



IALTA

***La qualité professionnelle
dans la signature électronique***

**Conclusions du Groupe de Travail
sur la Gestion des Attributs (GT-GA)**

Février 2004

Version 1.10

Membres du groupe de travail ayant participé à la rédaction de ce document :

	(adresse email)
Claire Albouy (CNAM-TS)	claire.albouy@cnamts.fr
Gérard Brayer (Crédit Lyonnais)	gerard.brayer@creditlyonnais.fr
Michel Chevrier (Ialta)	mp.chevrier@wanadoo.fr
Nathanaël Cottin (U. Techno. Belfort)	nathanael.cottin@utbm.fr
Paul Frausto (Ecole des Mines d'Alès)	paul.frausto@ema.fr
Yves Gailly (BNP)	yves.gailly@bnpparibas.com
Jordane Hurier (Thalès Communication)	Jordane.hurier@fr.thalesgroup.com
Isabelle Petit-Peucelle (Advance Techno.)	ipp@advanceinknowledge.com
Thierry Piette-Coudol (avocat)	piettecoudol@wanadoo.fr
Frédérique Tastet (Thalès Communication)	frederique.tastet@fr.thalesgroup.com

Les membres du GT tiennent tout particulièrement à remercier de leurs contributions les personnes et entreprises suivantes : Nadia Antonin (Banque de France), Bruno Couderc (BJC consultant), François Coutillard (Teamlog), Gérard Faure (Ordre des vétérinaires), Yvan Lauzon (Conseil du Trésor - Gouvernement du Québec), Emmanuel Layot (Compagnie Nationale des Commissaires aux Comptes), Martin Lethielleux (Chambre de Commerce de Paris), Jean-Louis Matthieu (ordre des Experts-Comptables), Réza Meralli, Jean-Claude Monnier (MSG Software), Etienne Pelletier (Ialta), Yannick Quenec'hdu (Cartel Sécurité), Vincent Roustan (Omnikles), Herve Schauer (HSC consultant), Ahmed Serhrouchni (Ecole Supérieure des Télécoms)

Sous la direction de Thierry Piette-Coudol, avocat, Cabinet d'avocats Bertrand & associés, Président de l'association IALTA.

Un Comité de Suivi procédera à une mise à jour du document. Toute observation, contribution ou critique peut lui être communiquée à l'adresse suivante :

ialta@ialtafrance.org

Reproduction du document autorisée, moyennant la citation de l'intitulé exact du document "Guide de l'attribut professionnel dans la signature électronique" et de l'auteur, l'association IALTA, en mentions claires, apparentes et parfaitement lisibles, et son affectation à une utilisation personnelle ou strictement non commerciale, quel que soit le support. Cependant, toute reproduction sur un support tel que CD / DVD, disquette ou tout autre média permettant une diffusion de masse, y compris mais sans limitation une diffusion sonorisée, visualisée, etc., doit être autorisée préalablement par écrit par l'auteur. La demande d'autorisation doit être envoyée à l'adresse électronique suivante : ialta@ialtafrance.org.

Table des matières

1 Introduction	5
2 Les besoins applicatifs professionnels	6
21 Les entreprises et les administrations, partenaires dans les téléprocédures	6
211 Les notions voisines en cause : habilitation, délégation et mandat	6
212 Les mandataires de téléprocédures	8
2121 Les entreprises et leurs mandataires en contexte électronique	8
2122 Le mandat face à l'obligation déclarative	9
2123 La théorie du mandat apparent	9
2124 Les impératifs d'organisation et de sécurité de certaines entreprises	10
22 Les besoins des professions réglementées	11
221 Notion de signature professionnelle	11
222 Notion de profession réglementée	12
223 L'appartenance à une profession réglementée	12
2231 Les positions professionnelles de la carrière	12
2232 Le tableau professionnel	13
3 Les solutions actuelles entre certificat d'identité et annuaire électronique	15
31 La gestion par le certificat d'identité	15
311 Le statut juridique du certificat électronique et de l'attribut professionnel	15
312 L'exemple du dépôt électronique de brevets	16
313 L'exemple de la Carte de Professionnel de Santé	17
32 La gestion par une hiérarchie d'autorisations : l'exemple de Copernic	18
33 La gestion par annuaire électronique	19
331 La notion d'annuaire électronique	19
332 Critique de l'intérêt des annuaires au sein des ICP	20
3321 Apports des annuaires pour les ICP	20
3322 Annuaire et gestion des habilitations	21
4 les certificats d'attributs, Une solution d'avenir ?	22
41 L'antériorité des habilitations de sécurité	22
42 Du certificat d'identification au certificat d'attribut	23
421 Les certificats d'attributs et l'IETF	23
422 Les groupes PKIX et SPKI de l'IETF	23
423 Le groupe SDSI du MIT	24
424 Unification de SPKI et SDSI dans l'IETF	24
43 Approche des certificats d'attributs	24
431 La gestion par les certificats d'attributs à proprement parler	24
432 L'habilitation/ délégation	25
433 La certification de rôles	26
434 Multisignature électronique contrôlée	27
44 La gestion de l'infrastructure	27
441 L'infrastructure de gestion des certificats d'attribut	27
4412 Les composantes de l'IGP	28
442 Principes de la gestion des attributs / des certificats	29
4421 Gestion au sein des entreprises	29
4422 Gestion extérieure	29
443 Intérêt et limites du certificat d'attribut	30
Conclusion	32
Annexe technique : Les formats des certificats d'attributs	34
Glossaire	37

ABRÉVIATIONS

Liste des abréviations utilisées dans ce rapport. A chacune d'elle est associé entre parenthèses le terme anglais correspondant.

- AA : (Attribute Authority) – Autorité d'Attribut.
ACRL : (Attribute Certificate Revocation List) – Liste de révocation de certificat d'attribut.
API : (Application Programming Interface) - Interface de programmation applicative.
ASN. 1: (Abstract Syntax Notation One) - Notation de syntaxe abstraite numéro 1; Standard ISO/ IEC des règles de codage.
CA : (Certification Authority) - Autorité de certification.
CPS : (Certification Practices Statement) - Pratique de déclaration de certificat.
CRL : (Certificates Revocation List) - Liste de révocation de certificat.
DN : (Distinguished Name) - Nom distinctif de la norme X.500.
DTD : (Document Type Definition) – Définition du type de document.
IETF : (The Internet Engineering Task Force) - Groupe de normalisation de l'Internet.
ISO : (International Organization for Standardization) - Organisation de standardisation internationale.
ITU-T : (International Telecommunication Union - Telecommunication) - Union internationale pour les télécommunications.
KEYNOTE : Proposition de PKI utilisant notamment les Certificats d'attribut.
LDAP (Lightweight Directory Access Protocol) - Protocole léger d'accès à un répertoire.
PKCS : (Public Key Crypto Standards) - Standards de crypto à clé publique.
PKI : (Public Key Infrastructure) - Infrastructure à Clé Publique.
PKIX : (Public Key Infrastructure X.509) - Infrastructure à Clé Publique basé sur le certificat X.509.
PMI : (Privileges Management Infrastructure) - Infrastructure d'administration de privilèges (pour les certificats d'attribut)
RA : (Registration Authority) - Autorité d'enregistrement.
RFC : (Request for Comment) -Demande de Commentaire
SPKI : (Simple Public Key Infrastructure) - Infrastructure à Clé Publique Simple.
SSL : (Secure Socket Layer) - Couche socket sécurisée (Protocole de sécurité)
UTC : (Universal Coordinated Time) - Coordonnées horaires universelles définissant le temps selon les standards mondiaux (World Time Standard)
W3C : (World Wide Web Consortium) - consortium du WWW.
X.500 : Norme de noms proposée par l'ITU-T, ISO (annuaires).
X.509 : Norme du certificat numérique proposée par l'ITU-T, ISO.
XML : (Extensible Markup Language) - Langage de description de pages Web.

1 INTRODUCTION

Les travaux des Groupes de Travail de l'association IALTA portent sur la sécurisation des échanges électroniques, particulièrement sur la signature électronique et tous ses composants comme les certificats électroniques :

- Les travaux du GT Archivage ont défini une utilisation des certificats X.509 et des signatures pour sécuriser les échanges électroniques entre l'utilisateur et le tiers archiveur distant,
- Les conclusions du GT Horodatage ont montré l'intérêt d'un nouveau type de certificat pour certifier le temps dit "jeton temporel".

Dans le cadre d'une application professionnelle de la signature, le certificat électronique X.509, certifie la clé publique du signataire et contient naturellement le nom de celui-ci. L'identification du signataire s'arrête généralement à son nom de sorte qu'il manque un élément technique garantissant sa qualité professionnelle ou sa fonction dans l'entreprise.

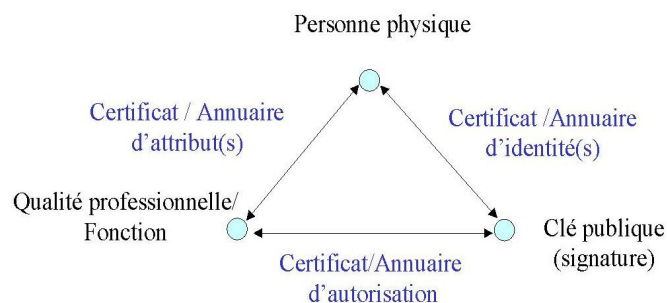
Cette précision est importante. Comme exemples, nous pouvons citer :

- les membres des professions réglementées (experts comptables, commissaires aux comptes, notaires, avocats, médecins ou architectes, etc.) qui signent les documents es qualité, qualité de professionnel en exercice contrôlée généralement par leur Ordre
- les téléprocédures avec l'administration qui doivent être signées par une personne habilitée à le faire, surtout si cette personne n'est pas membre de l'entreprise (le cas des experts-comptables).

Il existe toutefois un inconvénient à faire figurer cette qualité dans le certificat : le sort du certificat suit le sort de la qualité du détenteur.

Le présent document expose les besoins en matière de contrôle de la "qualité professionnelle" du signataire. Le système de gestion des attributs doit garantir la disponibilité, la cohérence et la validité de cette information. Les trois solutions techniques existantes, les certificats d'identité, l'annuaire électronique et les certificats d'attribut, font l'objet d'une étude critique dans ce document.

Le schéma ci-dessous présente les différents moyens de lier la clé publique utilisée pour signer à une qualité professionnelle ou fonction :



2 LES BESOINS APPLICATIFS PROFESSIONNELS

La signature électronique reste la signature d'une personne privée. Cependant dans le cadre de sa profession, la personne privée signe en qualité de membre de sa structure professionnelle (commerciale, administrative ou autre). Les deux exemples donnés ci-dessous ne sont pas exhaustifs, ils illustrent deux catégories de besoin bien ciblé de signature professionnelle :

- les téléprocédures que l'entreprise adresse à l'administration doivent être signées par un membre de l'entreprise spécialement habilité,
- les membres des professions réglementées (notaires, experts-comptables, médecins...) ne signent qu'en qualité.

21 Les entreprises et les administrations, partenaires dans les téléprocédures

Les téléprocédures qui se substituent aux déclarations administratives sur papier ne peuvent être effectuées que par un mandataire de l'entreprise. Dans le contexte de l'utilisation de moyens d'échanges électroniques, cette notion demande à être différenciée d'autres notions proches.

211 Les notions voisines en cause : habilitation, délégation et mandat

Le droit de l'entreprise prévoit que les *mandataires sociaux* s'expriment au nom et pour l'entreprise. Faute de pouvoir remplir cette vaste mission, les mandataires sociaux se reposent sur leurs employés dans le cadre de relations relevant de l'habilitation, de la délégation ou du mandat.

