Projet ICare

La notion d'A.C. et le Droit

Référence : ICARE/CAB/TPC/DOC_7/v1
Type : Note de travail
Diffusion : Générale

Date : 02/05/2002
Titre : **ICare – La notion d'AC et le Droit.**

Auteur(s) : Thierry Piette-Coudol, avocat

Résumé :
Cette note de travail décrit l'organisation et le fonctionnement des Autorités de Certification (appelées "Prestataires de Services de Certification Electronique" –PSCE-) selon les textes juridiques français.

TABLE DES MATIERES

1. Préambule

La présente note de travail présente une réflexion actualisée sur la notion d'autorité de certification face au Droit.

Cette contribution a vocation, avec d'autres contributions sur des thèmes complémentaires ou connexes, a être intégrée dans le document "*Etat de l'art – Déliverable 1.4.*", préparé par l'ENST dans le cadre du projet ICARE, plus particulièrement dans sa 5ème partie.

2. AC et PSCE

2.1. La liberté d'accès à la profession

Les prestataires de certification sont définis ainsi qu'il suit par le Décret no 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique. Définition de l'article 2-11° du décret : *Prestataire de services de certification électronique : toute personne qui délivre des certificats électroniques ou fournit d'autres services en matière de signature électronique".*

Aucune autorisation n'est nécessaire pour s'installer sur le marché comme PSC. Selon la Directive, favoriser la fourniture à l'échelle communautaire de services de certification sur des réseaux ouverts nécessitent que les prestataires de service de certification soient libres d'offrir leurs services sans autorisation préalable. Le marché intérieur permet aux prestataires de service de certification de développer leurs activités internationales en vue d'accroître leur compétitivité, et d'offrir ainsi aux consommateurs et aux entreprises de nouvelles possibilités d'échanger des informations et de commercer en toute sécurité par voie électronique indépendamment des frontières. Aussi l'article 3.1. dispose-t-il que : "*les Etats membres ne soumettent la fourniture des services de certification à aucune autorisation préalable."*

2.2. Les obligations professionnelles pesant sur les PSCE

2.2.1. Obligations professionnelles générales

Ces obligations générales sont issues de l'article 6-II du Décret. Le PSCE doit

- a] Faire preuve de la fiabilité des services de certification électronique qu'il fournit ;
- e] Employer du personnel ayant les connaissances, l'expérience et les qualifications nécessaires à la fourniture de services de certification électronique ;
- f] Appliquer des procédures de sécurité appropriées ;
- g] Utiliser des systèmes et des produits garantissant la sécurité technique et cryptographique des fonctions qu'ils assurent ;

Une autre obligation au demeurant bien compréhensible figure dans l'*annexe II Exigences concernant les prestataires de service de certification délivrant des certificats qualifiés*, celle qui consiste à *disposer des ressources financières suffisantes pour fonctionner conformément aux exigences prévues par la présente directive, en particulier pour endosser la responsabilité de dommages, en contractant, par exemple, une assurance appropriée.*

Pour des raisons de hiérarchie entre les normes juridiques, il n'était pas possible de l'inclure dans le décret et la loi modifiant le Code Civil ne s'y prêtait guère. La question sera traitée dans la Loi sur la Société de l'Information (LSI).

2.2.2. Obligations spécifiques au traitement des certificats

Selon le Décret, un prestataire de services de certification électronique doit satisfaire aux exigences suivantes :

- Assurer le fonctionnement, au profit des personnes auxquelles le certificat électronique est délivré, d'un service d'annuaire recensant les certificats électroniques des personnes qui en font la demande ;
- 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 ;
- Prendre toute disposition propre à prévenir la falsification des certificats électroniques ;
- Dans le cas où il fournit au signataire des données de création de signature électronique, garantir la confidentialité de ces données lors de leur création et s'abstenir de conserver ou de reproduire ces données ;
- Veiller, dans le cas où sont fournies à la fois des données de création et des données de vérification de la signature électronique, à ce que les données de création correspondent aux données de vérification ;
- Conserver, éventuellement sous forme électronique, toutes les informations relatives au certificat électronique qui pourraient s'avérer nécessaires pour faire la preuve en justice de la certification électronique.
- 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 ;
- S'assurer au moment de la délivrance du certificat électronique :
  - que les informations qu'il contient sont exactes ;
  - que le signataire qui y est identifié détient les données de création de signature électronique correspondant aux données de vérification de signature électronique contenues dans le certificat.

