HASHLOGIC
security solutions

Version 1.0 de Janvier 2007

Web Key Server

Solution de déploiement des certificats à grande échelle

A propos de HASHLOGIC …

HASHLOGIC est Editeur spécialisé dans l'authentification forte et la sécurisation des échanges de données, des flux transactionnels et des applications.

Comment démocratiser l'usage des certificats ?

Les solutions HASHLOGIC répondent à des enjeux stratégiques tels que la dématérialisation des échanges, la webification des applications, la sécurisation des flux EDI ou transactionnels, l'ouverture sans risque des systèmes d'information,… Elles bénéficient de plusieurs années de Recherche et Développement et de mise en production sur des sites sensibles de grands groupes.

Le Web Key Server a été développé pour répondre à la problématique de déploiement à grande échelle des certificats. Cette problématique se trouve au cœur des préoccupations des entreprises et de leur politique de modernisation.

Le Web Key Server est une solution logicielle d'infrastructure, complémentaire aux infrastructures PKI, pour le déploiement en toute sécurité des certificats sans avoir à stocker les certificats sur le poste de l'utilisateur et sans avoir à fournir des supports physiques tels que des tokens ou des cartes à puce, …

Chaque utilisateur relié au réseau (intranet ou internet), accède de manière automatique et transparente à travers les applications (navigateurs, logiciels de messagerie, logiciels VPN, …) à leur propre coffre-fort dans lequel se trouve l'ensemble de leurs certificats au moment où l'utilisateur est confronté à des besoins d'authentification forte, de signature électronique et de chiffrement.

Le coffre-fort de certificats est situé sur un serveur qui centralise la gestion des certificats et clés numériques.

A quoi sert le Web Key Server ?

Le Web Key Server permet de démocratiser l'usage des certificats à partir desquels sont mis en œuvre les fonctions d'authentification, de signature électronique et de chiffrement / déchiffrement.

Grâce à l'utilisation des certificats, l'entreprise se donne les moyens d'une politique de sécurisation homogène et transversale à l'ensemble des ressources de son infrastructure. Ainsi, l'entreprise peut satisfaire à l'ensemble de ses besoins de sécurité :

- l'accès aux applications web ou non web
- l'accès à la station de travail de l'utilisateur et aux ressources du système d'information.
- la protection des documents sensibles
- la sécurisation des messages électroniques
- la sécurisation des flux transactionnels

Pourquoi choisir le Web Key Server ?

Grâce à une architecture centralisée, le Web Key Server permet de :

- **Palier à la vulnérabilité des certificats logiciels**

  Les certificats logiciels peuvent être perdus, volés, effacés accidentellement ou volontairement, copiés, dupliqués ou mêmes compromis. Les certificats logiciels ne permettent pas la mobilité des personnes. Les coûts de gestion et d'exploitation sont élevés en raison d'une architecture décentralisée.

- **Offrir une alternative à l'utilisation des supports physiques**

  Le Web Key Server est également une solution alternative séduisante à l'utilisation de supports externes tels que les Tokens ou les cartes à puce compte tenu du coût de la technologie et de la structure organisationnelle nécessaire pour supporter un déploiement à grande échelle.

- **Permettre la mobilité des personnes**

  Une même personne peut posséder plusieurs certificats accessibles depuis n'importe quel ordinateur relié au réseau. L'utilisateur a juste à sélectionner le certificat parmi les certificats rattachés à son compte pour satisfaire une fonction d'authentification, de signature ou de chiffrement.

- **Réduire les coûts de gestion et d'exploitation**

  La maîtrise des coûts de gestion est une préoccupation majeure pour les entreprises. La gestion centralisée des certificats permet de réduire considérablement le coût d'exploitation d'une infrastructure PKI.

- **Suivre une politique de mise en œuvre progressive et appropriée aux risques**

  Une démarche progressive permet de garantir un management maîtrisé des risques de sécurité. En fonction des risques identifiés pour une population, un site ou une application, le recours à des moyens d'authentification forte peut se limiter aux seuls utilisateurs concernés.

  Ainsi, il est possible de renforcer la sécurité en choisissant une technologie appropriée pour une population choisie ou une application jugée critique.

  Par exemple, grâce à la modularité du WKS, il est possible de planifier des investissements liés à l'acquisition des supports physiques. Ces investissements peuvent se faire par palier et progressivement ; Indépendamment du déploiement des fonctions de sécurité : authentification forte, signature, messagerie sécurisée, …

En conclusion, le Web Key Server accroît la sécurité mais pas la complexité, augmente la capacité de déploiement mais pas les coûts.

