Projet ICare

Aspects réglementaires des certificats électroniques

Référence : ICARE/CAB/TPC/DOC_33/v1
Type : Document
Diffusion : Membres du consortium

Date : 06/02/2003
Titre : **ICare – Aspects réglementaires des certificats électroniques**

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

Objet :
Cette note tente d'analyser le statut des certificats électroniques (qualifiés et référencés) dans le contexte réglementaire.

TABLE DES MATIERES

1. Introduction

La présente note constitue une analyse juridique sur la notion de certificat électronique telle qu'elle est récemment apparue dans le droit français.

2. Le certificat et les autres composants de la Signature Electronique

Il s'agit ici reprendre ici les éléments techniques qui composent la signature électronique, mais sous l'angle du droit dont l'approche est différente de celle de la technique.

La signature électronique retenue par les juristes est basée sur la cryptographie asymétrique qui présente la particularité de mettre en œuvre un *bi-clé* cryptographique formé d'une *clé privée* et d'une *clé publique*. Les clés sont définies par divers textes juridiques, la Directive 199/93[1] au niveau européen et le Décret d'application de l'article 1316-4 du Code Civil[2], pour le droit interne. Les clés répondent aux définitions de la façon suivante :

Directive Européenne	Décret SE_{SES}
Données afférentes à la création de signature», des données uniques, telles que des codes ou des clés cryptographiques privées, que le signataire utilise pour créer une signature électronique ;	*Données de création de signature électronique: les éléments propres au signataire, tels que des clés cryptographiques privées, utilisés par lui pour créer une signature électronique ;*
Données afférentes à la vérification de signature, des données, telles que des codes ou des clés cryptographiques publiques, qui sont utilisées pour vérifier la signature électronique ;	*Données de vérification de signature électronique : les éléments, tels que des clés cryptographiques publiques, utilisés pour vérifier la signature électronique ;*

Le "tracé" de la signature est réalisé par un composant spécialisé, matériel ou logiciel, qualifié de *dispositif de création de signature*. Les textes juridiques en donnent la définition suivante :

Directive Européenne	Décret SE_{SES}
Dispositif de création de signature», un dispositif logiciel ou matériel configuré pour mettre en application les données afférentes à la création de signature ;	*« Dispositif de création de signature électronique » : un matériel ou un logiciel destiné à mettre en application les données de création de signature électronique ;*

Le Dispositif de création met en effet en application la clé privée, ce qui ne donne pas vraiment d'information sur le fonctionnement et l'utilité du dispositif. En fait, le dispositif est chargé de procéder au hachage du message électronique à signer. Par opposition à la signature manuscrite qui est un graphisme propre au signataire apposée sur le papier, la signature électronique est un *condensat* du message que l'auteur personnalise et protège en le chiffrant par le biais d'un code qui lui est personnel, la clé privée. Il en résulte que le dispositif contient une fonction de hachage et une fonction de chiffrement, cette dernière ne pouvant être activée que si on lui fournit une clé privée. La question du tirage des clés est discrètement traitée par la loi. Le tirage des clés est généralement effectué par le certificateur. A défaut, le Dispositif est susceptible d'assurer également cette fonction, dans une phase d'initialisation du dispositif. La clé publique est envoyée chez un tiers de confiance particulier, le certificateur. Cette entité appelée autorité de certification dans la technique est baptisée *prestataire de services de certification*. Cette appellation juridique qui est plus lourde que la dénomination technique permet toutefois d'éviter une incompréhension sur le fondement de la mission du certificateur. Le certificateur n'est pas une *autorité* qui procède de l'Etat ou de la Nature ; c'est un prestataire de service lié à son client par un contrat de service. Le *prestataire de service de certification*, auquel le droit français ajoute "*électronique*" répond aux définitions suivantes :

[1] Directive 1999/93/CE du parlement européen et du conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques (JOCE du 17.1.2002 n°L 15/24) .

2 Décret n°2001-272 du 30 mars 2001 modifié pris pour l'application de l'article 1316-4 du Code Civil et relatif à la signature électronique (JO du 31 mars 2001 p. 5070) .