Ces concepts sont voisins :

- L'habilitation permet de rendre quelqu'un juridiquement capable d'exercer certains pouvoirs. Le concept est proche de celui d'autorisation.
- La délégation est sensiblement plus large puisque le délégué est susceptible de déléguer lui-même sa capacité à quelqu'un d'autre. Aussi la délégation est-elle généralement qualifiée : délégation de vote, délégation de pouvoirs et surtout pour ce qui concerne ce groupe de travail, *délégation de compétence* à distinguer de la *délégation de signature* (le délégant habilite le délégué à exercer concurremment son pouvoir de signature).
- Le mandat est selon l'article 1984 et suivants du Code civil un acte par lequel une personne est chargée d'en représenter une autre pour l'accomplissement d'un ou plusieurs actes juridiques. Le mandat peut résulter de la loi ou d'un jugement, ou encore être conventionnel et prendre la forme d'un contrat. Les professions réglementées bénéficient souvent d'un mandat vis-à-vis de leurs clients : les experts-comptables demandent à chacun de leurs clients un mandat spécifique (lettre de mission), alors que les avocats bénéficient d'un mandat légal et général octroyé par le Code de procédure pénale

Le *Groupement d'Intérêt Public Modernisation des Déclarations Sociales* (GIP-MDS) qui s'attache au développement des téléprocédures dans la sphère sociale s'est préoccupé de la qualité du déclarant dans l'entreprise. Dans des travaux réalisés en 2000¹, le GIP établit le parallèle entre "les délégations de pouvoirs en droit des sociétés" et "les délégations de compétences en droit administratif" et les délégations, dans le cadre de l'utilisation de

¹ Le GIP-MDS a réalisé une étude sur les certificats d'attributs en octobre 2000. Sachant que ce travail reposait sur des études préliminaires de l'IETF qui préparait le futur rfc3280. Le travail a abouti à une page présentant de manière succincte les certificats d'attributs : http://www.gip-mds.fr/groupe/f_set.htm

certificats d'identité et de certificats d'attributs. Du résultat des travaux disponibles sur le Web, on peut tirer les conclusions suivantes quant à la typologie des délégations :

Tableau récapitulatif des délégations

	Délégation de pouvoir (droit des sociétés)	Délégation de compétences (droit Administratif)	Délégation de signature	
			Droit des sociétés	Droit Administratif
Définition	Délégation d'une partie des pouvoirs (délégation de la totalité des pouvoirs interdite)		Délégation du pouvoir de signer en lieu et place de la personne qui l'accorde	
Pouvoirs du déléguant	La délégation ne dessaisit pas le déléguant des pouvoirs	Le délégant est dessaisi de ses pouvoirs	La délégation ne dessaisit pas le déléguant de ses attributions	
Responsabilité du déléguant	Le déléguant conserve la responsabilité des actions des délégués (sauf cas particuliers)			
Origine de la délégation	La délégation engage la société	La délégation doit être publiée	La délégation n'émane pas de la société mais du dirigeant	
Maintien de la délégation	La délégation perdure après le départ du déléguant		La cessation des fonctions du délégué ou du délégant met fin à la délégation	
Subdélégation	Subdélégation de pouvoirs autorisée	Subdélégation de signature autorisée. Subdélégation de pouvoirs interdite	non précisé	Subdélégation interdite

A partir de ces notions de délégation, le GIP MDS évoque le besoin du contrôle par une autorité de certification du droit d'une autorité de déléguer ses pouvoirs ou sa signature. De même, dans le cadre de la révocation d'un certificat d'attribut appartenant à une chaîne de délégation, les possibilités du maintien ou du non-maintien de cette chaîne de délégation sont envisagées.

D'autre part, les documents présentés sur ce site n'expliquent cependant pas le lien entre les certificats de rôle et les certificats d'attributs : il semble que l'appellation «certificat d'attribut » soit la description technique du format standard d'un «certificat de rôle ».

D'après une présentation réalisée par le GIP-MDS dans le GT habilitation le 27 février 2003, les certificats ne sont actuellement pas utilisés pour l'inscription d'un Tiers Déclarant sur le portail Net Entreprise².

² Net Entreprises est un portail spécialisé dans les télédéclarations sociales : <http://www.netentreprise.fr>

212 Les mandataires de téléprocédures

2121 Les entreprises et leurs mandataires en contexte électronique

Les besoins sont partagés entre les administrations et les entreprises³, en particulier, dans les téléprocédures pour les entreprises qui émettent des télédéclarations et les administrations qui les reçoivent. Il serait intéressant de disposer d'une procédure d'habilitation répondant aux besoins du plus grand nombre d'entreprises et qui pourrait, si cela était nécessaire, être affinée par personne et par composant du secteur fonctionnel. En effet, 80 % des entreprises ont des besoins simples qui peuvent être standardisés.

Les administrations pourraient souhaiter pouvoir utiliser un certificat rattaché seulement à une personne et non au binôme personne/entreprise. Si un certificat identifie un individu, certificat qu'il conservera durant toute sa carrière professionnelle, il faut un dispositif qui permette de rattacher la personne à une entreprise. Par rapport à une entreprise, une ou plusieurs personnes sont mandataires sociaux, c'est à dire qu'elles ont la capacité de représenter l'entreprise vis à vis des tiers. Le mandataire social peut déléguer à une autre personne la capacité de le remplacer pour accomplir certains actes. La problématique de la délégation est double :

- Rattacher le mandataire social à une entité juridique (pour une société les justificatifs peuvent être les statuts ou un compte rendu d'assemblée générale)
- Gérer la liaison mandataire social / délégué / droits sur lesquels porte la délégation

Pour assurer l'identification des déclarants, l'administration se repose sur un certificat électronique (seul ou en support d'une signature électronique). Dans ce cas, le certificat n'a qu'une fonction, celle d'identifier une personne⁴, et non de définir les droits. Le certificat doit-il être enrichi d'autres informations ? Le certificat ne contiendrait plus l'information entreprise, l'objectif étant de gérer cette information au niveau applicatif par une gestion de droits. De manière générale, l'administration ne valide pas les certificats au fil de l'eau et ne contrôle la validité du certificat que sur exception. La gestion au niveau applicatif des liens entre porteurs de certificats et entreprises pourrait rendre moins cruciale la gestion des certificats périmés. Il paraît important d'étudier plus précisément les impacts d'une telle décision avant de se prononcer. Les certificats d'attributs constituent une piste technique intéressante qui pourrait être utilisée pour donner d'autres informations. A ce stade de la réflexion, il s'agit avant tout de définir les besoins fonctionnels de chacun des acteurs.

³ Un groupe de travail (GT) spécialisé a été créé au sein d'EDIFRANCE à l'été 2002 sur la notion d'habilitation. Parmi les membres du GT, on peut citer au titre des personnes morales participantes : GIP-MDS, DGI, MINEFI (COPERNIC), Banques : BNP-Paribas, Banques Populaires, Crédit Lyonnais, BFBP, CS-OEC (Conseil Supérieur de l'Ordre des Experts-Comptables). L'objectif général de ce GT est de définir les obligations des parties sur les droits et habilitations de faire des opérations sous forme électronique (en particulier, de signer) tant au niveau déclaratif qu'au niveau des paiements. Cependant les raisons qui ont été à l'origine de la création de ce nouveau groupe de travail reposent dans les besoins des utilisateurs à partir des retours d'expérience sur la TVA. Ainsi les entreprises ont-elles des besoins spécifiques de gestion des droits face aux administrations et face aux banques. Ces besoins sont généralement les suivants : gestion d'identification des intervenants, capacité des intervenants à faire telle ou telle opération, gestion des éléments de preuve (archivage des signatures et des données, horodatage...)

⁴ En notant au passage que la signature de personne morale n'existe pas dans le droit français. La signature est celle d'une personne travaillant dans /pour l'entreprise. Le certificat correspondant est celui d'une personne et non un certificat d'entreprise, même si cette dernière paye le certificat de la personne.

2122 Le mandat face à l'obligation déclarative

La déclaration est une obligation qui pèse sur une entreprise. L'entreprise étant une personne morale, elle doit se faire représenter par une personne physique pour l'accomplissement de la formalité. Toute personne "parlant" pour l'entreprise peut effectuer la formalité pour l'entreprise. La formalité n'est pas accomplie au bénéfice de la personne déclarante, mais de l'entreprise. La personne qui "parle" au nom de l'entreprise le fait dans le cadre d'une relation juridique appelée "mandat", notion définie par le Code Civil. Par contre, ce cadre n'est pas applicable à n'importe qui, car les personnes titulaires d'un mandat jouent généralement un rôle connu dans l'entreprise. Pour l'administration qui reçoit une déclaration, sur support papier ou sous forme électronique, la question se pose de savoir à quel titre le déclarant peut parler pour l'entreprise et quelle est la nature de son mandat. Il est nécessaire d'appliquer les éléments du mandat à une situation de déclaration.

L'entreprise en tant que personne morale existe au regard du droit et peut ester en justice. Comme ses prérogatives ne peuvent être exercées que par une personne physique, la loi crée un "représentant légal". Il n'est pas besoin de chercher plus loin le fondement de son mandat, puisque c'est la Loi. A priori, le dirigeant d'entreprise possède tous les pouvoirs. Mais le dirigeant n'est pas toujours seul à détenir les pouvoirs puisque dans certains cas, comme pour les sociétés, il doit partager son pouvoir avec d'autres organes dirigeants, par exemple Conseil d'administration ou Assemblée Générale. Le principe est la liberté de gestion et d'administration de l'entreprise. Les pouvoirs des organes ne sont pas déterminés par la loi mais par le contrat de société. Tous les pouvoirs concernant les actes d'administration et de disposition concernant l'entreprise sont de la compétence générale des dirigeants.

L'encadrement des pouvoirs du dirigeant est plutôt une question de partage que de limitation des pouvoirs. Tout partage de l'accomplissement des formalités déclaratives entre plusieurs organes de l'entreprise ne créerait que complexité. Quant à la limitation ou à l'interdiction du dirigeant pour l'accomplissement des formalités administratives, elle se ferait aux dépens de l'efficacité de la gestion de l'entreprise. Il n'y a nul motif de limiter le pouvoir du dirigeant de faire des déclarations au nom de l'entreprise, d'autant que la formalité déclarative est obligatoire. Cependant le principe juridique se heurte à la pratique : une gestion de droits bien pensée au niveau sécurité prévoit souvent qu'un dirigeant qui valide une opération ne puisse pas s'en saisir ou procéder à des modifications. Il ne garde pas tous les pouvoirs quelle que soit sa position dans l'entreprise.

2123 La théorie du mandat apparent

Déléguer ses pouvoirs est pour le dirigeant une pratique courante. Si l'interlocuteur de l'entreprise n'est pas en présence du représentant normal, le chef d'entreprise, il peut se demander légitimement à quel titre le représentant de l'entreprise lui parle. Ce représentant a-t-il un mandat ? Cette question est à rapprocher de la règle du Code Civil qui veut que le mandat puisse être vérifié par les tiers. Comme la vérification n'est pas toujours aisée, la loi permet qu'on s'en tienne à l'apparence des choses. C'est pour cela qu'a été créée la *théorie du mandat apparent*. Selon celle-ci, la société peut être engagée par toute personne, même non régulièrement habilitée, si les tiers avec lesquels cette personne a contracté ont légitimement pu croire que celle-ci disposait des pouvoirs nécessaires. Mais pour que la validité du mandat apparent soit reconnue, il faut que les circonstances ou les usages commerciaux, les documents présentés ou les relations entre les parties, autorisent les tiers à ne pas vérifier les limites exactes des pouvoirs du mandataire.

Le mandat apparent n'est pas un élément d'une typologie des risques qui couvrirait l'insécurité juridique lors de la recherche du contenu des pouvoirs des dirigeants. Bien au contraire, c'est une théorie qui vise à renforcer la situation de l'interlocuteur qui devrait vérifier le mandat de celui qui parle, mais qui ne peut pas ou qui n'y a pas accès. L'interlocuteur ou le tiers en l'occurrence, c'est l'administration. Comme tout particulier, l'administration semble dépourvue par rapport à un mandat dont elle ignore l'existence et le contenu. A cela, on rétorquera que, comme tout particulier, l'administration est protégée par la théorie du mandat apparent. On se demande quel serait le risque encouru pour l'administration pour ne pas avoir pu vérifier le mandat ? Qu'une entreprise répudie une déclaration faite en son nom ? De toute façon, l'administration reste maître de déterminer si la formalité déclarative a bien été faite par l'entreprise en question et dans le délai fixé.

Dans le monde de l'écrit-papier, il n'y a généralement pas de contrôle a priori des documents (publicité) qui énonceraient les restrictions de pouvoirs des dirigeants (s'ils existent) ou de les rechercher à travers les documents obligatoires de l'entreprise. On peut s'attendre à ce que le déclarant interne de l'entreprise, à défaut du chef d'entreprise, soit le directeur général, le secrétaire général, le Directeur administratif et financier, le directeur juridique ou le comptable. Même sans publicité de la délégation ou du mandat, même sans vérification de celui-ci, une déclaration effectuée par une de ces personnes dont les rôles sociaux sont bien connus, présente de fortes chances d'être régulière.

Si une déclaration ne provenait pas d'une de ces personnes et que son lien avec l'entreprise était tellement ténu que le mandat apparent ne puisse être retenu, le *système du dirigeant de fait* pourrait trouver à s'appliquer : toute personne physique ou morale qui, sans avoir été régulièrement désignée en qualité de dirigeant, se sera distinguée par une activité positive dans la direction et la gestion de la société, en toute indépendance, pour influencer sur celles-ci de manière déterminante, est susceptible d'engager la société. Mais en l'espèce, toute personne qui sans aucun titre ni mandat (un dirigeant de fait) aurait établi une déclaration, surtout avant la date limite (accompagné d'un paiement !) pour l'entreprise ne se serait-elle pas *distinguée par une activité positive* ?

Au total, la théorie du dirigeant de fait et la théorie du mandat apparent plutôt que de traduire l'insécurité des relations juridiques permettent très concrètement à l'administration d'accepter toute déclaration ou télédéclaration faite pour le compte de l'entreprise sans vérifier outre mesure les qualités, titres et mandat du déclarant. Le danger est plutôt du côté de l'entreprise en cas de fausse déclaration. Et puis au titre de sa compétence discrétionnaire, l'administration peut toujours décider si l'obligation déclarative a été assurée ou non.

Actuellement, les professions libérales (avocats, commissaires aux comptes, experts-comptables, huissiers, notaires, géomètres, etc.) sont chargées de faire un certain nombre de formalités administratives pour le compte de leurs entreprises clientes. Quand la Loi ne leur reconnaît pas un mandat légal, elles recourent au mandat tacite ou exprès pour les accomplir auprès des administrations concernées. Dans ce dernier cas, il s'agit toujours d'un document papier (procuration, mandat, etc.) signé par l'entreprise pour laquelle une formalité ponctuelle ou régulière est accomplie.

