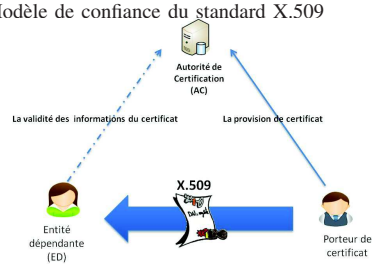
Etude du concept de confiance pour les infrastructures à clés publiques

Ahmad Samer Wazan, Romain Laborde, François Barrère, Abdelmalek Benzekri

Étude du concept de confiance pour les Infrastructures à Clés Publiques

Ahmad Samer Wazan, Romain Laborde, François Barrere and Abdelmalek Benzekri
Université Paul Sabatier
IRIT/SIERA
Email : {Ahmad-Samer.Wazan, Laborde, Barrere, Benzekri}@irit.fr

FIGURE 1. Modèle de confiance du standard X.509



***Résumé*—Les infrastructures à clés publiques (ICPs) constituent à ce jour un élément majeur de la construction d'espaces sécurisés dans les environnements numériques. L'ICP se base sur un modèle de confiance composé de trois entités, à savoir les autorités de certification (ACs), les porteurs de certificat et les entités dépendantes (EDs). Historiquement, ce modèle de confiance a été conçu pour des cas où les porteurs de certificat et les EDs ont des relations directes avec les ACs (par exemple tous font partie de la même entreprise). Aujourd'hui dans Internet, les EDs n'ont aucune relation directe avec les ACs. Cette nouvelle situation nécessite donc une définition plus précise de la notion de la confiance entre les ACs et les EDs. Nous montrons que l'évaluation de la confiance selon cette définition nécessite des expertises juridiques et techniques. Nous proposons donc de modifier le modèle de confiance à trois entités en ajoutant le rôle de l'expert technique et juridique qui aide les EDs à prendre des décisions sur les certificats.**

I. INTRODUCTION

Les infrastructures à clés publiques (ICPs) constituent à ce jour un élément majeur de la construction d'espaces sécurisés dans les environnements numériques. Les ICPs sont basées sur un modèle de confiance composé de trois entités (Figure 1) : (1) l'autorité de certification (AC) qui représente le composant central de cette infrastructure et qui valide par sa signature les informations contenues dans le certificat (2) le porteur de certificat et (3)enfin l'entité dépendante (ED) qui cherche à avoir des informations fiables sur l'identité du porteur de certificat pour pouvoir établir des transactions avec lui. Dans ce modèle, le porteur de certificat dépend de l'AC pour la provision de son certificat, et l'ED dépend de l'AC pour la validité des informations contenues dans le certificat.

Historiquement, ce modèle de confiance a été conçu pour une application bien précise qui est l'annuaire X.500. Cet annuaire a été un cas d'étude simple car c'est un système hiérarchique où toutes les relations entre les porteurs de certificat et les entités dépendantes sont préétablies. Dans ce type d'application, la question de la confiance ne se pose pas car la relation de confiance entre les trois entités du modèle de confiance est naturelle : les trois entités font partie de la même entreprise et les certificats ne sont utilisés que pour des services qui concerne les activités de l'entreprise.

Aujourd'hui, l'annuaire X.500 a été abandonné, mais pas le modèle de confiance à trois entités qui a été largement adopté dans Internet. Internet est composé aujourd'hui de plusieurs ICPs où chaque ICP possède ses propres procédures pour la gestion des certificats. On appelle ce nouveau modèle de déploiement *le modèle ouvert*, car d'un côté l'ED n'a peut être aucune relation préétablie avec aucune ICP et d'un autre côté, les certificats qui sont générés par ces ICPs sont définis pour un contexte d'utilisation ouvert. Ce nouveau modèle de déploiement a créé un problème de gestion de la confiance pour les EDs : comment une ED peut-elle faire confiance à une AC plutôt qu'à une autre ?

Répondre à cette question nécessite de définir préalablement ce qu'est la confiance dans une AC du point de vue des EDs. Définir la confiance du point de vue de porteur de certificat n'est pas nécessaire car *le modèle ouvert* n'a pas d'effet sur la relation entre le porteur de certificat et l'AC ; cette relation reste toujours régulée par des contrats directs entre les porteurs de certificat et les ACs. N'ayant pas été considéré initialement dans l'environnement des annuaires X.500, la confiance dans les ACs du point de vue des EDs dans *le modèle ouvert* est aujourd'hui une notion ambiguë et considérée souvent comme un concept ad hoc par les fournisseurs des services des ICPs.