Directive Européenne	Décret SE_{SES}
Prestataire de service de certification», toute entité ou personne physique ou morale qui délivre des certificats ou fournit d'autres services liés aux signatures électroniques ;	*Prestataire de services de certification électronique » : toute personne qui délivre des certificats électroniques ou fournit d'autres services en matière de signature électronique*

Le certificateur émet un certificat contenant, entre autres données, la clé publique du signataire qui répond aux définitions suivantes :

Directive Européenne	Décret SE_{SES}
«certificat», une attestation[3] électronique qui lie des données afférentes à la vérification de signature à une personne et confirme l'identité de cette personne ;	*« Certificat électronique » : un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire ;*

Enfin chez le destinataire du message signé, le dispositif de vérification extraira la clé publique du certificat pour procéder au contrôle de la signature. Le dispositif est ainsi défini :

Directive Européenne	Décret SE_{SES}
«dispositif de vérification de signature», un dispositif logiciel ou matériel configuré pour mettre en application les données afférentes à la vérification de signature.	*Dispositif de vérification de signature électronique » : un matériel ou un logiciel destiné à mettre en application les données de vérification de signature électronique.*

3. La Typologie des certificats

3.1. Le certificat selon la technique : le certificat X.509

3.1.1. Origine et définition

X.509 est le cadre d'authentification appartenant aux services d'annuaires électroniques X.500. Les deux Recommandations X.509 et X.500 font partie de la série X des normes internationales adoptées conjointement par l'Union Internationale des Télécommunications (UIT) et par l'Organisation Internationale de Normalisation (ISO). La norme X.500 est conçue pour fournir des services d'annuaires aux grands réseaux d'ordinateurs. L'annuaire X.500 est similaire à un répertoire de téléphone où, à partir du nom d'une personne, on peut trouver des informations complémentaires sur cette personne. Cependant X.500 fournit plus que les nom, adresse et numéro de téléphone. Une entrée au répertoire peut contenir un ensemble d'attributs, tels que le nom de l'entreprise qui emploie cette personne, sa qualification professionnelle et l'adresse email, etc. D'autre part outre les personnes et les entreprises, une entrée X.500 peut contenir des identifiants d'ordinateurs, de centres serveurs, d'imprimantes ou de pays et d'administrations. Enfin elle peut contenir un certificat de clé publique.

X.509 fournit un cadre d'Infrastructure à clé publique pour authentifier les services X.500. La recommandation a été créée pour remplacer le système des mots de passe et des numéros personnels d'identification qui peuvent être percés à jour par de multiples attaques mises au point par les fraudeurs comme la divulgation externe, l'estimation et la relecture, l'espionnage des systèmes et la compromission du système hôte. Une première version de X.509 est parue en 1988 et a été rapidement adoptée par de grandes firmes de niveau mondial ou par de grands réseaux comme Visa et MasterCard. La version 3 de X.509 qui permet de doter le certificat d'extensions a été adoptée par l'IUT et l'ISO. Désormais un certificat peut contenir une large quantité d'informations, qui va au-delà de la fourniture de la clé, comme l'algorithme à utiliser ou le certificat de date

3 On s'étonne devant les termes employés par les rédacteur. Le terme fonctionnel *attestation* devrait céder le pas à un terme plus matériel, "message électronique" ou "fichier" par exemple. Si le décret français précise utilement que le certificat est électronique, pourquoi le certificat est-il un document ? Ce terme encore peu usité en droit français (qui a préféré le terme écrit jusqu'à la loi n°2000-230) renvoie inévitablement à un écrit-papier.

d'expiration. D'autres informations pourraient être volontaires et dépendraient du but dans lequel la clé est utilisée et du niveau de confiance requis. Selon la définition de l'ISO, un certificat est :
"*un objet informatique qui permet de lier de façon intangible une identité d'entité à certaines des caractéristiques de cette entité*".

Les champs de base d'un certificat ont été définis dès la première version de la norme. Ce sont les suivants :
- Version
- Numéro de série
- Informations sur la signature du certificat par l'AC (algorithmes et paramètres)
- Nom du fournisseur du certificat
- Période de validité du certificat
- Nom du porteur de certificat
- Informations sur la clé publique (valeur de la clé publique, algorithme et paramètres).