2124 Les impératifs d'organisation et de sécurité de certaines entreprises

Sans forcément être en contradiction avec les règles juridiques en vigueur, l'organisation des entreprises peut occuper une place importante dans la problématique des mandataires. En

effet, pour des besoins de séparation de pouvoir (et donc de sécurité) ou de rationalisation des tâches, une entreprise de taille importante est parfois amenée à confier à plusieurs personnes distinctes des parties de tâches pouvant juridiquement et techniquement être accomplies par une personne unique. Chaque personne est alors responsable au sein de son entreprise de la partie du processus dont elle est chargée, et n'est pas autorisée à réaliser les autres parties.

Par exemple, au sein de l'Assurance Maladie, les ordres de virement des prestations aux assurés sociaux sont généralement saisis par une personne ou un système, contrôlés par une autre personne, et validés par une troisième, chacune ayant un rôle bien défini et limité, et n'ayant pas l'autorisation, pour une prestation donnée, de réaliser plus d'une des trois actions. D'un point de vue technique, cela peut se traduire par la création de droits différents, associés à des rôles différents pour chacune des trois personnes, qui ont au départ un métier similaire, dans un même service (comptable). Une telle répartition a pour but d'éviter des erreurs mais aussi des virements abusifs, une coalition de personnes étant alors nécessaire. Le besoin de pouvoir changer ces rôles dans le temps de manière relativement courante (congrés, surcroît de travail d'un des intervenants...) pourrait peut-être être satisfait par l'utilisation d'attributs.

De la même manière, dans le cadre des téléprocédures, le besoin exprimé par certaines grandes entreprises⁵ est «une indépendance entre les modules de déclaration et ceux de paiement (séparation des fonctions comptables et de trésorerie, le trésorier étant l'ordonnateur du paiement). Pour assurer un bon niveau de sécurité, le principe de ne jamais attribuer à une même personne la possibilité de saisir et de valider, quel que soit son niveau hiérarchique, est souvent retenu. »

22 Les besoins des professions réglementées

221 Notion de signature professionnelle

Toute personne physique est conduite fréquemment à valider des actes juridiques et administratifs de toute nature en apposant sa signature sur le document qui lui sert de support. La personne physique qui se livre à une activité professionnelle est également appelée à signer des documents, au titre de sa qualité professionnelle cette fois, de sorte que l'on peut parler de *signature es qualité*⁶. Cette qualité professionnelle est décernée au signataire par une autre personne de la même entité professionnelle, souvent d'un niveau hiérarchique supérieur. C'est à cette dernière que tout processus de contrôle de la qualité professionnelle peut s'adresser aux fins de vérification d'une signature es qualité.

Lorsque le signataire pratique professionnellement dans une entreprise, les dirigeants de cette structure ont compétence pour répondre à toute demande en matière de vérification de la qualité professionnelle d'un signataire ou autrement dit, de son appartenance à l'entreprise. Le schéma est similaire dans le monde administratif. Il en va différemment pour les professions libérales qui peuvent pratiquer indépendamment leur métier. Parmi ces dernières, certaines professions sont réglementées et un organisme central et de régulation surveille la profession. Toute personne pratiquant l'activité en question doit être connue de l'entité de régulation auprès de laquelle l'appartenance peut être contrôlée.

⁵ Réunions du groupe habilitation d'EDIFRANCE du 27 février et du 31 mars 2003

⁶ En dehors de leurs activités professionnelles, les membres des professions réglementées redeviennent de simples particuliers. Ils ont droit alors à une signature électronique comme tous les citoyens du pays. Dans le monde réel, c'est la même signature. Dans le monde électronique, ce sera-t-il deux signatures ou deux certificats ?

222 Notion de profession réglementée

Les professions réglementées sont soumises aux règles du droit public français. Le droit public constate dans la population et l'administration du pays des besoins d'*intérêt général* ou d'*utilité publique*. Il y répond par le *Service Public*. Le service public est un moyen d'affecter des moyens juridiques et économiques, matériels ou humains à la satisfaction d'un besoin d'intérêt général. Différents modes de gestion du service public existent. Parmi ceux-ci, certaines professions répondant à l'intérêt général (ex.: médecins pour la santé, avocats devant les tribunaux) ne sont pas confiées directement à des fonctionnaires de l'Etat. La Loi considère que les professionnels concernés sont maîtres de l'organisation et du fonctionnement de leur profession par l'intermédiaire d'un organisme spécialisé doté de *prérogatives de puissance publique*, l'*Ordre professionnel*.

Dans leur pratique professionnelle, les membres des professions réglementées signent des documents *es qualité* c'est-à-dire que leur signature ne suffit pas. Il faut encore qu'ils aient été en fonction au moment de la signature des documents. C'est à l'intention de ces professions que ce document a été rédigé.

En première analyse, les professions réglementées suivantes ont été recensées :

Professions	Structure
Architectes	Conseil National de l'Ordre des Architectes
Avocats	181 Ordres d'Avocats
Avoués près les CA	Chambre nationale des Avoués auprès des CA
Chirurgiens-dentistes	Conseil National de l'Ordre des Chirurgiens Dentistes
Commissaires aux comptes	Compagnie Nationale des Commissaires aux Comptes
Conseils en PI	Compagnie Nationale des Conseils en Propriété Industrielle
Experts-comptables	Conseil Supérieur de l'Ordre des Experts Comptables
Géomètres-experts	Conseil Supérieur de l'Ordre des Géomètres-experts
Greffiers des TC	Conseil National des Greffiers
Huissiers	Chambre nationale des huissiers de justice
Médecins	Conseil national de l'Ordre des médecins
Notariat	Chambre Nationale de notaires
Pharmaciens	Conseil National de l'Ordre des Pharmaciens
Vétérinaires	Conseil Supérieur de l'Ordre des Vétérinaires

223 L'appartenance à une profession réglementée

2231 Les positions professionnelles de la carrière

L'exercice professionnel par les membres d'une profession réglementée est défini généralement par le texte législatif qui crée la profession et intronise l'Ordre. Comme pour les fonctionnaires, on peut considérer que le membre d'une profession réglementée connaît dans sa vie professionnelle des "positions" qui sont les suivantes :

- L'inscription au tableau : cette étape correspond à l'entrée puis au maintien en exercice d'une personne (quelquefois d'une structure collective) dans la profession. Cette entrée nécessite généralement la possession de certains titres universitaires, le passage par un examen ou un concours professionnel et un stage auprès d'un professionnel installé.

- Le transfert d'inscription : En cas de pluralité d'ordre, si un inscrit transporte son lieu d'exercice dans une autre circonscription régionale, son inscription est transférée, à la diligence de l'intéressé, au tableau de la nouvelle circonscription dont il dépend.
- La cessation provisoire des fonctions / l'omission : Tout membre de l'ordre peut demander à cesser provisoirement d'en faire partie. La demande est adressée à l'organe central ou régional. Selon les cas, elle est motivée ou non, précise la nouvelle activité que l'intéressé désire exercer et peut indiquer la date à laquelle celui-ci entend cesser son activité de membre de l'ordre. L'intéressé peut, quand il le désire, et s'il remplit à ce moment les conditions nécessaires fixées par le statut de l'Ordre, obtenir sa réinscription au tableau suivant la procédure prévue pour l'inscription. La cessation provisoire des fonctions ou l'omission n'est pas une sanction disciplinaire.
- La suspension : Un membre a été sanctionné par la formation disciplinaire de son Ordre et ne peut plus pratiquer sa profession pendant une certaine période de temps.
- La radiation : Un membre peut être réputé démissionnaire et être radié du tableau si sans motif valable et pendant deux années consécutives, il n'a pas payé sa cotisation professionnelle annuelle ou les cotisations dont il est personnellement tenu au titre des régimes de sécurité sociale et de retraite qui lui sont applicables. Peut encore être radiée d'office du tableau toute personne physique ou morale qui vient à ne plus satisfaire aux conditions exigées pour être inscrite au tableau (sauf questions touchant à la moralité qui relèvent de la procédure disciplinaire).
- La démission : Tout membre est susceptible de démissionner de l'Ordre pour des raisons personnelles.
- La retraite : La fin normale de la carrière du professionnel.

2232 Le tableau professionnel

L'entrée dans la profession met au premier plan le "tableau", liste nominative des professionnels, personnes physiques et/ou morales de la profession intéressée. Le tableau est tenu par l'instance de régulation de la profession, l'Ordre professionnel. Les modalités pratiques de la tenue du tableau dépendent de l'organisation de l'Ordre à l'échelle du pays :

- pour les professions comprenant plusieurs ordres en France, chaque ordre gère le tableau de ses ressortissants,
- pour les professions ne comprenant qu'un ordre en France (ordre national), celui gère le tableau national, sauf s'il possède des conseils régionaux qui gèrent comme dans le cas précédent le tableau de leurs ressortissants.

Par rapport au tableau, les positions de l'exercice correspondent uniquement à des périodes d'inscription et à des périodes où on ne l'est pas (qu'on qualifiera ci-dessous de *désinscription*). En parcourant les positions sous cet angle de vue, on peut procéder à une classification qui laisse apparaître des opérations uniques. Ainsi l'entrée dans la profession (inscription), la radiation (qui est définitive) (désinscription) sont des opérations uniques. La retraite est également marquée par la radiation du tableau. Cependant certains professionnels qualifiés *d'honoraires* peuvent conserver une pratique réduite.

Au contraire, d'autres positions sont des opérations doubles :

- Le transfert d'inscription puisqu'on apparaît sur un tableau après avoir été supprimé d'un autre tableau où on était antérieurement inscrit,
- La suspension (disciplinaire) puisque à la fin de la période de suspension, on revient au plein exercice,

- La cessation provisoire ou l'omission puisqu'un jour on revient (généralement) dans la profession en se réinscrivant au tableau

Les opérations sont présentées dans le tableau ci-dessous :

Inscription	La sortie de la profession
Entrée dans la profession	
Le transfert d'inscription	(Radiation du tableau)
(Réinscription)	La cessation provisoire des fonctions
(Réinscription)	La suspension
	La radiation
	La retraite

3 LES SOLUTIONS ACTUELLES ENTRE CERTIFICAT D'IDENTITE ET ANNUAIRE ELECTRONIQUE

Dans le domaine de la signature électronique, le moyen technique qui garantit l'identité du signataire est le certificat électronique⁷. Parmi les mentions requises par les normes techniques pour les certificats figure en bonne place le nom du porteur (du certificat). Il est possible de compléter ce nom par diverses informations comme son appartenance professionnelle. Cette pratique présente des inconvénients et d'autres solutions sont employées.

31 La gestion par le certificat d'identité

311 Le statut juridique du certificat électronique et de l'attribut professionnel

Avant 2000, les textes légaux ne connaissaient pas la notion de certificat électronique, telle que normalisée dans la Recommandation X.509. C'est à l'occasion de la mise en œuvre de la signature électronique de l'article 1316-4 du Code civil, principalement de la vérification de la signature, que la notion de certificat est introduite dans l'édifice juridique. Le Décret n°2001-272 du 30 mars 2001 indique dans son article 1-9° ce qu'est ce composant : "*Certificat électronique - un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire*".

Dans la technique, les *attributs* correspondent aux *droits* (techniques) que possèdent les individus dans un système d'information de procéder à certaines opérations techniques, d'accéder à certains services ou certaines parties du système. Le Décret n°2001-272 du 30 mars 2001 modifié, texte d'application de la signature électronique de l'article 1316-4 du Code civil, fait référence à deux éléments pouvant correspondre à des attributs. Toutefois la perspective est très ciblée puisqu'il s'agit d'une signature électronique et d'attributs à caractère juridique.

Ces attributs sont cités comme partie intégrante de la variété de certificats électroniques reconnus par le droit, les certificats *qualifiés*. Dans ces cas, les attributs inclus dans le certificat d'identité, ne nécessitent pas l'utilisation d'un certificat d'attribut spécifique. Les attributs sont visibles dans la liste des composants des certificats qualifiés dressée par l'article 6-I du Décret précité :

- | |
|---|
| <ul style="list-style-type: none">a) Une mention indiquant que ce certificat est délivré à titre de certificat électronique qualifié ;b) L'identité du prestataire de services de certification électronique ainsi que l'Etat dans lequel il est établi ;c) Le nom du signataire ou un pseudonyme, celui-ci devant alors être identifié comme tel ;d) Le cas échéant, l'indication de la qualité du signataire en fonction de l'usage auquel le certificat électronique est destiné ;e) Les données de vérification de signature électronique qui correspondent aux données de création de signature électronique ;f) L'indication du début et de la fin de la période de validité du certificat électronique ;g) Le code d'identité du certificat électronique ;h) La signature électronique sécurisée du prestataire de services de certification électronique qui |
|---|

⁷ Ceci n'est qu'une présentation incomplète du rôle du certificat. Le certificat atteste en réalité de la concordance entre une clé cryptographique publique et l'identité de son porteur. L'exactitude de l'identité du signataire (lorsqu'elle est nécessaire) est vérifiée au moment de la phase d'enregistrement qui précède la confection du certificat.

délivre le certificat électronique ;
i) *Le cas échéant, les conditions d'utilisation du certificat électronique, notamment le montant maximum des transactions pour lesquelles ce certificat peut être utilisé.*

Les attributs identifiés par le présent Décret sont :

- la qualité professionnelle du titulaire du certificat dans l'entreprise (voir en d)),
- le montant maximal des transactions auquel le certificat sert de support (voir en i)).

