Projet ICare

Régime juridique prospectif du certificat d'attributs

Référence : ICARE/CAB/TPC/DOC_18/v1
Type : Note de travail
Diffusion : Générale

Date : 05/11/2002
Titre : **ICare – Régime juridique prospectif du certificat d'attributs**

Sous-Projet :
Auteur(s) : Thierry Piette-Coudol, avocat

Résumé :
Cette note constitue une première réflexion sur le régime juridique susceptible de s'appliquer aux certificats d'attributs, en extrapolation des règles s'appliquant aux certificats de signature.

1 Introduction

Le composant technique connu sous le nom de *certificat d'attribut* ne possède aucun régime juridique à l'heure actuelle. Pourtant cet élément est fondamental dans la démarche de recherches et développement du projet Icare en complément des certificats électroniques de signatures, également étudiés et mis en pratique.

Une des objectifs d'ICare est de développer la complémentarité des deux types de certificats sans ignorer le contexte juridique des certificats électroniques et des signatures électroniques. Mais si la loi détermine le régime juridique de la signature électronique et des certificats qui interviennent en support de celle-ci, rien n'est encore dit sur le régime juridique des certificats d'attributs. Comme les certificats et les signatures possèdent une importante facette juridique, les certificats d'attributs doivent montrer également ce caractère. L'analyse juridique doit suppléer, ici et pour l'instant, à la carence du droit positif.

L'objet de ce document est de procéder à une réflexion juridique prospective des certificats d'attributs en regard de la réglementation encadrant les éléments et composants électroniques connexes.

Il importe d'approcher la notion de certificat d'attribut (2.) avant de tenter de circonscrire son régime juridique (2). La finalité de ce document étant juridique, les éléments basiques d'analyse sont empruntés au droit existant.

2 Approche de la notion d'attributs et de certificat d'attributs

Tout d'abord, on dira qu'il n'existe à ce jour aucun texte juridique qui établisse le régime juridique du certificat d'attributs ni même qui mentionne son existence. L'approche de la notion ne peut être que spéculative. Aussi commencera-t-on par se pencher sur la notion d'attributs puis de certificats d'attributs.

2.1 Notion d'attributs

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 et 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*. Les attributs sont visibles dans la liste des composants des certificats qualifiés dressée par l'article 6-I du Décret précité :

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 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 Droit 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)).

Le premier attribut, fonction du titulaire, est simple à saisir et ouvre immédiatement une large gamme d'utilisations pratiques, ainsi :
- Cas 1 : les téléprocédures, émises par une entreprise en direction d'une administration, est effectué par un déclarant. Ce déclarant peut être membre ou non de l'entreprise. Dans tous les cas, il doit posséder un mandat pour déclarer. La question posée est celle de son *habilitation*.
- Cas 2 : certaines professions ou certains secteurs désireront être informés de la qualité professionnelle du titulaire du certificat par rapport à l'opération en cours. C'est un besoin proche du précédent. On peut penser aux banques, surtout lorsqu'elles ont émis le certificat correspondant.
- Cas 3 : la validité de certains actes juridiques dépend moins de la signature du document que de la qualité du signataire : seul l'expert-comptable peut signer (certifier) les comptes annuels de l'entreprise, seul le notaire peut dresser et signer un acte notarié, etc. C'est le cas de tous les professionnels assemblés dans un ordre professionnel en ce qui concerne ce qu'on peut appeler une *signature institutionnelle*[1].

[1] 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 réelle, c'est la même signature. Dans le monde électronique, serait-ce deux signatures... ou deux certificats ?

Le second attribut, le montant maximal des transactions, est moins simple. Il est aisément incompréhensible pour les juristes qui n'ont pas participé directement à l'élaboration de la Directive européenne dont le droit français à tiré sa législation sur la signature. Le texte parle de "*montant maximum des transactions pour lesquelles ce certificat peut être utilisé*". Au bilan, le certificat électronique permettrait i) de valider l'appartenance d'une clé publique à quelqu'un, ii) pour servir de support à la vérification d'une signature électronique, iii) à finalité juridique, iv) sur un message électronique de type acte sous-seing privé, v) dont la valeur maximale de la transaction, s'il y a lieu, ne doit pas dépasser un certain montant. Un raisonnement bien alambiqué ! Cela explique peut-être que les professionnels a priori concernés ne semblent pas toujours intéressés. Ainsi les banques pourraient-elles s'intéresser davantage à la vérification de la qualité professionnelle de la personne dans l'entreprise dont le pouvoir d'engagement financier dépend de sa position dans la hiérarchie. Bref, on revient facilement au cas 2 exposé ci-dessus.

