Projet ICare

La qualification des PSC – l'arrêté du 31 mai 2002

Référence : ICARE/CAB/TPC/DOC_12/v1
Type : Note d'information
Diffusion : Publique

Date : 03/07/2002
Titre : **ICare – La qualification des PSCE**

Auteur(s) : Thierry Piette-Coudol, avocat

Résumé :
La procédure de contrôle conduisant à la "qualification" des PSCE" est fixée par l'arrêté du 31 mai 2002 relatif à la reconnaissance de la qualification des PSCE et à l'accréditation des organismes chargés de l'évaluation. Commentaires de l'arrêté.

1 Préambule

La procédure et les modalités de la qualification[1] des Prestataires de Services de Certification Electronique (PSCE) sont désormais connus depuis un *Arrêté du 31 mai 2002 relatif à la reconnaissance de la qualification des PSCE et à l'accréditation des organismes chargés de l'évaluation*, publié au JO n° du 8 juin 2002 p.10223. Comme annoncé dans notre DOC_09 à propos du *Décret n°2002-535 du 18 avril 2002*, cet arrêté est le seul subsistant dans la liste des 5 arrêtés prévus initialement par le Décret d'application (n°2001-272) de l'article 1316-4 du Code Civil sur la signature électronique[2].

2 Rappel du contexte juridique et technique

On rappelle ci-dessous la conception juridique de la signature électronique. Les PSCE interviennent dans les traitements techniques de la Signature Electronique prévue par l'article 1316-4 du Code Civil. Ils émettent un *certificat électronique* contenant *les données de vérification de signature* (en termes techniques, la "clé cryptographique publique" du signataire). Les données permettent au destinataire d'un message électronique signé de lancer la vérification de la signature.

L'article 1316-4 du Code Civil octroie une valeur de preuve à la signature électronique à condition que le procédé technique employé soit réputé fiable c'est-à-dire respecte les conditions prévues par le Décret 2001-272 précité. L'article 2 du Décret instaure une *signature électronique sécurisée* fiable : elle est basée sur un *dispositif sécurisé de création de signature* et sa vérification repose sur l'utilisation d'un *certificat électronique qualifié*. La qualification du certificat[3] sera acquise si le PSCE qui l'émet est lui-même *qualifié*[4], d'où l'arrêté du 30 mai 2002 annoncé par l'article 7 du décret précité[5].

En amont, cette construction prend sa source dans la Directive 1999/93/CE sur un cadre communautaire pour les signatures électroniques. Ainsi l'*article 3 Accès au marché* rappelle que chaque Etat doit instaurer un système adéquat permettant de contrôler les PSCE établis sur son territoire et délivrant des certificats qualifiés au public. Mais le système de contrôle doit rester facultatif pour les PSCE dont le nombre ne peut être limité au niveau national et dont l'accès au marché ne peut être entravé par des autorisations administratives préalables. Ce qui n'empêche pas les Etats d'instaurer ou de maintenir des régimes volontaires d'accréditation visant à améliorer le niveau du service de certification fourni. L'article 3 fixe que "*tous les critères relatifs à ces régimes doivent être objectifs, transparents, proportionnés et non discriminatoires*".

3 La procédure de qualification des PCSE

D'après l'arrêté du 31 mai 2002, la qualification d'un PSCE est prononcée après une évaluation de sa pratique professionnelle et des certificats émis. L'évaluation des PSCE est effectuée par un *organisme accrédité* et aux frais du PSCE, comme on l'a vu en matière d'évaluation des dispositifs de création de signature (cf. Décret 2002-535). L'objet de l'évaluation porte sur le respect des exigences techniques et organisationnelles de l'article 6 du

---

[1] Décret 2001-272, article 1 définitions : "*Qualification des prestataires de services de certification électronique : 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*".

