Projet ICare

Les A.C. et leurs opérateurs (OSC)

Référence : ICARE/CAB/TPC/DOC_6/v1
Type : Note de travail
Diffusion : Générale

Date : 02/05/2002
Titre : **ICare – Les A.C. et leurs opérateurs (OSC)**

Auteur(s) : Thierry Piette-Coudol, avocat

Résumé :
Cette note de travail explique les relations entre les Autorités de Certification (appelées Prestataires de Services de Certification Electronique –PSCE- dans le droit français) avec leurs O.S.C. (Opérateurs de Services de Certification) ainsi que la prise en compte de ces relations par le droit interne.

TABLE DES MATIERES

1. Préambule

La présente note de travail présente une réflexion actualisée sur les autorités de certification et leurs sous-traitants chargés des opérations sur les certificats électroniques, les *opérateurs de services de certification*.

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. Les Autorités de certification et les opérateurs de services de certification

2.1. La PKI orientée utilisateurs

Les communautés professionnelles sont intéressées au premier chef par les systèmes de signature électronique. Mais comme elle l'ont fait auparavant pour la pratique de l'échange de données en formant des groupes d'utilisateurs EDI (par exemple avec les Groupes Opérationnels Sectoriels au sein d'Edifrance), elles doivent réfléchir à la création de PKI dédiée à leurs besoins. Il est préférable d'éviter de se lancer tête baissée dans le montage d'un système de signature électronique, alors qu'une réflexion de fond est à mener sur la sécurisation des échanges de données et de messages, surtout si on choisit Internet comme vecteur. Certaines dérives sont à éviter.

La sécurisation des échanges comprendra sans doute l'emploi d'une signature électronique, mais également des fonctions de chiffrement de messages, d'archivage et d'horodatage. L'Infrastructure à clés publiques est le modèle conceptuel qui permet de mettre en relation les besoins de sécurité à prendre en charge, les acteurs et les prestataires qui vont apporter des solutions, les normes et protocoles, les instruments juridiques et techniques à appliquer. Toutefois on constate actuellement que la notion de PKI est ignorée ou écartée, ce qui produit certaines tendances.

Ignorer la notion de PKI a pour conséquence actuelle une importance exagérée donnée à la notion d'*autorité de certification*. Le succès du concept est tel que les communautés professionnelles veulent créer leur propre *autorité de certification*. Mais comme la prestation de services de cryptographique n'est pas leur vocation, elles en confieront l'exercice pratique aux *opérateurs de services de certification*. Ignorer la notion de PKI a pour conséquence le dédoublement du certificateur en deux entités complémentaires. D'où un management contractuel délicat à bâtir entre les deux entités.