Il est donc possible d'intégrer dans le certificat de type X.509 un nom accompagné d'une qualité professionnelle. Le système comporte un certain nombre d'inconvénients, par exemple :

- Le sort du certificat d'identité suit celui de la qualité professionnelle : si un utilisateur dispose d'un certificat mentionnant son appartenance à une entreprise, il perd son certificat (certificat révoqué) à son départ. Pourtant il conserve son droit à disposer d'une signature électronique.
- La vérification de la qualité professionnelle : la plupart du temps le PSCE déléguera à une Autorité d'Enregistrement (AE) spécialisée le soin de vérifier l'identité d'une personne qui s'enregistre en vue d'obtenir un certificat électronique pour une application de signature électronique juridique⁸. Cette AE aura-t-elle nécessairement la compétence nécessaire pour apprécier la qualité du professionnel au sein de son entité, pour les professions réglementées par exemple ?

Cela étant, il semble possible de recourir à une gestion de la qualité professionnelle par le certificat d'identité à condition d'agir dans une communauté d'acteurs relativement fermée. On en verra des exemples ci-dessous.

312 L'exemple du dépôt électronique de brevets

Le premier exemple illustre la gestion des mandats dans la téléprocédure de dépôt électronique de demande de brevet à l'Institut National de la Propriété Industrielle (INPI).

Les seules personnes habilitées à déposer une demande de brevet auprès de l'INPI sont les suivantes :

- Les personnes physiques ou morales souhaitant déposer en leur nom propre des demandes de brevet ou de certificat d'utilité ;
- Les conseils en propriété industrielle, avocats ou autres mandataires autorisés par le code de la Propriété Intellectuelle à représenter les tiers devant l'INPI, dès lors qu'au moins une personne physique possède la qualification correspondante pour effectuer les dépôts de demande de brevet.

L'INPI a ouvert le 15 janvier 2003 un pilote opérationnel pour le dépôt électronique des demandes de brevet d'invention et de certificat d'utilité (FR et EP, puis PCT), régi par une politique de certification provisoire disponible sur son site institutionnel ; les dépôts de personnes physiques ne sont pas autorisés dans le cadre de ce pilote. Le dépôt en ligne consiste en l'envoi par Internet à l'INPI à l'aide d'un logiciel client spécifique, des fichiers électroniques constituant la demande de brevet et préalablement convertis au format PDF.

La sécurité du dépôt électronique est assurée grâce à deux certificats d'identité, dont les bi-clés correspondants sont stockés sur une carte à microprocesseur personnalisée :

⁸ Par exemple, qui s'enregistre dans une procédure dite de "face à face".

- un premier certificat est dédié à la signature électronique XML des documents encapsulés constituant la demande ;
- un second certificat sert à l'authentification du déposant et au chiffrement en ligne lors de la session SSL de transmission vers le serveur de l'INPI.

L'accès aux prestations et services fournis dans le cadre de cette téléprocédure est subordonné à la signature d'un contrat préalable d'abonnement ; c'est par ce biais que la qualité des déposants est contrôlée. L'abonné, qui doit, dans ce cas, être autorisé à représenter les tiers devant l'INPI, désigne dans son contrat et sous sa responsabilité les personnes physiques à qui l'INPI doit délivrer des certificats de signature et/ou d'envoi ; l'INPI vérifie à cette occasion ainsi qu'au reçu des formulaires de demande de certificats, la qualité des personnes désignées pour recevoir des certificats de signature ; ces personnes signent en outre un engagement «porteur de certificats » lors de la remise en face à face des cartes à microprocesseur, à l'INPI ou dans ses délégations régionales.

Par conséquent, l'enrichissement des certificats électroniques d'identité par un certificat d'attribut spécifiant la qualité du déposant n'est pas utile pour l'instant compte tenu des contrôles préalables effectués ; l'usage de certificats d'attribut permettra à l'avenir plus de souplesse et d'efficacité, car il permettra de minimiser la fréquence de révocation des certificats d'identité ; ainsi, un conseil en propriété industrielle changeant de cabinet n'aura pas obligatoirement à révoquer son certificat initial de signature.

313 L'exemple de la Carte de Professionnel de Santé

Pour la Carte de Professionnel de Santé la vérification de la qualité professionnelle repose sur un service réservé à l'usage d'une certaine catégorie de professionnels.

Pour améliorer la qualité des soins apportés au patient ou répondre à des obligations légales comme la loi du 4 mars 2002 sur l'accès du patient à son dossier médical, la communication de données de santé informatisées entre Professionnels de Santé ou entre Professionnels de Santé et patients est amenée à se généraliser. Les échanges électroniques doivent se faire de façon sécurisée, dans le cadre légal et dans un format compréhensible par l'ensemble des acteurs concernés. A cet effet, deux grands modes d'accès aux données de santé informatisées ont été développés : le serveur de données auquel le professionnel de santé peut accéder directement et la messagerie Internet sécurisée pour le transfert d'informations entre les professionnels de santé.

L'accès aux données de santé via un serveur doit se faire par une authentification forte des utilisateurs reposant sur la Carte de Professionnel de Santé* (CPS) et des mécanismes de cryptographie. La CPS est une carte à microprocesseur incorporant les biclés d'authentification et de signature du professionnel propriétaire de la carte. L'établissement de santé est certain de l'identité du professionnel de santé qui se connecte à son serveur. Cela permet de personnaliser et de restreindre l'accès en fonction des utilisateurs : un médecin de ville ne pourra accéder qu'aux dossiers de ses patients (qui auront donné au préalable leur autorisation à la clinique).

La messagerie sécurisée a l'avantage d'être très simple à mettre en œuvre et d'être «bidirectionnelle » entre établissement de santé et ville. A la simplicité et la souplesse d'une messagerie Internet, ce service ajoute les fonctionnalités de chiffrement de message (128 bits) et de signature électronique à valeur légale. Il utilise les cartes de la famille CPS et le système

de certificats du GIP-CPS. L'établissement de santé et les médecins peuvent s'échanger des messages signés/chiffrés pour lesquels l'identité de l'émetteur (authentification du signataire d'un message) et la non-altération du message pendant son transport sont assurées. Enfin l'émetteur ne pourra pas nier ultérieurement le fait qu'il ait envoyé ce message. Les données du message (et ses pièces jointes éventuelles) ne circuleront pas "en clair" sur le réseau.

32 La gestion par une hiérarchie d'autorisations : l'exemple de Copernic

Ce moyen de gestion est illustré par la hiérarchie d'autorisations⁹ mise en place par le MINEFI dans le cadre d'un projet appelé *Copernic*¹⁰. Ce dernier vise à offrir aux usagers professionnels un accès au "Compte Fiscal Simplifié (CFS)"¹¹ au travers de l'utilisation de e-services au sein de son espace nominatif. Le projet doit garantir un accès sécurisé au CFS et aux services Copernic individualisés. Il s'agit de :

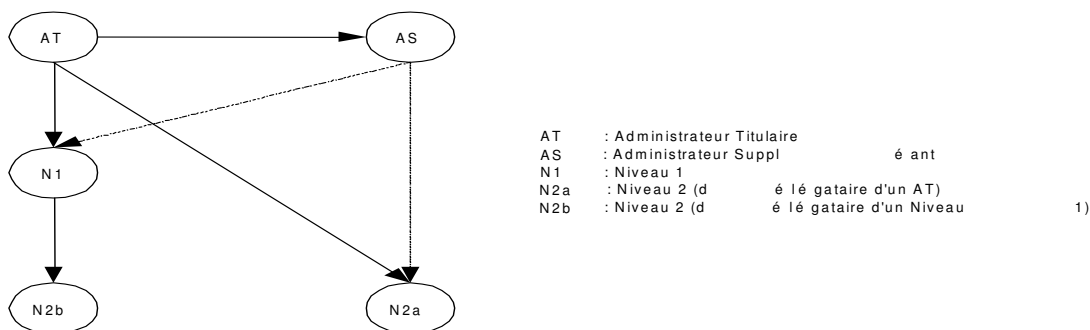
- adapter l'abonnement des professionnels aux spécificités organisationnelles des différents intervenants (entrepreneurs individuels, PME, entreprises DGE, Experts-Comptables),
- permettre des délégations étendues,
- palier les contraintes liées aux ré-adhésions consécutives à un changement de SIRET ou à l'expiration du certificat numérique,
- proposer une adhésion "dématérialisée"

L'architecture est organisée autour de la notion d'*usager* considéré comme un acteur en relation avec le MINEFI pour le compte d'une entreprise. L'utilisateur peut-être :

- déléguant : il possède un droit de délégation des habilitations
- délégataire : il est bénéficiaire des habilitations déléguées par les usagers déléguants

	Mandataire social	Administrateur titulaire	Administrateur suppléant	Niveau 1	Niveau 2
Déléguant		X	X	X	
Délégataire				X	X

La hiérarchie des usagers comprend 3 niveaux. Elle est représentée dans le tableau ci-dessous.



⁹ D'après une présentation de l'équipe Copernic 5 faite au GT habilitation le 14 janvier 2003.

¹⁰ <http://www.minefi.gouv.fr/archives/dossiersdeprelse/2001/portailfiscal/copernic.htm>

¹¹ Le Compte Fiscal Simplifié est un projet visant à fournir à chaque contribuable un ensemble de données cohérentes et en temps réel décrivant la totalité de la situation fiscale. Elle sera accessible par différents canaux technologiques internes et externes (téléphone, courrier, minitel, guichet, Internet, centres d'appels, bornes interactives, autres...). Elle intégrera la gestion des événements qui caractérisent la relation entre contribuable et administration. L'identification, l'authentification et la gestion des habilitations garantiront le respect des textes relatifs au secret fiscal.

Un usager ne peut déléguer que des habilitations qu'il possède. Le mandataire social de l'entreprise se place au sommet de la hiérarchie des habilitations. Selon les entreprises, il peut être ou non l'administrateur titulaire.

Le fonctionnement du système est basé sur deux niveaux de procédures :

- les procédures d'adhésion et d'inscription,
- les procédures de gestion des habilitations.

La procédure d'adhésion a pour but de créer l'espace nominatif qui permettra de gérer les habilitations et les accès. Les modalités d'adhésion au système dépendent du fait que le mandataire social de l'établissement déclaré possède ou non un certificat¹² :

- adhésion matérialisée (sans certificat) : envoi d'un formulaire-papier d'adhésion à l'administration fiscale,
- adhésion dématérialisée : inscription en ligne avec usage du certificat.

La procédure d'inscription a pour but d'enregistrer un usager dans l'annuaire d'authentification, le référentiel adhérent et le système d'information du MINEFI. Cette procédure conduit donc à l'attribution d'un espace nominatif à l'utilisateur concerné. Les modes d'exécution de cette procédure dépendent du fait que l'adhésion s'est déroulée de façon matérialisée ou non. Les abonnés disposent de 4 types de services :

- la gestion de l'adhésion/inscription,
- l'accès aux applications professionnelles ("e-services" : TéléTVA, SATELIT, ...) et aux "newsletters",
- la gestion des tiers,
- la gestion du compte adhérent.

Le service de gestion des tiers permet à tout adhérent possesseur d'un espace nominatif de gérer une population de délégataires ainsi que leurs habilitations. Les fonctionnalités permises sont :

- la création, la suppression, le remplacement et la "mise en veille" d'un délégataire,
- la création, la suppression, le remplacement et la "mise en veille" d'une habilitation,
- la consultation de la liste des délégataires et délégués ainsi que le suivi des accès.

La "mise en veille" permet de conserver la chaîne de délégation en attendant le remplacement d'un usager délégué.

Le service de gestion du compte adhérent permet à tout adhérent possesseur d'un espace nominatif de modifier ses données personnelles :

- mise à jour des données identifiées,
- remplacement d'un certificat,
- réactivation de l'espace nominatif dans le cas où le certificat a été révoqué ou a atteint sa date de validité.

33 La gestion par annuaire électronique

331 La notion d'annuaire électronique

Le principe de ces solutions est la constitution d'une base de données centrale ou d'un annuaire central (par exemple de type LDAP) comprenant l'ensemble des droits d'accès de tous les utilisateurs recensés. Toute mise à jour des informations centrales est répercutée par propagation à l'ensemble des fichiers de sécurité des plates-formes informatiques. En amont le

¹² Il s'agit d'un certificat "référéncé" émis par une autorité de certification du marché.

système de gestion des données centrales relatives aux droits est connecté aux fichiers de gestion des ressources humaines de façon à détecter tout changement d'affectation ou de fonction. Ce type de gestion comprend des procédures permettant de gérer les circuits d'attribution, de suppression ou de changement des données utilisateurs.

Les annuaires garantissent la validité et cohérence des informations. Par contre, du fait du cloisonnement des réseaux informatiques (Internet et Intranet), l'accès aux annuaires peut poser problème. Pour des raisons de sécurité ou par manque de ressources, les postes de travail dans les entreprises ou dans les administrations ne sont pas toujours reliés à l'Internet ou au réseau interne. Interroger à distance les annuaires depuis de tels postes est physiquement impossible.