[2] Il s'agit de l'arrêté E (cf. DOC_09). L'article 7 du décret 2001-272 modifié prévoit que "*l'arrêté du ministre chargé de l'industrie prévu à l'alinéa précédent détermine la procédure d'accréditation des organismes et la procédure d'évaluation et de qualification des prestataires de services de certification électronique*". Les autres arrêtés ont disparu pour être remplacés par le Décret 2002-535 dans la mouvance de la réforme de la Direction Centrale de la Sécurité des Services d'Information (DCSSI).

[3] En combinant les définitions du Décret 2001-272, on peut estimer qu'un certificat électronique qualifié est un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire et répondant pour ce faire aux exigences techniques définies à l'article 6 du Décret.

[4] Décret 2001-272, article 6 : "*Un certificat électronique ne peut être regardé comme qualifié que s'il comporte les éléments énumérés au I et que s'il est délivré par un prestataire de services de certification électronique satisfaisant aux exigences fixées au II*".

[5] Décret 2001-272, article 7 premier alinéa : "*Les prestataires de services de certification électronique qui satisfont aux exigences fixées à l'article 6 peuvent demander à être reconnus comme qualifiés. Cette qualification, qui vaut présomption de conformité auxdites 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. Elle est précédée d'une évaluation réalisée par ces mêmes organismes*".

Décret 2001-272 ainsi que les normes, les prescriptions techniques et les règles de bonne pratique applicables en matière de certification électronique.

A l'issue des contrôles, le (ou les) organisme(s) accrédité(s) établi(ssen)t un rapport qui est notifié au prestataire afin que celui-ci puisse, le cas échéant, formuler des observations sur son contenu. Le rapport d'évaluation est communiqué par les organismes accrédités à la DCSSI sur demande[6] de celle-ci. En conclusion de l'évaluation, l'organisme accrédité reconnaît ou non la qualification du prestataire de services de certification électronique à partir de son rapport et des éventuelles observations du prestataire. Lorsqu'il reconnaît la qualification d'un prestataire, l'organisme accrédité produit une *attestation* décrivant les prestations de services couvertes par la qualification ainsi que la durée, qui ne peut excéder un an, pendant laquelle elle est valable. A titre d'application de l'article 6-II-o du Décret[7], les prestataires dont la qualification est reconnue communiquent à toute personne qui en fait la demande une copie de l'attestation délivrée par l'organisme accrédité.

4 L'accréditation des évaluateurs par le COFRAC

Comme on l'a noté, le processus de qualification dépend d'organismes accrédités[8]. Le Comité français d'accréditation (COFRAC), association déclarée le 4 mai 1994, est chargé[9] d'accréditer les organismes qui procéderont à l'évaluation des prestataires de services de certification électronique en vue de reconnaître leur qualification. Selon la procédure ISO d'accréditation, il n'y a qu'un organisme d'accréditation par pays. Au niveau international existe un système d'audits croisés entre les différents pays afin d'assurer la reconnaissance mutuelle, dans tout l'Espace Economique Européen, des attestations émanant d'organismes accrédités. L'accréditation permet d'harmoniser, dans un contexte européen et international, les pratiques des organismes en mettant en œuvre des règles, des critères et des processus de décision communs à tous les secteurs. Aussi le COFRAC est-il membre de l'*European Co-operation for Accreditation* et signataire de l'*Accord multilatéral Européen d'Accréditation* pour les essais, les étalonnages et la certification.

Dans le droit interne, la demande d'accréditation adressée par un organisme au COFRAC doit comprendre un certain nombre d'informations élémentaires sur le demandeur (voir l'article 2 de l'arrêté pour le détail), notamment la description des activités de l'organisme, de sa structure et de ses moyens techniques. Il y joindra la description des procédures et des moyens qui seront mis en œuvre pour évaluer les PSCE en vue de reconnaître leur qualification, compte tenu des normes ou prescriptions techniques en vigueur. L'organisme demandeur doit signaler au centre d'accréditation les liens éventuels qu'il a avec des prestataires de services de certification électronique. En ce cas, il doit préciser les mesures qu'il compte mettre en œuvre pour éviter tout conflit d'intérêts[10]. Le COFRAC instruira la demande d'accréditation. Il pourra solliciter tous renseignements complémentaires de l'organisme demandeur et effectuer des vérifications dans les locaux de l'organisme demandeur. A l'issue de l'instruction, le centre d'accréditation prend une décision motivée qu'il notifie à l'organisme demandeur. L'accréditation est accordée pour une durée de deux ans. Elle peut être renouvelée pour une durée identique.