2.2. Le dédoublement de l'AC en AC-OSC

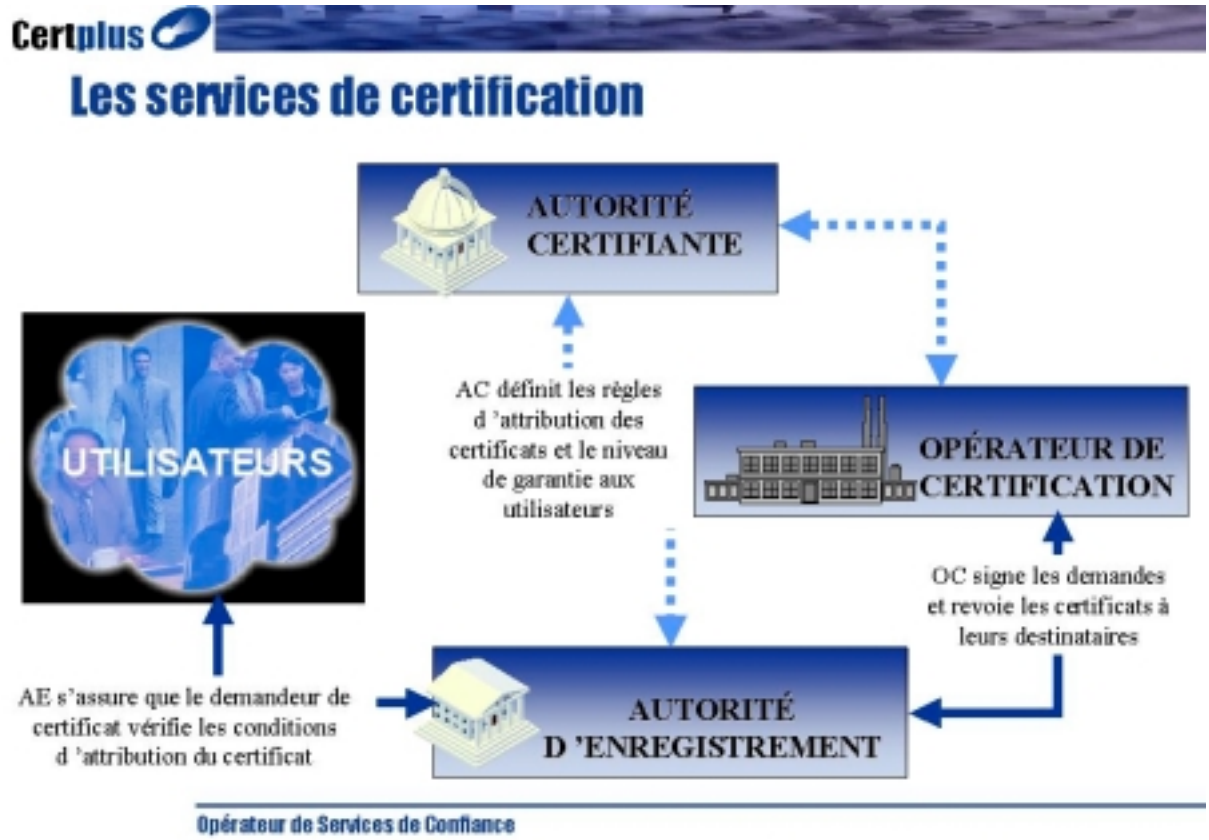
La tendance est à ce que les communautés d'utilisateurs forment leur propre Autorité de certification. Dans la pratique, cette tendance conduit à une différentiation de l'AC dans un couple de type AC – opérateur de certification. L'AC n'est en effet pas capable de procéder aux traitements techniques appliqués aux certificats, ce qui l'oblige à recourir à un prestataire spécialisé.

2.2.1. Les définitions selon le MINEFI

On peut voir nettement apparaître la différentiation entre deux entités complémentaires dans la version 2 de la PC du MEFI/MINEFI par opposition à la version 1:

Références document	AC	OSC
PC type V1 Du MINEFI	**(-)**	**Opérateur de service de certification (OSC)** : composante de l'PKI disposant d'une plate-forme lui permettant de générer et émettre des certificats auxquels une communauté d'utilisateurs fait confiance (également connue sous l'appellation autorité de certification (AC)).
PC type V2	**Autorité de Certification (AC)** : terme employé ici pour nommer l'entité interlocutrice du MEFI responsable des certificats signés en son nom. Par commodité pour la suite de ce document l'AC sera considérée comme le maître d'ouvrage de l'PKI. L'AC doit assurer au moins les fonctions suivantes: • mise en application des PC • gestion des certificats • gestion des supports et de leurs données d'activation si les bi-clés et les certificats sont fournis aux abonnés sur des supports matériels, • publication des certificats valides et des listes de certificats révoqués, • journalisation et archivage des événements et informations relatives au fonctionnement de l'PKI • éventuellement fonction de séquestre Pour assurer ces fonctions, l'AC peut s'organiser de la façon qui lui convient le mieux : en les prenant elle-même en charge, en les sous-traitant à un OSC ou en obtenant la collaboration d'autres entités, du moment que les accords entre les différentes parties sont clairement définis. La fonction d'enregistrement des certificats fait partie des fonctions indispensables d'une PKI. 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.	**Opérateur de Service de Certification (OSC)** : composante de l'PKI disposant d'une plate-forme lui permettant de générer et émettre des certificats auxquels une communauté d'utilisateurs fait confiance.