Le Conseil Supérieur de l'Ordre de vétérinaires¹³ est en train de devenir bureau d'une autorité d'enregistrement lié à une autorité de certification quant à la signature électronique. Il s'agit de pouvoir vérifier en temps réel le droit à l'exercice d'un vétérinaire avant qu'il puisse apposer sa signature certifiée qui deviendra alors une signature professionnelle certifiée selon les termes même de notre prochain Code de Déontologie pris par décret en Conseil d'Etat. Le vétérinaire pourra donc signer des certificats, ordonnances ou prescriptions, et les adresser sécurisés par courrier électronique. La vérification du droit à l'exercice est faite en temps réel par échange chiffré de données avec une base centrale mise à jour toutes les nuits. Elle peut donc tenir compte d'une radiation de la veille ou d'une inscription enregistrée, par exemple. Actuellement les filtres permettent de trier les catégories de vétérinaires et de réaliser ce type d'identification sur bien des sites Web aux pages privées, permettant leur accès via le site sécurisé d'authentification. Enfin certains sites Web (pharmacologie animale, recherche animale, génétique) contiennent des parties privées qui nécessitent l'identification des utilisateurs. La mise en place de filtres faisant appel à l'annuaire géré par Le Conseil Supérieur de l'Ordre de vétérinaires permettra de réserver l'accès à ces parties privées aux seuls vétérinaires.

332 Critique de l'intérêt des annuaires au sein des ICP

3321 Apports des annuaires pour les ICP

Les annuaires (LDAP ou autres tels que les bases de données interrogeables à distance) sont utilisés par les ICP afin de fournir une « liste blanche » publique. Celle-ci doit notamment permettre à l'émetteur d'un message chiffré de prendre connaissance du certificat du destinataire. Un second emploi possible concerne la signature électronique. Le récepteur d'un message signé peut désirer contrôler la validité du certificat du signataire. Le recours à un annuaire public lui offre la possibilité de confronter le certificat du signataire au certificat inclus dans l'annuaire. Cette pratique, peu utilisée cependant, participe à la dénonciation de fausses signatures, et ce même lorsque l'ensemble du chemin de certification semble correct à première vue.

Cependant, l'utilisation des annuaires LDAP (préconisés par l'IETF) est soumise à des limitations techniques : au départ, ces annuaires manipulent des informations de type X.500 et il est difficile d'intégrer les certificats X.509 car X.500 n'est pas prévu pour. L'utilisation de LDAP pour les ICP semble donc superflue, le recours alternatif à une base de données étant possible. Cependant, les requêtes permettant d'interroger la base (via un serveur public par

¹³ URL : www.veterinaire.fr

exemple) doivent être normalisées afin que les applicatifs clients (de chiffrement, signature ou encore les logiciels de messagerie et les butineurs) puissent y accéder.

Enfin, la consultation par annuaire suppose que le demandeur connaisse non seulement l'autorité émettrice mais également des informations d'identification afin de sélectionner le certificat adéquat parmi la liste des réponses fournies par l'annuaire. Ceci est particulièrement problématique lorsque l'annuaire est consulté à des fins de chiffrement et que l'émetteur du message chiffré ne connaît pas le destinataire (il ne dispose pas d'informations relatives à son certificat).

Pour conclure, le maintien d'une "liste blanche" semble incontournable, non pas parce qu'elle permet de prendre connaissance d'un certificat, mais parce qu'elle offre la possibilité de vérifier l'existence d'un certificat d'époque : le vérificateur peut s'assurer que le certificat qui lui est présenté est authentique, et ce même lorsque la clé d'émission de l'autorité de certification est compromise (indépendamment du fait que la compromission intervient avant ou après expiration de la clé). D'un point de vue technique, les annuaires de type LDAP semblent peu adaptés aux besoins des usagers qui préféreront recourir uniquement aux services de contrôle de révocation des ICP tels que les CRL ou OCSP, bien que les réponses fournies soient incomplètes. En effet, ces techniques ne permettent pas de contrôler si le certificat est authentique ou faux (car généré après compromission de la clé d'émission de l'AC).

3322 Annuaire et gestion des habilitations

Les annuaires protégés (locaux au sein des entreprises ou orientés extranet, c'est-à-dire accessibles uniquement aux personnes autorisées, telles que des partenaires commerciaux [à valider, compléter]) mettent à disposition du vérificateur des informations venant compléter le certificat d'identité : peut-il cependant se substituer aux certificats d'attributs ? Il est évident qu'un annuaire peut contenir les mêmes informations relatives aux habilitations et rôles associés aux certificats tout en conservant l'avantage de l'indépendance par rapport à la durée de vie du certificat d'identité.

Le vérificateur ayant accès à l'annuaire est en mesure de contrôler que le signataire est effectivement autorisé à signer ou au contraire ne dispose pas des autorisations suffisantes. Il n'est pas nécessaire de demander l'intervention d'une autorité d'attributs (AA) tierce pour permettre à l'entreprise de gérer les autorisations de ses employés. Cette tâche peut être confiée à un administrateur d'attributs (qui peut être l'administrateur système) qui engage sa responsabilité sur la mise à jour régulière et la sauvegarde de l'annuaire des attributs.

Dans l'hypothèse où le serveur hébergeant l'annuaire est sécurisé et qu'il dispose de sa propre signature électronique, le vérificateur peut conserver la trace de sa requête afin d'authentifier la provenance des informations d'attributs et apporter la preuve de leur intégrité. En cas de problème d'acceptation de la signature sous couvert des attributs fournis par l'entreprise alors que ces derniers ne reflètent pas la réalité, le vérificateur peut montrer sa bonne foi.

L'utilisation des certificats d'attributs (ou toute autre technique) générés par une AA tierce (et neutre) permet d'apporter des indices supplémentaires pour démontrer l'existence effective des attributs pendant la période considérée. L'AA conserve un double des certificats d'attributs générés afin de les fournir en cas de besoin.

Les annuaires permettent-ils d'apporter cette preuve ? En effet, de manière indirecte. L'entreprise peut conserver l'historique des attributs générés au sein de « dossiers employés » et des requêtes effectuées sur le serveur d'annuaire (fonctions d'audit). Le vérificateur peut quant à lui archiver les signatures reçues et les attributs authentifiés par le serveur de l'entreprise contactée. Chacun dispose alors de son propre moyen de preuve.

Reste à traiter la délégation des attributs, mais là encore, le certificat d'attributs et le système de gestion associé semblent plus complexes à mettre en œuvre que le recours aux annuaires.

4 LES CERTIFICATS D'ATTRIBUTS, UNE SOLUTION D'AVENIR ?

41 L'antériorité des habilitations de sécurité

Certifier l'appartenance d'une personne à une organisation est une préoccupation de niveau professionnel. Une préoccupation identique existe au niveau de l'accès au système de l'information de l'entreprise qui n'est possible qu'à l'individu disposant de *privilèges* reconnus et vérifiés. Aussi l'antériorité de la gestion des privilèges dans les systèmes d'information permet-elle de définir plus précisément les besoins au niveau professionnel et dégager certaines solutions pour la *gestion des attributs*.

Les systèmes d'information des entreprises et des administrations doivent gérer une masse croissante de données disponibles ainsi que l'accès à ces données. Le système d'information traditionnel cloisonné ou fermé disparaît au profit d'une interconnectivité des acteurs via l'Internet ou l'Intranet. La diffusion de l'information sous forme numérique est potentiellement immédiate et universelle avec les dangers que cela comporte. Il faut donc sensibiliser les utilisateurs sur la valeur des informations qu'ils manipulent et rétablir un contrôle sur l'accès à ces informations ou services.

Comme l'indiquait une étude récente de l'Université Technologique de Compiègne (UTC), "*L'institution de la sécurité ou comment s'en désintéresser*", réalisée dans le cadre du projet RNRT Icare¹⁴ les utilisateurs de systèmes d'information ne perçoivent pas les besoins de sécurité. La sécurité pour eux est avant tout une sécurité physique et la dématérialisation des informations et des échanges ne correspond pas à ce besoin de concret.

Un droit d'accès résulte du croisement entre les droits théoriques d'un opérateur, du niveau de sensibilité (besoins de confidentialité, d'intégrité, de non-répudiation, par exemple) de l'information objet de l'accès et des règles en vigueur dans le système. Les politiques de sécurité regroupent ces règles d'application des droits d'accès dans le contexte particulier d'un système. Le contrôle d'accès correspond, à la fois, au contrôle des droits d'accès, et aux dispositions et dispositifs de protection des informations (essentiellement traduits par des procédures d'identification – authentification, des cloisonnements physiques ou logiques, des procédures).

Il y a donc 3 composantes dans la mise en œuvre de systèmes d'information sécurisés :

- le juridique

¹⁴ Pour une présentation du projet Icare (programme RNRT) voir : http://www.cert-i-care.org/ICare_accueil.htm
Pour accéder au document de l'UTC de Compiègne, voir http://www.cert-i-care.org/ICare_documents.htm

- l'organisation (définition d'une politique de sécurité, mise en œuvre de cette politique et surtout diffusion auprès des utilisateurs)
- la technique (infrastructure de sécurité type PKI, logiciels de signature et de chiffrement, contrôle d'accès des utilisateurs aux données -portail Web sécurisé ou répertoires protégés)

Actuellement, la sécurité est assurée (?) par l'identification des utilisateurs par un compte informatique et le contrôle du mot de passe associé. L'accès aux informations est conditionné par cet identifiant ainsi que par une partition des documents.

A terme, il faut définir plus précisément l'accès à l'information des utilisateurs en leur attribuant des droits ou privilèges et des documents en leur associant un label.

42 Du certificat d'identification au certificat d'attribut

421 Les certificats d'attributs et l'IETF

Les documents cités font partie d'un ensemble de travaux réalisés par le groupe de travail PKIX. Le groupe de travail PKIX a été mis en place en automne 1995 afin d'ériger un standard X.509 orienté vers les applications Internet. La portée du travail de PKIX a largement dépassé ce premier objectif. PKIX ne travaille plus seulement à partir des normes de l'ITU PKI, mais développe également de nouveaux standards sur l'utilisation des PKI basés sur X.509 en ce qui concerne Internet. Dans ce cadre, le groupe de travail a récemment intégré les certificats d'attributs dans le document relatif au certificat numérique (rfc2459), le document est maintenant le rfc3280¹⁵. Il présente en sus des certificats "classiques" X.509 un cadre de standardisation des certificats d'attributs. Par la suite, un RFC définissant les certificats d'attributs pour une utilisation limitée au service d'authentification d'application Internet (SSL, IPsec, etc.) a été mis en place : RFC3281¹⁶.

422 Les groupes PKIX et SPKI de l'IETF

Des groupes de travail de l'IETF tels que PKIX et SPKI¹⁷ considèrent dans leurs travaux, la structure et le traitement de certificat. PKIX a pour but de développer un ensemble de normes définissant, spécifiquement pour l'Internet, une IGC (infrastructure de gestion des clés) basée sur les certificats X.509 avec des attributs étendus, des spécifications ASN.1, encodage et décodage DER.

Le certificat d'autorisation est la forme fondamentale de certificat SPKI (voir le RFC 2693¹⁸). Il sert à transférer une habilitation au moyen d'un certificat. En particulier, SPKI abandonne l'idée qu'un certificat permet de lier une clé à une identité pour considérer que le rôle d'un certificat est plus général et attribue également des permissions au possesseur d'une clé. SPKI se focalise sur l'autorisation et la délégation plutôt que l'authentification. SPKI offre une simplicité par rapport au standard X.509 en utilisant un schéma d'encodage "S-expressions"

¹⁵ Le texte peut être téléchargé à <http://www.ietf.org/rfc/rfc3280.txt>

¹⁶ Le texte peut être téléchargé à <http://www.ietf.org/rfc/rfc3281.txt>

¹⁷ SPKI, acronyme de Simple Public Key Infrastructure a pour but de spécifier une PKI simplifiée qui supporte la délégation (voir RFC 2692 - C. Ellison, " SPKI Requirements", Internet Draft IETF, juillet 1999. <http://www.ietf.org/rfc/rfc2692.txt>)

¹⁸ C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, T. Ylonen, "SPKI Certificate Theory", RFC 2693 IETF, septembre 1999. <http://www.ietf.org/rfc/rfc2693.txt>

plus accessible que la notation ASN.1 utilisée par X.509 . Les "S-Expressions sont similaires au langages XML et lisibles par un être humain, contrairement aux encodages. ASN.1 et DER utilisés par X509.

SPKI estime préférable d'émettre plusieurs certificats spécifiques, chacun pour une application donnée plutôt qu'un certificat universel, mettant en danger l'intimité numérique de son détenteur. SPKI a été proposé pour devenir une alternative au X.509 basé sur les PKIX. Cependant, malgré sa grande souplesse d'utilisation et de mise en œuvre, le standard SPKI ne s'est jamais imposé face à son concurrent X.509, largement déployé en natif dans les navigateurs.