Les facteurs clés de réussite …

La réussite d'un projet de déploiement de certificats à grande échelle nécessite la maîtrise de plusieurs facteurs techniques et organisationnels :

- Utiliser une technologie ouverte et évolutive aussi bien dans l'environnement Microsoft que pour les produits Open source qui séduisent de plus en plus d'utilisateurs.
- Adopter une démarche par étapes successives maîtrisées car il est essentiel de capitaliser sur l'existant pour conduire une stratégie de modernisation.
- Mettre à la disposition des utilisateurs une technologie de qualité surtout lorsque celle-ci peut affecter la productivité de l'entreprise.
- Mettre à la disposition des exploitants un outil simple et convivial pour garantir la maîtrise tant des coûts d'exploitation que de la maintenance.

Seule la maîtrise de ces facteurs permet d'obtenir l'adhésion des utilisateurs.

Web Key Server

Généraliser et augmenter l'usage des certificats, pas les coûts

Simplicité d'utilisation

Une même personne peut posséder plusieurs certificats accessibles depuis n'importe quel ordinateur relié au réseau.

L'utilisateur a juste à mémoriser un seul et même code confidentiel valable pour chaque certificat présent dans le coffre-fort.

A l'aide d'un simple navigateur, l'utilisateur consulte le contenu de son coffre-fort : certificats, ACs habilitées, journal d'activités, … peut récupérer le certificat de chiffrement d'un correspondant à l'aide de son adresse email.

Les utilisateurs qui possèdent déjà des certificats peuvent les importer dans leur coffre-fort. Le chargement s'effectue à partir d'un fichier au format PKCS#12. Le protocole de sécurité prend en charge la sécurisation, le transfert et le stockage des clés numériques et du certificat.

Plusieurs personnes peuvent se partager un ordinateur et avoir chacun accès à leur propre coffre-fort de certificats.

Simple et facile à déployer à grande échelle

Aucune installation de progiciels n'est requise ni même de plug-in au niveau des applications.

Une simple installation du Provider HASHLOGIC (dll WKS-C) permet aux utilisateurs d'avoir accès à leur coffre-fort de certificats.

Une gestion centralisée pour une optimisation des coûts d'exploitation

Les gestionnaires déclarés sur le Web Key Server accèdent à l'aide de leur navigateur et via un canal sécurisé (https) à la console d'administration pour réaliser l'ensemble des opérations de gestion et d'exploitation des certificats.

Respect des normes et standards

La fourniture d'une interface PKCS#11 et d'une interface CSP permet de …

garantir une compatibilité avec tous les logiciels qui respectent ces interfaces : Internet Explorer, Outlook, Microsoft Office, Netscape, Firefox, Mozzila, Thunderbird, Lotus Notes, Adobe, …

Les postes utilisateurs sont banalisés et standardisés.

Une solution qui s'intègre à votre infrastructure PKI

Le Web Key Server s'appuie sur la PKI de votre choix.

Il a été qualifié avec un grand nombre de PKI du marché qui intègrent les interfaces PKCS#11 et CSP, la norme X509 v3 et utilise une procédure d'enregistrement avec interface web.

Par exemple : GIP CPS, Idéalx, Windows CA, VériSign, Thawte, Comodo, Trustify …

Externalisation possible (Hébergement par un tiers de confiance)

La solution peut être externalisée sans compromettre la sécurité du système puisque aucune information secrète non chiffrée n'est présente sur le Web Key Server.

Le Web Key Server stocke des informations protégées qui ne peuvent être accessibles que sur les postes utilisateurs et sous le contrôle d'un code confidentiel utilisateur.

Web Key Server

Une gestion centralisée pour une optimisation des coûts d'exploitation

La maîtrise des coûts de gestion est une préoccupation majeure pour les entreprises. La gestion centralisée des certificats permet de réduire significativement le coût d'exploitation d'une infrastructure PKI.

L'accès à la console d'administration est réservé aux gestionnaires qui ont été déclarés sur le web Key server. Ainsi, les gestionnaires à l'aide de leur navigateur et via un canal sécurisé (ssl) disposent d'un outil simple et convivial pour une administration centralisée.

Plusieurs catégories de gestionnaires

Le Web Key Server est administré par plusieurs catégories de groupes de Gestionnaires : Administrateurs du domain, Gestionnaires Principaux et Gestionnaires Auxiliares.

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 …

Définition de la politique de sécurité

Chaque coffre-fort dans lequel sont stockés les certificats numériques, est caractérisé par une politique de sécurité.

La console d'administration permet de configurer :

- La politique de recouvrement du code confidentiel,
- La politique de saisie des codes sur clavier physique ou clavier virtuel,
- La politique de gestion des certificats, verrouillage—déverrouillage des certificats révoqués ou expirés,
- La politique de séquestre des certificats de chiffrement,
- La politique de changement des codes, paramétrage de la fréquence et des modalités pour différer l'opération,
- L'attribution des ACs autorisées,
- L'activation du journal d'activités,
- Le nombre de code faux avant le blocage d'un compte

Gestion des coffres-forts utilisateurs

Les Gestionnaires habilités peuvent :

- Consulter les comptes utilisateurs,
- Gérer le cycle de vie applicatif des comptes utilisateur (suppression, suspension, levée de suspension) et pour chacun d'eux, gérer le cycle de vie applicatif des certificats associés (suppression, suspension, levée de suspension),
- Détecter les comptes débloqués,
- Consulter le journal d'activité associé à un compte.

