle-ci est généralement couplée à un générateur fournisseur d'identités. Cette supposition sera faite dans un premier temps pour simplifier l'explication du fonctionnement. L'autorité couplant le rôle de fournisseur d'identités et de service de découverte sera nommé IdP/DS. Lorsque le consommateur souhaite obtenir des attributs certifiés sur l'initiateur, il le redirige dans un premier temps par une délégation d'authentification sur l'IdP/DS, cela afin qu'un certificat comprenant une référence vers le service de découverte y soit incluse. Ce certificat permet l'établissement de l'identité sur le consommateur mais rien ne l'oblige à l'utiliser à cette fin. Il est possible qu'il serve seulement de référence vers le point d'entrée applicatif du DS. Le fragment du certificat ayant ce rôle est nommé « EPRbootstrap ». Le consommateur fait ensuite une requête de découverte des sources d'attributs en indiquant à l'IdP/DS les attributs qu'il souhaite obtenir. Cette requête est faite par redirection de l'initiateur.

Le service de découverte ne peut traiter cette requête que si l'utilisateur a préalablement enregistré auprès du service de découverte ses sources potentielles d'attributs, en indiquant pour chacune ce qu'elles peuvent fournir. Cela se fait généralement au travers d'une interface de navigation sur les fournisseurs d'attributs. Nous indiquions que le rôle de service de découverte et de fournisseur d'identités sont généralement couplés car il est nécessaire que le service de découverte puisse établir l'identité de l'initiateur afin de savoir quelles sont ses sources, d'une part, et de lui demander son consentement, d'autre part. L'IdP/DS indique alors à l'initiateur quels attributs sont requis par le consommateur. Il lui demande son consentement pour autoriser le consommateur à obtenir ses attributs auprès des fournisseurs d'attributs. Éventuellement, il demande à l'initiateur de faire le choix d'une source si plusieurs sont possibles. L'IdP/DS redirige ensuite l'initiateur sur le consommateur accompagné d'un ou de plusieurs certificats d'autorisation permettant au consommateur d'interroger directement les fournisseurs d'attributs. La réponse de

10. Unique Ressource Identifier.

11. Nous revenons sur la question de l'établissement des relations de confiance entre les générateurs et les consommateurs au chapitre 8.

l'IdP/DS contient également des références sur l'emplacement des fournisseurs d'attributs ainsi qu'un identifiant de l'initiateur sur le fournisseur d'attributs. Ce mécanisme ne nécessite pas que le consommateur et les fournisseurs d'attributs se fassent confiance directement. Le fournisseur d'attributs fait confiance à l'IdP/DS et autorise une requête d'attributs dès lors qu'elle est certifiée par celui-ci. Les identités de l'initiateur entre le consommateur et les fournisseurs d'attributs ne nécessitent pas non plus d'être fédérées. C'est pour cela que l'IdP/DS délivre un identifiant de l'utilisateur au consommateur afin que les fournisseurs d'attributs puissent savoir pour quelle identité le consommateur est autorisé à mener une requête d'attributs. Cet identifiant est basé sur la fédération entre le fournisseur d'attributs et l'IdP/DS. Enfin, l'autorisation d'accès aux attributs est donnée par le consentement de l'utilisateur sur le DS. Ainsi, l'utilisateur donne l'autorisation au consommateur d'obtenir ses attributs, et le fournisseur d'attributs autorise le consommateur grâce à la confiance qu'il a dans l'IdP/DS, notamment pour que l'IdP/DS demande le consentement de l'utilisateur. Il n'y a pas d'échange de méta-données entre un consommateur et un fournisseur d'attributs. Il n'est pas non plus obligatoire, selon les spécifications, qu'il y ait un échange de certificats. Le fournisseur répond donc à la requête du consommateur sans que le consommateur authentifie cette réponse. On ne peut donc pas parler de certificat. Cependant, le consommateur fait confiance dans le fournisseur d'attributs parce qu'il a confiance dans un IdP/DS qui lui a donné cette référence. On pourrait donc compléter les spécifications en supposant que l'IdP/DS donne également dans sa réponse un certificat à clé publique du fournisseur d'attributs ce qui pourrait permettre d'authentifier sa réponse. Ainsi, le consommateur obtiendrait un certificat d'attributs et aurait confiance en celui-ci par sa confiance dans l'IdP/DS. L'IdP/DS peut ne pas avoir confiance dans le consommateur, cela n'a pas d'importance puisque c'est l'utilisateur qui donne son consentement pour la diffusion des attributs.

Ces mécanismes soulèvent quatre éléments que l'on considère irrespectueux de la vie privée des usagers si le générateur et le consommateur sont des organisations distinctes :

1. L'IdP/DS peut délivrer des autorisations pour des requêtes d'attributs sans en avoir demandé le consentement à l'utilisateur. Il a en effet potentiellement la capacité d'obtenir tous les attributs de l'utilisateur.
2. La capacité de profilage des utilisateurs par l'IdP/DS est encore plus forte.
3. Les générateurs et consommateurs peuvent lier les transactions et donc mettre leurs identités respectives d'un même initiateur en correspondance.
4. Ce mécanisme impose la délégation de l'authentification auprès de l'IdP/DS pour obtenir l'identifiant de l'usager sur le fournisseur d'attributs.

Il faut ajouter à cela la complexité des interactions requises de la part de l'utilisateur. Jusque-là, il y a les multiples liaisons de comptes et les multiples interactions au niveau de

l'IDP/DS. Si l'on choisit de ne pas déléguer l'authentification des fournisseurs de services, il faut ajouter à cela les authentifications multiples. Si l'on souhaite exploiter cette architecture pour répondre aux objectifs fixés, l'architecture devient complexe. L'utilisateur doit lister toutes ses sources auprès d'un DS. Mais les fournisseurs d'attributs peuvent ne pas faire confiance en ce DS. Il est donc nécessaire que l'utilisateur enregistre ses sources auprès des DS de confiance de celui-ci. Dans ce cas, il faut que le consommateur obtienne un certificat d'établissement d'identité d'un fournisseur d'identités contenant les « EPR bootstrap » de plusieurs DS. Ainsi, le rôle de DS peut être découplé de celui d'IdP. On pourra supposer que l'utilisateur possède un IdP par défaut auprès duquel il référence les DS sur lesquels il a enregistré ses sources. On peut alors logiquement anticiper le fait que les autorisations pour les générateurs de certificats d'attributs soient délivrées par leur DS, qui eux-mêmes les obtiendront de l'IdP par défaut de l'utilisateur. Cela n'empêche pas le fait que les DS peuvent toujours obtenir les certificats de l'initiateur. Si l'on ne délègue pas l'authentification, il sera nécessaire que les DS authentifient par eux-mêmes les initiateurs, la fédération des identités entre les DS et l'IdP étant requise pour permettre l'obtention de l'autorisation. Si l'on accepte la délégation de l'authentification par les DS auprès de l'IdP, cela lui accorde le pouvoir d'obtenir tous les d'attributs des fournisseurs d'attributs. Á cela s'ajoute la complexité à laquelle fait face l'utilisateur lorsqu'il est redirigé successivement sur plusieurs DS afin de sélectionner les attributs, les sources ou de donner son consentement. Une autre architecture possible serait que l'utilisateur s'appuie sur un IdP/DS par défaut, lié de confiance avec les DS des fournisseurs d'attributs. Cela peut avoir l'avantage de réduire la complexité pour l'utilisateur, mais également, de gérer les liens de confiance entre organisations. Ceux-ci seraient établis entre DS, supprimant ainsi la charge de gestion de la confiance par les fournisseurs d'attributs qui n'auraient besoin de faire confiance qu'à un seul DS. Cependant, c'est augmenter encore le pouvoir de l'IdP/DS.

Enfin, soulignons une problématique à laquelle est soumis le concept de fédération d'identités. Rappelons qu'il s'agit au travers d'un identifiant, le plus souvent souhaité persistant, de lier les identités entre un générateur et un consommateur. L'identifiant est créé par le générateur et c'est l'initiateur qui va associer, au travers d'une authentification, cet identifiant à une identité existante sur le consommateur. Il est donc possible pour deux entités de fédérer des identités d'IdP différents avec une même identité d'un fournisseur de services. Il est donc possible que les utilisateurs cumulent des certificats afin d'obtenir des droits supérieurs à ce que chacun aurait obtenu indépendamment.