L'objectif de cet article est de donner une définition formelle de la confiance du point de vue des EDs. Nous montrons ensuite que l'évaluation de la confiance ainsi définie ne peut se faire que par des experts qui ont une connaissance technique et juridique dans le domaine des ICPs. Par conséquent, nous proposons de modifier le modèle de confiance de base défini par le standard X.509 en introduisant le rôle de l'expert technique et juridique. Le rôle de l'expert consiste à aider les EDs à prendre des décisions informées sur les certificats.

L'article est organisé de la manière suivante : dans la section 2, nous analysons les différentes définitions de la confiance abordées dans la littérature. Dans la section 3, nous introduisons la notion de confiance dans les ACs, et nous adoptons une définition de confiance appropriée pour ces outils. Dans la section 4, nous présentons un nouveau

modèle de confiance qui considère le rôle de l'expert et nous présentons notre approche qui vise à aider les EDs à prendre des décisions de confiance dans les certificats. Enfin dans la section 5, nous présentons nos conclusions.

II. Qu'est-ce que la confiance ?

Donner une définition de la confiance dans les ACs nécessite forcément d'expliquer la notion de confiance. Cependant, contrairement à ce que l'on pourrait penser, la notion de confiance n'est pas un concept clair en soi. Ce concept est défini différemment selon la culture de la société ou selon la discipline des personnes qui ont essayé de définir ce concept.

A. Différences sémantique et terminologique entre les cultures

Des significations et des terminologies différentes du concept de confiance peuvent être identifiées par pays et/ou par culture. Ces différences renforcent l'ambigüité et le flou de ce concept. Tout d'abord, nous présentons les significations et les terminologies différentes utilisées dans les langues française et anglaise qui peut amener différente interprétation entre personnes francophones et anglophones.

La langue anglaise fournit deux termes pour exprimer deux dimensions de la confiance : « *trust* » et « *confidence* », tandis que la langue française ne connait que le terme « confiance ». La langue anglaise fournit également des termes concis et précis pour désigner les partenaires d'une relation de confiance : respectivement « *trustor* » et « *trustee* », tandis que la langue française manque d'un substantif pour désigner ces termes et l'on n'en connaît que la transcription [5]. Mais la confiance correspond t-elle au terme « *trust* » en anglais ou au terme « *confidence* » ? Ou bien aux deux ?

Luhmann [11] a expliqué la différence entre « *confidence* » et « *trust* » dans la langue anglaise. Il a expliqué que les deux termes indiquent l'attente qui peut conduire à la déception, mais « *confidence* » est un sentiment que nos attentes ne seront pas déçues, tandis que « *trust* » requiert un engagement personnel de celui qui fait confiance et évalue rationnellement les risques. Selon Luhmann, si on n'a pas d'alternatives pour une action donnée alors nous sommes dans une situation de « *confidence* ». Si nous devons choisir une action parmi d'autres, malgré la possibilité d'être déçu, nous sommes dans une situation de « *trust* ». Le « *trust* » en anglais est donc un mécanisme de réduction des risques pour une action donnée.

Le dictionnaire de l'académie française définit la confiance comme :

Confiance n. f. XIIIe siècle, confience. Emprunté du latin confidentia, « confiance », dérivé de confidere.

a) *Espérance ferme que l'on place en quelqu'un, en quelque chose, certitude de la loyauté d'autrui.*

b) *Espérance ferme que les autres placent en vous ; conviction qu'ils peuvent avoir de votre sincérité, de votre dévouement, de votre honnêteté.*

c) *Sentiment de sécurité qu'éprouve celui qui compte sur lui-même.*

d) *Sentiment d'assurance que donne la foi en l'avenir.*

Les deux premières parties de cette définition font référence au terme *trust* et mettent en évidence l'aspect social du concept de confiance en induisant une relation de confiance d'une entité, *trustor*, vers le *trustee*. La troisième et quatrième partie de la définition font référence au terme *confidence*.