2.2.3. Autres obligations du décret

Le décret permet d'identifier des obligations accessoires :
- Confidentialité : il ne doit ni stocker ni copier les données afférentes à la création de signature de la personne à laquelle le prestataire de service de certification a fourni des services de gestion de clés.
- Rôle pédagogique : Avant d'établir une relation contractuelle avec une personne demandant un certificat à l'appui de sa signature électronique, le
- PSCE doit informer cette personne par un moyen de communication durable des modalités et conditions précises d'utilisation des certificats, y compris des limites imposées à leur utilisation, de l'existence d'un régime volontaire d'accréditation et des procédures de réclamation et de règlement des litiges. Cette information peut être faite sur papier ou par électronique, dans une langue aisément compréhensible. Des éléments pertinents de cette information doivent également être mis à la disposition, sur demande, des tiers qui se prévalent du certificat.

2.2.4. Obligations issues d'autres textes

2.2.4.1. La déontologie

Si la certification électronique n'est pas une opération aussi solennelle qu'on pourrait s'y attendre, un semblant de déontologie professionnelle serait la bienvenue. D'une part, les PSCE devront respecter les principes fixés par les autorités publiques via la procédure d'accréditation et/ou par les utilisateurs via les Politiques de Certification des PKI. Ils pourraient également se doter de leurs propres règles professionnelles qui seraient fortement teintées de déontologie. D'autre part, l'utilisateur isolé de service de certification n'aura comme ultime rempart en cas de litige que des règles déontologiques.

Le Livre Blanc de IALTA s'est risqué dans cette matière. Pour lui, la déontologie présente l'avantage et la force d'être un ensemble de règles édictées par des professionnels qui précise le comportement du professionnel dans l'exercice de son activité. La déontologie représente un engagement des professionnels quant à la manière dont ils opèrent ; elle est ainsi un gage de sécurité. La règle déontologique est produite par ceux qui connaissent le mieux le fonctionnement de leur activité ; elle peut être modifiée et complétée plus vite que le processus législatif. La faculté pour un professionnel d'adhérer ou non à un code de conduite crée une distinction entre les intervenants et par là, constitue une protection pour les consommateurs, utilisateurs et clients qui peuvent choisir les professionnels avec lesquels ils souhaitent travailler.

Comme la déontologie doit être efficace, les autorités qui l'élaboreront devront jouir d'un certain statut ou disposer d'un pouvoir de sanction ; ce pouvoir pouvant se manifester par une sanction disciplinaire, une publicité

négative, une exclusion d'un groupe. Un groupe de professionnels devra s'ériger en une entité qui définira les principes à respecter, en déduira des règles de conduite et sera à même de les faire respecter. Cette entité, lors de la phase d'élaboration des règles de conduite, devrait regrouper ou impliquer toutes les parties concernées : les professionnels, les tiers de confiance, les opérateurs, les commerçants, et les consommateurs. Ils pourraient mettre au point une charte qu'ils s'engageraient à respecter. Ce serait le point de départ d'une démarche déontologique. Les opérateurs pourraient proposer un contrat-type labellisé, et respecter un cahier des charges-type. Ils pourraient encore s'engager à appliquer un code de conduite.

Des travaux sont actuellement encours sur la déontologie à la Fédération Nationale des Tiers de Confiance (FNTC, www.fntc.org).

2.2.4.2. L'interopérabité et certification croisée

L'interopérabilité est une notion essentielle des télécommunications érigée au rang d'exigences essentielles de l'article L.32-12° du Code des Postes et télécommunications. Tous les services et les réseaux de télécoms doivent être capables d'interopérer. En matière de certification électronique, l'interopérabilité signifie qu'un PSCE est susceptible de s'appuyer sur des services de confiance apportés par un autre PSCE. Comme les services dont il question traitent des certificats électroniques, l'interopérabilité prend le nom de *certification croisée*. Il s'agit pour un PSCE d'accepter ou de garantir pour le compte de l'utilisateur final un certificat provenant d'un autre PSCE.