A.4.2 Évaluation

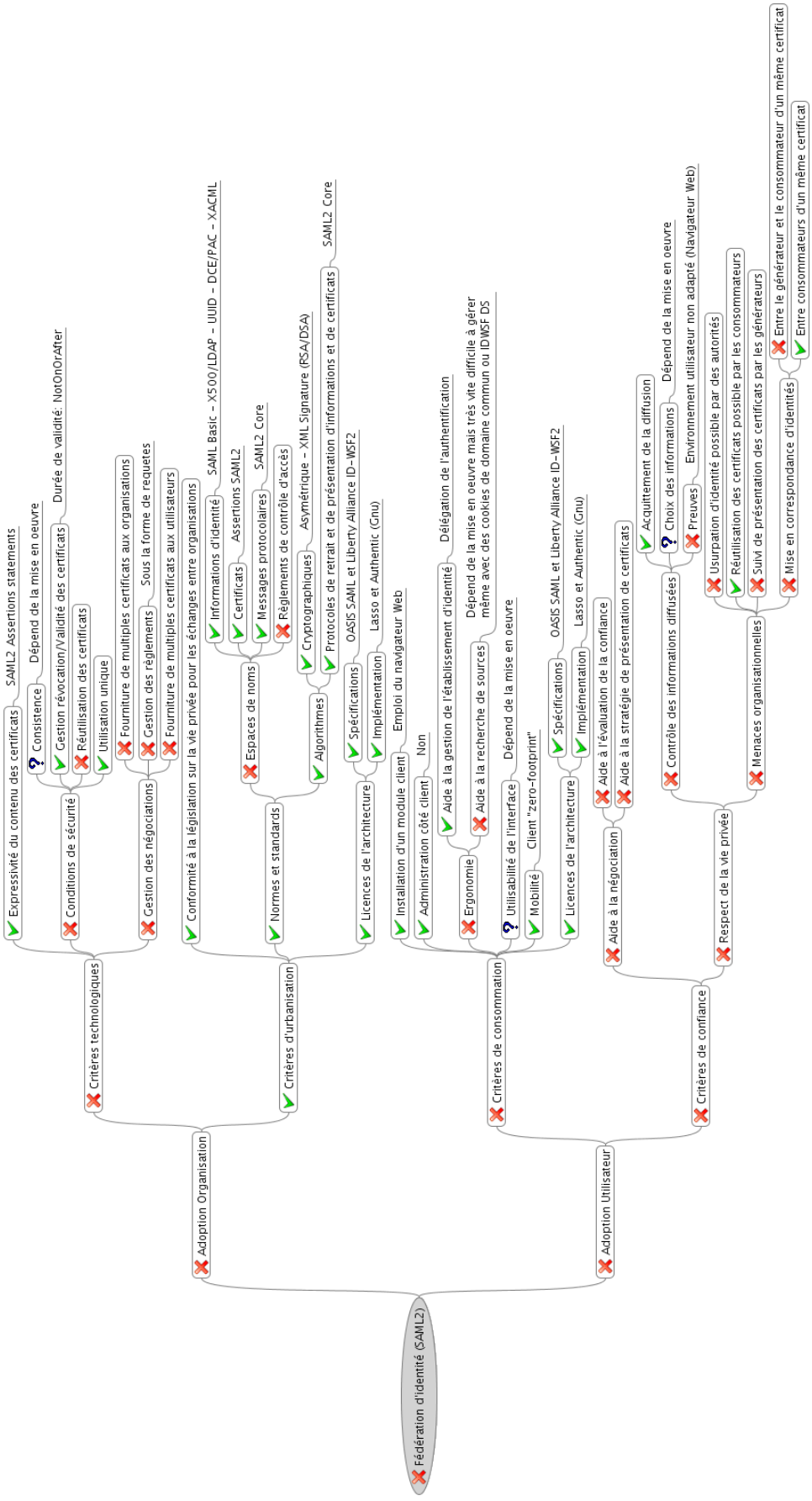

FIG. A.4 – *Evaluation de la fédération d'identités.*

A.5 Le client avancé Liberty Alliance ID-WSF

A.5.1 Description et analyse

Le client avancé ID-WSF (Cahill, 2007) se base sur les principes des spécifications ID-WSF pour navigateurs Web standards. Cette spécification décrit un environnement client implémentant, entre autres, certaines fonctionnalités des rôles d'IdP et de DS. Muni d'un tel client, l'initiateur est par exemple capable d'établir son identité de lui-même sur les consommateurs et les générateurs en générant ses propres certificats. Il y enregistre également ses sources de certificats ce qui lui permet, à partir de la connaissance des règlements des fournisseurs, de déterminer quelles sources satisfont aux conditions des consommateurs. Cela suppose que les fournisseurs d'attributs signent leurs réponses pour en faire des certificats. Les spécifications prévoient notamment le cas où l'utilisateur puisse produire un certificat indiquant qu'il est connu d'un tiers de confiance du consommateur. Pour cela, le générateur délivre un certificat à clés publiques à l'initiateur[12]. Les certificats générés par l'initiateur peuvent ne pas être utilisés pour établir son identité sur les consommateurs, mais simplement pour apporter une preuve d'appartenance à l'organisation ayant délivré le certificat à clé publique. Dans le cas contraire, celui-ci peut avoir lui-même généré la paire de clés empêchant ainsi le générateur de pouvoir usurper son identité sur les consommateurs. Il est également possible d'utiliser le mécanisme de délégation de l'authentification de SAML2. Le client ID-WSF peut alors stocker le certificat et le réutiliser[13]. Cependant, en plus du problème précédemment cité, celui de l'usurpation de l'identité de l'initiateur par le générateur se pose à nouveau. Pour ces deux fonctionnalités, il sera nécessaire de gérer la durée de validité des certificats ainsi que leur révocation éventuelle.

Notons que dans un environnement Web, l'agent utilisé par l'initiateur est un navigateur standard qui lui permet de consommer des services et des ressources Web. Jusqu'ici, nous considérions que l'initiateur faisait une requête sur un fournisseur et obtenait en retour un règlement. Or, c'est généralement suite à une requête de l'agent applicatif de l'initiateur que le fournisseur va déclencher une négociation en retournant un règlement. Cela signifie que lors d'une navigation Web, si l'initiateur n'utilise qu'un navigateur Web standard, il ne sera pas à même de gérer un règlement, ni même conscient qu'une négociation vient d'être ouverte par le fournisseur. Deux écoles s'affrontent :

- soit l'environnement client enrichi suppose un client Web enrichi,
- soit il s'agit d'un module indépendant appelé par le navigateur lorsque celui-ci analyse une balise spéciale dans les réponses HTTP.

12. On parle de "Minting assertions".
13. On parle de "Hoarding assertion".

ID-WSF fait le premier choix. Dans la section suivante nous étudierons « CardSpace » qui repose sur le second.

Le client ID-WSF sert donc à la navigation Web. Il inclut dans chacune des requêtes le fait qu'il est un client ID-WSF, ce qui permet aux fournisseurs de savoir qu'ils peuvent entamer une transaction en ID-WSF avec l'initiateur. Le client ID-WSF est donc en capacité de pouvoir analyser les requêtes de certificats émises par le fournisseur que l'on peut assimiler à l'expression de son règlement. Le stockage des preuves, et leur production, sont supposés régis par un module indépendant, appelé module de confiance[14].

Le client ID-WSF est très empreint de la technologie de fédération d'identités pour navigateur Web standard. Les spécifications n'adressent pas le fait que l'initiateur puisse obtenir de lui-même les certificat d'attributs. En effet, ces spécifications préconisent de conserver le mécanisme où le DS de l'utilisateur va spécifier le fournisseur d'attributs. Les mécanismes précédemment décrits, où le consommateur interroge directement le générateur, sont donc conservés. Il est cependant possible de modifier ce comportement. L'initiateur peut répondre à la requête de découverte du consommateur en indiquant qu'il est le fournisseur d'attributs. Á la réception de la requête, l'initiateur se comporte alors en consommateur en interrogeant lui-même le générateur. Il fait ensuite suivre le certificat au fournisseur en guise de réponse. Cela suppose que le client est à même de recevoir une connexion, ce qui n'est généralement par le cas des environnements utilisateurs. Il est alors nécessaire de s'appuyer sur des mécanismes de relais, notamment proposés dans les spécifications. Cela pose cependant la problématique du suivi des activités de l'initiateur par une entité tierce.

A.5.2 Évaluation

14. trad. Trust module.

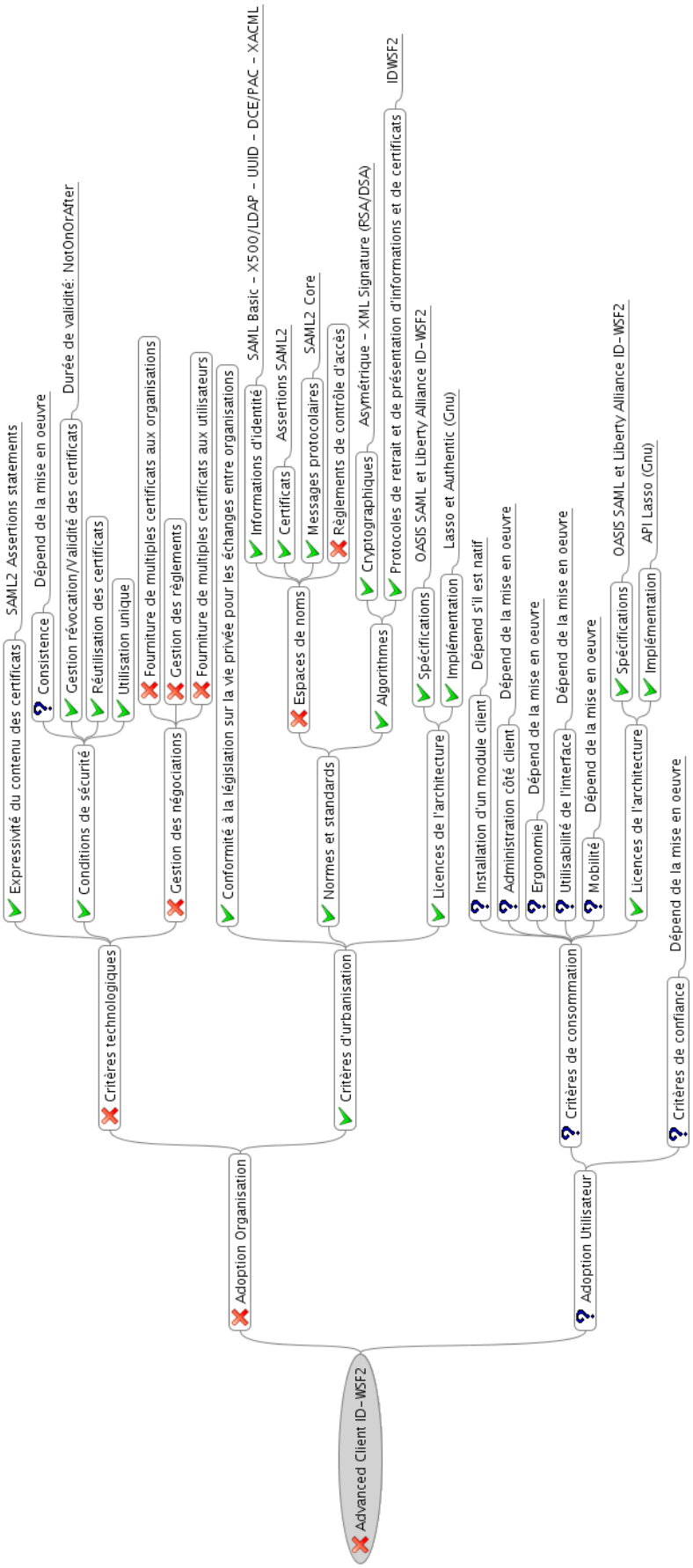

FIG. A.5 – *Evaluation du client avancé ID-WSF2.*

A.6 CardSpace

A.6.1 Description et analyse

CardSpace est un environnement client riche destiné à la gestion de la vie numérique de l'utilisateur de manière générale (Nanda & Jones, 2008). C'est à la fois une architecture, qui repose sur les mêmes spécifications que WS-Federation (WS-*), et l'implémentation d'un logiciel client[15]. Comme nous l'avions souligné à la section précédente, l'agent CardSpace est un module indépendant qui peut être appelé par un navigateur Web ou une autre application. S'il l'est par un navigateur, celui-ci déclenche l'ouverture de CardSpace dès lors qu'une balise d'appel correspondante est contenue dans une entête HTTP[16]. La philosophie originale de CardSpace, qui lui donne son nom, vient de la métaphore des sources d'informations d'identité, certifiées ou non, par des cartes. Les méta-données obtenues, permettant à l'agent CardSpace d'interroger les générateurs, sont appelées cartes d'informations ou « InfoCards », et permettent à l'utilisateur d'indiquer les sources d'informations requises par un consommateur.

