Association pour le Développement des e-Procédures

Trait d'union

Lettre d'information Novembre 2001

Dossier Spécial n°3:

Sécurité des e-procédures

Sécurité : décrypter les procédures

Pas de garantie et de certification des e-procédures sans sécurité informatique sur l'ensemble de la chaîne de dématérialisation. L'Internet n'a pas franchement une réputation de réseau fiable. Pirates, virus, nombre d'épouvantails font peur et en freinent le développement. Le déploiement des univers de confiance sur l'Internet, le contrat électronique et sa valeur juridique supposent la sécurisation des transactions, leur notarisation. Il ne saurait y avoir de compromis sur la sécurité. La valeur d'une chaîne de confiance est égale à la valeur de son maillon le plus faible. A quelques jours de la livraison au SIVU des Inforoutes de l'Ardèche du premier serveur de sécurité créé en collaboration avec la société Ingénico Data System, partenaire de l'ADeP, l'occasion de faire le point sur la chaîne de sécurité qui contribuera à assurer la validité juridique de l'ensemble de nos e-procédures.

Les moyens de la signature : les bonnes cartes à jouer

- Carte citoyenne : pour tout et tous

L'ambition de la carte citoyenne est de fournir à l'ensemble des acteurs des e-procédures (mairies, collectivités locales, entreprises et citoyens) un moyen universel de signature électronique. La sécurité de la signature électronique est la clé de base de l'architecture de confiance du modèle de PKI (Public Key Infrastructure) mis en place par l'ADeP.

- Pourquoi la carte à puce ?

La loi précise que chaque signataire doit être seul détenteur des moyens de sa signature électronique. La carte à puce remplit cette condition et a démontré sa fiabilité technique. Par ailleurs, la France,

berceau de la carte, a une culture d'usage très forte (carte bancaire, carte vitale), ce qui en fait un outil facilement démocratisable. D'autres techniques existent, mais sont moins familières ou plus complexe.

La signature électronique ne saurait être réservée à une caste d'internautes ou d'informaticiens branchés, la carte est en effet un outil populaire.

- Quel type de carte ?

Le projet de la carte citoyenne s'appuie sur une carte à puce à cryptoprocesseur. La carte citoyenne utilise une puce qui permet non seulement de signer numériquement, mais également de crypter les données signées. Le code PIN de la carte est personnalisable, comme l'exige la loi, par son détenteur. La puce stocke à la fois la paire de clés asymétriques (privée et publique), et le certificat. GemPlus, leader mondial et partenaire de l'ADeP, nous a proposé sa carte GemSAFE 8Ko International ayant une capacité de stockage de 7.4 Kbytes. D'autres fournisseurs proposent des cartes comparables.

- Un certificat qualifié…

Les certificats utilisés par la carte citoyenne répondent aux normes internationales. De plus, leur production et leur maintenance respectent un cahier

des charges précis qui fait l'objet d'une homologation de la part des services du Premier Ministre. CertPlus, partenaire de l'ADeP, met à disposition de notre projet des certificats qui répondent à ces exigences de sécurité. Il existe aussi, sur ce secteur, d'autres fournisseurs répondant à ces critères.

PIN…PAD compromis sur la sécurité

Des lecteurs de cartes à puce sans PIN-PAD (clavier de saisie intégré au lecteur) obligent le signataire à taper son code secret sur le clavier de l'ordinateur. Il devient alors aisé à l'aide d'un petit programme d'intercepter le code saisi. Pour remédier à cela, le lecteur doit donc intégrer un PIN-PAD qui garantit la communication directe avec la carte comme illustré ci-contre par le lecteur Cyber-Comm d'Ingenico. *« Des chercheurs de l'université de Bonn en Allemagne, n'ont eu besoin que de deux heures pour mettre à mal la signature électronique saisie sur un clavier d'ordinateur. Avec le programme mis au point par leurs soins, le professeur Armin CREMERS, le Docteur Adrian SPALKA, et leur collaborateur Hanno LANGWEG récupèrent le PIN de la carte à puce contenant la clé privée pour utiliser la signature. La porte est alors ouverte à toute modification ou à toute transmission de document à l'insu de l'utilisateur. »*

Source : magazine @pplications n°3 – juillet août 2001

Une autre protection, parmi de nombreuses innovations en cours, serait d'utiliser un lecteur de carte biométrique qui remplacerait le code PIN par l'empreinte digitale du signataire.

Le serveur de sécurité : sur un plateau technique

L'ADeP a défini l'architecture d'un serveur de sécurité dont l'objectif principal est de garantir l'intégrité des données des e-procédures et à conférer à celles-ci une valeur juridique. Sous la direction de Philippe ROUSSELET, Emmanuel HAYDONT, Louis JENNY et Emmanuel CHAUDRON du groupe Ingenico, partenaire de l'ADeP, finalisent actuellement le développement de ce serveur qui sera installé à suivre sur le plateau technique du SIVU des Inforoutes de l'Ardèche et qui sera interfacé avec l'application de gestion du contrôle de légalité dématérialisé de Berger-Levrault, partenaire de l'ADeP.