3.1.2. La diversité des certificats techniques

Selon la définition de l'ISO, le certificat de base 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. Au point de vue technique, les principaux certificats sont :
- Le certificat d'attribut : un 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 (définition ISO).
- Le certificat d'identité : un ensemble composé de l'identité d'une entité et d'une clé publique asymétrique (avec d'autres informations de gestion), rendus indissociables par la signature du certificat avec la clé privée de l'autorité de certification qui émet le certificat (définition ISO).
- Le certificat de clé publique : Processus de création d'un lien intangible (certificat) entre l'identité d'une entité et sa clé publique ou entre l'identité d'une entité et ses attributs (Définition ISO).

3.2. La vision juridique des certificats

Il s'agit naturellement de la vision juridique du droit interne où les certificats sont définis par le Décret n°2001-272 du 30 mars 2001. Cependant on constate l'existence d'une autre catégorie de certificat dit référencé.

3.2.1. Le certificat qualifié de la SES

Le Décret n°2001-272 précité définit les certificats en support d'une signature électronique de l'article 1316-4 du Code civil de la façon suivante :

> *"Certificat électronique" : un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire.*

Cependant le Décret stipule que le procédé de signature électronique qui emporte le maximum d'effets juridiques (présomption de fiabilité) est composé au niveau technique d'un logiciel de création de signature et d'une prestation de certification. Selon l'article 2 du même Décret :
"La fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve contraire lorsque ce procédé met en œuvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié."

Ce certificat montre les caractéristiques suivantes :

> *"Certificat électronique qualifié": un certificat électronique répondant aux exigences définies à l'article 6.*

Selon l'article 6-I du décret, un certificat électronique qualifié doit comporter :

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.

Outre le contenu qui lui est assigné, le certificat électronique doit être porté à la qualification. La qualification du certificat sera acquise si le PSCE qui l'émet est lui-même *qualifié*, d'où l'arrêté du 30 mai 2002 annoncé par l'article 7 du décret précité. La qualification, qui vaut présomption de conformité à ces exigences, est délivrée par les organismes ayant reçu à cet effet une accréditation délivrée par une instance désignée par arrêté du ministre chargé de l'industrie[4].

3.2.2. Le certificat référencé des téléprocédures

A la mi-1999, le Ministère des Finances (MEFI) lançait un premier appel d'offres en vue de la préparation du cadre d'échanges électroniques nécessaires aux *téléprocédures*[5] c'est-à-dire les déclarations que les entreprises peuvent produire aux administrations aujourd'hui par voie télématique. Sur ce point, le Ministère offrira la possibilité aux entreprises de déclarer par le Web, mais à condition de sécuriser les échanges. Naturellement la sécurisation des échanges aura une dimension particulière puisque les échanges électroniques visent en définitive à opérer une déclaration administrative et présentent une dimension de droit administratif indéniable. Compte tenu des sanctions qui peuvent peser sur les déclarants qui ne se sont pas acquittés dans les délais de la formalité déclarative (et du paiement qui peut y être associé), le MINEFI accepte les AC du marché. Des exigences sont néanmoins formulées puisque la téléprocédure doit mettre en œuvre un certificat *référencé*. Une entité spécialisée audite les AC du commerce pour faire la liste de ceux qui répondent aux exigences dans le cadre d'une procédure spécifique dite *référencement*[6].

Le texte de base pour les certificats référencés n'est ni une loi ni un décret mais un recueil de spécifications techniques nommés Politique de Certification - type. Une Politique de certificat (PC) (*Certificate Policy*) est définie par le protocole X.509 de la façon suivante : "*Un ensemble dénommé de règles qui indique l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'application avec des exigences de sécurité*". Les certificats électroniques comprennent parmi informations contenues l'appellation ou le numéro d'identification de la Politique visée. En plaçant cette mention, l'autorité de certification s'engage à ce que le certificat ait été produit dans le respect des stipulations de cette Politique. Pour le MINEFI, la version courante de la PC est la version 3.A du 23 janvier 2002 qui précise dans son chapitre 2. présentation générale de la pc-type les sources techniques du document :

Cette PC version de la PC-Type a été conçue sur la base des documents suivants :
- *La PC-type v2.0*
- *Le document « Procédures et Politiques de Certification de Clés (PC²) » émis par*
- *la Commission Interministérielle pour la Sécurité des Systèmes d'Information*
- *(CISSI)*
- *Le RFC 2527 "Certificate Policy and Certification Practises Framework".*