Pour l'exigence interopérabilité, la Commission Européenne encourage la reconnaissance mutuelle des certificats. La Commission dans son document COM503 insiste sur la nécessité d'instaurer une reconnaissance mutuelle en matière de certificat :
"Reconnaissance mutuelle - Dans un cadre réellement international pour le commerce électronique, les certificats alloués par des AC étrangères doivent être reconnus mutuellement dans différents pays, de manière à permettre une vérification rapide et efficace de chaque certificat international. Les structures nationales pourraient être complétées par un mécanisme de coordination au niveau européen. Un tel concept serait cohérent avec la stratégie de négociation communautaire existante en matière de reconnaissance mutuelle, et pourrait encourager le développement de services de certification en Europe. Des accords avec des pays tiers seront à la fois plus faciles à conclure et économiquement plus avantageux s'ils sont basés sur un régime commun au niveau communautaire".

Et plus loin, dans les orientations de travail, la Commission fixe des objectifs précis pour aboutir à la reconnaissance mutuelle :
Orientations : ... (iv) Compte tenu de la nature universelle de la communication et du commerce électroniques, des accords internationaux pourraient s'avérer nécessaires entre la Communauté et d'autres pays, une fois qu'un système harmonisé aura été mis en place. Le but doit être de lever les obstacles existants de manière à créer un cadre international compatible pour le commerce électronique, en particulier pour l'établissement de normes techniques communes et pour la reconnaissance mutuelle des certificats.

Mais comment organiser juridiquement la certification croisée ? Comme d'habitude par un contrat. Mais l'expérience montre que ce contrat peut posséder un assez beau design juridique, alors que son efficacité peut être médiocre. En théorie, il suffira d'opérer un rapprochement entre les *Pratiques de Certification (CPS)* des PSCE en cause. Mais dans le concret, comment mettre en coïncidence les certificats de l'un et ceux de l'autre, alors que plusieurs classes de certificats peuvent exister, en nombre différent chez ces PSCE et avec une palette de garanties distinctes ? La solution est naturellement dans la norme. Il faudra normaliser les classes de certification et leur contenu, créant ainsi des profils de sécurité dans les classes de certificats. Ou encore, comme y songent les québécois à normaliser ou à créer des *subsets*[1] au certificat électronique de structure X.509.

2.2.4.3. La protection de la vie privée

Dans le contexte actuel des technologies de l'information et de la communication, il n'est plus guère possible de célébrer une de ces dernières sans un rappel sur la protection des données personnelles et informations nominatives. La certification électronique n'échappe pas à la règle. Le document COM503 de la Commission est intéressant dans la mesure où il signale des pratiques du secteur nécessitant une attention particulière :

[1] Dans le monde de l'EDI, un *subset* est la déclinaison d'un message normalisé au niveau international en un message exploitable par une collectivité professionnelle nationale.

"Protection de la vie privée -...C'est pourquoi dans de nombreux cas les personnes vont disposer de plusieurs paires de clés correspondant à leurs différents rôles. Les personnes ne désirant pas, ou n'étant pas légalement obligées de communiquer sous leur nom, peuvent choisir un pseudonyme leur permettant de sauvegarder leur anonymat dans les transactions et communications (bien que le signataire soit identifié auprès de l'AC), tout en exploitant au maximum les fonctions d'intégrité et d'authentification des signatures numériques. Cette possibilité est également requise par la Directive communautaire sur la protection des données et soutenue par les Directives de l'OCDE en matière de politique cryptographique. Sans cette garantie en matière de vie privée, les signatures numériques pourraient être utilisées de manière abusive comme instrument efficace permettant de suivre les habitudes individuelles de consommation et de communication en ligne, ou pour l'interception, l'enregistrement ou l'usage abusif de documents et de messages."