L'architecture CardSpace intègre un mécanisme permettant à l'utilisateur d'obtenir des règlements de la part des consommateurs. La balise d'appel du module indique également une référence vers un emplacement sur le consommateur où l'initiateur obtient à l'aide du protocole WS-MetadataExchange (Ballinger, 2006) un règlement au format WS-SecurityPolicy (Lawrence & Kaler, 2009b). L'agent de l'initiateur analyse ce règlement, en déduit les certificats à obtenir, et les sources éventuellement indiquées. Il présente ensuite à l'utilisateur les cartes sélectionnées pour l'obtention de son consentement, ou un choix de générateurs. Les certificats sont obtenus des générateurs par le protocole WS-Trust (Lawrence & Kaler, 2009d). Suite à l'obtention des certificats, l'agent les présente au consommateur. L'utilisateur accompagne sa réponse au consommateur d'une preuve de son identité. Les certificats sont appelés « jetons » et sont au format WS-Security (Lawrence, 2006). Pour pallier au suivi de l'activité de l'utilisateur par les générateurs, tout en permettant que les jetons soient spécifiques aux consommateurs, l'agent peut produire un identifiant du consommateur. L'authentification peut ne pas être déléguée, l'environnement permettant de faciliter les authentifications multiples de l'utilisateur. CardSpace est également parfaitement adapté pour gérer l'auto-saisie d'informations personnelles.

15. Intégré aux systèmes d'exploitation Windows Vista et XP SP3.
16. Les navigateurs compatibles sont à ce jour Internet Explorer 7 et Firefox 3.

A.6.2 Évaluation

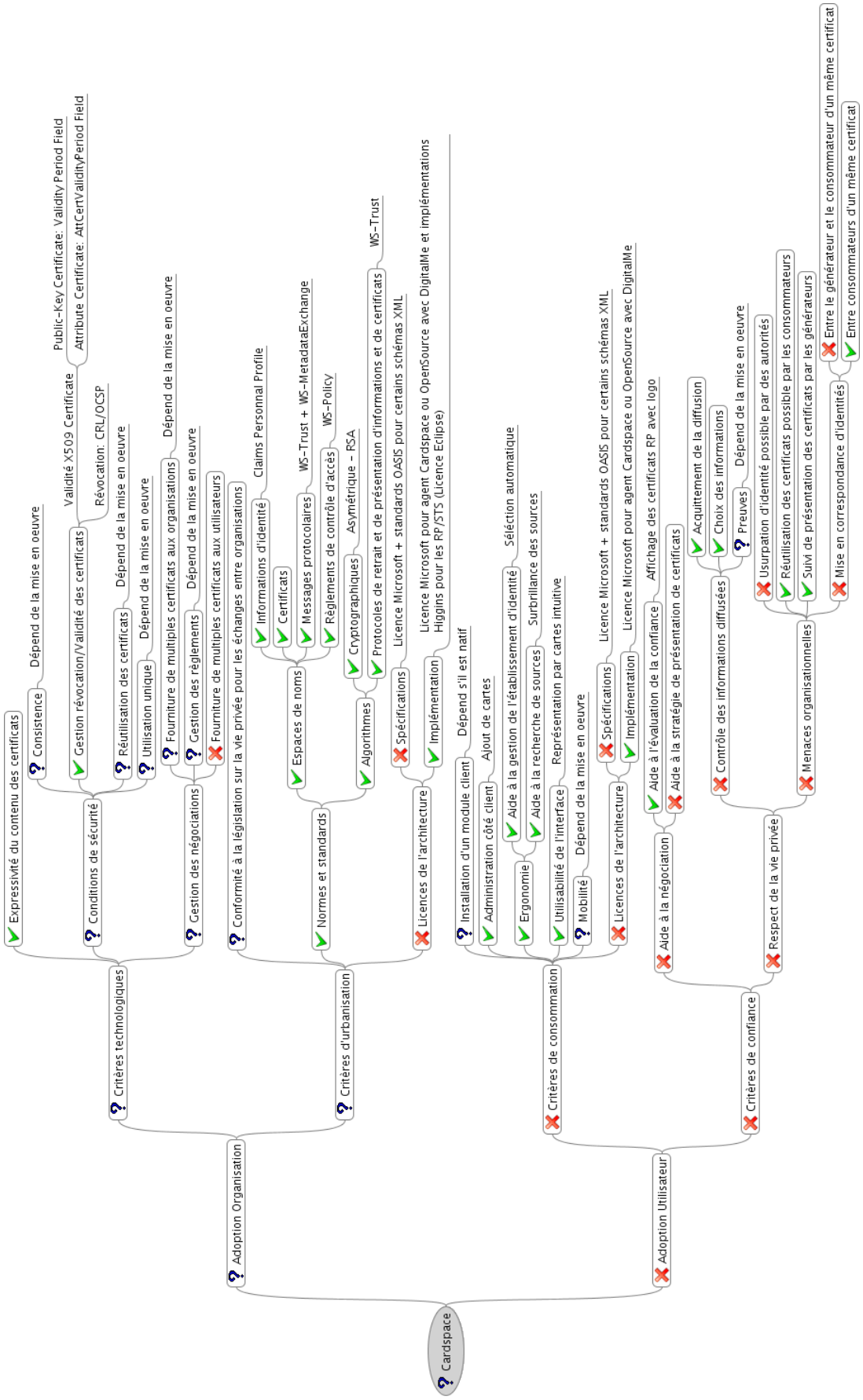

FIG. A.6 – *Evaluation de l'architecture et des implémentations Cardspace.*

ANNEXE B

Exemple de règlements locaux en langage ATNL

B.1 Règlement fournisseur

Certificates:

r_1: ACFCI.Identite
⟵ CCI42.Identite

r_2: CCI42.Identite(nom='loueuraleur',adresse='Cours Fauriel')
⟵ Loueuraleur

r_3: GBAF.Evaluation
⟵ BAF42.Evaluation

r_4: BAF42.Evaluation
⟵ EvalLoueurVoiture42.Evaluation

r_5: EvalLoueurVoiture42.Evaluation(nom='loueuraleur',resultat='honnete')
⟵ Loueuraleur

Attributes:

r_6:	alias	= 'Loueuraleur'	:: EvalLoueurVoiture42.Evaluation	:: sensitive
r_7:	resultat	= 'honnete'	:: EvalLoueurVoiture42.Evaluation	:: sensitive
r_8:	alias	= 'Loueuraleur'	:: CCI42.Identite	:: sensitive
r_9:	adresse	= 'Cours Fauriel'	:: CCI42.Identite	:: sensitive

Règles:

r_{10}: disclose(ac,EvalLoueurVoiture42.Evaluation)
⟵ true

r_{11}: disclose(full,EvalLoueurVoiture42.Evaluation.alias)
⟵ MinistereInterieur.PermisConduire

r_{12}: disclose(full,EvalLoueurVoiture42.Evaluation.resultat)
⟵ MinistereInterieur.PermisConduire

r_{13}: Loueuraleur.devis(date/lieu/depart/arrivee = x_4)
⟵ MinistereInterieur.PermisConduire(dateAcquisition = x_1)
∩ MinistereInterieur.PointsPermis(nombre=x_2)
∩ NotairesDeFrance.gage(montant=x_3)
∩ Any.date/lieu/depart/arrivee(val ⇒ x_4);
$(3 \leqslant \text{experienceConducteur}(x_1)) \wedge (x_2 > 0) \wedge (x_3 > 10000)$

r_{14}: Loueuraleur.location
⟵ EtatCivil.PieceIdentityAnonRevoc
∩ BanqueDeFrance.Argent(montant=x)
∩ Loueuraleur.devis;
applicationMetier(x)

r_{15}: disclose(full,CCI42.Identite.alias)
⟵ MinistereInterieur.permisConduire ∪ Loueuraleur.devis

r_{16}: disclose(full,CCI42.Identite.adresse)
⟵ MinistereInterieur.permisConduire ∪ Loueuraleur.devis

B.2 Règlement de l'usager

Certificates:

i_1: EtatCivil.PieceIdentityAnonRevoc
⟵ MairieSaintEtienne.PieceIdentityAnonRevoc

i_2: MairieSaintEtienne.PieceIdentityAnonRevoc ⟵ Mikaël

i_3: MinistereInterieur.PermisConduire ⟵ Prefecture42.PermisConduire

i_4: Prefecture42.PermisConduire
(nom=commit('ates'),
dateAcquisition=commit('02/02/2000')) ⟵ Mikaël

i_5: MinistereInterieur.PointsPermis ⟵ Prefecture42.PermisConduire

i_6: Prefecture42.PointsPermis(nombre=commit('12')) ⟵ Mikaël

i_7: NotairesDeFrance.Gage ⟵ NotaireLambda.Gage

i_8: NotaireLambda.Gage(montant=commit('12000')) ⟵ Mikaël

i_9: BanqueDeFrance.Argent ⟵ BanqueA.Argent

i_{10}: BanqueA.Argent(montant='undefined') ⟵ Mikaël

i_{11}: BanqueDeFrance.Argent ⟵ BanqueB.Argent

i_{12}: BanqueB.Argent(montant='undefined') ⟵ Mikaël

Attributes:

i_{13}: nom = 'Ates' :: Prefecture42.PermisConduire ::

i_{14}: nombre = '12' :: Prefecture42.PointsPermis ::

i_{15}: montant = '12000' :: NotaireLambda.Gage ::

i_{16}: montant = 'undefined' :: BanqueA.Argent ::

i_{17}: montant = 'undefined' :: BanqueB.Argent ::

Règles:

i_{18}: Initiateur.Any ⟵ GBAF.Evaluation
∩ Initiateur.estPseudoReconnu(val = x);x=false

i_{19}: disclose
(ac,Initiateur.PieceIdentityAnonRevoc) ⟵ ACFCI.Identite(nom=x_1,adresse=x_2)

i_{20}: disclose(ac,Initiateur.PermisConduire) ⟵ Any

ANNEXE C

Schéma W3C XML Signature pour la sérialisation x23 et métadonnées publiques

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema
 targetNamespace="urn:fr:univ-st-etienne:tse:satin:ates:negociation"
  xmlns="urn:fr:univ-st-etienne:tse:satin:ates:negociation"
 xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 elementFormDefault="qualified"
 blockDefault="#all">

 <xsd:import namespace="http://www.w3.org/2000/09/xmldsig#" schemaLocation=
↳  "schemas/xmldsig-core-schema.xsd"/>

 <xsd:complexType name="generatorType">
  <xsd:simpleContent>
   <xsd:extension base="xsd:string">
    <xsd:attribute name="id" type="xsd:string" use="required"/>
   </xsd:extension>
  </xsd:simpleContent>
 </xsd:complexType>