De plus, une autre différence fondamentale marque les deux langues sur le fait que le « *trust* » en anglais est un contrat. Dans ce contexte, le *trust* joue un rôle vital dans la société britannique et dans les pays autrefois gouvernés par la Grande Bretagne comme les États-Unis, le Canada, l'Australie, la Nouvelle-Zélande et l'Inde [9]. Voyons par exemple l'une des définitions fournies par le dictionnaire Merriam Webster pour le « *trust* » : « *a combination of firms or corporations formed by a legal agreement* » ou encore « *a property interest held by one person for the benefit of another* ». Cette défintion montre clairement l'aspect juridique de la notion de trust dans la culture anglaise. Cette signification n'est pas explicitement définie dans la langue française.

Dans la suite de cet article, nous allons utiliser le terme de confiance pour désigner uniquement la notion de « *trust* » en anglais, le terme *trustee* pour désigner celui à qui la confiance est accordée, et le terme *trustor* pour désigner celui qui fait confiance.

B. Une pléthore de définitions dans la littérature

Des différences entre les définitions de la confiance apparaissent aussi selon la discipline des auteurs. En effet, plusieurs disciplines, chacune selon sa perspective, ont étudié le concept de confiance. La psychologie [3], la sociologie [10] [2], et la philosophie [1] [4] sont autant de disciplines ayant consacré des efforts à l'étude de la confiance.

D'un point de vue philosophique, la philosophe Annette Baier [1] a offert une définition intéressante : *One leaves others an opportunity to harm one when one trusts, and also shows one's confidence that they will not take it. Reasonable trust will require good grounds for such confidence in another's good will, or at least the absence of good grounds for expecting their ill will or indifference. Trust, then, on this first approximation, is accepted vulnerability to another's possible but not expected ill will (or lack of good will) toward one.*

Ainsi, lorsque nous faisons confiance, nous sommes vulnérables aux autres, tout en croyant qu'ils ne vont pas nous nuire, même s'ils ont les moyens de le faire. La décision de "faire confiance" nécessite l'estimation de la bonne ou de la mauvaise volonté des autres envers nous. Dans la même discipline, Gambetta [4] a défini la confiance comme suit : *trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action.* La définition de Gambetta fournit plusieurs aspects liés à la confiance. Tout d'abord, cette définition souligne la nature subjective de la confiance. Ensuite, il insiste sur la dépendance du trustor à l'égard d'une action donnée que le trustee doit effectuer. La dépendance ainsi définie s'apparente à la notion de vulnérabilité évoquée par Baier. Il considère également l'incertitude (ou l'ignorance) en spécifiant que la confiance est accordée préalablement à

l'exécution, à l'observation et au résultat attendu d'une action. De plus, Gambetta estime que la confiance est contextuelle. Enfin, Gambetta considère la confiance comme une notion quantifiable.

D'un point de vue psychologique, le travail de Deutsch [3] a abouti à la définition suivante de confiance :

- *If an individual is confronted with an ambiguous path, a path that can lead to an event perceived to be beneficial (Va+) or to an event perceived to be harmful (Va-) ;*
- *He perceives that the occurrence of Va+ or Va- is contingent on the behaviour of another person ; and*
- *He perceives the strength of Va- to be greater than the strength of Va+.*
- *If he chooses to take an ambiguous path with such properties, I shall say he makes a trusting choice ; if he chooses not to take the path, he makes a distrustful choice.*

Deutsch a expliqué cette définition en donnant un exemple d'un couple voulant embaucher une baby-sitter. Selon les attentes du couple vis-à-vis de la garde des enfants, et de l'idée qu'ils se font de la capacité de la baby-sitter, ils décideront de lui faire ou non confiance pour la garde des enfants. Ainsi, le couple estime que le mal (Va-) qui pourrait être fait à leurs enfants est beaucoup plus coûteux que de passer une soirée ailleurs, considéré comme un plus (Va+). Ainsi, cette définition introduit la notion d'utilité pour la prise d'une décision de confiance. L'une des exigences principales pour la confiance est alors la présence éventuelle des résultats négatifs et positifs. Selon Deutsch, la conséquence d'un résultat négatif est nécessairement perçue comme plus importante que le gain procuré par un résultat positif. Ainsi, pour Deutsch, une prise de décision qui à la base se veut de confiance devient un choix irrationnel, car si l'inverse est vrai (Va+ $>$ Va-), le choix serait juste une rationalité garantie sans aucun risque à prendre par le décideur. Cependant, il y a désaccord quant à l'idée que les impacts des résultats positifs devraient être inférieurs aux résultats négatifs pour que la confiance soit établie [12].