Le document rappelle avec raison que certaines opérations commerciales y compris les paiements peuvent être accomplis de façon anonyme sans altérer la validité juridique globale de l'opération. Cependant en ces circonstances, il a la plupart du temps un agent ou un intermédiaire qui connaît l'identité réelle de l'utilisateur. En l'occurrence, ce serait le PSCE. Plus loin, on peut lire dans le document de la Commission qu'une Directive communautaire trouve à s'appliquer même si les législations internes des pays membres sont insuffisantes sur cette protection : *"...Dans la mesure où les AC doivent être en mesure d'identifier le propriétaire de la clé et donc de collecter de l'information sur les individus, elles sont soumises aux obligations de la Directive communautaire sur la protection des données en matière de traitement des données, de sécurité et de transferts vers les pays tiers. Les AC peuvent, par exemple, collecter et traiter des données personnelles uniquement si l'individu concerné a donné son accord ou si elles y sont autorisées par la loi."*

2.3. Responsabilité professionnelle des PSCE

2.3.1. Réflexions sur la pratique professionnelle des PSC

2.3.1.1. La pratique professionnelle, responsabilité et étendue des services

Quelques développements du document COM503 de la Commission à propos de la responsabilité des PSCE appellent à renforcer les exigences de la procédure d'évaluation :
"*Des règles claires contribueraient à l'acceptation des services des AC (…) La responsabilité dépend largement de l'offre de services fournie par l'AC, telle que stipulée par le contrat. Un catalogue juridique des obligations juridiques pourrait former la base des obligations contractuelles. Il pourrait également fixer la responsabilité minimale et maximale des AC ou des garanties, par exemple concernant l'exactitude du certificat ou du répertoire de clés.* Les "règles claires" en question doivent former d'une part les règles d'accès à la profession, l'évaluation par les utilisateurs selon l'expression utilisée par l'Information Security Committee (ISC) de l'American Bar Association et d'autre part, la déontologie professionnelle pour se maintenir dans la profession.

"Il n'existe normalement pas de relations contractuelles entre une AC et des tierces parties, telle que le destinataire d'un message signé numériquement ou une autre AC, ayant confiance en la validité des certificats. C'est pourquoi les Etats membres devraient examiner la question de savoir s'il est nécessaire d'établir des règles de responsabilité spéciales". L'intervention de l'Etat n'est pas encore obligatoire en cette matière. La solution repose dans le niveau de confiance que les utilisateurs peuvent avoir dans les PSCE pris collectivement. D'où l'intérêt que l'accès à la profession, la déontologie permanente et le maintien de l'interopérabilité dans la certification électronique soient assurés par une structure permanente, la structure de gestion de l'Infrastructure à clé publique.

2.3.1.2. La pratique professionnelle selon le MEFI

Dans la Politique de Certification du MEFI que l'on retient pour son aspect exemplaire, le PSCE et les composants de la PKI se voient imposer des conditions sur la sécurité physique des installations, sur les procédures et sur les personnels. La sécurité physique sera contrôlée sous l'angle de la situation géographique et la construction de sites, l'accès physique, l'énergie employées et l'air conditionné, l'exposition aux liquides, la prévention et la protection des incendies, la conservation des médias, la destruction des déchets, la sauvegarde hors site. Les contrôles sur les procédures portent sur la répartition des personnels entre les différents rôles (les 4 rôles étant l'ingénieur système, les administrateurs, les opérateurs, les responsables sécurité), le nombre de personnes nécessaires à chaque tâche, l'identification et l'authentification des rôles. Les contrôles sur le personnel devront s'intéresser au passé professionnel, la qualification, l'expérience et les habilitations.

Les responsables du PSCE doivent être attentifs à toute tentative de violation de l'intégrité du système de gestion des certificats y compris les équipements physiques, l'environnement d'exploitation et le personnel. Les journaux d'événements journaliers doivent être contrôlés pour identifier des anomalies liées à des tentatives en échec. Le PSCE doit s'assurer que ses journaux sont revus par son personnel à une fréquence hebdomadaire, et que tous les éléments importants sont expliqués dans un résumé.

2.3.2. Responsabilité sur le contenu du certificat

Selon l'article 6.1. de la Directive, le PSC qui délivre à l'intention du public un certificat présenté comme qualifié est responsable du préjudice causé à toute entité ou personne physique ou morale qui se fie raisonnablement à ce certificat. Les points visés sont :

- l'exactitude de toutes informations contenues dans le certificat qualifié à la date où il a été délivré et la présence, dans ce certificat, de toutes les données prescrites pour un certificat qualifié ;
- l'assurance que, au moment de la délivrance du certificat, le signataire identifié dans le certificat qualifié détenait les données afférentes à la création de signature correspondant aux données afférentes à la vérification de signature fournies ou identifiées dans le certificat ;
- l'assurance que les données afférentes à la création de signature et celles afférentes à la vérification de signature puissent être utilisées de façon complémentaire, dans le cas où le prestataire de service de certification génère ces deux types de données, sauf si le prestataire de service de certification prouve qu'il n'a commis aucune négligence.