 <xsd:complexType name="generatorsType">
  <xsd:sequence>
   <xsd:element name="generator" type="generatorType" minOccurs="1" maxOccurs=
↳  "unbounded"/>
   <xsd:element name="geneblind" type="xsd:string" minOccurs="1" maxOccurs="1"/>
   <xsd:element name="genecheck" type="xsd:string" minOccurs="1" maxOccurs="1"/>
  </xsd:sequence>
  <xsd:attribute name="nb" type="xsd:string" use="required"/>
 </xsd:complexType>

 <xsd:complexType name="iiType" mixed="true">
  <xsd:sequence>
   <xsd:any minOccurs="0" maxOccurs="unbounded" namespace="##other"
↳   processContents="lax"/>
  </xsd:sequence>
  <xsd:attribute name="name" type="xsd:string" use="required"/>
  <xsd:attribute name="geneID" type="xsd:string" use="required"/>
  <xsd:anyAttribute namespace="##any" processContents="lax"/>
 </xsd:complexType>
```

```
<xsd:complexType name="iisType">
  <xsd:sequence>
    <!--Faire un type et mettre du lax-->
    <xsd:element name="ii" type="iiType" minOccurs="1" maxOccurs="unbounded"/>
  </xsd:sequence>
  <xsd:attribute name="nb" type="xsd:string" use="required"/>
</xsd:complexType>

<xsd:complexType name="certAttrType" mixed="true">
  <xsd:sequence>
    <xsd:any minOccurs="0" maxOccurs="unbounded" namespace="##other"
    processContents="lax"/>
  </xsd:sequence>
  <xsd:attribute name="name" type="xsd:string" use="required"/>
  <xsd:attribute name="geneID" type="xsd:string" use="required"/>
  <xsd:anyAttribute namespace="##any" processContents="lax"/>
</xsd:complexType>

<xsd:complexType name="certAttrsType">
  <xsd:sequence>
    <xsd:element name="certAttr" type="certAttrType" minOccurs="1" maxOccurs=
    "unbounded"/>
  </xsd:sequence>
  <xsd:attribute name="nb" type="xsd:string" use="required"/>
</xsd:complexType>

<xsd:complexType name="quantityType" mixed="true">
  <xsd:sequence>
    <xsd:any minOccurs="0" maxOccurs="unbounded" namespace="##other"
    processContents="lax"/>
  </xsd:sequence>
  <xsd:attribute name="geneID" type="xsd:string" use="required"/>
  <xsd:anyAttribute namespace="##any" processContents="lax"/>
</xsd:complexType>

<xsd:complexType name="quantitiesType">
  <xsd:sequence>
    <xsd:element name="quantity" type="quantityType" minOccurs="1" maxOccurs=
    "unbounded"/>
  </xsd:sequence>
  <xsd:attribute name="nb" type="xsd:string" use="required"/>
</xsd:complexType>
```

```
<!--
    Provider public metadata
-->

<xsd:element name="CLSIGPublicKey" type="CLSIGPublicKeyType"/>
<xsd:complexType name="CLSIGPublicKeyType">
    <xsd:sequence>
        <xsd:element name="modulus" type="xsd:string" minOccurs="1" maxOccurs="1"/>
        <xsd:element name="generators" type="generatorsType" minOccurs="1" maxOccurs=
↳ "1"/>
        <xsd:element name="exponent" type="xsd:string" minOccurs="1" maxOccurs="1"/>
    </xsd:sequence>
</xsd:complexType>


<xsd:element name="providerPublicMD" type="providerPublicMDType"/>
<xsd:complexType name="providerPublicMDType">
    <xsd:sequence>
        <xsd:element name="alias" type="xsd:string" minOccurs="1" maxOccurs="1"/>
        <xsd:element ref="ds:KeyInfo" minOccurs="1" maxOccurs="1"/>
        <xsd:element name="iis" type="iisType" minOccurs="0" maxOccurs="1"/>
        <xsd:element name="certAttrs" type="certAttrsType" minOccurs="0" maxOccurs="1"
↳ />
        <xsd:element ref="ds:Signature" minOccurs="0" maxOccurs="unbounded"/>
    </xsd:sequence>
</xsd:complexType>


<!--
    Provider private metadata
-->

<xsd:element name="CLSIGPrivateKey" type="CLSIGPrivateKeyType"/>
<xsd:complexType name="CLSIGPrivateKeyType">
    <xsd:sequence>
        <xsd:element name="firstPrimeFactor" type="xsd:string" minOccurs="1" maxOccurs=
↳ "1"/>
        <xsd:element name="secondPrimeFactor" type="xsd:string" minOccurs="0"
↳ maxOccurs="1"/>
        <xsd:element name="firstSafePrime" type="xsd:string" minOccurs="0" maxOccurs="1"
↳ />
        <xsd:element name="secondSafePrime" type="xsd:string" minOccurs="0" maxOccurs
↳ ="1"/>
        <xsd:element name="order" type="xsd:string" minOccurs="0" maxOccurs="1"/>
        <xsd:element name="phi" type="xsd:string" minOccurs="0" maxOccurs="1"/>
        <xsd:element name="invExponent" type="xsd:string" minOccurs="0" maxOccurs="1"/>
    </xsd:sequence>
</xsd:complexType>
```

```
<xsd:element name="providerPrivateMD" type="providerPrivateMDType"/>
<xsd:complexType name="providerPrivateMDType">
    <xsd:sequence>
        <xsd:element ref="ds:KeyInfo" minOccurs="1" maxOccurs="1"/>
        <xsd:element ref="ds:Signature" minOccurs="0" maxOccurs="unbounded"/>
    </xsd:sequence>
</xsd:complexType>

<!--
    Certificate metadata
-->

<xsd:element name="CLSIGSignatureValues" type="CLSIGSignatureValuesType"/>
<xsd:complexType name="CLSIGSignatureValuesType">
    <xsd:sequence>
        <xsd:element name="signatureValue" type="xsd:string" minOccurs="1" maxOccurs=
↳ "1"/>
        <xsd:element name="blindFactor" type="xsd:string" minOccurs="1" maxOccurs="1"/>
        <xsd:element name="quantities" type="quantitiesType" minOccurs="0" maxOccurs=
↳ "1"/>
    </xsd:sequence>
</xsd:complexType>

<xsd:element name="certificateMD" type="certificateMDType"/>
<xsd:complexType name="certificateMDType">
    <xsd:sequence>
        <xsd:element name="issuer" type="xsd:string" minOccurs="1" maxOccurs="1"/>
        <xsd:element name="dateOfIssuing" type="xsd:string" minOccurs="0" maxOccurs=
↳ "1"/>
        <xsd:element ref="CLSIGSignatureValues" minOccurs="1" maxOccurs="1"/>
        <xsd:element ref="ds:Signature" minOccurs="0" maxOccurs="unbounded"/>
    </xsd:sequence>
</xsd:complexType>

</xsd:schema>
```

FIG. C.1 – *Schéma W3C XML Signature pour la sérialisation x23.*

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<negotiation:providerPublicMD xmlns="http://www.w3.org/2000/09/xmldsig#"
  xmlns:negotiation="urn:fr:univ-st-etienne:tse:satin:ates:negociation">
 <negotiation:alias>Provider_TSE</negotiation:alias>
 <KeyInfo>
  <KeyName>CLSIG</KeyName>
  <KeyValue>
   <negotiation:CLSIGPublicKey>
    <negotiation:modulus>
02FDE51B3ADA1C897BE86EDA1E3362F69A8E725A4A4AE7C71489864171400AF85A44F4
82A9150BB44D6C0244DBAF2F538ECD739F8A49FEC4335741783880C389DD
    </negotiation:modulus>
    <negotiation:generators nb="3">
     <negotiation:generator id="0">
011DEECACB6941BB8A7725829FE7A59010F5617A0687D61F3FC7F9CD01338D01D45DAA
448C5B19EE3329FD6E8917F2066AE8EA4E98A668788FAC17E8CBF44CD7FD
     </negotiation:generator>
     <negotiation:generator id="1">
FA4361FD374F4B59A659D93378DE10F63BD14B61B9995D4E9DAC83E50B19576D694F16
1E6FAB0D403B715F2CD20445FB0E9B85F7D2E0E517B0B5A2B800CC2E14
     </negotiation:generator>
     <negotiation:generator id="2">
01A09A9F8C760C5DB2E374004A2D053F9310B0091B76212533A294572D78CE5140FA4B
2D3C180F28E88ACC3DFAD34E76628C7E0E73274E041F4BDE355584718E7B
     </negotiation:generator>
     <!--S-->
     <negotiation:geneblind>
01EA7979DB78569DD0B4761AEFD295738C100C0EBE25F48637CA737CA6D2E65E97550D
069718DB46AF49C4C9A746931C69E0942C4E674AE7115998220180021 24A
     </negotiation:geneblind>
     <!--Z-->
     <negotiation:genecheck>
0286FC64F4F2A4F89CD785096F37F4D9438845ADBE898E3A9988D18F19A4FB9C09E07D4
44AE7F8E5BDCE2ADC67C026DEDE41F834D96CE10CB33EA98A25399437A8
     </negotiation:genecheck>
    </negotiation:generators>
    <negotiation:exponent>
E9150066A54B5455B27D91C6991B7C2FEBC0692D8153C88AD144370AF806F6DFC902AA
0425CF5134F82D85E07EBC37CE6426D9B291E826B8D64FA5DD825A26D9
    </negotiation:exponent>
   </negotiation:CLSIGPublicKey>
  </KeyValue>
 </KeyInfo>
```

```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<Reference>
<Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>+2OlsQZnnYdbk4XiCECQqCDmkUc=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>
↳ ARniEiBhePefn//hQcWo+oczI7yuOexMhT6U7V0ym7v4Yh18vD58phMt8owu2joc
0LCDX34t/Txy4JqeCfNxF7Y=</SignatureValue>
<KeyInfo>
<X509Data>
<X509Certificate>
↳ MIICWjCCAUICCQDOQbwkDEvh6jANBgkqhkiG9w0BAQUFADAyMRUwEwYDVQQDFAxD
QV9ST09UX1RFU1QxDDAKBgNVBAoTA1RTRTELMAkGA1UEBhMCRllwHhcNMDkwOTE0
MDgxODI2WhcNMDkxMDE0MDgxODI2WjAzMRYwFAYDVQQDFA1QUk9WSURFUl9URVNU
MQwwCgYDVQQLEwNUU0UxCzAJBgNVBAYTAkZSMIGcMA0GCSqGSIb3DQEBAQUAA4GK
ADCBhgJBAv3lGzraHll76G7aHjNi9pqOclpKSufHFImGQXFACvhaRPSCqRULtE1s
AkTbry9Tjs1zn4pJ/sQzV0F4OIDDid0CQQDpFQBmpUtUVbJ9kcaZG3wv68BpLYFT
yIrRRDcK+Ab238kCqgQlz1E0+C2F4H68N85kJtmykegmuNZPpd2CWibZMA0GCSqG
SIb3DQEBBQUAA4IBAQBmvEnwrjrVfwxye3PVatE3LnycpmX81xeU2XWYY6blzm3f
0NmpwSMbpqwF4HQDjqsNf3QXpT6SZ/y/TVnkD6gLOjd5b03ablLzpvc+/BC+tFY5
zIMpSFGLXM/S3QivNIIktHdI5JF05WWWJZlgnw59nkBxEMIVyXzQUqt76NC0Fhg4
FrwoKdk4CDyb6Lid2LVMPdmWh1//nI2esapQXoRSF7TdHEpsZAf4jDiqwahP8h3r
6s9X7TO/hCyeYZq0THwjLma6XkMw204PCWbFRkpMOMtwIHD6c1vVvNmneQ/NI3IH
Mb28xeWse52zg2fmQAA+dHOnS28GYXavs1wXQWHN</X509Certificate>
</X509Data>
</KeyInfo>
</Signature>
</negotiation:providerPublicMD>
```

FIG. C.2 – *Exemple d'un document de métadonnées publiques de générateur.*

Bibliographie

Adams Carlisle & Lloyd Steve. **1999**. *Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations.* Macmillan Technical Publishing.