Rôle du serveur de sécurité

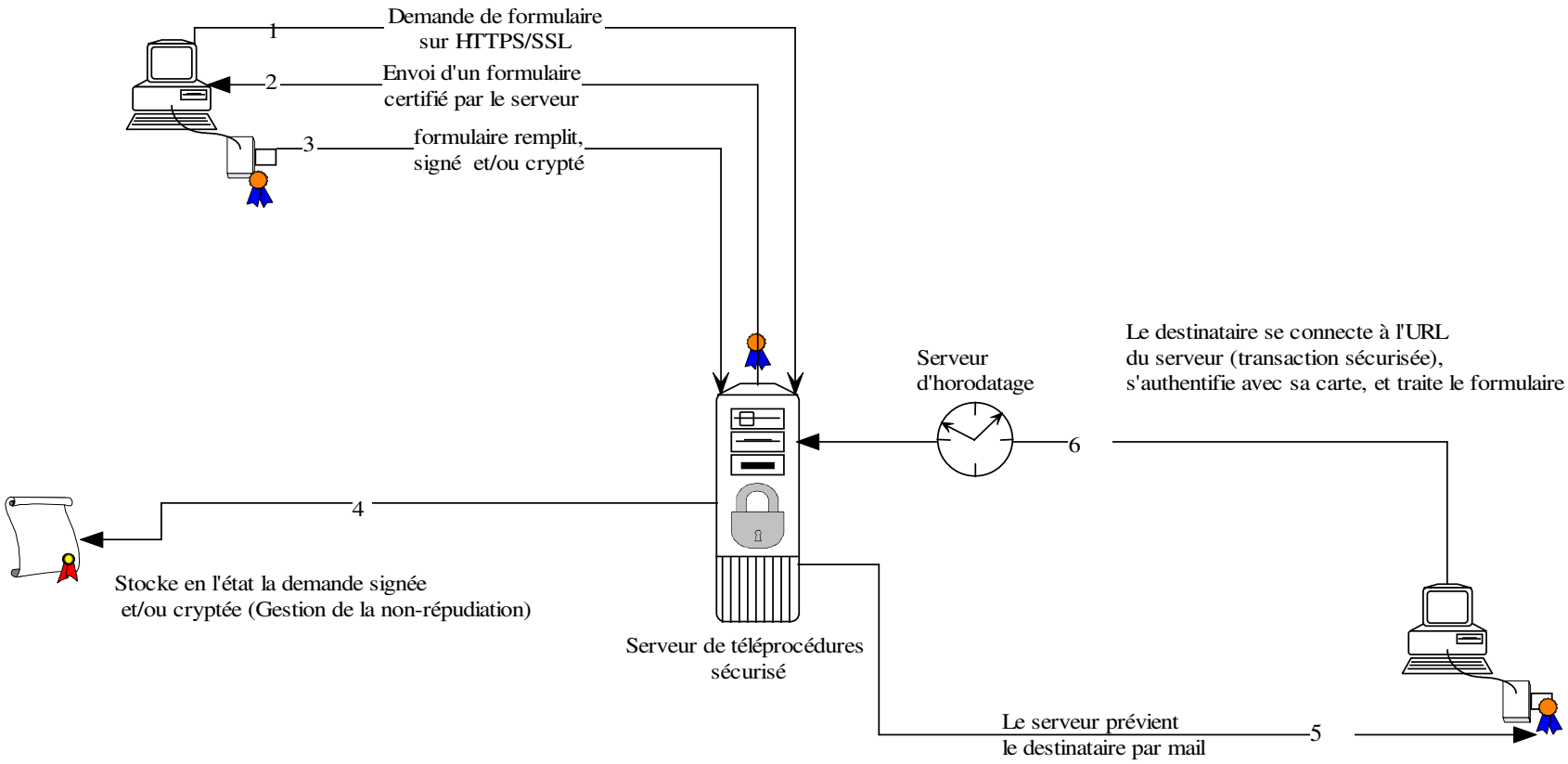
Un serveur de e-procédures doit fournir les fonctionnalités suivantes :

- Mise à disposition de formulaires garantis
- Identification de l'expéditeur et contrôle de son certificat
- Contrôle de l'habilitation
- Intégrité des données
- Alerte du destinataire
- Horodatage

Comment ça marche

Le serveur intervient dès qu'un expéditeur d'une e-procédure (mairie, citoyen, entreprise…) envoie un document signé à un destinataire. L'expéditeur se connecte alors au serveur, établit une connexion SSL (Secure Sockets Layer) et signe l'envoi de son document, celui-ci pouvant avoir été signé au préalable (séparation possible entre le signataire donnant valeur juridique et le "service courrier"). Le serveur reçoit le document, vérifie la validité de la signature (vérification du certificat, de la signature, et de la liste de révocation des certificats), demande un horodatage de l'empreinte du document au serveur d'horodatage. Il envoie alors un mail au destinataire, l'informant que quelqu'un lui a envoyé un document, et transmet enfin l'horodatage de réception à l'expéditeur. Le serveur intervient ensuite lorsque le destinataire, suite à la lecture de son mail, désire récupérer le document. Le destinataire se connecte sous protocole sécurisé au serveur qui vérifie son certificat. Dûment authentifié, le destinataire peut récupérer le document. Le serveur horodate la récupération du document par le destinataire et en informe l'expéditeur par mail.

e-procédure formulaire générique utilisant le serveur de sécurité



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. adep.projet@wanadoo.fr