Dans le même sens que Deutsch, McKnight et Chervany [13], ont défini la confiance comme suit : *the extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible*.

D'après cette définition, la raison qui pousse le trustor à établir la confiance envers quelqu'un ou quelque chose (le trustee) est le sentiment relatif de sécurité. Tout comme Deutsch, cette définition suggère l'existence d'impacts positifs et négatifs. Le risque comme le contexte et la dépendance sont également présents lorsque le trustor prend une décision. Josang et al. [7] ont modifié légèrement cette définition en considérant que le trustee n'est pas forcément un être humain mais qu'il pourrait être un objet.

D'un point de vue social, Luhmann et Barber [10] [2] ont essayé de donner une définition de la confiance : elle dépend des relations humaines au sein des réseaux sociaux. Ils se démarquent ainsi des approches de Deutsch et Gambetta qui considèrent que la confiance est établie à partir des évaluations individuelles. Pour prendre une décision de confiance, toute personne a besoin de s'appuyer soit sur des informations clairement explicitées, soit sur des indices (en anglais *evidences*). Ces dernières apportent un regard critique sur les individus et le milieu dans lequel ils évoluent. Les différences de situation peuvent conduire à une complexité plus ou moins grande, car le nombre d'informations (explicites ou implicites) peut être si important qu'il semble difficile, voire impossible, de toutes les considérer. Dans ce type d'environnement, la confiance est recherchée en tant que moyen pour réduire la complexité. Elle laisse une place à l'incertitude qui vient essentiellement de la complexité de la situation rencontrée.

Nous pouvons ajouter que le processus d'analyse de l'information est polymorphe. Au cours d'une première expérience, si l'on se sent hésitant ou démuni et donc dans l'incapacité de prendre une décision, un appel peut être fait à autrui, pour tenter de recueillir des recommandations sur l'entité inconnue. En d'autres termes, l'individu cherche à prendre connaissance de la réputation de l'entité inconnue en se basant sur les recommandations des autres. La réputation est définie dans le dictionnaire de l'académie française comme suit :

RÉPUTATION. n. f. Renom ; estime, opinion que le public a d'une personne.

Dans d'autres situations, lorsque l'entité sur laquelle doit porter une décision a déjà donné lieu à une première expérience, la décision de confiance est impactée à la fois par le résultat de l'expérience personnelle passée et de l'expérience communiquée par les autres. La confiance est donc un concept multidimensionnel : elle peut être basée sur la connaissance, l'expérience, l'émotion, et la perception du trustor. Elle peut être également basée sur des recommandations envoyées par d'autres entités. Ou encore, la confiance peut être déduite par les trustors grâce aux rôles sociaux joués par les trustees dans leurs communautés.

Quelque soit l'environnement où la confiance devrait être appliquée, l'existence du risque, de l'utilité, de l'incertitude et de la dépendance/vulnérabilité est importante pour que la confiance soit pertinente dans cet environnement. En d'autres termes, l'ensemble de ces éléments constitue les conditions de confiance dans un environnement donné.

Néanmoins, les définitions données restent génériques et donc applicables à plusieurs domaines. Elles peuvent implicitement inclure de nombreux aspects. Il y a donc nécessité de spécifier des définitions qui détaillent explicitement tous les aspects importants de la confiance dans un domaine donné. Dans ce travail, nous raffinons ces définitions pour proposer une définition appropriée de la confiance des EDs dans les ACs.

III. La confiance dans les autorités de certifications

La confiance envers les autorités de certifications dans *le modèle ouvert* est une notion ambiguë, et considérée souvent comme un concept ad hoc par les fournisseurs de services des ICPs. Il est nécessaire donc de déterminer la sémantique exacte de la confiance envers le tiers de confiance fournissant les services des ICPs.

Généralement, ces services sont interfacés par les autorités de certifications (ACs). Une ICP peut avoir une ou plusieurs ACs où chaque AC est responsable de la gestion d'un type de certificat. Pour cela, nous utilisons le terme AC pour indiquer

l'ensemble des services mis à la disposition de l'AC par une ICP.

