HASHLOGIC
security solutions

Version 1.0 de Janvier 2007

Web Secure Server

Serveur de validation et gestion de preuves

Pourquoi choisir le Web Secure Server ?

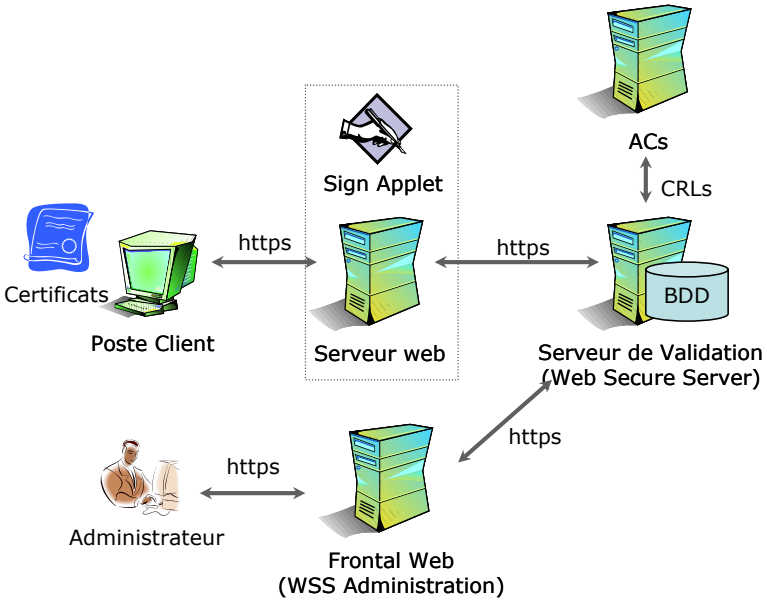
La dématérialisation des échanges tels que les factures, les commandes, les contrats, les déclarations administratives, le courrier, … est un enjeu majeur pour les entreprises qui veulent ouvrir leur système d'information pour faire face à des problématiques croissantes de partage de données, de rapidité d'accès à l'information et de réduction des coûts.

Les entreprises ont pris conscience de la nécessité de concilier l'essor d'Internet devenu inéluctable et la disponibilité des informations chaque jour plus stratégiques et confidentielles au niveau des applications bureautiques.

L'utilisation quotidienne d'outils de chiffrement et de signature devient de plus en plus incontournable.

Pour satisfaire à cette demande, HASHLOGIC propose des solutions simples et conviviales, qui permettent à tous d'accéder aux fonctions de signature et de chiffrement afin de leur garantir la confidentialité et la sécurité de leurs échanges électroniques.

Les solutions HASHLOGIC bénéficient de plusieurs années de Recherche & Développement et de mise en production sur des sites sensibles de grands groupes.



HASHLOGIC propose des solutions simples et conviviales, qui permettent à toutes les applications d'accéder aux fonctions de signature et de chiffrement afin de garantir la confidentialité et la sécurité des échanges électroniques

Sign Applet :

Signature d'un formulaire web

Web Secure Server :

WSS est une solution logicielle qui s'appuie sur les standards Internet et s'adapte à chaque nouvelle application pour fournir les services :

- validation des certificats,
- contrôle des signatures électroniques,
- chiffrement/déchiffrement,
- création de preuves,
- gestion des preuves

Administration centralisée

Le Web Secure Server (WSS) dispose d'une console d'administration accessible à partir d'un navigateur via un canal sécurisé (ssl) pour une administration centralisée.

L'accès à la console d'administration est réservé aux gestionnaires qui ont été déclarés sur le serveur.

© Copyright HASHLOGIC 2005-2007. Reproduction et diffusion interdites sans accord écrit préalable

Sign Applet : signature d'un formulaire web

Sous la forme d'une applet Java, **Sign Applet** s'adapte à chaque nouvelle application pour proposer dans des formulaires web la fonction de signature électronique à partir d'un certificat de signature pouvant être stocké dans une carte à puce ou situé dans un coffre fort de certificats (Web Key Server).

Le processus de signature respecte le principe de « What You See Is What You Sign » afin d'empêcher la signature sur des données cachées à l'utilisateur.

Les données signées sont construites en respectant la norme la plus répandue actuellement à savoir PKCS#7.

Intégration légère à l'aide des webservices

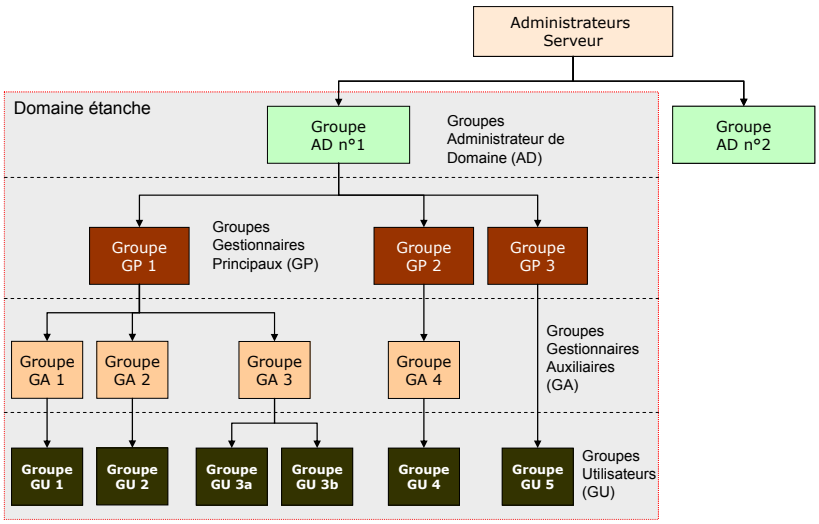
WSS propose un ensemble de fonctions accessibles par les applications web ou non web pour l'intégration des services de validation et de gestion de preuves.

