



La garantie de la sécurité avec Naxfer

Naxfer permet l'envoi et la réception de tous types de documents sans limite de volume, et de façon entièrement sécurisée. La sécurité du transfert est effectivement garantie grâce à la somme d'outils à la pointe de la performance et reconnus par la communauté informatique internationale :

En premier lieu, Naxfer dispose d'une authentification forte. On peut considérer que l'authentification est forte lorsqu'elle suit des fondations essentielles pour garantir :

- L'autorisation ou contrôle d'accès (qui peut y avoir accès)
- La confidentialité (qui peut le voir)
- L'intégrité (qui peut le modifier)
- La traçabilité (qui l'a fait)

- L'authentification est assurée par le certificat X.509. Il s'agit d'un standard de cryptographie de l'Union internationale des télécommunications pour les infrastructures à clés publiques (PKI). X.509 établit entre autres les formats standards de certificats électroniques et un algorithme pour la validation de chemin de certification.¹

- Elle est également certifiée par une clé USB HASP d'Aladdin, qui a remporté le Codie award 2008 dans la catégorie Best Digital Rights Management (Meilleure gestion des droits numériques) de la SIIA (Software & Information Industry Association).²

HASP SRM établit un canal de communications sécurisé pour chaque session de communication entre le moteur de cryptage AES 256 bits hautement sécurisé et impénétrable de la clé HASP et l'application.

Cela crée un canal de bout en bout pratiquement hermétique au piratage qui assure un niveau de protection supplémentaire contre les attaques tentant de contourner l'utilisation de la clé de protection. En outre, chaque clé HASP HL intègre un système de licence évolué, proposant la capacité de stockage nécessaire pour un grand nombre de licences. La technologie unique Aladdin LicenseOnChip™, intégrée à chaque clé HASP HL, assure que vos licences sont protégées d'un point de vue matériel et réellement inviolables.³

- Le cryptage AES assure la confidentialité du transfert. En effet, il consiste en un processus qui transforme des données en une forme qui peut uniquement être lue par le destinataire prévu. Pour décoder le message, le destinataire des données cryptées doit posséder la clé de décryptage appropriée (mot de passe).

¹ <http://fr.wikipedia.org/wiki/X.509>

² <http://www.aladdin.fr/news/2008/hasp/srm-codie-winner.aspx>

³ <http://www.aladdin.fr/hasp/srm-protection-keys.aspx>



AES fournit un cryptage fort et est suffisamment sécurisé pour protéger les informations classifiées jusqu'au niveau TOP SECRET selon le gouvernement américain, en 2003.⁴ Naxfer implémente la confidentialité grâce au cryptage AES 256 bits. Le gouvernement a délivré à la société éditrice les autorisations nécessaires pour son utilisation au niveau européen.

- Troisième élément de sécurité de Naxfer, la conformité est respectée grâce à la **signature numérique**. Il s'agit d'un mécanisme permettant d'authentifier l'auteur d'un document électronique et de confirmer son intégrité.

Elle fait aujourd'hui l'objet d'une réglementation claire et rationnelle. Elle permet au lecteur d'un document d'identifier la personne ou l'organisme qui a apposé sa signature et garantit que le document n'a pas été altéré entre l'instant où l'auteur l'a signé et le moment où le lecteur le consulte.

- Enfin, Naxfer fait l'objet d'une clause de non-répudiation. Cette dernière offre la possibilité de vérifier que l'expéditeur et le destinataire sont bien les parties qui disent avoir respectivement envoyé ou reçu le message.

Autrement dit, la non-répudiation de l'origine prouve que les données ont été envoyées, et la non-répudiation de l'arrivée prouve qu'elles ont été reçues. C'est l'apparition d'un certificat de conformité numérique en fin d'envoi et à la réception qui confirme cette signature numérique. Elle a une valeur juridique en cas de litige.

⁴ <http://www.bitzipper.com/fr/aes-encryption.html>