423 Le groupe SDSI du MIT

SDSI¹⁹ est l'acronyme de Simple Distributed Security Infrastructure, c'est un modèle de PKI créé dans le laboratoire de sciences informatiques du MIT en 1996. SDSI combine une PKI avec une méthode de définition de groupes et de publication de certificats. SDSI simplifie la terminologie pour définir des listes de contrôle d'accès et de politiques de sécurité. SDSI met en évidence la liaison entre les espaces de noms locaux (local name space) plutôt que de favoriser la hiérarchie de l'espace globale de X.500.

424 Unification de SPKI et SDSI dans l'IETF

La spécification du groupe SPKI de l'IETF et celle de SDSI du MIT se sont regroupé en 1997, en associant les avantages des deux spécifications. La spécification SPKI/SDSI utilise les noms locaux (identifiables dans un espace local) pour identifier et/ou autoriser un ou plusieurs utilisateurs de certificats. L'ETSI (European Telecommunications Standards Institute) a produit un certain nombre de textes (même s'ils restent très proches de ceux de l'IETF). Ces textes sont disponibles sur le portail : <http://www.etsi.org>, en particulier le texte ETSI TR 102 044 v1.1.1 (2002-12), intitulé "*Electronic Signatures and Infrastructures (ESI) ; Requirements for role and attribute certificates*". En mars 2000²⁰, un document de travail qui définit une forme standard pour encoder les certificats SPKI en XML, a été déposé à l'IETF. En novembre 2001²¹, un autre document de travail proposait une grammaire XML pour décrire les certificats SPKI.

43 Approche des certificats d'attributs

431 La gestion par les certificats d'attributs à proprement parler

Pour permettre l'ajout d'informations, telles que des attributs ou des privilèges, dans un certificat d'identité, la version 3 de X.509 a introduit des options d'extension sous forme de blocks d'informations. Ces extensions permettent de spécifier des informations en fonction de l'usage que l'on souhaite donner au certificat. Malheureusement, l'ajout de ces extensions a induit des problèmes d'interopérabilité et de gestion de la révocation.

19 R. Rivest, B. Lampson, "A Simple Distributed Security Infrastructure version 2" MIT, février 1998. <http://theory.lcs.mit.edu/~rivest/sdsi11.html>

²⁰ XML Encoding of SPKI Certificates : <http://world.std.com/~cme/draft-paajarvi-xml-spki-cert-00.txt>

²¹ SPKI-XML Certificate Structure: <http://www.ecom.tifr.res.in/~vtp/pki/SPKI/draft-orri-spki-xml-cert-struct-00.txt>

La solution de l'ITU-T est de scinder un certificat X.509 en deux : un certificat d'identité qui va consigner des informations sur l'identité et un certificat d'attribut [ITU-X509 00] qui va enregistrer des informations sur l'attribut (d'autorisation - contrôle d'accès). Cette solution simplifiera énormément le processus d'émission des certificats et pourra, dans certaines situations, éliminer le problème de la révocation. Les certificats d'attribut ayant une durée de vie très courte, leur révocation n'est pas obligatoire, ils expirent tout simplement.

Comme l'ont montré les résultats des études entreprises par le GIP-MDS comme par le projet ICARE, la séparation certificat d'identité / certificat d'attribut est nécessaire car :

- Au niveau logique, la durée de vie des attributs est différente de celle du certificat d'identité. En effet, si un directeur commercial d'entreprise perd sa position dans la hiérarchie interne, ces attributs sont invalidés et partant son certificat ; pourtant il a toujours droit à une signature électronique stricto sensu. Comme on dit en droit, le sort de l'accessoire suit le sort du principal.
- Au niveau technique, les attributs sont garantis par diverses Autorités qui n'ont pas nécessairement de relations avec le certificateur ayant émis le certificat : toute organisation a vocation à certifier l'appartenance et la position de ses membres en son sein.
- Enfin les attributs ne sont pas nécessairement demandés au même moment que la demande de certificat d'identité.

Le certificat d'identité X.509 dans sa forme la plus classique ne rend pas compte de la qualité de professionnel. Aussi rencontre-t-on des services où seuls les professionnels préalablement identifiés comme tels peuvent y accéder. Le certificat d'attribut constitue une réelle évolution. Le certificat d'attribut proposé se présente comme un instrument technique permettant d'ajouter des fonctionnalités à la signature électronique classique. Son utilisation rend possible la délégation des droits, la signature avec un rôle et le contrôle de la multiscriture électronique. Dans ce contexte nous pouvons considérer trois grands services : l'habilitation / délégation, la certification de rôles, la multiscriture électronique contrôlée.

432 L'habilitation/ délégation

L'habilitation donne l'autorisation à une entité (généralement un subordonné) d'exercer un pouvoir à sa place. Et la délégation donne l'autorisation de transférer ce pouvoir à un tiers. Il faut remarquer qu'on peut habiliter tout ou une partie de ce pouvoir avec un attribut particulier. Dans le cas de l'habilitation de signature, le type de document à signer (feuille de congé, réservation de salle, etc.) peut aussi être pris en compte.

Pour pouvoir obtenir une telle habilitation, les certificats d'attribut peuvent être employés. Une entité A fournit un certificat d'attribut à une entité B, pour qu'elle puisse effectuer en son nom des actions pendant une durée déterminée. Par exemple, A permet à B de signer un document en son nom avec un certificat. Ce certificat est alors joint à tout document signé par B à la place de A, il prouvera que B a bien le droit de signer. Le certificat d'attribut de B est composé de :

- ses droits,
- son identificateur,
- le temps de validité de droits,
- l'identifiant de A,
- la signature de A, la capacité de B à déléguer à un tiers.

B peut donc, dans certains cas et dans les mêmes conditions, habiliter à C et/ou D la signature de A, et ainsi de proche en proche pour créer une chaîne de délégation de signature dans laquelle le niveau de confiance ne se dégrade pas. L'identité des entités est alors garantie (sur demande) par l'émetteur du certificat d'attributs. Il vérifiera les certificats d'identité au moment de faire l'habilitation.

Au total, ce schéma se présente comme une solution dans laquelle le propriétaire de l'application n'a pas besoin de stocker les droits des personnes autorisées (ou uniquement ceux d'un responsable par entreprise), il a uniquement besoin de connaître le haut de la hiérarchie :

- soit parce que comme expliqué plus haut, cette personne a des droits juridiques, par exemple, en tant que patron de l'entreprise, droits que l'application peut vérifier en s'adressant à un référentiel officiel,
- soit par enregistrement classique dans un fichier, mais uniquement pour une personne par entreprise.

Ensuite, tel qu'expliqué, la chaîne de signature de délégations de droits permet de vérifier les droits de l'utilisateur final. Cependant cette solution nécessite la vérification de toute une chaîne de signatures.

433 La certification de rôles

Afin d'associer un pouvoir à une personne, en particulier le droit de signer, la sécurité emploie le concept de rôle. Une identité peut jouer un ou plusieurs rôles, voire aucun. Dans ce contexte, il y a quatre scénarios possibles :

- Il existe plusieurs entités liées à un rôle.
- Il existe une seule entité liée à un rôle.
- Il existe plusieurs rôles liés à une entité.
- Il existe une entité sans rôle.

Le porteur du certificat d'attribut peut être une entité quelconque. Son identification peut-être constituer notamment un rôle. Ce rôle est la représentation des privilèges du signataire dans sa fonction, il a la possibilité de garder l'anonymat dans certaines transactions. Ces rôles constituent une liaison indirecte entre les identités et leurs prérogatives. Ainsi, chacun peut choisir de déléguer (ou de ne pas déléguer) sa signature ou bien seulement une partie du pouvoir associé à cette signature.

Prenons pour exemple les rôles suivants de A :

- Direction de projet
- Direction de projet - signature des congés du personnel
- Direction de projet - embauche du personnel

Dans le cas d'habilitation de la signature pour une demande de congés, A délègue son rôle "Direction de projet - signature des congés du personnel " à B. En revanche, A ne va déléguer à personne son rôle "Direction de projet - embauche du personnel", ainsi il est sûr que personne ne pourra embaucher du personnel à l'exception de lui-même. Il existe aussi la possibilité de déléguer sa signature de manière totale, c'est à dire transmettre l'ensemble de son pouvoir avec le rôle "Direction de projet".

Avec les certificats d'attribut les rôles peuvent être assignés de manière dynamique, par exemple si un employé change de fonction, il faut seulement révoquer l'ancien certificat et

générer un certificat d'attribut qui lui assigne sa nouvelle fonction (ou rôle). Cela permet de garder le même certificat d'identité pour la signature de documents. L'utilisation de certificat d'attribut permet ainsi la certification de rôles assumés par les individus.

434 Multisignature électronique contrôlée

La multisignature électronique (aussi appelée signature de groupe) se base sur les mêmes principes de la signature électronique classique. Elle est nécessaire quand plusieurs entités doivent signer un document, par exemple un bon de commande, un contrat de travail, un projet du groupe, etc. La multisignature contrôlée est un service de multisignature utilisant le certificat d'attribut. Celle-ci permet d'étendre la multisignature d'un document en ajoutant des autorisations ou des contraintes particulières. L'application contrôle la séquence et les priorités des signatures.

Dans ce service, on attache un certificat d'attribut à un document. Ce certificat indique les entités (clés publiques ou identificateur) qui peuvent signer le document et établi aussi l'ordre dans lequel les signataires doivent signer le document. Les informations essentielles à protéger par cette signature sont :

- Le contenu de la transaction.
- L'heure et la date de la signature (Horodatage - "Time Stamping").
- Les politiques de signatures (qui, quand, comment doit-on signer le document).

Des informations additionnelles peuvent être indiquées pour faciliter le caractère légal de la signature :

- La référence des certificats qui valident la signature.
- Le type de transaction (afin d'appliquer les règles valables)
- Le lieu de la signature (afin de savoir quel droit appliquer pour la défense du signataire)

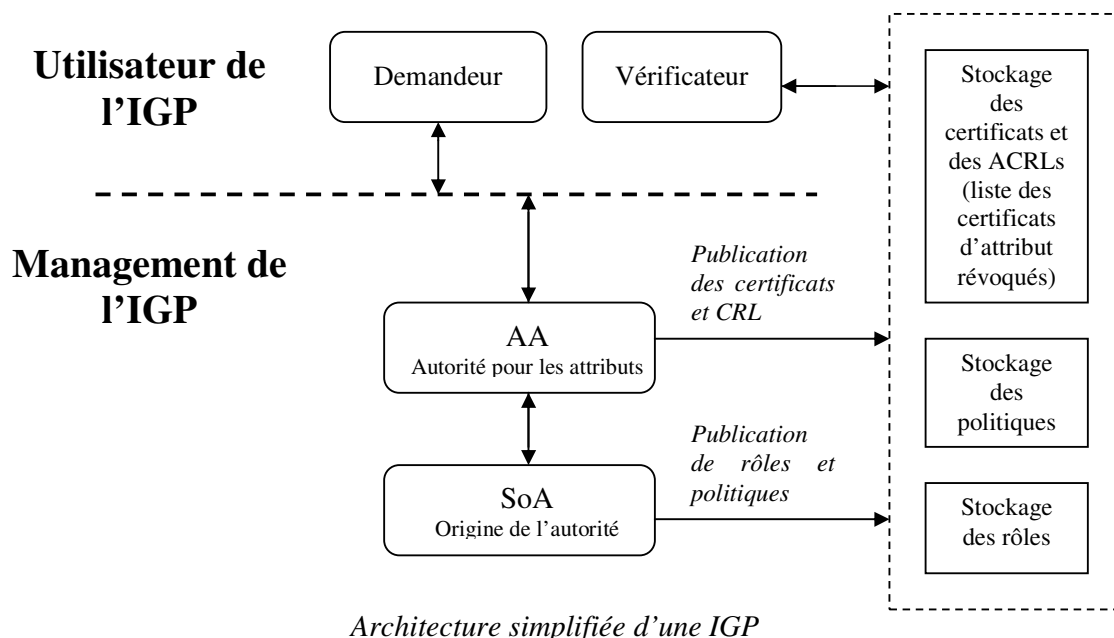
44 La gestion de l'infrastructure

441 L'infrastructure de gestion des certificats d'attribut

Plusieurs systèmes utilisent les certificats à clé publique (certificats d'identité) pour contrôler l'accès des utilisateurs, dès lors qu'il suffit de vérifier l'identité de propriétaire du certificat. Mais de plus en plus de systèmes exigent des règles d'accès qui ne sont pas présentes dans les certificats à clé publique, ni dans les extensions de ces derniers. C'est pour donner cette information que les certificats d'attribut ont été créés, ainsi qu'une infrastructure pour les administrer, l'Infrastructure de Gestion des Privilèges (IGP) ou PMI en anglais (Privileges Manager Infrastructure).

L'IGP est une infrastructure de gestion de privilèges, de matériel, de logiciel, de personnes, de politiques et de procédures, nécessaire pour créer, administrer, stocker, distribuer et révoquer les certificats d'attribut.