L'utilisation des web services est réservée à des applications déclarées sur le serveur WSS.

Pour chaque flux traité, quelque soit le résultat obtenu, une preuve est constituée. Chaque preuve est signée par une autorité de séquestre afin de garantir l'intégrité des données.

Les preuves peuvent être horodatées par une Autorité d'horodatage et archivées sur des supports permettant leur consultation ou leur extraction ultérieures.

Une preuve contient toutes les données permettant d'être « rejouée » à n'importe quel moment.



Plusieurs catégories de gestionnaires

Le Web Secure Server est administré par plusieurs catégories de groupes de Gestionnaires : Administrateurs du domaine, Gestionnaires Principaux et Gestionnaires Auxiliaires.

La gestion est pyramidale pour que les opérations d'administration soient réalisées par les personnes proches des utilisateurs.

Par exemple, le Gestionnaire Principal gère les Autorités de Certification, la politique de sécurité, la création ou la suppression des groupes de gestionnaires auxiliaires, … et les Gestionnaires Auxiliaires quant à eux gèrent les comptes utilisateurs, les certificats, le help desk …

© Copyright HASHLOGIC 2005-2007. Reproduction et diffusion interdites sans accord écrit préalable

Administration des preuves

A l'aide d'une interface Web, le gestionnaire habilité dispose d'un moteur de recherche pour la consultation des preuves, l'extraction et la vérification des preuves.

Le WSS enregistre les données telles qu'envoyées sauf dans le cas où les données ont été chiffrées ou compressées alors l'enregistrement de celles-ci s'effectue en clair et non compressées.

Les données reçues font l'objet systématiquement d'un contrôle anti-virus. Ce contrôle est fait après déchiffrement et décompression des données.

Pour chaque flux, le WSS effectue une recherche de doublon pour la période donnée dans la base des preuves pour garantir l'unicité des transactions

Administration des pistes d'audit

WSS dispose d'un système de pistes d'audit pour chaque exécution de fonctions sur la console d'administration ou lors de l'exécution des web services.

Toutes les actions effectuées sur le serveur par les exploitants sont également enregistrées dans une piste d'audit.

A l'aide d'une interface Web, le gestionnaire habilité dispose d'un moteur de recherche pour la consultation des pistes d'audit.

Administration des Autorités de Certifications

Les Autorités de Certification sont enregistrées dans la base de données du Serveur par le gestionnaire habilité à partir de la chaîne de certification.

Administration des certificats

L'enregistrement d'un certificat permet aux gestionnaires d'une application de disposer de fonctions d'administrations notamment pour limiter l'accès à une application uniquement aux certificats référencés ou de suspendre l'utilisation d'un certificat instantanément sans attendre sa révocation par l'AC.

Administration des applications

La création et la configuration d'une application se fait via l'interface Web du Serveur par le gestionnaire habilité. Pour chaque application, un certain nombre d'éléments sont demandés :

Nom de l'application,

Liste des Autorités de Certification acceptées pour cette application,

Méthode d'enregistrement des certificats (auto enregistrement, enregistrement préalable, aucun enregistrement)

Caractéristiques de SignApplet

Navigateurs supportés :
Microsoft IE 5+, Netscape 4.7+, Mozilla 1.5+, Firefox 1.0+

Applet Java :
Signature de l'applet.

Format :
PKCS 7, SMIME V2, CMS

Type de support :
Compatible PKCS#11

Taille des clés RSA :
1024 ou 2048 bits

Algorithme de hachage :
SHA_1

Plate forme Java :
SUN JRE 1.3

Caractéristiques de Web Secure Server

Système d'exploitation :
Windows 2000, XP, Linux, JRE 1.4.1 de SUN.

Serveur d'application :
JBoss, WebMethods Integration Server 6.1+, WebLogic

Stockage des données :
compatible JDBC et LDAP

Module de sécurité (HSM) :
Tout matériel disposant d'une interface PKCS 11

Kit cryptographique :
IAIK JCE toolkit (Common Criteria EAL 3+)

Algorithmes cryptographiques :
RSA, TDES, AES, SHA 1, MD5, etc.

Protocoles de sécurité :
PKCS 7, PKCS 12, SMIME V2, CMS, XML DSIG, SSL V3,

Codages :
ASN 1, PEM, DER

Contraintes de disponibilité :
24H/24 et 7jours/7 + plan de secours.
Cluster pour gérer le "load balancing" ou pour s'intégrer avec tout autre load balancer

© Copyright HASHLOGIC 2005-2007. Reproduction et diffusion interdites sans accord écrit préalable