Projet ICare

La notion d'A.E. et le Droit

Référence : ICARE/CAB/TPC/DOC_8/v1
Type : Note de travail
Diffusion : Générale

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

Auteur(s) : Thierry Piette-Coudol, avocat

Résumé :
Cette note de travail décrit le fonctionnement des Autorités d'Enregistrement d'après les quelques textes juridiques disponibles.

1. Préambule

La présente note de travail présente une réflexion actualisée sur la notion d'autorité d'enregistrement (AE) face au Droit.

Cette contribution a vocation, avec d'autres contributions sur des thèmes complémentaires ou connexes, à 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. L'AE et le Droit

2.1. Les bases juridiques des fonctions d'AE

2.1.1. Les fonctions d'AE et le droit

Ni les fonctions d'enregistrement ni l'entité chargée de ces fonctions, l'autorité d'enregistrement, ne sont mentionnées dans la Directive ou dans la loi.

Pourtant la question de l'identification / authentification est particulièrement importante dans le domaine juridique puisque :
- d'une part, il ne s'agit plus d'identifier une ressource technique, mais un *sujet de droit*, en particulier une personne physique, le signataire, même si le signataire représente une personne morale (entreprise),
- d'autre part, l'identification de la personne peut être, selon les prérequis de certains textes juridiques, extrêmement pointue c.a.d. correspondant à l'état civil de la personne (voir ci-dessous).

L'obligation incombe au PSCE[1] d'après l'article 6-II-m du Décret[2]. Le PSCE doit :
"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 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 ;"

C'est cette obligation qui est prise en charge concrètement par la fonction d'enregistrement. En choisissant comme référence la Politique de Certification-type du MINEFI, on peut y lire le classique principe technique suivant : "*la fonction d'enregistrement des certificats fait partie des fonctions indispensables d'une ICP. L'AC doit s'assurer qu'elle est remplie par une Autorité d'Enregistrement, distincte de l'AC avec laquelle elle collabore ou qui lui est rattachée*".

Plus loin, la PC-type définit l'AE ainsi qu'il suit :
"Autorité d'Enregistrement (AE) : entité qui vérifie que les demandeurs ou les porteurs de certificat sont identifiés, que leur identité est authentique et que les contraintes liées à l'usage d'un certificat sont remplies, tout cela conformément à la politique de certification".

En définitive, la nécessité de vérifier l'identité des personnes dans la signature électronique des juristes entraîne l'intervention d'une AE[3]. La responsabilité des vérifications opérées par l'AE dont l'existence n'est pas connue du droit est reportée sur le PSCE.

---

[1] Rappel : PSCE, Prestataire de Service de Certification Electronique, l'équivalent juridique de l'AC.
[2] Décret n°2001-272 du 30 mars 2001 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)
[3] On ajoutera : intervention d'une AE avec la quasi-nécessité d'une procédure d'authentification face à face.

2.1.2. Réflexions juridiques sur l'identification des personnes

La question de l'enregistrement préalable des personnes ou de la vérification a posteriori de l'identité électronique des personnes ouvre un débat de fond qui oscille entre la crainte de Big Brother et la protection des données nominatives. La question est de savoir jusqu'où faut-il pousser la connaissance de l'identité exacte de la personne pour que la confiance soit présente? On peut remonter le chemin de l'authentification de la façon suivante :

- l'authentification est garantie par la clé publique certifiée par un PSCE,
- la clé publique comme la clé privée seront tirées, puis le logiciel de création ou de vérification de signature sera activée lorsque l'utilisateur se sera fait reconnaître par une procédure spécifique, par exemple au moyen d'une carte à puce comportant son identité électronique.

Le besoin de connaître avec précision le nom de l'utilisateur est-il justifié en droit ? Si on prend le cas de la formation des contrats, en négligeant la question de la cause et de l'objet qui doivent être licites selon le Code Civil, on verra que l'identité est moins demandée que la compétence, la capacité de l'auteur et un consentement non vicié. Naturellement les contrats se passent entre des personnes, mais souvent une *identité apparente* est suffisante. La véritable identité, l'*identité de l'état civil*, n'est pas requise. On ajoutera que c'est avec les contrats formalisés sur un support papier que, tout naturellement et en dehors de toute obligation, les noms des signataires apparaissent. Les contrats oraux, pour peu qu'ils se forment et s'exécutent entre personnes présentes, ne nécessitent aucune connaissance précise de l'identité des parties. C'est le cas lorsqu'on *tope dans la main*. Le fait de ne pas avoir été préalablement en relations contractuelles ne compte pas plus. Prenons le cas du commerce de détail, le fait pour toute personne de rentrer dans un magasin et de réclamer un objet traduit le consentement au contrat de vente. Pour peu que manifestement, l'acheteur en puissance soit muni de moyens de paiement convaincants (des billets en main), l'identité peut rester apparente. On peut ajouter qu'une identité empruntée ou déguisée ne change rien à l'affaire tant que le consentement ne peut être mis en cause.