Pour qu'une ED puisse faire confiance dans une AC, cela implique que l'ED a la capacité de répondre à ces types de questions : que se passe-t-il lorsqu'une AC ne vérifie pas correctement l'identité du propriétaire, ou pire, lorsqu'elle délivre délibérément un certificat à une personne ayant une fausse identité ? En outre, que se passe-t-il si une clé privée correspondant à la clé publique est divulguée par accident, suite à un vol d'information (spyware) ou pire, de manière intentionnelle ? [8].

De tels événements pourraient conduire les vérificateurs des certificats (systèmes et/ou utilisateurs) à faire des hypothèses totalement fausses sur les identités des entités dans les environnements numériques. En conséquence, la confiance dans une ICP (ou dans une AC) doit symboliser son niveau de performance juridique et technique dans la gestion des clés et des certificats numériques.

La confiance doit donc être établie en termes de sécurité et de fiabilité des ACs. Cela nécessite bien évidement une identification de la nature des entités impliquées dans les ACs afin de pouvoir établir la sémantique exacte de la sécurité et la fiabilité dans les ACs. Nous adoptons la définition de McKnight et al. énoncée dans la section précédente.

Bien que cette définition soit relativement générale, elle inclut explicitement et implicitement les ingrédients de base de la confiance qui sont 1) la dépendance des personnes ou des systèmes ayant joué le rôle du trustee, 2) la fiabilité et la sécurité du trustee, et 3) le risque encouru au cas où le trustee ne réalise pas les tâches comme prévu.

Mais la sémantique des motifs de la confiance présentés dans cette définition (la sécurité et la fiabilité) diffère selon la nature du trustee. En effet, les caractéristiques sur lesquelles nous nous basons pour faire confiance à une technologie sont différentes de celles des êtres humains. Josang [6] a expliqué la différence entre la sécurité et la fiabilité appliquées aux êtres humains ou aux systèmes technologiques dans le domaine de la sécurité de l'information comme suit :

- La sécurité qui se dégage d'un être humain représente la bienveillance de cette personne, tandis que la sécurité d'un système représente sa capacité à résister aux attaques
- La fiabilité d'une personne représente ses qualités comme ses expériences, ses compétences, tandis que la fiabilité d'un système représente sa capacité à réaliser une tâche spécifique, et le fonctionnement continu de ce système

La bienveillance d'une personne signifie qu'elle est honnête car elle tient ses promesses et qu'elle est droite car elle respecte les règles. A contrario, la malveillance signifie qu'une personne est malhonnête car elle ne tient pas ses promesses, et qu'elle est corrompue car elle ne respecte pas les règles.

Évaluer la confiance dans une personne consiste donc à évaluer le degré de bienveillance/malveillance de cette personne. Cependant, nous ne pouvons jamais être absolument certains de la bienveillance (ou la malveillance) de quelqu'un. Ainsi, la confiance ne serait donc qu'une croyance sur la personne.

Il y a une différence importante entre les bases de la confiance dans la vie traditionnelle, et dans Internet. Les êtres humains peuvent être irrationnels, et la confiance en eux peut être aussi irrationnelle. La confiance irrationnelle n'est pas basée sur la connaissance, mais sur d'autres éléments (par exemple les sentiments, la foi...) et peut parfois persister en dépit de la connaissance. Ce type de confiance peut être utile dans certaines situations, mais il peut être risqué dans Internet et surtout dans une technologie ayant pour objectif de prouver l'identité des choses. La confiance dans Internet doit donc être autant que possible basé sur la connaissance [6].

Bien évidemment, il serait intéressant de n'avoir à considérer qu'un nombre limité de facteurs pour déterminer le comportement bienveillant ou malveillant d'un être humain. Malheureusement, il est impossible d'obtenir une connaissance parfaite des êtres humains et de tous les facteurs qui les influencent. Le comportement d'un être humain est donc impossible à prédire avec certitude, même pour soi [6]. En conséquence, ce qui constitue un comportement qualifié de bienveillant (ou malveillant) ne peut jamais être absolu et ne peut être défini que par rapport à un référentiel comme une politique de sécurité, des règles morales, des contrats ou une législation.