Une disposition de l'article 6.2 envisage le cas de la révocation, le PSCE est responsable s'il a omis de faire enregistrer la révocation du certificat, sauf s'il prouve qu'il n'a commis aucune négligence.

2.3.3. Responsabilité pour clause abusive

Les dispositions de la directive 93/13/CEE du Conseil du 5 avril 1993 concernant les clauses abusives dans les contrats conclus avec les consommateurs s'appliquent.

2.3.4. Les limites de la responsabilité

- Limite de l'utilisation du certificat : d'après l'article 6.3. de la Directive, le PSC peut indiquer, les limites fixées à l'utilisation d'un certificat qualifié, à condition que ces limites soient discernables par des tiers. Le prestataire de service de certification ne doit pas être tenu responsable du préjudice résultant de l'usage abusif d'un certificat qualifié qui dépasse les limites fixées à son utilisation.
- Limite de valeur : d'après l'article 6.4., le PSC peut indiquer la valeur limite des transactions pour lesquelles le certificat peut être utilisé, à condition que cette limite soit discernable par des tiers. Le prestataire de service de certification n'est pas responsable des dommages qui résultent du dépassement de cette limite maximum.

Pour en finir, on n'oubliera pas qu'on se place dans un contexte juridique. Aussi l'objection est-elle fondamentale : la validité du certificat n'emporte pas la validité du message électronique. A propos de l'utilisation de la cryptographie en support de la signature électronique, un document intitulé "*Etude des questions de droit entourant la sécurité des renseignements électroniques*", produit en juin 1995 par un Groupe de travail juridique dans le cadre du programme gouvernemental fédéral canadien "stratégie pour la sécurité des technologies de l'information" fait un heureux rappel. Le document affirme : "*Il y a lieu de distinguer la fonction de certification et la transaction sous-jacente. Le certificat électronique atteste du lien entre la personne et la clé publique. Elle ne certifie pas que la transaction est légalement autorisée ou valide par ailleurs".* Et plus loin, on peut lire : *"Le certificat valide ne garantit pas l'honnêteté du possesseur ni la validité de la transaction."*

Dit d'une autre façon, un délinquant comme toute autre personne de la société peut avoir une signature électronique de la même façon qu'il est capable de signer manuellement un document écrit. Le même personnage est capable selon le droit de passer, par exemple, une transaction commerciale valide. Aussi il est discutable, juridiquement parlant, et dangereux au point de vue commercial qu'un PSCE offre comme service de se porter garant de l'identité exacte de la personne, étendue à son honnêteté, ou sur la validité de la transaction finale, garantie par la signature électronique. Les seules exceptions possibles doivent être minutieusement soupesées, à moins d'être une pratique professionnelle habituelle, comme la garantie de solvabilité en matière de paiement. Une prise de risque conséquent par un PSCE doit être considérée comme une Valeur Ajoutée.

2.4. La reconnaissance administrative de la compétence professionnelle du PSCE

2.4.1. La procédure d'accréditation de la Directive

En amendant le principe du libre accès aux fonctions de PSCE, l'absence d'autorisation préalable à l'installation dans les fonctions de tiers certificateur ne signifie pas que les Etats ne procède pas à certains contrôles de l'activité des certificateurs. Selon le considérant 11 de la Directive : "*il est nécessaire que de[s] régimes [d'accréditation] incitent à mettre au point des règles de bonne pratique entre prestataires de service de certification ; il y a lieu que ces derniers restent libres de souscrire à ces régimes d'accréditation et d'en bénéficier.* Mais même pour les régimes d'accréditation, il n'y a pas d'obligation, la seule sanction ne pouvant résulter que du marché. Considérant 12, "l'*Etat ne peut pas interdire aux prestataires de service de certification d'opérer en dehors des régimes d'accréditation volontaires. Les régimes d'accréditation ne limitent pas la concurrence dans le secteur des services de certification".*

L'article 2 définition explique dans son point 13 ce qu'il faut entendre par "accréditation volontaire" : "*toute autorisation indiquant les droits et obligations spécifiques à la fourniture de services de certification, accordée, sur demande du prestataire de service de certification concerné, par l'organisme public ou privé chargé d'élaborer ces droits et obligations et d'en contrôler le respect, lorsque le prestataire de service de certification n'est pas habilité à exercer les droits découlant de l'autorisation aussi longtemps qu'il n'a pas obtenu la décision de cet organisme*".