2.2 Notion de certificat d'attributs

Le *certificat d'attribut* s'il vise les attributs est également un *certificat électronique* au sens du droit. Les textes de niveau légal ne connaissent pas la notion de certificat électronique, prise isolément. Ce n'est qu'à l'occasion de la mise en œuvre de la signature électronique, 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 précité 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".*

En faisant abstraction du contexte signature électronique, on peut extraire de cette définition les éléments essentiels d'un certificat électronique : c'est un fichier ou un message électronique qui atteste du lien entre une donnée et une autre.

La question basique est la suivante : pourquoi et comment gérer les certificats d'attributs, puisque les attributs peuvent être portés directement dans le certificat de signature ?

Comme l'ont montré les résultats d'une étude entreprise par le GIP-MDS, les attributs ne sont pas incorporés dans le certificat de signature parce que :

- Au niveau logique, la durée de vie des attributs est différente de celle du certificat. En effet, si un directeur commercial d'entreprise perd sa position dans la hiérarchie interne, ces attributs sont invalidés et donc 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.

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

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

AttributeCertificateInfo ::= SEQUENCE {
     Version                   AttCertVersion DEFAULT v1,
     owner                     Owner,
     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 cet endroit du certificat :

```
Owner ::= SEQUENCE {
    baseCertificateID   [0] IssuerSerial OPTIONAL,
                    -- the issuer and serial number of
                    -- the owner's Public Key Certificate
     entityName           [1] GeneralNames OPTIONAL,
                    -- the name of the claimant or role
     objectDigestInfo    [2] ObjectDigestInfo OPTIONAL
                       -- if present, version must be v2
}
```

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

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

AttCertIssuer ::= SEQUENCE {
       issuerName              GeneralNames  OPTIONAL,
       baseCertificateId   [0] IssuerSerial OPTIONAL
           }

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

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

Enfin, le certificat d'attribut n'est pas un électron libre. Puisqu'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 « owner ». 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).

3 Régime juridique prospectif du certificat d'attributs

Dans les cas envisagés plus haut, l'approche est juridique. Aussi le certificat d'attributs connaîtra-t-il un régime juridique par contagion ou à titre accessoire : ce sera par exemple, l'attribut "qualité professionnelle" qui sera extirpé du certificat X.509 de signature pour être géré et recevoir sa validation par le certificat d'attribut. Pour produire de pleins effets juridiques, le certificat de signature doit être qualifié. Par contagion, le certificat d'attributs pourrait devoir l'être.

Comme tout certificat qualifié, le certificat d'attribut devra respecter le contenu listé à l'article 6-I du Décret, à l'adaptation près. Il est nécessaire de tenter l'assimilation du régime du certificat d'attributs avec celui du certificat de signature et ce, à partir de la grille d'analyse ci-dessous.

Contenu du certificat qualifié	**Interprétation relative au certificat d'attributs**
a) Une mention indiquant que ce certificat est délivré à titre de certificat électronique qualifié	A reconsidérer si la syntaxe du C.A. le permet
b) L'identité du prestataire de services de certification électronique ainsi que l'Etat dans lequel il est établi	Mention obligatoire
c) Le nom du signataire ou un pseudonyme, celui-ci devant alors être identifié comme tel	Mention obligatoire
d) Le cas échéant, l'indication de la qualité du signataire en fonction de l'usage auquel le certificat électronique est destiné	Rubrique absente, par définition
e) Les données de vérification de signature électronique qui correspondent aux données de création de signature électronique	Cette mention devra être remplacée par celle de la qualité professionnelle
f) L'indication du début et de la fin de la période de validité du certificat électronique	Mention obligatoire
g) Le code d'identité du certificat électronique	Mention obligatoire
h) La signature électronique sécurisée du prestataire de services de certification électronique qui 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.	Rubrique absente, par définition