Le document intitulé "*Politique de certification-type*" émane du Ministère de l'Economie, des Finances et de l'Industrie. Cette Politique a été rédigée à partir du guide spécialisé intitulé "*Procédures et Politiques de Certification de Clés*" (ou PC2) de la Commission Interministérielle pour la Sécurité des Systèmes d'Informations (CISSI). Pour différencier ce document des autres instruments des ICP, il est précisé que la PC établit ce à quoi il faut se conformer lors de la gestion des certificats concernés, alors que la déclaration relative

[4] Cf. Notre DOC_12 *La qualification des PSCE – l'arrêté du 31 mai 2002.*

[5] Les *téléprocédures* sont définies par un rapport administratif de même nom dont certains éléments ont été précisés par le Groupe COSIFORM-ICP qui a étudié en 1997-1998 l'Infrastructure à clé publique (ICP) sous l'angle du secteur public.

[6] Pour procéder au référencement des services des ACs, l'Agence Autorité du MEFI sous-traite les opérations à une Entité d'Audit et de Référencement (EAR) de son choix qui n'a partie liée avec aucune des ACs. L'EAR a pour mission de référencer les certificats utilisables pour les échanges dématérialisés avec les services du MINEFI. Au cours de cette mission, l'EAR peut être conduite à un contrôle, par exemple chez l'AC ou son OSC. Le contrôle de conformité portera sur l'identification et l'authentification, les besoins opérationnels, les contrôles de sécurité physique, des procédures et du personnel, les contrôles de sécurité, les profils des certificats et LRC, les spécifications d'administration.

aux procédures de certification (appelé habituellement CPS ou DPC) décrit comment ces exigences sont atteintes dans la pratique.

Les déclarants des téléprocédures se font préalablement connaître par une autorité d'enregistrement. Les déclarants peuvent choisir de chiffrer leur message. Par cette initiative, le MINEFI vise exclusivement la dématérialisation des déclarations et des paiements de TVA des entreprises, d'une part et d'autre part, les déclarations d'échanges de biens (DEB). La finalité des opérations est la dispense de déclarations écrites. La technologie à employer consiste en des Echanges de Formulaires Informatisés (EFI) sécurisés sur Internet (Web) et dans certains cas pour reprendre l'existant d'Echanges de Données Informatisé (EDI). La sécurisation profitera des garanties offertes par la signature électronique et le chiffrement des messages, les deux moyens de sécurité mettant en œuvre des certificats électroniques issus d'autorités de certification.

3.2.3. L'usage respectif des certificats qualifiés et certificats référencés

Deux types de certificats coexistent au niveau réglementaire[7]. Malgré les hésitations de certains experts, ils ne se confondent pas. Ils se différentient comme le déclare le MINEFI sur son site[8] :

> *Le référencement doit être distingué de la qualification décrite au chapitre III du décret no 2001-272 du 30 mars 2001 relatif à la signature électronique. Le référencement est prononcé dans le cadre des téléprocédures du MINEFI et uniquement dans ce cadre. A ce titre, le MINEFI dégage toute responsabilité relative à l'usage des certificats référencés en dehors de ses téléprocédures. Le ministère agissant en tant qu'Agence Autorité prononçant les référencements de certificats de fournisseurs n'est pas, et ne prévoit pas d'être, dans le cadre du référencement, un organisme accrédité par une instance désignée par arrêté.*

La PC v3 apporte des indications complémentaires dans son préambule où on peut lire ce qui suit[9] :

Poursuivant un triple objectif de modernisation des services, de simplification des démarches administratives et de recherche d'une plus grande efficacité, le Ministre de l'Economie, des Finances et de l'Industrie a décidé la dématérialisation des déclarations de TVA et d'échanges de biens faites par les entreprises en offrant la possibilité à celles qui souhaitent en bénéficier de les transmettre sous forme électronique, via Internet...
La signature électronique et, le cas échéant, le chiffrement des informations apportent une solution au problème de sécurité que pose potentiellement tout transfert d'information par Internet.