4411 L'architecture et les services offerts par l'IGP



Une IGP permet de:

- Demander un certificat d'identification
- Demander un certificat d'attribut
- Vérifier les droits (attributs)
- Vérifier l'identité
- Créer un certificat d'attribut
- Déléguer des attributs
- Révoquer un certificat d'identité
- Révoquer un certificat d'attribut
- Signer un objet (avec certificat de délégation)
- Multisigner un objet
- Vérifier la signature

4412 Les composantes de l'IGP

- Origine de l'autorité (SoA, "source of Authority")

C'est l'AA de plus au niveau, qui est responsable des accès à une ressource. Toutes les demandes d'accès à une ressource doivent prouver que leurs privilèges découlent de la SoA qui contrôle la ressource (chaînage).

- Autorité pour les Attributs (AA)

L'entité qui peut générer un certificat d'attribut : compte tenu de la délégation, si la SoA lui a donné cette autorisation, cela peut être un simple utilisateur.

- Demandeur

C'est l'entité qui fait la requête des attributs.

- Vérificateur

C'est celui qui vérifie les attributs du demandeur :

- vérifie l'origine du certificat (remonte jusqu'à la SoA)
- extrait les droits, en passant par la relation rôle -> privilège si nécessaire,
- les vérifie contre la politique d'accès

- donne ou refuse le droit au demandeur
- peut authentifier le demandeur

Certains éléments sont très importants dans l'architecture :

- **Le rôle**, qui est une «collection » des privilèges, permet d'ajouter un niveau d'abstraction dans les droits présentés par le demandeur [base LDAP, par exemple].
- **Les politiques d'accès (Policy)** : La SoA, en plus de son rôle d'émetteur d'attributs au demandeur, peut décrire des politiques avancées d'accès grâce à un langage abstrait. Ceci permet de développer une API pour le vérificateur indépendant des différentes ressources et façons d'y accéder. Le vérificateur accède à un module contenant les politiques et vérifie que les conditions décrites étaient valides pour permettre l'accès. [base LDAP, par exemple]

Certains éléments ne figurent pas directement dans l'architecture, ils peuvent être considérés comme optionnels :

- Serveur Web pour des interfaces http aux services
- Bases de données pour stocker :
 - les associations rôles-attributs
 - les certificats de rôles pour les employés
 - les politiques d'accès
 - les attributs définis
- Module de régénération automatique des certificats d'attribut

442 Principes de la gestion des attributs / des certificats

Les attributs peuvent être gérés soit au sein des entreprises, soit par un organisme extérieur reconnu comme tiers de confiance ; ce sera le cas pour l'appartenance à une profession réglementée où la gestion des attributs sera effectuée sous l'autorité de l'Ordre professionnel. Dans tous les cas, un responsable de distribution s'avère nécessaire. Cette personne prend en charge la création des attributs et la possible liaison avec un certificat de clé publique.

4421 Gestion au sein des entreprises

Les entreprises peuvent gérer en interne leurs attributs dès lors qu'elles mettent en place une infrastructure adaptée.

L'intérêt est de délocaliser les politiques de validation des accès aux systèmes d'information et de s'affranchir de la gestion des utilisateurs.

Une telle gestion interne est cependant impraticable pour deux raisons :

- elle nécessite une coûteuse gestion d'une architecture similaire à une PKI
- elle n'est a priori pas reconnue par l'extérieur et en particulier par les clients étrangers lors de la production de documents à valeur légale. Cette reconnaissance peut être facilitée par une gestion externe des attributs

4422 Gestion extérieure

La validation d'une signature électronique par rapport à un contenu ne peut être complète qu'après examen et approbation d'un ensemble d'attributs déterminant les caractéristiques du signataire. Une gestion interne, bien que possible, est toutefois improbable. La gestion par un organisme externe, de confiance, est ainsi privilégiée. Cet organisme délivre des attributs certifiés et dispose au sein des entreprises d'un acteur habilité à délivrer des attributs pour le

compte de son entreprise appelé mandataire. Ces attributs sont alors certifiés par l'organisme extérieur dès lors que les attributs du mandataire sont valides. Le conteneur d'attributs (certificat d'attributs ou autre) devra alors référencer de manière non ambiguë le mandataire pour des raisons de répudiation.

Bien que le passage par un tiers de confiance facilite la reconnaissance externe des attributs, en particulier vis à vis des clients et des organismes d'état, les problèmes suivants peuvent être soulevés :

- la non-divulgaration d'informations sensibles à l'extérieur. Les attributs doivent être protégés afin que le vérificateur ne puisse prendre connaissance que des attributs dont il a besoin et non de l'ensemble des attributs du signataire
- la gestion d'attributs destinés uniquement à un usage interne. Une caractéristique des attributs (telle qu'une extension critique) doit donc spécifier leur portée

Une solution envisageable au premier point consiste à autoriser tout détenteur d'attributs à auto-générer un sous-ensemble d'attributs.

443 Intérêt et limites du certificat d'attribut

Sur un plan purement technique, un certificat d'attribut est utilisable pour gérer des habilitations dans des structures complexes nécessitant la gestion des délégations. Le projet RNRT ICARE prouve que cela peut fonctionner techniquement. En mettant en place une gestion des certificats d'attributs adaptée (et relativement complexe), il est par exemple possible de s'assurer que la personne qui signe a bien l'attribution ou la délégation pour le faire. Et il semble que cette gestion des délégations est un des avantages du certificat d'attribut par rapport à d'autres moyens utilisés pour procéder aux habilitations (annuaires...). Il convient toutefois de noter que l'utilisation de certificats d'attributs dans ce contexte, pour préserver un certain niveau de sécurité, nécessite la mise en place d'une infrastructure de gestion de certificats d'attributs, qui engendre une certaine lourdeur.

Les besoins en terme de signature électronique étant ponctuels, on peut envisager une infrastructure qui génère "à la volée" des certificats d'attribut d'une durée de validité de la journée. Ces certificats seraient générés à partir d'un annuaire et archivés par l'ordre dans le cas des professions réglementées.

Un certificat d'attribut ne contient que des informations relatives aux attributs d'un individu. Il est donc généralement associé à un certificat d'identité. Le certificat d'identité est rattaché à un individu, le certificat d'attribut fait le lien avec l'entreprise. Un des avantages est alors qu'il n'est pas nécessaire de re-générer le certificat d'identité à chaque changement de société ou d'attribut, un nouveau certificat d'attribut étant généré dans ce cas.

Mais en quoi la génération d'un certificat d'attribut est-elle moins contraignante que celle d'un certificat d'identité ?

Pour que les partenaires puissent avoir confiance dans un certificat d'attribut, il doit être généré avec un certain nombre de garanties, du type de celles applicables sur un certificat d'identité. Il n'y a donc pas réellement de gain en matière de temps ou de simplification au moment de la génération. Toutefois, l'infrastructure de génération d'un certificat d'attribut

pouvant être en partie indépendante de celle d'un certificat d'identité, cette séparation des pouvoirs peut être un argument en faveur de la sécurité dans des entreprises.

Par contre, un certificat d'attribut est généré pour une période courte, ce qui permet de ne pas gérer les révocations. Un certificat d'attribut offre donc un gain en matière de gestion, mais cette caractéristique peut limiter ses utilisations possibles. Il n'est en effet pas forcément intéressant de re-générer sans cesse des certificats d'attribut pour exprimer un attribut pérenne pour un individu. La génération de certificats d'attribut ayant une durée de vie plus longue n'alourdirait-elle pas considérablement le processus ? De même, pour la gestion des révocations de ces certificats.

Par ailleurs, un certificat d'attribut étant associé à un certificat d'identité, il est parfois nécessaire sur le plan de la sécurité de contrôler ce certificat d'identité avant d'utiliser le certificat d'attribut correspondant. Cette démarche est devenue la plupart du temps une précaution technique que d'aucuns appliquent même lorsqu'elle n'est pas justifiée par des aspects juridiques. Sur un plan légal, le contrôle de la qualité (attribut) d'un individu est en effet souvent suffisant dans la vie « réelle » (non dématérialisée), alors que l'identité d'un individu est généralement requise dans les procédures de dématérialisation. Il peut alors se poser le problème du droit d'un individu à l'anonymat, qui existe aussi dans le monde dématérialisé.

Sur un tout autre plan, le concept même de séparation du certificat d'attribut et du certificat d'identité offre la possibilité de générer un certificat d'identité « unique » par individu, une multitude de certificats d'attributs étant par ailleurs générés par domaine, ou activité. Quelles seront les implications juridiques de l'utilisation d'un certificat d'identité généré à titre personnel, dans un contexte professionnel ?

Tel qu'il est défini, le certificat d'attribut semble donc offrir d'importantes possibilités pour un besoin toutefois assez ciblé, celui d'utilisations ponctuelles (voire uniques) par un individu couvrant de très nombreux domaines. Tant qu'il a une durée de vie si courte, il semble donc à première vue assez peu adapté à une gestion pérenne d'habilitations dans une entreprise. En rallongeant sa durée de vie, l'infrastructure à mettre en place serait nettement plus lourde, et nécessiterait donc une réelle étude du contexte, au cas par cas. Dans une entreprise, l'utilisation de certificats d'attributs semble donc à l'heure actuelle ne pouvoir répondre qu'à des besoins très ponctuels, ou bien nécessiter une infrastructure d'une certaine envergure.

Par contre, une courte durée de vie semble rendre le certificat d'attribut particulièrement bien adapté aux besoins des professions libérales. Toutefois, dans certains cas, certains contrôles (exemple : contrôle du certificat d'identité), qui ne sont pas toujours justifiés juridiquement, alourdissent cette utilisation sans apporter de réelle valeur ajoutée.

Outre l'utilisation de certificats d'attribut « classique », peut-être pourrait-il être pertinent de définir un modèle de certificat d'attribut « simplifié », qui répondrait plus simplement et efficacement aux contraintes de ce type de profession ?

CONCLUSION

CERTIFICATS D'IDENTIFICATION ET D'HABILITATION... JUSQU'OU NE PAS ALLER TROP LOIN ?

Le monde électronique a pour défi de remplir les fonctions dévolues au papier pour l'accomplissement d'actes juridiques dans l'espace des communications dématérialisées. Les travaux donnent toutefois l'impression que la galaxie du World Wide Web tend fortement à diverger de la galaxie Gutenberg.

Vers une modélisation électronique de l'organisation juridique de l'entreprise ?

Dans le commerce juridique classique, l'identification est généralement peu sécurisée et les cas d'authentification d'identité et de certification des pouvoirs et des droits, sont réservés aux transactions les plus importantes : actes de disposition portant sur des immeubles, testaments, donations, contrats de mariage et, dans le domaine des affaires, les opérations de constitution ou de restructuration des sociétés et des groupes, les garanties et sûretés, etc. Les notaires, ainsi que les avocats et leurs homologues étrangers remplissent cette fonction importante pour la sécurisation de la vie juridique.

L'apparition de modes de transaction dématérialisés impose de transposer ces modes traditionnels dans l'univers dématérialisé. Des solutions ont été mises en place, par exemple pour le règlement des transactions à distance par carte bancaire, ou dans le cadre de téléprocédures proposées, voire imposées, aux contribuables et cotisants sociaux. D'un autre côté, il est concevable de dématérialiser les services d'authentification et de certification pour en faciliter et élargir l'emploi aussi bien dans le cadre des relations de proximité que pour les besoins des services et procédures à distance ainsi que du commerce électronique.

L'enjeu est donc d'importance... mais cela ne va-t-il pas transformer la pratique des actes juridiques au point que l'achat d'un journal dans un kiosque de gare ferait appel à un procédé d'authentification du client, que l'envoi d'un ordre de virement par une entreprise mettrait systématiquement en œuvre une cascade de certificats ou un certificat comprenant une cascade d'habilitations, et que le traitement d'une réclamation relative à l'abonnement à une revue ou à un service déclencherait, au minimum, outre une demande de certification d'identité, un certificat de règlement de l'année en cours...

La disponibilité prochaine de cartes individuelles d'identité électronique ouvre la possibilité de l'identification à distance et en temps réel des personnes physiques. Il est probable que cela provoquera une utilisation de l'instrument bien au-delà de la pratique actuelle des titres d'identité. Mais l'utilisation de la carte d'identité ne sera bientôt que l'élément premier d'une guirlande de certificats à l'appui des attributs les plus divers comme Prévert nous invite à en ouvrir le catalogue infini : extraits du registre du commerce, déclarations d'association, diplômes et distinctions de toutes natures, titres et inscriptions professionnelles en cours de validité pour établir la qualité et la qualification de médecins, vétérinaires, avocats..., décorations, titres nobiliaires, arrêtés de nomination, permis de conduire, de chasse et de pêche etc., et bien sûr tout ce qui concerne les pouvoirs d'une personne de signer un acte pour une personne morale ou pour un tiers.

Les travaux actuels au sein d'EDIFRANCE et du CFONB se concentrent sur les méthodes de

certification des pouvoirs des opérateurs intervenant pour une entreprise. La diversité des notions (compétences, pouvoirs, mandat, délégation...) et surtout la disparité de leur contenu compliquent la démarche de normalisation.

Mais, en supposant que l'on parvienne à surmonter ces difficultés, l'exercice ne va-t-il pas déboucher sur une véritable modélisation électronique de l'ensemble des habilitations de l'entreprise ?

Faudra-t-il un certificat en toutes circonstances ?