Angal Rajeev. **2005** (april). *Web Single Sign-On Interoperability Profile.* Tech. rept. Microsoft Corp. and Sun Microsystems Corp.

Aringhieri Roberto, Damiani Ernesto, Di Vimercati Sabine De Capitani, Paraboschi Stefano & Samarati Pierangelo. **2006**. Fuzzy techniques for trust and reputation management in anonymous peer-to-peer systems: Special Topic Section on Soft Approaches to Information Retrieval and Information Access on the Web. *J. Am. Soc. Inf. Sci. Technol.*, **57**(4), 528–537.

Association International Ergonomics. *http://www.iea.cc/browse.php?contID=what-is-ergonomics.*

Ateniese Giuseppe, Camenisch Jan, Joye Marc & Tsudik Gene. **2000**. A Practical and Provably Secure Coalition-Resistant Group Signature Scheme. *Pages 255–270 de : CRYPTO '00: Proceedings of the 20th Annual International Cryptology Conference on Advances in Cryptology.* London, UK : Springer-Verlag.

Ates Mikaël, Gravier Christophe, Lardon Jeremy, Fayolle Jacques & Sauviac Bruno. **2007**. Interoperability between Heterogeneous Federation Architectures: Illustration with SAML and WS-Federation. *Pages 1063–1070 de : SITIS '07: Proceedings of the 2007 Third International IEEE Conference on Signal-Image Technologies and Internet-Based System.* Washington, DC, USA : IEEE Computer Society.

Ates Mikaël, Fayolle Jacques, Gravier Christophe & Lardon Jeremy. **2008a**. Complex federation architectures: stakes, tricks & issues. *Pages 152–157 de : CSTST '08: Proceedings of the 5th international conference on Soft computing as transdisciplinary science and technology.* New York, NY, USA : ACM.

Ates Mikaël, Gravier Christophe, Fayolle Jacques & Sauviac Bruno. **2008b**. Marrying Heterogeneous Circles of Trust: No Silver Bullet Yet. *Pages 240–243 de : IECCS'07: Proceedings of the International Electronic Conference on Computer Science 2007*, vol. 1060. AIP Conf. Proc.

Ates Mikaël, Fayolle Jacques, Gravier Christophe, Lardon Jeremy & Garg Rahul. **2009a**. Privacy for RFID-enabled distributed applications - Design notes.

Dans : ICEIS09.

Ates Mikaël, Fayolle Jacques, Gravier Christophe & Lardon Jeremy. **2009b**. The User-Centric Vision Matches Credentials Exchanges. *Pages 870–876 de : ARES09: The forth International Conference on Availability, Reliability and Security 2009.* Washington, DC, USA : IEEE Computer Society.

Baker Stewart A. **1996**. Don't worry be happy – why Clipper is good for you. *Wired.*

Ballinger K. **2006** (august). *Web Services Metadata Exchange (WS-MetadataExchange) v1.1.* Tech. rept. BEA, Computer Associates, IBM, Microsoft, Sun Microsystems, SAP, WebMethods Corp.

Bartel Mark, Boyer John, Fox Barb, LaMacchia Brian & Simon Ed. **2008** (June). *XML Signature Syntax and Processing (Second Edition).* Tech. rept. W3C World Wide Web Consortium and IETF Internet Society.

Barth Adam, Datta Anupam, Mitchell John C. & Nissenbaum Helen. **2006**. Privacy and Contextual Integrity: Framework and Applications. *Pages 184–198 de : SP'06: Proceedings of the 2006 IEEE Symposium on Security and Privacy.* Washington, DC, USA : IEEE Computer Society.

Beckett Dave. **2004** (February). *RDF/XML Syntax Specification (Revised).* Tech. rept. W3C World Wide Web Consortium and IETF Internet Society.

Beek Maurice Ter, Moiso Corrado & Petrocchi Marinella. **2007**. Towards Security Analyses of an Identity Federation Protocol for Web Services in Convergent Networks. *Dans : AICT'07 - Proceedings of the Third Advanced International Conference on Telecommunications.*

Bellare Mihir & Rogaway Phillip. **1993**. Random oracles are practical: a paradigm for designing efficient protocols. *Pages 62–73 de : CCS '93: Proceedings of the 1st ACM conference on Computer and communications security.* New York, NY, USA : ACM.

Benantar Messaoud. **2005**. *Access Control Systems: Security, Identity Management and Trust Models.* Secaucus, NJ, USA : Springer-Verlag New York, Inc.

Berners-Lee T. **2000, mise à jour en 2007**. *W3C Semantic Web Stack.*

Berners-Lee Tim. **1998**. Uniform Ressource Identifiers (URI) Syntax. *Dans : IETF RFC 2396.*

Bertino Elisa, Ferrari Elena & Squicciarini Anna. **2004**. Trust Negotiations: Concepts, Systems, and Languages. *Computing in Science and Engg.*, **6**(4), 27–34.

Bianchi G., Bonola M., Falletta V., Proto F. S. & Teofili S. **2008**. The SPARTA pseudonym and authorization system. *Sci. Comput. Program.*, **74**(1-2), 23–33.

Bishop Matt. **2002**. *Computer Security - Art and Science.* Addison Wesley.

Blaze M., Feigenbaum J. & Lacy J. **1996a**. Decentralized Trust Management. *Pages 164–173 de : Proceedings of the 17th Symposium on Security and Privacy.*

Blaze M., Feigenbaum J. & Lacy J. **1996b**. The role of trust management in distributed systems security. *Dans : Proceedings of the 17th Symposium on Security and Privacy.*

Blaze M., Feigenbaum J., Ioannidis J. & Keromitys A.D. **1999**. *The Keynote trust management system (Version 2).*

Bonatti P & Samarati Pierangela. **2002a**. A unified framework for regulating access and information release on the web. *Journal of Computer Security*, **10**, 241–272.

Bonatti Piero A. & Samarati Pierangela. **2002b**. A uniform framework for regulating service access and information release on the web. *J. Comput. Secur.*, **10**(3), 241–271.

Brachman R. J. & Schmolze J. G. **1985**. An overview of the KL-ONE knowledge representation system. *Pages 171–216 de : Cognitive Science*, vol. 9.

Brands Stefan. **1993**. *An Efficient Off-line Electronic Cash System Based On The Representation Problem.* Tech. rept. Amsterdam, The Netherlands, The Netherlands.

Brands Stefan. **1994**. Untraceable off-line cash in wallet with observers. *Pages 302–318 de : CRYPTO '93: Proceedings of the 13th annual international cryptology conference on Advances in cryptology.* New York, NY, USA : Springer-Verlag New York, Inc.

Brands Stefan. **1995**. Off-Line Electronic Cash Based on Secret-Key Certificates. *Pages 131–166 de : LATIN '95: Proceedings of the Second Latin American Symposium on Theoretical Informatics.* London, UK : Springer-Verlag.

Brands Stefan A. *Non-Intrusive Identity Management.*

Brands Stefan A. *A Technical Overview of Digital Credentials.*

Brands Stefan A. **2000**. *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy.* Cambridge, MA, USA : MIT Press.

Bray Tim, Hollander Dave, Layman Andrew & Tobin Richard. **2006** (August). *Namespaces in XML 1.0 (Second Edition).* Tech. rept. W3C World Wide Web Consortium and IETF Internet Society.

Bray Tim, Paoli Jean, Sperberg-McQueen C. M., Maler Eve & Yergeau François. **2008** (November). *Extensible Markup Language (XML) 1.0 (Fifth Edition).* Tech. rept. W3C World Wide Web Consortium and IETF Internet Society.

Brey P. **2006**. Freedom and Privacy in Ambiant Intelligence. *Pages 157–166 de : Ethic and Information technology.*

Burr William E., Dodson Donna F & Polk W. Timothy. **2006**. *Electronic Authentication Guidelines - NIST800-63.* Tech. rept. National Institute of Standards and Technology - The Information Technology Laboratory.

Burrows Michael & Needham Roger. **1990**. A logic of authentication. *ACM Transactions on Computer Systems*, **8**, 18–36.

Cahill Conor P. **2007**. *Liberty ID-WSF Advanced Client Technologies Overview*. Tech. rept. Liberty Alliance Project.

Camenisch Jan. **2008**. The Camenisch-Lysyanskaya Private Credential System Explained.

Camenisch Jan & Damgård Ivan. **2000**. Verifiable Encryption, Group Encryption, and Their Applications to Separable Group Signatures and Signature Sharing Schemes. *Pages 331–345 de : ASIACRYPT '00: Proceedings of the 6th International Conference on the Theory and Application of Cryptology and Information Security*. London, UK : Springer-Verlag.

Camenisch Jan & Herreweghen Els Van. **2002**. Design and implementation of the idemix anonymous credential system. *Pages 21–30 de : CCS '02: Proceedings of the 9th ACM conference on Computer and communications security*. New York, NY, USA : ACM.

Camenisch Jan & Lysyanskaya Anna. **2001**. An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. *Pages 93–118 de : EUROCRYPT '01: Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques*. London, UK : Springer-Verlag.

Camenisch Jan & Lysyanskaya Anna. **2003**. A Signature Scheme with Efficient Protocols. **2576/2003**, 268–289.