---

[6] Cette communication permet de faire circuler les informations. Lorsque la DCSSI procédera à un contrôle de l'activité d'une PSCE suite à une réclamation dont elle aurait été saisie, elle informera des résultats de ce contrôle l'organisme de qualification (article 9-II du Décret) qui pourra en tirer des conclusions quant à la qualification accordée.

7 Selon l'article 6-II-o du Décret, avant la conclusion d'un contrat de prestation de services de certification électronique, le PSCE doit informer par écrit la personne demandant la délivrance d'un certificat électronique du fait qu'il s'est soumis ou non au processus de qualification volontaire des prestataires de services de certification électronique de l'article 7 du Décret.

[8] C'est par erreur que la Directive 1999/93/CE sur un cadre communautaire pour les signatures électroniques parle d'*accréditation des PSC(E)* (cf. art. 3 de la Directive). Il s'agit en fait d'*accréditation* de l'organisme de contrôle qui procédera à la *qualification* des PSCE.

[9] ainsi que les organismes d'accréditation signataires de l'accord européen multilatéral pris dans le cadre de la coordination européenne des organismes d'accréditation

[10] La *Décision de la commission du 6 novembre 2000* énonce les critères auxquels les Etats membres doivent se référer pour désigner les organismes nationaux chargés d'évaluer en toute indépendance la conformité des dispositifs (*Décision de la commission du 6 novembre 2000 relative aux critères minimaux devant être pris en compte par les Etats membres lors de la désignation des organismes visés à l'article 3, paragraphe 4. de la directive 1999193/Œ du Parlement européen et du Conseil sur un cadre communautaire pour les signatures électroniques).*

5 Annexe – le texte de l'arrêté

Arrêté du 31 mai 2002 relatif à la reconnaissance de la qualification des prestataires de certification électronique et à l'accréditation des organismes chargés de l'évaluation

NOR : ECOI0200314A - J.O. Numéro 132 du 8 Juin 2002 page 10223

Le ministre de l'économie, des finances et de l'industrie,
Vu 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,

Arrête :

Chapitre Ier

Accréditation des organismes qui procèdent à l'évaluation des prestataires de services de certification électronique en vue de reconnaître leur qualification

Art. 1er. - Le Comité français d'accréditation (COFRAC), association déclarée le 4 mai 1994, ainsi que les organismes d'accréditation signataires de l'accord européen multilatéral pris dans le cadre de la coordination européenne des organismes d'accréditation, sont chargés d'accréditer les organismes qui procèdent à l'évaluation des prestataires de services de certification électronique en vue de reconnaître leur qualification. Ils sont nommés ci-après centres d'accréditation.

Art. 2. - La demande d'accréditation, adressée par un organisme à un centre d'accréditation, doit comprendre les éléments suivants :

1. Les statuts de l'organisme, son règlement intérieur et tous autres textes régissant son fonctionnement ;
2. Les noms et qualités des dirigeants de l'organisme et des membres de son conseil d'administration ou des organes en tenant lieu ;
3. Les noms et les qualifications des personnels de l'organisme prenant part à la procédure d'évaluation ;
4. La description des activités de l'organisme, de sa structure et de ses moyens techniques ;
5. Les comptes des deux exercices précédents ;
6. La description des procédures et des moyens qui seront mis en œuvre par l'organisme pour évaluer les prestataires de certification électronique en vue de reconnaître leur qualification, compte tenu des normes ou prescriptions techniques en vigueur.