En cela, le MEFI se serait-il aligné sur la position de Certplus qui déclarait sa position à Identech'99 en septembre 1999 ?



2.2.2. Définitions légales

Il est remarquable qu'au plan juridique (voir le projet de décret), les notions d'AC et d'OSC n'existent pas. Il faut en rechercher la correspondance avec les concepts juridiques.

⇨ Définitions

Directive	*11) "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 ;*
Projet de décret	*8) "Prestataire de service de certification électronique" : toute personne physique ou morale qui délivre des certificats électroniques ou fournit d'autres services liés aux signatures électroniques.*

La Directive cite encore les PSC à propos des certificats :

ANNEXE I

Exigences concernant les certificats qualifiés

Tout certificat qualifié doit comporter : (...)
b- l'identification du prestataire de service de certification ainsi que le pays dans lequel il est établi ;
h - la signature électronique avancée du prestataire de service de certification qui délivre le certificat ;
(...)

⇨ Conclusion : l'AC de la PC du MINEFI n'est autre que le PSC de la Directive et l'OSC n'est cité en aucun moment.

L'éclatement de l'AC entre deux entités complémentaires, le PSC et l'OSC, montre deux caractéristiques qui sont surtout des avantages pour les "certificateurs" du marché :

- C'est la communauté d'utilisateurs via le PSC qui supporte les risques et donc la responsabilité du métier (le certificat porte la signature du PSC).

- La communauté d'utilisateurs est liée à UN SEUL certificateur du marché qu'elle intègre en tant qu'OSC. Cela permet d'apporter une clientèle captive et de créer un sous-marché sans concurrence au bénéfice de l'OSC. Dans l'architecture PKI classique, les fonctions d'AC et d'OSC sont assumées par une même entité qui se trouve en concurrence avec d'autres AC du marché pour subir une *évaluation* (American Bar Association) ou un référencement (comme pratique le Minefi à son profit).

2.2.3. Les effets induits

Pourtant, ce qui importe aux membre d'une communauté professionnelle… c'est de se faire reconnaître comme membre de cette communauté pour bénéficier de prestations et de services spécifiques ! Cette fonction de reconnaissance professionnelle, on dira "identité de la personne" et "attribut professionnel", est prise en charge par une *autorité d'enregistrement* qui fournit l'identité de la personne. Cette identité professionnelle garantie est alors transmise au certificateur qui n'a plus qu'à juger de l'appartenance d'une clé publique considérée à un détenteur professionnellement identifié. Il va de soi que la fonction d'enregistrement appartient à la structure de gestion de la communauté professionnelle. Pour prendre un exemple, les professions organisées ont-elles besoin d'une autorité de certification spécifique, alors que leur Ordre peut assurer tout naturellement les fonctions d'autorité d'enregistrement ?

On notera ici une conséquence pratique concernant la Politique de Certification et la Déclaration des Pratiques de Certification. PC et DPC sont en première analyse des documents antagonistes, l'un étant établi par la PKI et l'autre par le certificateur. Lorsque la configuration de certification montre une AC et un OSC, la DPC dérive directement de la PC. La PC décrit les grandes lignes et la DPC donne des détails sur les procédures ; ils sont du même côté de la barrière. Il arrive également que sous des appellations diverses, un document unique montre les caractéristiques de la PC et de la DPC. Pour la grande joie du rédacteur qui doit gérer ce qui revient à l'un et à l'autre en terme d'obligations, avec pour toile de fond leur responsabilité collective vis à vis de l'utilisateur en ce qui concerne l'émission de certificat.