A partir de cet instant, on peut poursuivre vers l'anonymat. Si l'acheteur en puissance peut acquitter le prix au moyen de la monnaie légale, le paiement est alors anonyme. Il est à remarquer que parmi les moyens de paiement moderne dont les paiements électroniques, seule la monnaie légale permet un paiement anonyme. Pourquoi le contrat devrait-il être passé entre personnes identifiées alors que le paiement reste anonyme ? On objectera que le paiement n'est qu'un effet du contrat. Qu'importe qu'il soit anonyme si la formation ne l'est pas ? C'est oublier que le Commerce Electronique fonctionne d'une autre manière et change les perspectives. Malgré l'intention louable d'assujettir la formation du contrat en ligne du Commerce Electronique à la théorie de l'offre et de l'acceptation, l'incertitude sur l'existence contrat est grande pendant l'échange des messages électroniques. Le lancement d'une procédure de paiement en ligne traduit une mesure d'exécution d'un contrat, donc l'existence de celui-ci. Si par hasard, on a choisi un système de paiement électronique anonyme, l'ensemble de la transaction pourra rester anonyme. Le contrat ne sera pour cela irrégulier ou inexistant.

L'obligation de faire connaître son identité d'état civil précise est variable selon les circonstances et les branches du droit concernées. Si comme montré plus haut, l'identité exacte n'est pas requise en matière civile[4] et commerciale, elle peut l'être au contraire dans le droit administratif. Les *téléprocédures* lancées par le Ministère des Finances nécessitent la connaissance de l'identité exacte du *déclarant*[5]. Aussi l'emploi d'une autorité d'enregistrement sera pratiquement indispensable dans tous les cas de figures. On peut le voir en consultant la Politique de Certification-type du MINEFI. D'autre part, qui sait si au niveau du droit européen, l'AE ne sera pas introduite prochainement ? L'article 12 de la Directive prévoit que la Commission procédera à l'examen de la mise en œuvre de la directive et en rendra compte au Parlement européen et au Conseil pour le 19 juillet 2003 au plus tard. Une nouvelle directive pourrait faire référence aux AE[6] ?

Enfin pour montrer que le besoin d'authentification n'est pas ce qu'on croit, il est possible d'observer, ce qui peut être une source d'étonnement pour les juristes, la possibilité d'employer un pseudonyme pour le signataire. Voir l'article 6-I-c du Décret qui règle la question avec un certificat électronique qui contient "*le nom du signataire ou un pseudonyme, celui-ci devant alors être identifié comme tel*".

---

[4] Et pourtant dans certains cas en matière de doit civil, l'identité doit être exacte, par exemple pour les contrats matrimoniaux !

[5] On voit ici le paradoxe. L'identité exacte du déclarant est requise, mais il n'est peut être pas la personne assujettie à la déclaration : l'expert-comptable identifié effectue la déclaration pour le compte de l'entreprise cliente.

[6] Et aux Opérateurs de Services de Certification (OSC)…

2.2. Le contenu des fonctions d'enregistrement

En croisant les principes des Politiques de Certification disponibles et les exigences de signature électronique, on peut établir la liste suivante des prestations des AE en direction des titulaires de certificat :
- remise des moyens cryptographiques et tirage du bi-clé,
- obtention des certificats électroniques,
- réception des demandes de révocation de certificats et transmission à PSCE pour traitement.

2.2.1. Enregistrement

La phase d'enregistrement du titulaire de certificat incombe à l'AE. Elle est consiste pour l'AE à recevoir du futur titulaire de certificat les informations relatives à ce dernier, de les vérifier, puis de les transmettre à PSCE. La phase d'enregistrement peut être complétée par une phase particulière relative à la cryptographie au terme de laquelle :
- l'AE procédera au tirage du bi-clé du titulaire de certificat,
- ou bien le titulaire tirera le bi-clé au vu de l'AE.

Ces procédures ont pour but de satisfaire à une exigence incombant au PSCE. L'article 6-II-n du Décret stipule que le PSCE doit "*s'assurer au moment de la délivrance du certificat électronique (…) 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*". De la même façon que l'AE prend en charge la fonction d'enregistrement pour le PSCE, le PSCE délègue à l'AE la vérification qu'une clé privée correspond bien à la clé publique transmise au PSCE.