Contrairement aux êtres humains, les connaissances sur les systèmes peuvent atteindre en théorie un degré élevé d'exactitude et d'exhaustivité. Toutefois, un utilisateur d'un système ne peut jamais obtenir une connaissance parfaite du système qu'il utilise, ni des menaces, et il est donc incapable d'évaluer exactement la sécurité et la fiabilité du système. L'incertitude existe toujours et vient donc de la complexité de l'évaluation des systèmes [6].

Nous retrouvons ici les mêmes problématiques traitées dans les ACs. En effet, une AC est un ensemble constitué de procédures humaines (pour les vérifications et les validations), de systèmes (ordinateurs, équipements cryptographiques, etc.), de logiciels et de lieux physiques en vue de gérer le cycle de vie des certificats des clés cryptographiques. La confiance dans une AC est établie à partir des critères de sécurité et de fiabilité associés à la fois aux êtres humains et aux entités non-humaines impliquées dans la gestion d'un certificat (systèmes, locaux, logicielle...).

En se basant sur la définition de McKnight de la confiance, nous pouvons définir la confiance dans une AC comme étant la dépendance sur la sécurité et la fiabilité qui se dégagent des personnes ainsi que celles des systèmes, des environnements physiques où ils se situent, et des logiciels utilisés par l'AC tout en acceptant un niveau minimum de risque.

Dans cette définition, nous entendons par personnes, aussi bien les personnes physiques travaillant pour le compte des ACs, que les personnes morales (fournisseurs d'ICPs). La sécurité, venant des fournisseurs et des personnels, caractérise leurs engagements vis-à-vis des politiques de sécurité et des législations en vigueur, tandis que la fiabilité représente la compétence et l'expérience des fournisseurs et des personnels dans le domaine des ICPs.

La sécurité des systèmes et des logiciels représente la capacité de ces entités à résister aux attaques, tandis que leur fiabilité signifie qu'ils sont capables d'exécuter infailliblement

FIGURE 2. les différences entre les modèles ouvert et fermé

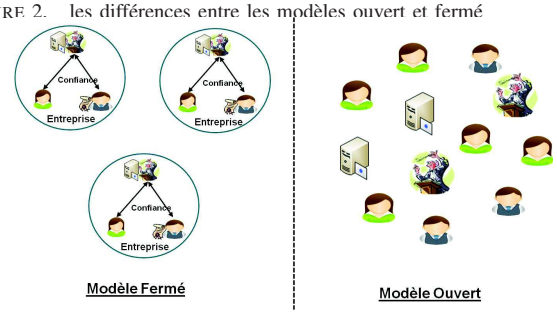
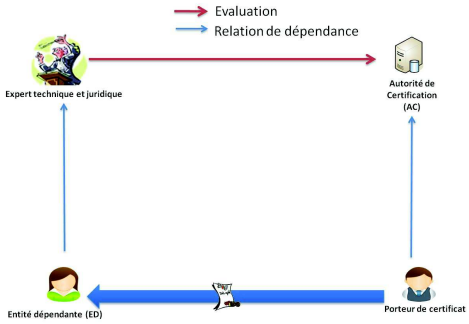


FIGURE 3. le nouveau modèle de confiance



les tâches qui leur sont confiées (fonctionnement continu et sans erreurs).

Nous élargissons les interprétations de Josang sur la fiabilité et la sécurité pour qu'elles couvrent les environnements physiques. La sécurité, à ce niveau couvre à la fois les risques naturels qui pourraient nuire au fonctionnement des ICPs et les attaques humaines qu'elles soient directes ou indirectes, internes ou externes. Ainsi, nous pouvons maintenant donner une définition plus détaillée : *la confiance dans une AC se caractérise par : la dépendance d'une ED quant aux compétences des personnes, des systèmes, des lieux physiques, et des logiciels de l'AC, ainsi que la bienveillance du fournisseur de l'ICP à fournir précieusement et infailliblement les services de sécurité nécessaires tout en respectant les législations concernées, l'ED acceptant un niveau minimum de risque associé à la décision de dépendance*.

La bienveillance des fournisseurs est mesurée par rapport à la politique de certification mise en place et aux législations concernées du pays d'implantation. Elle se caractérise aussi par la conformité de ses engagements (promesse de confiance).