Camenisch Jan & Pfitzmann Birgit. **2007**. Federated Identity Management. 213–238.

Camenisch Jan & Shoup Victor. **2003**. Practical verifiable encryption and decryption of discrete logarithms. *Pages 126–144 de : In Proceedings of Crypto 2003, Santa Barbara, USA*.

Camenisch Jan & Stadler Markus. **1997**. *Technical report TR 260: Proof Systems for General Statements about Discrete Logarithms*. Tech. rept.

Camenisch Jan, Hohenberger Susan, Kohlweiss Markulf, Lysyanskaya Anna & Meyerovich Mira. **2006**. How to win the clonewars: efficient periodic n-times anonymous authentication. *Pages 201–210 de : CCS '06: Proceedings of the 13th ACM conference on Computer and communications security*. New York, NY, USA : ACM.

Canard Sébastien, Malville Eric & Traoré Jacques. **2008**. Identity federation and privacy: one step beyond. *Pages 25–32 de : DIM '08: Proceedings of the 4th ACM workshop on Digital identity management*. New York, NY, USA : ACM.

Cantor Scott, Moreh Jahan, Philpott Rob & Maler Eve. **2005** (March). *Metadata for the OASIS Security Assertion Markup Language (SAML) v2.0.* Tech. rept. Organization for the Advancement of Structured Information Standards.

Chaum David. **1983**. Blind Signatures for untraceable payments. 199–203.

Chaum David. **1985**. Security without identification: transaction systems to make big brother obsolete. *Commun. ACM*, **28**(10), 1030–1044.

Chaum David. **1991**. Zero-knowledge undeniable signatures (extended abstract). *Pages 458–464 de : EUROCRYPT '90: Proceedings of the workshop on the theory and application of cryptographic techniques on Advances in cryptology.* New York, NY, USA : Springer-Verlag New York, Inc.

Chaum David & Evertse Jan-Hendrik. **1987**. A secure and privacy-protecting protocol for transmitting personal information between organizations. *Pages 118–167 de : Proceedings on Advances in cryptology—CRYPTO '86.* London, UK : Springer-Verlag.

Chaum David & Pedersen Torben P. **1993**. Wallet Databases with Observers. *Pages 89–105 de : CRYPTO '92: Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology.* London, UK : Springer-Verlag.

Chaum David, Fiat Amos & Naor Moni. **1990**. Untraceable Electronic Cash. *Pages 319–327 de : CRYPTO '88: Proceedings of the 8th Annual International Cryptology Conference on Advances in Cryptology.* London, UK : Springer-Verlag.

Chaum David L. **1981**. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM*, **24**(2), 84–90.

Chen Lidong. **1995**. Access with Pseudonyms. *Pages 232–243 de : Proceedings of the International Conference on Cryptography: Policy and Algorithms.* London, UK : Springer-Verlag.

Clarke R. **1988**. *Information Technology and Dataveillance.* Communications of the ACM.

Clercq Jan De. **2002**. Single Sign-On Architectures. *Pages 40–58 de : InfraSec '02: Proceedings of the International Conference on Infrastructure Security.* London, UK : Springer-Verlag.

Cofta Piotr. **2007**. *Trust, Complexity and Control - Confidence in a convergent world.* Wiley.

Cooper Alan. **1995**. The myth of metaphor. *Visual Basic Programmer's Journal.*

Cramer Ronald & Shoup Victor. **2000**. Signature schemes based on the strong RSA assumption. *ACM Trans. Inf. Syst. Secur.*, **3**(3), 161–185.

Damgård Ivan. **1990**. Payment Systems and Credential Mechanisms with Provable Security Against Abuse by Individuals. *Pages 328–335 de : CRYPTO '88: Proceedings*

of the 8th Annual International Cryptology Conference on Advances in Cryptology. London, UK : Springer-Verlag.

Damgård Ivan & Munkegade Ny. **2000**. Efficient concurrent zero-knowledge in the auxiliary string model. *Pages 418–430 de : Lecture Notes in Computer Science: Advances in Cryptology — EUROCRYPT 2000*, vol. 1807/2000. Springer Verlag.

Damiani Ernesto, De Capitani di Vermicati Sabrina & Samarati Pierangela. **2003**. Managing Multiple and Dependable Identities. *IEEE Internet Computing.*

Denning Dorothy E. & Sacco Giovanni Maria. **1981**. Timestamps in key distribution protocols. *Commun. ACM*, **24**(8), 533–536.

Diaz Claudia & Preneel Bart. **2007**. Accountable Anonymous Communication. 239–253.

Dierks T. & Allen C. **1999**. *The TLS protocole version 1.0.*

Dierks T. & Rescorla R. **2006**. *The TLS protocole version 1.1.*

Diffie W. & Hellman M.E. **1976a**. Cryptographic techniques. *Dans : Proceedings of the AFIPS National Computer Conference.*

Diffie W. & Hellman M.E. **1976b**. New directions in cryptography. *Dans : IEEE Transactions on Information Theory.*

Directorate-General XIII of the European Commission. **1997** (October). *Ensuring security and trust in electronic communication; towards a European framework for digital signatures and encryption.* Tech. rept. Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions.

Dwork Cynthia, Lotspiech Jeffrey & Naor Moni. **1996**. Digital signets: self-enforcing protection of digital information (preliminary version). *Pages 489–498 de : STOC '96: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing.* New York, NY, USA : ACM.

Eclipse. **2008**. *Higgins Project - http://www.eclipse.org/higgins.* Tech. rept.

Ellison C., Frantz B., Lampson B., Rivest R., Thomas B. & Ylonen T. **1999**. *SPKI Certificate Theory.*

EPCGlobal. **2006**. *EPCGlobal class 1 gen 2 RFID Specifications.* Tech. rept. Alien Technology RFID product and technology.

Feige U., Fiat A. & Shamir A. **1988**. Zero-knowledge proofs of identity. *J. Cryptol.*, **1**(2), 77–94.

Fiat Amos & Shamir Adi. **1987**. How to prove yourself: practical solutions to identification and signature problems. *Pages 186–194 de : Proceedings on Advances in cryptology—CRYPTO '86.* London, UK : Springer-Verlag.

Finkenzeller Klaus. **2003**. *RFID Handbook: Fundamentals and Applications in Contactless smartcards and Identification, 2nd edt.* John Wiley and Sons.

Freier A., Karlton P. & Kocher P.C. **1996**. The SSL Protocole Version 3.0. *Dans : Netscape Communications.*

Fujisaki Eiichiro & Okamoto Tatsuaki. **1997**. Statistical Zero Knowledge Protocols to Prove Modular Polynomial Relations. *Pages 16–30 de : CRYPTO '97: Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology.* London, UK : Springer-Verlag.

Gao Shudi (Sandy), Sperberg-McQueen C. M. & Thompson Henry S. **2009** (April). *W3C XML Schema Definition Language (XSD) 1.1 Part 1: Structures.* Tech. rept. W3C World Wide Web Consortium and IETF Internet Society.

Gevers Steven, Verslype Verslype & De Decker Bart. **2007**. Enhancing privacy in identity management systems. *Pages 60–63 de : WPES '07: Proceedings of the 2007 ACM workshop on Privacy in electronic society.* New York, NY, USA : ACM.

Giddens Anthony. **1991**. *Modernity and Self-Identity: Self and Society in the Late Modern Age.* Cambridge Polity Press.

Glover B. & Bhatt H. **2006**. *RFID Essentials.* O'Reilly.

Goldreich Oded, Pfitzmann Birgit & Rivest Ronald L. **1998**. Self-Delegation with Controlled Propagation - or - What If You Lose Your Laptop. *Pages 153–168 de : CRYPTO '98: Proceedings of the 18th Annual International Cryptology Conference on Advances in Cryptology.* London, UK : Springer-Verlag.

Goldwasser S, Micali S & Rackoff C. **1985**. The knowledge complexity of interactive proof-systems. *Pages 291–304 de : STOC '85: Proceedings of the seventeenth annual ACM symposium on Theory of computing.* New York, NY, USA : ACM.

Goldwasser S., Micali S. & Rackoff C. **1989**. The knowledge complexity of interactive proof systems. *SIAM J. Comput.*, **18**(1), 186–208.

Goodner M. **2007** (May). *Understand WS-Federation v1.0.* Tech. rept. IBM Corp. and Microsoft Corp.

Graham G.S. & Denning P.J. **1972**. Protection principles and practice. *Dans : AFIPS Spring Jt Computer Conference.*

Groß Thomas. **2003**. Security Analysis of the SAML Single Sign-on Browser/Artifact Profile. *Page 298 de : ACSAC '03: Proceedings of the 19th Annual Computer Security Applications Conference.* Washington, DC, USA : IEEE Computer Society.

Groß Thomas, Pfitzmann Birgit & Sadeghi Ahmad-Reza. **2005a**. Browser Model for Security Analysis of Browser-Based Protocols. *Pages 489–508 de : Lecture Notes in Computer Science: Computer Security – ESORICS 2005*, vol. 3679. Springer Berlin / Heidelberg.

Groß Thomas, Pfitzmann Birgit & Sadeghi Ahmad-Reza. **2005b**. Proving a WS-federation passive requestor profile with a browser model. *Pages 54–64 de : SWS*

'05: Proceedings of the 2005 workshop on Secure web services. New York, NY, USA : ACM.

Group Oxford Computer. **2007** (February). *Achieving Interoperability between Active Directory Federation Services and Shibboleth.* Tech. rept.

Gruber T. R., Gruninger M., Hayes P., Mc Guinness D. & Obrst L. **2007**. *Ontology Framework Draft.* Tech. rept. OntologySummit2007: Frameworks For Consideration.

Hayes Patrick J. **1979**. The Logic of Frames. *Pages 46–61 de : in D. Metzing (ed.), Frame Conceptions and Text Understanding.*

Herzberg Amir, Mass Yosi, Michaeli Joris, Ravid Yiftach & Naor Dalit. **2000**. Access Control Meets Public Key Infrastructure, Or: Assigning Roles to Strangers. *Page 2 de : SP '00: Proceedings of the 2000 IEEE Symposium on Security and Privacy.* Washington, DC, USA : IEEE Computer Society.

Hess Adam, Jacobson Jared, Mills Hyrum, Wamsley Ryan, Seamons Kent E. & Smith Bryan. **2002**. Advanced Client/Server Authentication in TLS. *Dans : Network and Distributed System Security Symposium.*

Hoare C. A. R. **1978**. Communicating sequential processes. *Commun. ACM*, **21**(8), 666–677.