A signaler cependant que la finalité d'une procédure d'accréditation n'est pas pour l'Etat de réguler ou de suivre la profession, mais au contraire de vérifier son adéquation aux besoins du marché. L'article 3.2. de la Directive indique qu'il s'agit d'améliorer le niveau du service de certification fourni. et les considérants expliquent que : *les régimes volontaires d'accréditation visant à assurer un meilleur service fourni peuvent constituer pour les prestataires de service de certification le cadre propice à l'amélioration de leurs services afin d'atteindre le degré de confiance, de sécurité et de qualité exigés par l'évolution du marché.* Enfin, le même article 3.2. informe que les critères relatifs à ces régimes d'accréditation doivent être objectifs, transparents, proportionnés et non discriminatoires.

2.4.2 La qualification du droit français

Au moment de la transposition dans le droit français, le décret d'application de l'article 1316-4 a tout d'abord corrigé une erreur de terminologie. Il ne s'agit pas d'accréditer des PSC, mais de les faire certifier[2] par un auditeur, lui-même accrédité par un organisme ad hoc[3]. Les pouvoirs publics ont préféré employer le terme de *qualification*, qui sert également pour le certificat électronique. Le Décret le définit de la façon suivante (Art. 12ème) : "*l'acte par lequel un tiers, dit organisme de qualification, atteste qu'un prestataire de services de certification électronique fournit des prestations conformes à des exigences particulières de qualité*".

La qualification procède du Ministre de l'Industrie et non plus du Ministre des Finances. Un PSCE pourra demander sa qualification a un organisme accrédité à cet effet. La qualification suppose d'avoir été audité favorablement sur les deux points suivants :

- les certificats doivent être qualifiés selon les termes de l'article 6. -I,
- le PSCE doit satisfaire aux exigences d'organisation et de fonctionnement listées dans l'article 6.-II. Ces exigences correspondent à celle de l'annexe II de la Directive.

Le tableau ci-dessous permet de comparer les exigences techniques correspondantes dans la Directive et le Décret.

[2] En fait, ce n'est pas l'auditeur qui certifie mais l'autorité administrative à qui l'auditeur fait le rapport de sa mission de vérification et de contrôle.

[3] L'accréditation est une procédure ISO. Elle est relayée au niveau européen par l'EAO (European Accréditation Organisation). Le correspondant français est le COFRAC, Comité Français d'Accréditation.