IV. REVISITER LE MODÈLE DE CONFIANCE DE BASE DU STANDARD X.509

Au regard de la définition donnée précédemment, il apparaît clairement que l'ED ne peut être le commun des mortels car de nombreux éléments techniques et juridiques sont à évaluer. Nous proposons donc de modifier le modèle de confiance de base, défini par le standard X.509, en introduisant ce rôle de l'expert technique et juridique qui est nécessaire.

Ce rôle existe déjà dans les deux modèles de déploiement des ICPs, sans qu'il soit explicitement défini (Figure 2). En effet, dans le modèle fermé des ICPs, les administrateurs des ICPs et les avocats de chaque organisation jouent le rôle d'experts techniques et juridiques pour aider les employés de l'organisation dans le traitement des certificats provenant d'autres organisations. Les EDs et les experts, faisant partie de la même organisation, ont une relation de confiance naturelle. La confiance des EDs dans leurs administrateurs n'est pas seulement liée à la qualité des certificats qu'ils fournissent mais aussi aux recommandations d'accepter ou pas un certificat signé par une autorité d'une autre organisation.

Dans le modèle ouvert, la situation est beaucoup plus complexe que le modèle fermé pour plusieurs raisons. Il n'existe pas de relation explicite prédéfinie entre les EDs et les experts. Les navigateurs Web jouent implicitement le rôle d'expert car ils gèrent la liste des autorités de certification dits de confiance, mais il n'existe aucun accord entre les EDs et les fabricants des navigateurs afin de les rendre responsables de l'information qu'ils fournissent. Toutes ces solutions ad-hoc, que ce soit pour le modèle ouvert (l'approche des navigateurs web) ou pour le modèle fermé, montrent la nécessité d'expliciter le rôle d'expert. Les différences résident dans la nature des entités qui jouent le rôle d'expert, le type de confiance reliant l'expert aux EDs et la nature des informations que les experts doivent leurs fournir.

Nous proposons de clarifier la situation en ajoutant explicitement le rôle d'expert dans le modèle X.509 de confiance (Figure 3). Les EDs dépendent uniquement de l'expert et non pas de toutes les ACs choisies par leurs partenaires (c'est-à-dire les porteurs de certificat). Dans ce cas, le modèle de confiance est plus équitable pour les EDs car elles sont protégées par des experts techniques et juridiques, exactement comme c'est le cas pour les porteurs de certificat qui sont protégés par les ACs.

La relation entre l'expert et les EDs doit être régulée par des contrats explicites. La définition de la confiance du point de vue de l'ED dans l'expert n'est pas nécessaire car leur relation est définie par les contrats (exactement comme c'est le cas entre le porteur de certificat et l'AC). Dans ces contrats, l'expert reconnaît sa responsabilité sur les recommandations fournies aux EDs et s'engage à respecter et à protéger la vie privée des EDs. D'un autre côté, l'expert doit être indépendant des ACs, sa relation avec les ACs doit également être régulée par des accords explicites, de sorte que l'expert puisse transférer la responsabilité à une AC lorsqu'une fausse recommandation résulte d'une information erronée fournie par une AC.

Il existe plusieurs types de documents qui permettent d'évaluer la confiance dans une AC :

- La politique de certification (PC) : ce document définit le domaine d'application d'un certificat et les exigences de sécurité à réaliser par Une AC.
- La déclaration des pratiques de certification (DPC) : ce document définit la façon dont l'AC a implémenté les exigences de sécurité.
- Le rapport d'audit : comme les documents PC/DPC sont déclaratifs, l'expert a l'obligation de lire le rapport fourni par un auditeur afin de pouvoir vérifier la véracité des déclarations fournies dans les documents PC/DPC

Ces documents sont exprimés aujourd'hui en langage naturel. Il est donc difficile pour un expert d'évaluer manuellement

chaque autorité de certification. Pour cela, nous avons proposé un processus semi-automatique qui permet à l'expert d'évaluer objectivement les ACs [14]. Ce processus présente trois types d'information :

1) La qualité de certificat (QoCER) : Un score entre 0 et 1 représentant le niveau de confiance qui peut être placé dans le certificat ;
2) La qualité de contrôle (QoCTRL) : un score comprise entre 0 et 1 qui indique le niveau de fiabilité du calcul de QoCER envoyé aux EDs ;
3) Informations complémentaires : des informations complémentaires vont être proposées aux EDs selon le contexte de l'utilisation des certificats.