Hoffman Mario. **2004**. User-Centric Identity Management in Open Mobile Environments. *Dans : Proceedings of the 2004 workshop on Security and Privacy in Pervasive Computing.*

Housley R. & Hoffman P. **1999**. Internet X509 Public Key Infrastructure Operationnal Protocols: FTP and HTTP. *Dans : IETF RFC 2585.*

Housley R., Ford W., W.Polk & Solo D. **1999**. Internet X509 Public Key Infrastructure Certificate and CRL Profile. *Dans : IETF RFC 2459.*

Hur Matt. **2004** (February). *Passive Requestor Federation Interop Scenario v0.4.* Tech. rept. Microsoft, IBM.

IETFWorkingGroup Hyper Text Transfer Protocol. **2009** (March). *Hyper Text Transfer Protocol (HTTP) 1.1 draft 6 Specifications.* Tech. rept. W3C World Wide Web Consortium and IETF Internet Society.

Imamura Takeshi, Dillaway Blair & Simon Ed. **2002** (December). *XML Encryption Syntax and Processing.* Tech. rept. W3C World Wide Web Consortium and IETF Internet Society.

Juels Ari. **2006**. RFID Security and Privacy: A Research Survey. *IEEE Journal on Selected Areas in Communication.*

Jøsang Audun, Gray Elizabeth & Kinateder Michael. **2006a**. Simplification and Analysis of Transitive Trust Networks. *Web Intelligence and Agent Systems*, **4**.

Jøsang Audun, Hayward Ross & Pope Simon. **2006b**. Trust network analysis with subjective logic. *Pages 85–94 de : ACSC '06: Proceedings of the 29th Australasian Computer Science Conference*. Darlinghurst, Australia, Australia : Australian Computer Society, Inc.

Kohl J. & Neuman C. **1993** (September). *The Kerberos Network Authentication Service v5*.

Kohnfelder L.M. **1978**. Toward a practical public-key cryptosystem. *Dans : B.Sc Thesis, MIT Department of Electrical Engineering*.

Lampson B. W. **1974**. Protection. *ACM Operating System Review*, **8**(1), 18–24.

Langheinrich M. **2001**. Privacy by design - Principle of Privacy-aware Ubiquitous Systems. **2201**, 273 – 291.

Langheinrich Marc. **2007**. Privacy and RFID. *Pages 433–450 de : Security, Privacy, and Trust in Modern Data Management*. Springer.

Lawrence K. **2006** (February). *Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)*. Tech. rept. Organization for the Advancement of Structured Information Standards.

Lawrence Kelvin & Kaler Chris. **2009a** (February). *Web Services Security Policy Language (WS-SecurityPolicy) v1.3*. Tech. rept. Organization for the Advancement of Structured Information Standards - Web Services Secure Exchange Technical Committee.

Lawrence Kelvin & Kaler Chris. **2009b** (February). *Web Services Security Policy Language (WS-SecurityPolicy) v1.3*. Tech. rept. Organization for the Advancement of Structured Information Standards - Web Services Secure Exchange Technical Committee.

Lawrence Kelvin & Kaler Chris. **2009c** (February). *Web Services Trust Language (WS-Trust) v1.4*. Tech. rept. Organization for the Advancement of Structured Information Standards - Web Services Secure Exchange Technical Committee.

Lawrence Kelvin & Kaler Chris. **2009d** (February). *Web Services Trust Language (WS-Trust) v1.4*. Tech. rept. Organization for the Advancement of Structured Information Standards - Web Services Secure Exchange Technical Committee.

Lee H., Yang J. & Kim K. **2006**. *Enhanced Mutual Authentication Protocol for Low-Cost RFID*. Tech. rept. Auto-ID Labs.

Li Jiangtao, Li Ninghui & Winsborough William H. **2005a**. Automated trust negotiation using cryptographic credentials. *Pages 46–57 de : CCS '05: Proceedings of the 12th ACM conference on Computer and communications security*. New York, NY, USA : ACM.

Li N. & Winsborough W. **2002**. Towards Practical Automated Trust Negotiation. *Page 92 de : POLICY '02: Proceedings of the 3rd International Workshop on Policies*

for Distributed Systems and Networks (POLICY'02). Washington, DC, USA : IEEE Computer Society.

Li Ninghui, Winsborough William H. & Mitchell John C. **2001**. Distributed credential chain discovery in trust management: extended abstract. *Pages 156–165 de : CCS '01: Proceedings of the 8th ACM conference on Computer and Communications Security*. New York, NY, USA : ACM.

Li Ninghui, Mitchell John C. & Winsborough William H. **2002**. Design of a Role-Based Trust-Management Framework. *Page 114 de : SP '02: Proceedings of the 2002 IEEE Symposium on Security and Privacy*. Washington, DC, USA : IEEE Computer Society.

Li Ninghui, Grosof Benjamin N. & Feigenbaum Joan. **2003**. Delegation logic: A logic-based approach to distributed authorization. *ACM Trans. Inf. Syst. Secur.*, **6**(1), 128–171.

Li Ninghui, Mitchell John C. & Winsborough William H. **2005b**. Beyond proof-of-compliance: security analysis in trust management. *J. ACM*, **52**(3), 474–514.

Lim C & Kwon T. **2006**. Strong and Robust RFID authentication enabling perfect ownership transfer. *Pages 1–20 de : Lecture Notes in Computer Science: ICICS'06 Conference on Information and Communications Security*, vol. 4307. Raleigh, North Carolina, USA : Springer-Verlag.

Linn John. **2006**. *Trust Models Guidelines*. Tech. rept. Organization for the Advancement of Structured Information Standards.

Lockhart H. **2006** (December). *Web Services Federation Language (WS-Federation) v1.1*. Tech. rept. BEA, BMC Software, CA Inc, IBM, Layer 7 Technologies Inc., Microsoft, Novell, VeriSign.

Lopez Diedo R & team GN2 JRA5. **2007** (march). *Best Practice Guide - AAI Cookbook - Second Edition - Guidelines for Connecting to the eduGAIN AA Infrastructure*. Tech. rept. GEANT2.

Lysyanskaya Anna, Rivest Ronald L., Sahai Amit & Wolf Stefan. **2000**. Pseudonym Systems. *Pages 184–199 de : Lecture Notes in Computer Science: Selected Areas in Cryptography*, vol. 1758. Springer Berlin / Heidelberg.

MacGregor W, Dutcher W & Khan J. **2006a** (October). *An ontology of Identity Credentials - Part 1: Background and Formulation*. Tech. rept. National Institute of Standards and Technology - U.S. Department of Commerce.

MacGregor William, Dutcher William & Khan Jamil. **2006b**. *An Ontology of Identity Credentials Part1: Background and Formulation - NIST800-103*. Tech. rept. National Institute of Standards and Technology - The Information Technology Laboratory.

Maler Eve. **2006** (October). *Security Assertion Markup Language v2.0 - Technical Overview.* Tech. rept. Organization for the Advancement of Structured Information Standards.

Mayfield Terry, Gligor Virgil D., Cugini Janet A., Boone John M. & Dobry Robert W. **1995**. *Security Criteria for Distributed Systems: Functional Requirements.* Tech. rept.

McGuinness Deborah L., Nardi Daniele & Patel-Shneider Peter F. **2003**. *The description logic handbook: Theory, implementation, and applications.* Cambridge University Press.

McKnight D.H. & Chervany N.L. **1996**. *The meanings of trust.* Tech. rept.

Menezes Alfred J., Vanstone Scott A. & Oorschot Paul C. Van. **1996**. *Handbook of Applied Cryptography.* Boca Raton, FL, USA : CRC Press, Inc.

Merkle R.C. **1978**. Secure Communications Over Insecure Channels. *Dans : Communications of the ACM.*

Minsky Marvin. **1975**. Minsky's frame system theory. *Pages 104–116 de : TINLAP '75: Proceedings of the 1975 workshop on Theoretical issues in natural language processing.* Morristown, NJ, USA : Association for Computational Linguistics.

Moffett Jonathan D. **1990**. *Delegation of Authority Using Domain Based Access Rules.* Thèse de doctorat, Dept of Computing, Imperial College, London.

Mont Marco Casassa & Brown Richard. **2002**. *Active Digital Credentials: Provision of Up-to-Date Identity and Profile Information.* Tech. rept. Hewlett Packard Laboratories, Trusted Systems Laboratory.

Mont Marco Casassa, Bramhall Pete, M Gittler, Pato Joe & O Rees. **2002**. *Identity Management: a Key e-Business Enabler, HPL-2002-164.* Tech. rept. Hewlett Packard Laboratories, Trusted Systems Laboratory.

Mont Marco Casassa, Bramhall Pete & Pato Joe. **2003**. *On Adaptative Identity Management: The Next Generation of Identity Management Technologies - HPL-2003-149.* Tech. rept. Hewlett Packard Laboratories, Trusted Systems Laboratory.

Motik Boris, Grau Bernardo Cuenca, Horrocks Ian, Wu Zhe, Fokoue Achille & Lutz Carsten. **2009** (June). *OWL 2 Web Ontology Language - Profiles.* Tech. rept. W3C World Wide Web Consortium and IETF Internet Society.

Nanda Arun & Jones Michael B. **2008**. *Identity Selector Interoperability Profile V1.5.* Tech. rept. Microsoft Corporation.

Needham Roger M. & Schroeder Michael D. **1978**. Using encryption for authentication in large networks of computers. *Commun. ACM*, **21**(12), 993–999.

Neuman C., Hartman S. & Raeburn K. **2005** (July). *The Kerberos Network Authentication Service v5.* Tech. rept. The Internet Engineering Task Force.

Nielsen Jakob. *Usability engineering.* Morgan Kaufmann.

Nissenbaum Helen. **1998**. Protecting Privacy in an Information Age: The problemù of Privacy in Public. *Washington Law Review*, **17**, 559–596.

Nissenbaum Helen. **2004**. Privacy as Contextual Integrity. *Washington Law Review*, **79**(1), 119–158.

OpenID-Community. **2008**. *OpenID Authentication 2.0 and OpenID Attribute Exchange 1.0 - http://openid.net/developers/specs/.* Tech. rept.

Organisation International Standardisation. *ISO 9241-11:1998 Exigences ergonomiques pour travail de bureau avec terminaux à écrans de visualisation (TEV) – Partie 11: Lignes directrices relatives à l'utilisabilité.*

Organisation International Standardisation. *ISO/TR 16982:2002 Ergonomie de l'interaction homme-système – Méthodes d'utilisabilité pour la conception centrée sur l'opérateur humain.*

Osborn S. **1997**. Mandatory Access Control and Role-Based Access Control Revisited.

Osborn S., Sandhu R. & Munawer Q. **2000**. Configuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies. *ACM Transactions on Information and System Security*, **3**(2), 85–106.