L'organisme demandeur doit en outre signaler au centre d'accréditation les liens éventuels qu'il a avec des prestataires de services de certification électronique. En ce cas, il doit préciser les mesures qu'il compte mettre en œuvre pour éviter tout conflit d'intérêts.

Art. 3. - Le centre d'accréditation instruit la demande d'accréditation. Il peut solliciter tous renseignements complémentaires de l'organisme demandeur. Il peut demander à effectuer des vérifications dans les locaux de l'organisme demandeur.
A l'issue de l'instruction, le centre d'accréditation prend une décision motivée qu'il notifie à l'organisme demandeur et dont il adresse copie à la direction centrale de la sécurité des systèmes d'information. Lorsqu'il accorde l'accréditation, le centre d'accréditation peut soumettre l'organisme bénéficiaire à des obligations particulières.

Art. 4. - L'accréditation est accordée pour une durée de deux ans. Elle peut être renouvelée pour une durée identique, à la demande de l'organisme bénéficiaire, après que le centre d'accréditation a vérifié que celui-ci remplit toujours l'ensemble des conditions requises.
Les organismes accrédités informent le centre d'accréditation de tout changement par rapport aux éléments communiqués dans le dossier de demande d'accréditation. Le centre d'accréditation peut s'assurer à tout moment que les organismes continuent à satisfaire aux critères au vu desquels ils ont été accrédités.
Lorsqu'un organisme ne satisfait plus aux conditions d'accréditation ou manque aux obligations fixées dans la décision d'accréditation, le retrait d'accréditation peut être prononcé par le centre d'accréditation après que le représentant de l'organisme concerné a été mis à même de présenter ses observations.

Art. 5. - Le centre d'accréditation met à la disposition du public, notamment sur un site internet, la liste des organismes accrédités. Cette liste est tenue à jour.

Chapitre II
Reconnaissance de la qualification des prestataires de services de certification électronique

Art. 6. - Un prestataire de services de certification électronique qui demande à être reconnu comme qualifié choisit un ou plusieurs organismes accrédités pour procéder à l'évaluation des services qu'il propose.
Le prestataire est tenu de fournir aux organismes qu'il a choisis tous les éléments nécessaires au bon accomplissement de la procédure d'évaluation.

Art. 7. - L'évaluation est effectuée par l'organisme aux frais du prestataire de services de certification. Son objet est notamment de vérifier que les services offerts par le prestataire respectent en tous points les exigences fixées par l'article 6 du décret du 30 mars 2001 susvisé ainsi que les normes, prescriptions techniques et règles de bonne pratique applicables en matière de certification électronique.
A l'issue de la procédure d'évaluation, l'organisme accrédité établit un rapport qui est notifié au prestataire afin que celui-ci puisse, le cas échéant, formuler des observations sur son contenu.

Art. 8. - Les rapports d'évaluation sont communiqués par les organismes accrédités à la direction centrale de la sécurité des systèmes d'information si celle-ci le demande.

Art. 9. - L'organisme accrédité reconnaît ou non la qualification du prestataire de services de certification électronique au vu du rapport d'évaluation et des éventuelles observations du prestataire.
Lorsqu'il reconnaît la qualification d'un prestataire, l'organisme accrédité délivre une attestation qui décrit les prestations de services couvertes par la qualification ainsi que la durée, qui ne peut excéder un an, pendant laquelle l'attestation est valable.
Les prestataires dont la qualification est reconnue communiquent à toute personne qui en fait la demande une copie de l'attestation délivrée par l'organisme accrédité.

Art. 10. - La directrice générale de l'industrie, des technologies de l'information et des postes est chargée de l'exécution du présent arrêté, qui sera publié au Journal officiel de la République française.

Fait à Paris, le 31 mai 2002.
Francis Mer