Au regard du nombre d'usagers concernés mais également de la volonté clairement affirmée d'utiliser une solution d'usage à vocation générale et non spécifique à l'administration des Finances, le ministère a opté pour un système de signature à clés publiques faisant un large appel à des autorités de certification indépendantes de lui, dans un esprit d'ouverture favorisant la concurrence. Les déclarants auront ainsi la liberté d'utiliser des certificats numériques acquis auprès d'autorités de certification (fournisseurs de certificats) de leur choix, sous réserve que ces certificats répondent aux normes et standards du marché, et soient émis dans des conditions de fiabilité et de sécurité recevables par le MINEFI.

Ne pourront être acceptées et traitées que les télédéclarations s'appuyant sur ces certificats référencés et sur des signatures électroniques et moyens de confidentialité conformes aux caractéristiques décrites dans la PC-Type, sous réserve que parmi les options de chiffrement/déchiffrement possibles, celles choisies par les usagers soient disponibles sur les serveurs concernés.
Les certificats définis par la PC-Type sont strictement conformes aux normes et ne contiennent aucune information spécifique aux applications du MINEFI. Ils sont de ce fait banalisés et le MINEFI ne voit que des avantages à ce que les usagers s'en servent dans d'autres contextes que les téléprocédures.

Le MINEFI n'entend pas intervenir sur le marché de la certification par la voie réglementaire. Il se présente comme un «consommateur » de certificats répondant à ses besoins.
Le MINEFI n'entend pas s'ériger en autorité d'homologation des fournisseurs, ni en autorité d'accréditation au sens de la réglementation relative à la signature électronique (textes en annexe). Le référencement d'une famille de certificats doit ainsi être vu comme une licence d'accès aux applications du MINEFI.

Notre appréciation est en conséquence la suivante : le certificat électronique qualifié est juridique, tandis que le certificat numérique reste technique.

[7] Quoique la PC du MINEFI parle de "certificats numériques" pour les certificats référencés.
[8] Cf. http://www.minefi.gouv.fr/dematerialisation_icp/dematerialisation_declar.htm#sommaire
[9] C'est nous qui avons souligné.

4. Le Cycle de vie des certificats

Le certificat va posséder ce qu'on peut appeler un cycle de vie, car il est évident que de la même façon que le certificat va apparaître à la demande, les impératifs de sécurité interdisent qu'il ait une durée de vie permanente. Il s'agit naturellement ici de certificat en support d'une signature électronique et non d'une opération de chiffrement du message[10].

Les principales étapes du cycle de vie d'un certificat sont indiquées ci-dessous. Les modalités pratiques et les paramètres d'utilisation des certificats sont définis dans une *Politique de Certification* (PC). Les principales étapes du cycle de vie du certificat sont les suivantes. Pour chaque étape, un tableau met en coïncidence les caractéristiques des deux types de certificats.

4.1. Préalable juridique

Type	***Qualifié***	***Référencé***
Référence	Art.6-II.o	
Exigence	Informer par écrit la personne demandant la délivrance d'un certificat électronique : des modalités et des conditions d'utilisation du certificat.	Faire référencer une famille de certificat

4.2. L'enregistrement et la vérification d'identité

La phase préalable de l'enregistrement n'appartient pas au cycle technique du certificat mais doit être prise en compte car il existe une obligation réelle que l'identité du possesseur de la clé publique soit vérifiée ou établie par une tierce personne[11].

Type	**Qualifié**	**Référencé**
Référence	Art.6-II.m	*4.2.3 Dossiers de demande de certificats individuels***.**
Exigence	Vérifier, d'une part, l'identité de la personne à laquelle un certificat électronique est délivré, en exigeant d'elle la présentation d'un document officiel d'identité	L'AE acceptera seulement les demandes de certificat appuyées par des dossiers constitués de pièces justificatives fiables tels que décrits ci-dessous. Ces dossiers de demandes diffèrent selon qu'il s'agit de certificats individuels ou de certificats d'entreprise.
Référence	Art.6-II.m	4.2.3.2 Dossier de demande de certificats d'entreprise
Exigence	... d'autre part, la qualité dont cette personne se prévaut et conserver les caractéristiques et références des documents présentés pour justifier de cette identité et de cette qualité	Le dossier doit comprendre : (...) - un mandat signé par un représentant de l'entreprise désignant la personne physique à qui le certificat doit être délivré. Ce mandat doit être signé pour acceptation par la personne physique bénéficiaire;