Tout utilisateur doit procéder à l'enregistrement préalable de son nom via l'AE. 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). Les bi-clés doivent être régénérées régulièrement. La PC établit des règles pour la période transitoire entre les anciens et les nouveaux certificats et des règles distinctives pour les clés des signatures et les clés de chiffrement.

2.2.2. Demande et remise du certificat

Après que la phase d'enregistrement a été menée à son terme, l'utilisateur enregistré peut obtenir son certificat auprès de PSCE. L'AE se charge de transmettre la demande du titulaire de certificat à PSCE après avoir effectué les contrôles nécessaires. La demande de certificat est faite par une personne physique soit à son propre titre soit pour le compte de la personne morale. Un certain nombre d'informations et de pièces justificatives devra être fourni en soutien à la demande.

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.

Après que le PSCE a procédé à la confection du certificat, il le transmettra à l'AE qui le remettra au titulaire après avoir effectué les contrôles nécessaires.

2.2.3. Révocation de certificat

S'il est saisi d'une demande de révocation de certificat, l'AE doit en vérifier l'origine et l'exactitude, et doit mettre en œuvre les moyens permettant de traiter la demande de révocation.

Lorsque l'une des circonstances précisées dans la PC se réalise, le certificat concerné doit être révoqué et placé par le PSCE dans une liste de certificats révoqués (LCR). Si une demande de révocation est déposée par le titulaire du certificat auprès de l'AE, celui transmet la demande sans délai à PSCE après avoir procédé aux contrôles indispensables indiqués dans la PC.

Si la demande est justifiée, le PSCE révoque le certificat. Le titulaire du certificat est informé de la révocation par un récépissé envoyé à l'adresse physique du certificat.

2.2.4. Renouvellement du bi-clé

Les bi-clés du titulaire de certificats sont renouvelés régulièrement après une durée de validité fixée par la PC. Les modalités du renouvellement du bi-clé, dans ou hors révocation du certificat sont précisées dans la PC.

2.2.5. Journalisation des événements et archivage

Toutes les opérations effectuées par l'AE sont journalisées automatiquement avec les éléments d'authentification des opérateurs et un horodatage local afin d'être en mesure de fournir une preuve de la certification. Il s'agit ici de satisfaire l'article 6-II-k du Décret aux termes duquel le PSCE doit "*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*". La PC précise notamment les éléments à mémoriser pour chaque événement, l'environnement d'exploitation et les événements techniques, les demandes et opérations relatives aux certificats, ainsi que mes modalités de journalisation, la rédaction et la conservation du journal.

Des traitements d'archivage doivent être réalisés. Les opérations d'archivage peuvent être réalisées suivant "les Recommandations pour l'archivage sécurisé", en date du 12 juillet 2000 par le groupe de travail commun de IALTA France et du Conseil Supérieur de l'Ordre des experts-comptables. La PC précise notamment le type de données à archiver, la période de rétention des archives, les mesures de protection des archives et les délais de conservation.

2.3. Les obligations de l'AE

2.3.1. Obligations générales de sécurité

L'AE garantit que les fonctions mises en œuvre sont conformes à l'état de l'art et respectent les exigences de sécurité formulées par les lois et règlements, notamment à la loi Informatique et Libertés. A cette fin, elle met en œuvre les moyens, techniques et humains, nécessaires à la réalisation des prestations visées, dans des conditions garantissant qualité et sécurité.

Comme les fonctions d'enregistrement visent à réunir des informations sur l'identité des personnes, toutes les prestations comprendront une phase d'identification précise des demandeurs. Notamment, l'AE vérifiera que :

- les demandeurs ou porteurs de certificat sont identifiés, leur identité est authentique et les contraintes liées à l'usage d'un certificat sont remplies ;
- l'authenticité des pièces justificatives et l'exactitude des mentions qui établissent l'identité du titulaire de certificat (personne physique ou mandataire habilité de l'entreprise).

Tous les dossiers de demande de certificats ou de révocation seront archivés.

La sécurité offerte par les postes de travail de l'AE répond à des exigences de sécurité détaillées dans la PC.

2.3.2. Obligation de confidentialité

La loi Informatique et Libertés oblige déjà l'AE a respecter la confidentialité des données personnelles. Une exigence de confidentialité complémentaire résulte des spécificités de la certification électronique. L'AE ne stockera ni ne copiera la clé privée de la personne à laquelle il est fourni des services de gestion de clés. En outre, les informations suivantes sont considérées comme confidentielles :

- Les données d'activation pour les titulaire de certificats,
- Les journaux d'événements des composantes du service de certification et/ou de signature électronique,
- Le dossier d'enregistrement du titulaire de certificat, et notamment les données personnelles.