



Lettre d'information
Décembre 2004 n°9

Les certificats numériques

Les télé-procédures, un enjeu au niveau central comme local

L'administration française, tant sur le plan central que local, est lancée dans un vaste chantier de mise en œuvre du potentiel des TIC. Les objectifs sont multiples :

- Améliorer la relation avec l'utilisateur
- Créer de nouveaux services centrés sur le citoyen
- Réduire les coûts pour dégager des marges financières
- Revaloriser les missions publiques
- Gagner en productivité

Les gains potentiels sont considérables, tant pour l'administration que pour l'utilisateur, à condition que ces services ne se construisent pas au mépris de la protection des libertés individuelles.

La double clef des champs... xml

EDITO

Les infrastructures de sécurité sont basées sur des techniques de cryptages de données. Les infrastructures à Clé Publique (PK) se justifient pour les actes administratifs (authentification forte et signature électronique à base de certificats numériques publics). Les infrastructures à clés symétriques réparties entre cartes et lecteurs sont adaptées pour des transactions rapides, à partir de bornes d'accès non connectées en permanence à un système d'information (« off-line »).

La CVQ « esp@ce administration », à technologie « à contact », permettra de réaliser des *télé-procédures* en liaison avec les collectivités locales ou territoriales de l'administration, dans une infrastructure PK.

Keynectis, partenaire important de notre projet a mis en place l'infrastructure que nous attendions. Nous avons maintenant la double clé des champs XML !

Une nécessité pour que les télé-services soient utilisés : la Confiance

Le manque de confiance est aujourd'hui le principal frein à l'utilisation des NTIC par les entreprises et les citoyens. Pour susciter l'adhésion des utilisateurs et prévenir les comportements frauduleux ou les dysfonctionnements, il est impératif de :

- Garantir la confidentialité des données personnelles dans leur transport (cryptage des connexions) et dans leur conservation (chiffrement persistant de message et de documents)...
- ... et le cloisonnement d'accès dans leur mise à disposition (authentification forte, gestion de droit ou d'habilitation)
- Garantir les systèmes contre l'usurpation d'identité (authentification, révocation en cas de vol ou perte, validation)
- Assurer l'intégrité des données dans leur transport et dans leur conservation (horodatage, archivage)
- Garantir l'équité et la transparence des transactions (signature, horodatage, accusés réception)
- Assurer la fiabilité des systèmes (performances, temps de réponse, disponibilité, continuité de service).

Pour répondre à l'ensemble de ces besoins de confiance, les technologies de la certification électronique offre une solution adaptée et éprouvée.

En pratique : qu'est-ce que c'est ? A quoi ça sert ?

Grâce au système de double clé (PKI), le certificat numérique va être la base de la signature électronique. Il permettra de "signer" un document (par son auteur), lui donnant ainsi "force probante" (loi du 13 mars 2000), de signer une transaction par l'expéditeur vers un destinataire sécurisé (clé publique), pour le destinataire de s'authentifier (clé privée), de crypter et décrypter un document ou une structure de données.

Comment ça marche ?

Dans le cadre des e-procédures, la délivrance de certificats est d'ores et déjà en fonctionnement avec une gestion déconcentrée et sécurisée.

Aujourd'hui, c'est l'ADeP en tant qu'entité fédératrice qui est « Autorité de certification » (garante du contenu du certificat) et « Autorité centrale d'enregistrement » (garante de l'adéquation identité personne/certificat). Elle produit des certificats à deux niveaux : pour les "opérateurs" et pour les simples usagers.

- Côté "opérateurs" : l'ADeP donne au maire (opérateur) une carte spécifique pour faire des certificats et les installer pour ceux qui dépendent de sa juridiction (élus, personnel délégataire...). Il est alors devenu « Autorité Locale d'Enregistrement » (ALE).

- Côté "usagers" : l'ADeP ainsi que les maires devenus opérateurs délivrent les certificats "usager". Demain, ce sera l'Etat qui sera Autorité de Certification et les maires Autorité d'Enregistrement.

Si vous souhaitez nous faire part d'informations, de réflexions en lien avec notre projet, n'hésitez pas à nous les communiquer. Nous les publierons dans un prochain numéro.

Contactez Audrey Amarguella :
facteur@chataigniers.fr

Un cadre de confiance

Les délivrances de certificats (que ce soit opérateur ou usager) ne peuvent se passer qu'en face à face. C'est la chaîne de confiance nécessaire à la sécurité du système.

En pratique

- Pour les adhérents, l'ADeP fournit à ses adhérents des cartes à puce personnalisées et des certificats opérationnels aux élus et à leurs collaborateurs (ayant délégation de signature).
- Pour les non-adhérents, il existe des conditions particulières et provisoires d'acquisition, à prix intéressant (pour plus de détails, veuillez contacter l'ADeP).