La sécurité juridique y gagnerait-elle autant qu'il y paraît ? Cela n'est pas certain, car le développement de techniques aisément accessibles permettant de s'informer sur la réalité et l'étendue des pouvoirs de celui avec lequel on contracte pourrait rendre à la doctrine de l'ultra vires une grande partie de l'espace qu'elle a perdu au profit de la théorie de l'apparence, dégagée par la jurisprudence, et dont le principe se retrouve dans certains textes, notamment en droit des sociétés (C. Com. art. L. 225-56 alin.2 ...). Celle-ci permet aux tiers de se prévaloir de la vraisemblance de la qualité et des pouvoirs d'une personne à partir de circonstances permettant de les présumer. Cette bonne à tout faire du droit privé rend depuis des décennies des services d'autant plus inestimables et essentiels qu'elle est omniprésente et invisible. Mais on peut supposer qu'au fur et à mesure que la certification va se développer au point de permettre d'attester de la qualité et des pouvoirs de tout représentant d'entreprise dans des conditions économiquement abordables au regard de l'importance de l'affaire traitée, les tribunaux accepteront plus facilement qu'à l'heure actuelle le fait que " compte tenu des circonstances ", le tiers ne pouvait ignorer que l'acte dépassait l'objet social (Art. L225-56 précité) ou qu'il n'entrait pas dans les attributions du salarié.

Pour que la présomption joue, il faut et il suffit que les circonstances de l'affaire rendent légitime la croyance de l'autre partie en la réalité des pouvoirs que s'attribue, de manière expresse ou implicite, son partenaire contractuel. La présence dans les locaux, l'accès téléphonique par la ligne indiquée par l'entreprise dans les " pages jaunes", la carte d'identité professionnelle voire la simple carte de visite, d'entreprise, sur laquelle le nom figure, la dénomination du poste occupé : directeur financier ; directeur commercial, etc. suffiront-ils, comme actuellement pour conférer une sécurité juridique excellente aux actes correspondant, selon la pratique habituelle, aux fonctions ainsi dénommées ?

Quant aux transactions dans l'espace virtuel, il est difficile d'apercevoir les " circonstances " qui permettront de se fier à la qualité et aux pouvoirs allégués si des certificats sont aisément accessibles. L'absence même de certificat pourrait donner à la transaction un caractère douteux et risqué empêchant le tiers contractant de se prévaloir de l'acte qu'il avait cru conclure avec une personne dûment habilitée. Toutefois, cela ne paraît pas absolument exclu, ainsi lorsque le contact aura été établi à partir du site Internet de l'entreprise... ou que l'intéressé se sera identifié grâce aux mentions d'un certificat certes présenté comme non qualifié mais émanant d'une autorité de bon aloi, telle une chambre de commerce, une banque ou un greffe, le tiers contractant sera peut-être admis à se prévaloir de la vraisemblance des pouvoirs de son contractant qui résulterait de ces circonstances.

ANNEXE TECHNIQUE : LES FORMATS DES CERTIFICATS D'ATTRIBUTS

Avec les certificats d'attribut la notion "un certificat permet de lier une clé à une identité" est étendue pour considérer que le rôle d'un certificat est plus général et consiste à attribuer des permissions au possesseur d'une clé. Un certificat d'attribut contient donc un ensemble d'attributs qui donnent des informations (éventuellement à caractère confidentiel) sur les privilèges du possesseur du certificat.

Les certificats d'attribut servent à indiquer les règles du contrôle d'accès. C'est une structure numérique signée par une AA. Cette structure relie les attributs à un ou plusieurs certificats afin d'attribuer des autorisations ou des droits. Par exemple un certificat d'attribut sera la représentation numérique d'un visa et le certificat d'identification le passeport.

1 Le format X509 du certificat d'attribut

Le certificat d'attribut est standardisé par l'IETF (RFC 3281). Sa syntaxe se présente sous la forme suivante :

```

AttributeCertificate ::= SEQUENCE {
    Acinfo             AttributeCertificateInfo
    signatureAlgorithm AlgorithmIdentifier,
    signatureValue     BIT STRING
}

AttributeCertificateInfo ::= SEQUENCE {
    Version             AttCertVersion -- version is v2,
    holder              Holder,          issuer
AttCertIssuer,
    signature           AlgorithmIdentifier,
    serialNumber        CertificateSerialNumber,
    attrCertValidityPeriod AttCertValidityPeriod
    attributes          SEQUENCE OF Attribute,
    issuerUniqueID      UniqueIdentifier OPTIONAL,
    extensions          Extensions      OPTIONAL
}

```

Le composant majeur du certificat d'attributs réside dans ces données du certificat :

```

Holder ::= SEQUENCE {
    BaseCertificateID  [0] IssuerSerial OPTIONAL,
    -- the issuer and serial number of
    -- the holder's Public Key Certificate
    entityName        [1] GeneralNames OPTIONAL,
    -- the name of the claimant or role
    objectDigestInfo  [2] ObjectDigestInfo OPTIONAL
    -- used to directly authenticate the holder,
    -- for example, an executable}

Attribute ::= SEQUENCE {
    type              AttributeType,
    values            SET OF AttributeValue
    -- at least one value is required
}

AttributeType ::= OBJECT IDENTIFIER

AttributeValue ::= ANY DEFINED BY AttributeType

```

Les autres composants du certificat d'attributs sont les suivants :

```

AttCertVersion ::= INTEGER {v1(0), v2(1) }

AttCertIssuer ::= CHOICE {
    v1Form    GeneralNames, -- MUST NOT be used in this
                                -- profile
    v2Form    [0] V2Form      -- v2 only
}

V2Form ::= SEQUENCE {
    IssuerName          GeneralNames OPTIONAL,
    baseCertificateID  [0] IssuerSerial OPTIONAL,
    objectDigestInfo   [1] ObjectDigestInfo OPTIONAL
    -- issuerName MUST be present in this profile
    -- baseCertificateID and objectDigestInfo MUST NOT
    -- be present in this profile
}

IssuerSerial ::= SEQUENCE {
    issuer          GeneralNames,
    serial          CertificateSerialNumber,
    issuerUID       UniqueIdentifier OPTIONAL
}

AttCertValidityPeriod ::= SEQUENCE {
    notBeforeTime  GeneralizedTime,
    notAfterTime   GeneralizedTime
}

```

Comme on extrait les attributs du certificat de signature pour les gérer dans certificat ad hoc, il est nécessaire de prévoir une liaison entre les deux certificats. Cette liaison est réalisée par le champ « holder ». Trois options pratiques sont possibles :

La première est recommandée et lie le certificat d'attributs avec le nom de l'émetteur du Certificat de signature et un numéro de série du certificat.

La seconde fait la liaison avec un nom (qui n'est pas nécessairement unique).

La troisième avec le condensé d'une information (hash value).

2 Le format XML du certificat d'attribut

Pour les services en ligne, l'encodage des certificats en format ASN.1 ou en « s-expressions » (proposition SPKI) n'est pas utile puisque les transactions se font via Internet. D'où cette proposition d'encoder les certificats au format XML (proposition de l'IETF).

Après trois ans de travail, le W3C vient de publier le XML Schéma. Avec ce standard, XML tourne la page de la gestion documentaire pour véritablement devenir le langage des données métier.

La structure de certificat d'attribut au format XML est la suivante :

```

<!-- *****
AttributeCertificate => CONTENT ELEMENT
***** -->
<!ELEMENT content (Issuer, Holder, Attribute+, Delegation )>
<!-- At least one attribute should always be present (+) or not (*) ? -->
<!-- Validity can be specified for the certificate (in the Holder Value)
and for each attribute-->
<!-- *****
CONTENT ELEMENT => elements
***** -->
<!ELEMENT Issuer EMPTY>
<!ATTLIST Issuer
%CertificateReference;
>
<!ELEMENT Holder EMPTY>
<!ATTLIST Holder
%CertificateReference;
%Validity; #IMPLIED
>
<!-- resource is not mandatory, depends on AttributeName signification --
>
<!-- not requested, for readable information -->
<!-- if no validity is specified... the certificate is forever valid! -->
<!ELEMENT Attribute EMPTY>
<!ATTLIST Attribute
AttributeName CDATA #REQUIRED
Resource CDATA #IMPLIED
AttributeDescription CDATA #IMPLIED
%Validity; #REQUIRED
>
<!ELEMENT Delegation EMPTY>
<!ATTLIST Delegation
Depth CDATA #IMPLIED
>
<!-- depth of delegation can be 0 (no delegatio), -->
<!-- -1 (infinite delegation), -->
<!-- >0 (depth of delegation path), -->
<!-- '1' means only direct child will have the ability to delegate -->

```

GLOSSAIRE

Autorité d'attributs (AA), *Attribute Authority (AA)* : Organisme ayant la confiance d'une ou plusieurs autres entités pour créer, attribuer et révoquer ou suspendre des certificats d'attributs. Une autorité de certification peut également être une autorité d'attributs. [ISO]

Autorité d'enregistrement (AE), *Registration Authority (RA)* : Organisme qui est responsable de l'identification et de l'authentification d'entités qui demandent un certificat, mais qui n'est ni l'autorité de certification ni l'autorité d'attributs. Une AE ne signe pas de certificat mais examine les pièces justificatives de l'entité qui demande le certificat. Elle ne donne l'ordre de certification à l'AC qui si elle considère les pièces justificatives conformes à l'usage qui veut être fait du certificat et conformément à la politique d'usage du certificat.

Certificat, *Certificate* : De façon générique c'est un objet informatique logique qui permet de lier de façon intangible une identité d'entité à certaines caractéristiques de cette entité. Lorsqu'une des caractéristiques est une clé publique, on parlera de certificat de clé publique. Si ce n'est pas le cas on parlera de certificat d'attributs. Le lien est créé par la signature de l'ensemble des données du certificat par la clé privée de l'autorité qui émet le certificat. [ISO]

Certificat d'attributs, *Attribute Certificate* : Ensemble composé de l'identité d'une entité et d'attributs (caractéristiques) de cette entité, rendus indissociables par la signature du certificat d'attributs avec la clé privée de l'autorité de certification qui émet le certificat d'attributs. [ISO]

Certificat référencé : certificat fourni par des autorités de certification du marché et que l'administration accepte pour la sécurisation des téléprocédures après un audit technique²².

Authentification : Processus visant à établir de manière formelle et intangible l'identification des parties à un échange ou une transaction électronique.

Autorité de certification : Organisme ayant la confiance d'une ou plusieurs entités pour créer, attribuer et révoquer ou suspendre des certificats de clés publiques.

Chiffrement : Processus de transformation de données pour les rendre incompréhensibles par un tiers non autorisé.

Clé privée : Partie non divulgable, et donc à usage exclusif de son détenteur, du jeu de clés nécessaire au fonctionnement d'un algorithme cryptographique asymétrique.

Clé publique : Partie divulgable du jeu de clés nécessaire au fonctionnement d'un algorithme cryptographique asymétrique.

Cryptographie : Discipline incluant les principes, moyens et méthodes de transformation des données, pour cacher leur contenu sémantique, pour empêcher leur utilisation non autorisée ou pour permettre la détection des modifications.

La cryptographie conçoit des algorithmes que l'on souhaite inviolables.

²² http://www.minefi.gouv.fr/dematerialisation_icp/dematerialisation_declar.htm

Délégation de compétences (droit administratif) : Mode d'organisation destiné à assurer une bonne répartition des pouvoirs dans l'administration. Une autorité administrative (le délégant) délègue à une autre autorité administrative (le délégataire) une ou plusieurs compétences que les textes permettent de déléguer.

Délégation de pouvoirs (droit des sociétés) : Transmission des pouvoirs, des responsabilités, de l'autorité de commandement et/ou de leurs instruments ou marques juridiques (délégation de signature) à une autre personne physique (le délégataire).

Délégation de signature : Transmission du simple pouvoir de signer en lieu et place de la personne qui l'accorde.

Habilitation : Droit accordé à un individu d'accéder à des informations dont le niveau de sécurité est inférieur ou égal à un niveau déterminé.

ICP (Infrastructure à clés publiques) ou IGP (Infrastructure de Gestion des Clés): Ensemble de composants, fonctions et procédures dédiées à la gestion de clés et de certificats utilisés par les services de sécurité basés sur de la cryptographie à clé publique.

Identification : Opération de vérification consistant à s'assurer sans ambiguïté de l'identité de l'utilisateur d'un service.

IETF (Internet Engineering Task Force) : Ensemble de groupes de travail qui développent les nouveaux standards pour l'Internet.

Mandat : Convention par laquelle une personne (le mandant) donne pouvoir à une autre personne (le mandataire) d'effectuer un acte en son nom et pour son compte, en l'y représentant.

Mandataire : Personne qui reçoit le mandat d'effectuer un acte pour le compte d'un tiers.

Mandataire social : Personne chargée d'administrer une société.

Signature électronique (electronic non handwritten signature) : Fonction mathématique consistant à calculer une valeur à partir des données d'un message et de la clé privée de son signataire de façon à garantir l'intégrité desdites données et la non-répudiation de la transaction.

Théorie du mandat apparent : Théorie selon laquelle une société peut être engagée par toute personne, même non habilitée régulièrement, si les tiers avec qui cette personne a traité ont légitimement cru que celle-ci disposait des pouvoirs nécessaires.

Sources : Rapport sur l'archivage électronique - Terminologie bancaire et financière du Comité français d'organisation et de normalisation bancaire.