Pour les certificats référencés, tout utilisateur doit procéder à l'enregistrement préalable de son nom. Les noms utilisés qui peuvent être ceux des entreprises ou ceux des particuliers sont décrits selon une forme normalisée (norme ISO/IEC 9594 Distinguished names). Ils doivent être explicites, distinctifs et susceptibles d'être imprimés (chaîne imprimable de type X.501). Au moment de l'enregistrement, le demandeur doit prouver la correspondance dans le bi-clé entre la clé privée et la clé publique pour laquelle il demande le certificat. Si l'AC ne tire pas le bi-clé, le demandeur pourra apporter cette garantie en signant la demande par sa clé privée.

[10] L'utilisation du certificat dans le cadre d'une signature électronique transparaît dans le certificat. Le choix (signature ou chiffrement) figurera dans le champ *KeyUsage* du certificat de clé publique de structure X.509. Le champ sera renseigné avec la donnée correspondante ou sera qualifié de *non critique* si le choix va à la mixité.

[11] L'étape intermédiaire du *tirage du bi-clé* ne sera étudiée ici.

4.3. La demande de certificat

La finalité du certificat est d'être remis au destinataire de la clé publique. Il faut qu'il soit préalablement créé à partir de la demande du détenteur de la clé publique. Cette demande peut être faite par une demande écrite ou par une demande électronique appelée *requête* également structurée selon le format X.509. Après que les informations à certifier aient été contrôlées (par exemple, la correspondance de la clé publique avec le porteur apparent de la clé), le certificat est créé avec une certaine durée de vie (de quelques semaines à quelques mois).

Pour les certificats référencés, la demande de certificat est présentée par écrit par une personne physique soit de son propre chef soit pour le compte de l'entreprise. Elle devra être accompagnée d'un dossier constitué de pièces justificatives comprenant :
- Une demande écrite signée par le chef d'entreprise ou son représentant.
- Un mandat signé par un représentant de l'entreprise désignant la personne physique à qui le certificat doit être délivré. Ce mandat doit être signé pour acceptation par la personne physique bénéficiaire.
- Un exemplaire des statuts de l'entreprise portant signature de ses représentants.
- Une pièce portant le numéro SIREN de l'entreprise (extrait Kbis ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Etablissements
- Deux justificatifs d'identité de la personne physique mandatée sous la forme de copies certifiées conformes selon les règles de la législation française (fiche individuelle d'état civil, photocopie certifiée conforme du permis de conduire, photocopie certifiée conforme de la carte d'identité nationale etc.)

Avant de décerner le certificat demandé, l'Autorité d'Enregistrement doit effectuer les contrôles suivants :
- établir l'identité du demandeur,
- vérifier l'autorisation des attributs demandés (lorsque cela est approprié),
- s'assurer que le demandeur a pris connaissance des modalités applicables d'utilisation du certificat,
- obtenir la clé publique du demandeur,
- s'assurer de la possession de la clé privée correspondante du demandeur.

Le décret est plus laconique qui indique dans son article 6-II-m) que le PSCE doit :

> *"Vérifier, d'une part, l'identité de la personne à laquelle un certificat électronique est délivré, en exigeant d'elle la présentation d'un document officiel d'identité, d'autre part, la qualité dont cette personne se prévaut et conserver les caractéristiques et références des documents présentés pour justifier de cette identité et de cette qualité*."

4.4. Confection du certificat électronique

Le certificat doit intégrer un certain nombre de mentions.

4.4.1. La nature du certificat

Type	***Qualifié***	***Référencé***
Référence	Art.6-I.a	
Exigence	Une mention indiquant que ce certificat est délivré à titre de certificat électronique qualifié ;	(?)