Directive ANNEXE II - Exigences concernant les prestataires de service de certification délivrant des certificats qualifiés	Décret
Les prestataires de service de certification doivent :	Un prestataire de services de certification électronique doit satisfaire aux exigences suivantes :
a) faire la preuve qu'ils sont suffisamment fiables pour fournir des services de certification ;	a) Faire preuve de la fiabilité des services de certification électronique qu'il fournit ;
b) assurer le fonctionnement d'un service d'annuaire rapide et sûr et d'un service de révocation sûr et immédiat ;	b) Assurer le fonctionnement, au profit des personnes auxquelles le certificat électronique est délivré, d'un service d'annuaire recensant les certificats électroniques des personnes qui en font la demande ; c) 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 ;
c) veiller à ce que la date et l'heure d'émission et de révocation d'un certificat puissent être déterminées avec précision ;	d) Veiller à ce que la date et l'heure de délivrance et de révocation d'un certificat électronique puissent être déterminées avec précision ;
d) vérifier, par des moyens appropriés et conformes au droit national, l'identité et, le cas échéant, les qualités spécifiques de la personne à laquelle un certificat qualifié est délivré ;	e) Employer du personnel ayant les connaissances, l'expérience et les qualifications nécessaires à la fourniture de services de certification électronique ;
e) employer du personnel ayant les connaissances spécifiques, l'expérience et les qualifications nécessaires à la fourniture des services et, en particulier, des compétences au niveau de la gestion, des connaissances spécialisées en technologie des signatures électroniques et une bonne pratique des procédures de sécurité appropriées ; ils doivent également appliquer des procédures et méthodes administratives et de gestion qui soient adaptées et conformes à des normes reconnues ;	f) Appliquer des procédures de sécurité appropriées ; g) Utiliser des systèmes et des produits garantissant la sécurité technique et cryptographique des fonctions qu'ils assurent ; h) Prendre toute disposition propre à prévenir la falsification des certificats électroniques ; i) Dans le cas où il fournit au signataire des données de création de signature électronique, garantir la confidentialité de ces données lors de leur création et s'abstenir de conserver ou de reproduire ces données ;
f) utiliser des systèmes et des produits fiables qui sont protégés contre les modifications et qui assurent la sécurité technique et cryptographique des fonctions qu'ils assument ;	j) Veiller, dans le cas où sont fournies à la fois des données de création et des données de vérification de la signature électronique, à ce que les données de création correspondent aux données de vérification ;
g) prendre des mesures contre la contrefaçon des certificats et, dans les cas où le prestataire de service de certification génère des données afférentes à la création de signature, garantir la confidentialité au cours du processus de génération de ces données ;	k) Conserver, éventuellement sous forme électronique, toutes les informations relatives au certificat électronique qui pourraient s'avérer nécessaires pour faire la preuve en justice de la certification électronique.
h) disposer des ressources financières suffisantes pour fonctionner conformément aux exigences prévues par la présente directive, en particulier pour endosser la responsabilité de dommages, en contractant, par exemple, une assurance appropriée ;	l) 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 ;
i) enregistrer toutes les informations pertinentes concernant un certificat qualifié pendant le délai utile, en particulier pour pouvoir fournir une preuve de la certification en justice. Ces enregistrements peuvent être effectués par des moyens électroniques ;	- 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 ; m) 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
j) ne pas stocker ni copier les données afférentes à la	

création de signature de la personne à laquelle le prestataire de service de certification a fourni des services de gestion de clés ; k) avant d'établir une relation contractuelle avec une personne demandant un certificat à l'appui de sa signature électronique, informer cette personne par un moyen de communication durable des modalités et conditions précises d'utilisation des certificats, y compris des limites imposées à leur utilisation, de l'existence d'un régime volontaire d'accréditation et des procédures de réclamation et de règlement des litiges. Cette information, qui peut être transmise par voie électronique, doit être faite par écrit et dans une langue aisément compréhensible. Des éléments pertinents de cette information doivent également être mis à la disposition, sur demande, de tiers qui se prévalent du certificat ; l) utiliser des systèmes fiables pour stocker les certificats sous une forme vérifiable de sorte que: - seules les personnes autorisées puissent introduire et modifier des données, - l'information puisse être contrôlée quant à son authenticité, - les certificats ne soient disponibles au public pour des recherches que dans les cas où le titulaire du certificat a donné son consentement et - toute modification technique mettant en péril ces exigences de sécurité soit apparente pour l'opérateur.	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 ; n) s'assurer au moment de la délivrance du certificat électronique : - que les informations qu'il contient sont exactes ; - que le signataire qui y est identifié détient les données de création de signature électronique correspondant aux données de vérification de signature électronique contenues dans le certificat ; o) Avant la conclusion d'un contrat de prestation de services de certification électronique, informer par écrit la personne demandant la délivrance d'un certificat électronique : - des modalités et des conditions d'utilisation du certificat ; - du fait qu'il s'est soumis ou non au processus de qualification volontaire des prestataires de services de certification électronique mentionnée à l'article 7 ; - des modalités de contestation et de règlement des litiges ; p) Fournir aux personnes qui se fondent sur un certificat électronique les éléments de l'information prévue au o qui leur sont utiles.

La mise en place de la procédure est la suivante procédure :
- Le Premier Ministre fixe par arrêté les règles d'évaluation.
- Le Ministre de l'Industrie fixe par un arrêté à venir la procédure d'accréditation des organismes et la procédure d'évaluation et de qualification des PSCE.
- Le Ministre de l'Industrie désigne par un arrêté à venir une entité qui accréditera certains organismes.
- Les organismes accrédités auditeront les PSCE.
- Les PSCE seront qualifiés par arrêté du Ministre de l'Industrie.