Paraboschi Stefano. **2003**. Managing and Sharing Servents' Reputations in P2P Systems. *IEEE Trans. on Knowl. and Data Eng.*, **15**(4), 840–854. Member-Damiani,, Ernesto and Member-De Capitani di Vimercati,, Sabrina and Member-Samarati,, Pierangela.

Parr B & Villars R. **2001**. *Digital Identitites: The Comming Struggle for the Future of the Net.* Tech. rept. IDC.

Pashalidis Andreas & Mitchell Chris. J. **2003**. A Taxonomy of Single Sign-On Systems. *Page 219 de: Lectures Notes in Computer Science: Information Security and Privacy*, vol. 2727. Springer-Verlag.

Pashalidis Andreas & Mitchell Chris J. **2004**. A Security Model for Anonymous Credential Systems. *Pages 183–189 de: Information Security Management, Education and Privacy, Proceedings of the 3rd Working Conference on Privacy and Anonymity in Networked and Distributed Systems.* Y. Deswarte, F. Cuppens, S. Jajodia and L. Wang (eds.) Kluwer Academic Publishers IFIP Conference Proceedings.

Pato Joe. **2003**. *Identity Management: Setting the Context - HPL-2003-72.* Tech. rept. Hewlett Packard Laboratories, Trusted Systems Laboratory.

Peterson David, Gao Shudi (Sandy), Malhotra Ashok, Sperberg-McQueen C. M. & Thompson Henry S. **2009** (April). *W3C XML Schema Definition Language (XSD) 1.1 Part 2: Datatypes.* Tech. rept. W3C World Wide Web Consortium and IETF Internet Society.

Pfitzmann Andreas & Kohntopp Marit. **2001**. Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology. *Pages 1–9 de: Lecture Notes in Com-*

puter Science: Designing Privacy Enhancing Technologies, vol. 2009. Springer Berlin / Heidelberg.

Pfitzmann Birgit. **2003**. Privacy in Enterprise Identity Federation: Policies for Liberty Single Signon. *Pages 189–204 de : Lecture Notes in Computer Science: Privacy Enhancing Technologies*, vol. 2760. Springer Berlin / Heidelberg.

Pfitzmann Birgit. **2004**. Privacy in Enterprise Identity Federation: Policies for Liberty 2 Single Signon. *Pages 45–58 de : Information Security Technical Report (ISTR)*, vol. 9. Elsevier.

Pfitzmann Birgit & Waidner Michael. **2002**. Privacy in browser-based attribute exchange. *Pages 52–62 de : WPES '02: Proceedings of the 2002 ACM workshop on Privacy in the Electronic Society*. New York, NY, USA : ACM.

Pfitzmann Birgit & Waidner Michael. **2004**. Federated Identity-Management Protocols - Where User Authentication Protocols May Go. *Lecture Notes in Computer Science*.

Philip Robinson, Harald Vogt Waleed Wagealla. **2005**. Some Research Challenges in Pervasive Computing. *Privacy, Security and Trust within the Context of Pervasive Computing*, **1**, 1–16.

Pointcheval David & Stern Jacques. **1996**. Security proofs for signature schemes. *Pages 387–398 de : Eurocrypt '96 - Lect Notes in Comp Sci, nr 1070*. Springer-Verlag.

projectconcordia.org. **2009**. *Etude sur l'utilisation de la fédération*. Tech. rept.

Quillian M. Ross. **1967**. Word Concepts: A Theory and Simulation of some Basic Semantic Capabilities. *Pages 410–430 de : Behavioral Science*, vol. 12.

Rabin M. **1989**. Digitalized Signatures. *Foundations of Secure Computation*.

Rigney C., Willats W. & Calhoun P. **2000a**. *RADIUS Extensions*.

Rigney C., Willens S., Rubens A. & Simpson W. **2000b**. *Remote Authentication Dial In User Service (RADIUS)*.

Rivest R. L., Shamir A. & Adleman L. **1978**. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, **21**(2), 120–126.

Saadi Rachid. **2009**. *Le contrôle d'accès et la gestion de la confiance dans les systèmes pervasifs*. INSA Lyon.

Sandhu Ravi S., Coyne Edward J., Feinstein Hal L & Youman Charles E. **1996**. Role-based access control models. *IEEE Computer*, **29**(2), 38–47.

Scavo Tom & Cantor Scott. **2005** (june). *Shibboleth Architecture - Technical Overview*. Tech. rept. Internet2.

Schechter Bruce. **1999**. *Seeing the light: IBM's vision of life beyond the PC*.

Schnorr Claus-Peter. **1990**. Efficient Identification and Signatures for Smart Cards. *Pages 239–252 de : CRYPTO '89: Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology*. London, UK : Springer-Verlag.

SCHOEMAN F. **1984**. *Introduction, Philosophical Dimensions of Privacy: An anthology.* Cambridge University Press.

SEAMONS K., WINSLETT M. & YU T. **2001**. Limiting the disclosure of Access Control policies during automated trust negociation. *Dans : Proceedings of the Network and Distributed Systems Security Symposium.*

SEAMONS KENT E., WINSLETT M, YU T, SMITH B, CHILD EVAN, JACOBSON J, MILLS H, & YU L. **2002**. Requirement for Policy Languages for Trust Negotiation. *Pages 68–79 de : Proceedings of the Third IEEE International Workshop on Policies for Distributed Systems and Netwroks.* IEEE Computer Society.

SEARLE J. **1985**. *Intentionalité.* Editions de minuit.

SHANK R & ABELSON R. **1977**. Scripts, Plans, Goals and Understanding. *Dans : Hillsdale, NJ: Erlbaum.*

SHIREY R. **2000** (may). *RFC 2828 - Internet Security Glossary.* Tech. rept. Network Working Group - The Internet Society.

SMITH DON. **2008**. The Challenge of Federated Identity Management. *Network Security*, April, 7–9.

SMYTH BEN, RYAN MARK & CHEN LIQUN. **2007**. Direct Anonymous Attestation (DAA): Ensuring Privacy with Corrupt Administrators. *Lecture Notes in Computer Science - Security and Privacy in Ad-hoc and Sensor Networks*, **4572/2007**, 218–231.

SONG BOYEON & MITCHELL CHRIS J. **2008**. RFID Authentication Protocol for Low-cost Tags. *Dans : WiSec'08: Proceedings of the 2008 ACM Conference of Wireless Security.* ACM.

SQUICCIARINI ANNA C. **2006**. Achieving Privacy in Trust Negotiations with an Ontology-Based Approach. *IEEE Trans. Dependable Secur. Comput.*, **3**(1), 13. Fellow-Bertino,, Elisa and Senior Member-Ferrari,, Elena and Member-Ray,, Indrakshi.

SULLIVAN ROGER K. **2005**. The Case for Federated Identity. *Network Security*, September, 15–19.

SURIADI SURIADI, FOO ERNEST & JOSANG AUDUN. **2007**. A User-centric Federated Single Sign-on System. *Pages 99–106 de : NPC '07: Proceedings of the 2007 IFIP International Conference on Network and Parallel Computing Workshops.* Washington, DC, USA : IEEE Computer Society.

THORNTON FRANK, HAINES BRAD, DAS ANAND M., BHARGAVA HERSH, CAMPBELL ANITA & KLEINSCHMIDT JOHN. **2006**. *RFID Security.* Syngress.

TOURZAN JONATHAN & KOGA YUZO. **2007**. *Liberty ID-WSF Web Services Framework Overview.* Tech. rept. Liberty Alliance Project.

TSANG PATRICK P., AU MAN HO, KAPADIA APU & SMITH SEAN W. **2007**. Blacklistable anonymous credentials: blocking misbehaving users without ttps. *Pages 72–81*

de : CCS '07: Proceedings of the 14th ACM conference on Computer and communications security. New York, NY, USA : ACM.

Varela Francisco J. **1988**. *Cognitive Science. A cartography of Current Ideas.*

Warren S.D. & Brandeis L.D. **1890**. *The right of Privacy, Harvard Law Review.* Harvard.

Wason T. **2005** (may). *Liberty ID-FF Architecture Overview.* Tech. rept. Liberty Alliance Project.

Weiser Mark. **1991**. The Computer for the 21st Century. *Scientific American*, 66–75.

Winsborough William H. & Li Ninghui. **2002**. Protecting sensitive attributes in automated trust negotiation. *Pages 41–51 de : WPES '02: Proceedings of the 2002 ACM workshop on Privacy in the Electronic Society.* New York, NY, USA : ACM.

Winsborough William H. & Li Ninghui. **2006**. Safety in automated trust negotiation. *ACM Trans. Inf. Syst. Secur.*, **9**(3), 352–390.

Winsborough William H., Seamons Kent E. & Jones Vicki E. **2000**. Automated Trust Negotiation. *DARPA Information Survivability Conference and Exposition,*, **1**, 0088.

Winslett M, Yu T, Seamons Kent E., Hess A, Jacobson J, Jarvis R, Smith B & Yu L. **2002**. Negotiating trust in the Web. *Pages 30– 37 de : Internet Computing, IEEE*, vol. 6.

Yao Dolev & Yao A. C. **1983**. On the security of public key protocols. *IEEE Transactions on on Information Theory*, **29**(2), 198 – 208.

Yu T., Ma X. & Winslett M. **2000**. Prunes: An efficient and complete strategy for trust negotiation over the internet. *Page 210–219 de : Proceedings of the 7th ACM Computer and Communication Security.* ACM Press.

Yu Ting & Winslett Marianne. **2003a**. Policy migration for sensitive credentials in trust negotiation. *Pages 9–20 de : WPES '03: Proceedings of the 2003 ACM workshop on Privacy in the electronic society.* New York, NY, USA : ACM.

Yu Ting & Winslett Marianne. **2003b**. A Unified Scheme for Resource Protection in Automated Trust Negotiation. *Page 110 de : SP '03: Proceedings of the 2003 IEEE Symposium on Security and Privacy.* Washington, DC, USA : IEEE Computer Society.

Yu Ting, Winslett Marianne & Seamons Kent E. **2003**. Supporting structured credentials and sensitive policies through interoperable strategies for automated trust negotiation. *ACM Trans. Inf. Syst. Secur.*, **6**(1), 1–42.

Zimmermann P.R. **1995**. *The Official PGP User's Guide.* Tech. rept.

Zrelli Saber, Medeni Tunc, Shinoda Yoichi & Medeni Tolga. **2007**. Improving Kerberos Security System for Cross-Realm Collaborative Interactions: An Innovative

Example of Knowledge Technology for Evolving & Verifiable E-Society. *Pages 211–219 de : Research, Innovation and Vision for the Future, 2007 IEEE International Conference.*