4.4.2. L'AC-PSCE

Type	***Qualifié***	***Référencé***
Référence	Art.6-I.b	7.1 Profil des certificats
Exigence	L'identité du prestataire de services de certification électronique ainsi que l'Etat dans lequel il est établi ;	Champ issuer (RFC 2549) = nom de l'AC contient le Distinguished Name (X.500) de l'AC qui a créé le certificat

4.4.3. Le nom du porteur

Type	*Qualifié*	*Référencé*
Référence	Art.6-I.c	7.1 Profil des certificats
Exigence	Le nom du signataire ou un pseudonyme, celui-ci devant alors être identifié comme tel ;	Champ subject (RFC 2549) = nom de l'abonné contient le Distinguished Name (DN) (X.500) de l'abonné

Les noms choisis pour désigner les porteurs de certificats référencés doivent être explicites. Le Distinguished Name (DN) doit être sous la forme d'une chaîne imprimable (printableString) de type nom X.501. Un nom distinctif (DN) doit être conforme aux besoins opérationnels et pour cela doit se composer au moins des éléments suivants pour un certificat individuel : Nom de pays (C), Nom usuel (CN) : ce champ doit contenir l'identité réelle du signataire ou son pseudonyme. Exemple : DN = { C=FR, CN= Jean Dupont}
(3.1.2 Nécessité d'utilisation de noms explicites).

4.4.4. La qualité du porteur de certificat

Type	*Qualifié*	*Référencé*
Référence	Art. 6-I.d	3.1.2 Nécessité d'utilisation de noms explicites.
Exigence	Le cas échéant, l'indication de la qualité du signataire en fonction de l'usage auquel le certificat électronique est destiné ;	Pour un certificat individuel, le DN de l'abonné peut aussi être spécifié par les attributs suivants : dNQualifier, OrganizationNames, organizationalUnitName postalAddress.

4.4.5. La clé publique du porteur

Type	*Qualifié*	*Référencé*
Référence	Art. 6-I.e	7.1 Profil des certificats
Exigence	Les données de vérification de signature électronique qui correspondent aux données de création de signature électronique ;	Champs selon RFC 2549 SubjectPublicKeyInfo Algorithm SubjectPublicKey contient l'identifiant de l'algorithme (OID) et la clé publique de l'abonné extensions

4.4.6. La période de validité du certificat

Type	*Qualifié*	*Référencé*
Référence	Art. 6-I.f	7.1 Profil des certificats
Exigence	L'indication du début et de la fin de la période de validité du certificat électronique	Champs selon RFC 2549 : validity notBefore notAfter période de validité du certificat contient les dates d'activation et d'expiration du certificat

4.4.7. Identification du certificat

Type	*Qualifié*	*Référencé*
Référence	Art. 6-I.g	7.1 Profil des certificats
Exigence	Le code d'identité du certificat électronique	Selon RFC 2549 Version = version du certificat contient la valeur entière 2 pour indiquer que le certificat est un certificat X.509v3 serialNumber = numéro de série unique du certificat contient une valeur entière pour indiquer le numéro de série du certificat. Cette valeur doit être unique pour chaque certificat émis par l'ICP

4.4.8. La signature de l'AC-PSCE

Type	*Qualifié*	*Référencé*
Référence	Art.6-I.h	7.1 Profil des certificats
Exigence	La signature électronique sécurisée du prestataire de services de certification électronique qui délivre le certificat électronique ;	Champ signature (RFC 2549) = signature de l'AC pour authentifier le certificat contient l'identifiant (OID) de l'algorithme utilisé par l'AC pour signer le certificat

4.4.9. L'utilisation du certificat

Type	*Qualifié*	*Référencé*
Référence	Art. 6-I.i	7.1 Profil des certificats
Exigence	Le cas échéant, les conditions d'utilisation du certificat électronique, notamment le montant maximum des transactions pour lesquelles ce certificat peut être utilisé.	Extension keyUsage. Cette extension définit l'utilisation prévue de la clé contenue dans le certificat. L'AC doit : inclure l'extension dans tous les certificats des abonnés ; indiquer l'usage prévu de la clé comme défini dans la PC gérer la criticité comme défini dans la PC