Le QoCER dépend de deux valeurs : la qualité de CPS (QoCPS) qui indique la qualité des procédures annoncées par les ACs dans les documents PC/DPC, et la qualité de l'AC (QoCA) qui indique le niveau de l'engagement réel de l'AC par rapport à ce qu'elle a annoncé dans les documents PC/DPC. Le modèle de calcul est présenté en détail dans [14].

Le contexte de l'utilisation des certificats électroniques est aussi un élément important à considérer, car les informations complémentaires à proposer aux EDs changent selon ce contexte. Par exemple, les recommandations sur un certificat qui authentifie un serveur de messagerie doivent être différentes de celles d'un certificat utilisé pour authentifier un serveur de payement. En effet, les informations envoyées par les EDs à ces serveurs (respectivement le couple login/passwd et les informations de carte bancaire) et les conséquences de ces transactions sont différentes. Dans le premier cas, les informations critiques sont le niveau de qualité du certificat et le niveau de la protection financière et juridique. Dans le deuxième cas, ces informations devraient être complétées par le montant maximal de la transaction financière effectuée par l'ED pour qu'elle puisse rester couverte par la protection financière offerte par une AC.

V. Conclusion

Le modèle de confiance à trois entités défini par le standard X.509 correspond à une époque où Internet était une communauté fermée et réservée à des échanges entre chercheurs et académiciens. L'ouverture de Internet a changé complètement la donne. Les EDs n'ont aucune relation directe avec aucune AC et la notion de confiance entre les EDs et les ACs est devenue floue. Nous avons donc proposé une définition de confiance basée sur la sécurité et la fiabilité des services fournis par les ICPs. L'évaluation de cette définition nécessite des expertises techniques et juridiques, d'où l'importance de modifier le modèle de confiance à trois entités. Nous avons contacté le comité du standard X.509 pour intégrer le rôle d'expert dans le modèle de confiance X.509. A leur demande, nous avons présenté cette proposition au comité X.509, qui a eu lieu le 17 Avril 2013 à Genève. Notre proposition a été acceptée et le premier draft officiel du standard X.509 version 8 vient d'être publié [15].

Références

[1] Annette Baier. Trust and antitrust. *Ethics*, 96(2) :231–260, 1986.

[2] Bernard Barber. *Logic and Limits of Trust*. Rutgers University Press, 1983.

[3] Morton Deutsch. Cooperation and trust : Some theoretical notes. *Nebraska Symposium on Motivation*, pages 275–319, 1962.

[4] Diego Gambetta. Can we trust trust ? In *Trust : Making and Breaking Cooperative Relations*, pages 213–237. Basil Blackwell, 1988.

[5] Schuller Guy. La confiance : un facteur indispensable, mais complexe, 2004.

[6] Audun Jøsang. The right type of trust for distributed systems. In *Proceedings of the 1996 workshop on New security paradigms*, NSPW 96, pages 119–131. ACM, 1996.

[7] Audun Jøsang, Elizabeth Gray, and Michael Kinateder. Simplification and analysis of transitive trust networks. *Web Intelligence and Agent Systems*, 4 :2006, 2006.

[8] Audun Jøsang, Ingar Glenn Pedersen, and Dean Povey. Pki seeks a trusting relationship, 2000.

[9] Bibaut Laurent. Le trust est-il un contrat ? http://www.lepetitjuriste.fr/droit-international/droit-international-prive/le-trust-est-il-un-contrat. [Online ; testé le 05-04-2013].

[10] Niklas Luhmann. *Trust and Power*. John Wiley and Sons Inc, 1982.

[11] Niklas Luhmann. Familiarity confidence trust : Problems and alternatives, 2000.

[12] Stephen Paul Marsh. Formalising trust as a computational concept, 1994.

[13] Harrison Mcknight and Norman Chervany. The meanings of trust. Technical report, 1996.

[14] Ahmad Samer Wazan, Romain Laborde, Francois Barrere, and Abdel-Malek Benzekri. A formal model of trust for calculating the quality of x.509 certificate. *Security and Communication Networks*, 4(6) :651–665, 2011.

[15] http://x500standard.com/index.php?n=Ig.X509ext