4.5. Révocation

Type	*Qualifié*	*Référencé*
Référence	Art. 6-II.c & 6-II.d	7.1 Profil des certificats
Exigence	Assurer le fonctionnement d'un service permettant à la personne à qui le certificat électronique a été délivré de révoquer sans délai et avec certitude ce certificat Veiller à ce que la date et l'heure de délivrance et de révocation d'un certificat électronique puissent être déterminées avec précision	Extension cRLDistributionPoints. Cette extension non critique identifie l'emplacement où l'utilisateur peut trouver une LCR. L'AC doit : inclure cette extension dans les certificats d'abonnés ; ne pas inclure cette extension dans les certificats auto-signés ; renseigner les champs directoryName et uniformRessourceIdentifier :

Le certificat est normalement périmé à l'issue de la période de validité prévue originellement, mais il peut l'être avant pour des raisons diverses. La plus caractéristique est la compromission de la clé privée. La révocation est alors directement faite dans les meilleurs délais par le PSCE ou est demandée par le détenteur par l'intermédiaire de l'AE. La révocation est portée à la connaissance de tous par publicité. Une *liste de révocation* (LCR) facilement accessible référence tous les certificats révoqués. La LRC est une liste horodatée des certificats révoqués, attestée par la signature de l'autorité de certification. Pour des raisons de même nature, une suspension d'un certificat peut être décidée et publiée dans une *liste de certificats suspendus*.

Le décret prévoit uniquement dans son article 6-II-c ce que doit faire en la matière le PSCE :

"Assurer le fonctionnement d'un service permettant à la personne à qui le certificat électronique a été délivré de révoquer sans délai et avec certitude ce certificat".

Pour les certificats référencés, lorsqu'un certificat a été révoqué, il est d'usage d'informer la communauté des utilisateurs que le certificat n'est plus valide. La révocation du certificat peut provenir des causes suivantes :

- les informations ou les attributs de l'abonné figurant dans son certificat ne sont plus en cohérence avec l'utilisation prévue du certificat et ce, avant l'expiration normale du certificat.
- il a été démontré que l'abonné n'a pas respecté les modalités applicables d'utilisation du certificat,
- la clé privée de l'abonné est suspectée de compromission,
- l'abonné ou une autre entité autorisée (hiérarchique par exemple), demande la révocation du certificat,
- le certificat du PSCE lui-même est révoqué (ce qui entraîne la révocation des certificats signés par la clé privée correspondante).

La demande de révocation est adressée par le titulaire du certificat au PSCE qui après vérification de l'identité du demandeur et de la réalité de la cause indiquée peut porter le numéro de référence du certificat dans une liste de révocation. Il n'y a pas de formes particulières prescrites pour la publication de la LRC.

4.6. Information sur le contexte d'utilisation du certificat

Le Décret prévoit dans son article 6-II-p que le PSCE doit :

"Fournir aux personnes qui se fondent sur un certificat électronique les éléments de l'information [modalités et des conditions d'utilisation du certificat, qualification ou non, modalités de contestation et de règlement des litiges] qui leur sont utiles".

Dans une PC traditionnelle, les "droits" de l'utilisateur du certificat sont précisés, à tel point que le destinataire du message électronique signé devient partie prenante de la PC. Cet engagement du destinataire est possible lorsque la PC, les certificats et les signatures conservent un cadre d'utilisation purement technique. Dans le monde juridique, cela semble difficile. Même si le destinataire, vérificateur de signature, peut consulter la PC via l'hyperlien qui doit figurer dans le certificat électronique, il n'est pas tenu de vérifier la signature électronique. De plus, il reste libre d'apprécier les effets juridiques attachés à l'acte signé quels que soient les résultats de a vérification de la signature.

4.7. Conservation

L'article 6-II-l du Décret indique les principes que le PSCE doit observer en la matière :

"Utiliser des systèmes de conservation des certificats électroniques garantissant que :

- *l'introduction et la modification des données sont réservées aux seules personnes autorisées à cet effet par le prestataire ;*
- *l'accès du public à un certificat électronique ne peut avoir lieu sans le consentement préalable du titulaire du certificat ;*
- *toute modification de nature à compromettre la sécurité du système peut être détectée".*

Parallèlement la question de l'archivage (chapitre 4.6. selon une structure de PC conforme à la RFC 2527) et de la journalisation des événements (chapitre 4.5 selon une structure de PC conforme à a RFC 2527) sont abondamment traités dans la PC[12].

[12] Voir notre DOC_4 *Archivage électronique (1) – les principes de la conservation juridique.*