Politique de sauvegarde sécurisée du code confidentiel

Les codes confidentiels sont utilisés pour protéger les clés privées et peuvent être sauvegardés en toute sécurité selon trois méthodes suivant le niveau de responsabilité accordé à l'utilisateur par le Gestionnaire Principal :

- Sous le contrôle exclusif de l'utilisateur (code oublié / code perdu)
- Sous le contrôle exclusif du/des Gestionnaire(s)
- Sous le contrôle conjoint du/des gestionnaires et de l'utilisateur.

En fonction du niveau de sécurité défini par le Gestionnaire, l'utilisateur à l'aide de son code PUK a la possibilité de récupérer son code confidentiel en ligne.

Gestion des informations sous séquestre

La console d'administration permet au gestionnaire désigné :

- d'extraire un code confidentiel rattaché à un compte en fonction de la politique de sécurité mise en place,
- de consulter la liste des certificats de chiffrement mis sous séquestre

- d’extraire un certificat de chiffrement mis sous séquestre

Référencement des Autorités de certification autorisées

Le Gestionnaire défini la liste des Autorités de certificats habilitées. Ainsi, un utilisateur pourra faire une demande de certificat uniquement auprès d'une AC reconnue ou importer dans son coffre un certificat appartenant à une des ACs référencées.

Mise à jour automatique de la disponibilité et de la validité des certificats

En fonction de la politique défini par le Gestionnaire, le Web Key Server verrouille ou déverrouille l'usage d'un certificat expiré ou révoqué. Cette option peut être définie sur les certificats de signature et/ou sur les certificats de chiffrement.

Ainsi, le Gestionnaire a la possibilité d'interdir en amont l'usage d'un certificat expiré ou révoqué.

Import export d’un compte utilisateur

Dans le cas d’une architecture composée de plusieurs serveurs Web Key Server, les gestionnaires disposent d’un service d’import et d’export d’un compte utilisateur pour gérer la problématique des mutations.

Gestion des versions

La diffusion d’une nouvelle version du Provider HASHLOGIC est automatique.

Lorsque une mise à jour est enregistrée sur le Web Key Server, l’utilisateur est informé dès qu’il se connecte par un message qui lui propose de confirmer la mise à jour ou de la différer.

Web Key Server

Accroître la sécurité, pas la complexité

Identification et authentification pour autoriser l'accès au Web Key Server

Avant d'autoriser l'accès au Web Key Server, l'utilisateur est préalablement identifié et authentifié à l'aide d'une valeur d'authentification calculée à partir du login et de son code confidentiel.

Un compte utilisateur se bloque après un nombre paramétrable de présentation d'un code d'authentification faux.

Le déblocage du compte s'effectue soit par l'utilisateur à l'aide de son code PUK soit par l'intervention d'un gestionnaire.

Espace de stockage étanche et sécurisé

L'utilisation des fonctionnalités du Web Key Server nécessite la création d'un compte utilisateur et l'allocation d'un espace de stockage étanche et sécurisé pour la gestion de plusieurs certificats (authentification, signature ou chiffrement).

Génération des codes confidentiels

Le code confidentiel et le code PUK (Public Unlock Key) sont générés aléatoirement sur le poste de l'utilisateur lors de l'activation du compte par son utilisateur.

L'utilisateur doit mémoriser le code confidentiel et garder précieusement le code PUK.

Sécurisation des échanges

Toutes les informations échangées entre le Web Key Server et les postes utilisateurs sont chiffrées.

Génération d'un bi-clé

Les clés privées d'un utilisateur sont générées puis chiffrées sur son ordinateur, et ensuite conservées chiffrées sur le Web Key Server, rendant toute compromission impossible même par les administrateurs du Web Key Server.

Téléchargement d'un coffre-fort de certificats

L'ensemble des certificats et clés privées chiffrées présents dans le coffre-fort de l'utilisateur est téléchargé en mémoire vive pour la durée d'une session sur l'ordinateur et effacé dès que l'utilisateur se déconnecte.

Séquestre des certificats de chiffrement

Suivant la configuration de la politique de sécurité, les certificats de chiffrement sont mis automatiquement sous séquestre et sous le contrôle des gestionnaires.

Utilisation d'une clé privée

Lorsque l'utilisateur a besoin d'un bi-clé et de son certificat pour signer un document ou s'authentifier, les clés sont déchiffrées juste le temps des calculs cryptographiques, soit quelques microsecondes, puis sont détruites.

Toutes les opérations sont faites dans la mémoire vive de l'ordinateur.

Aucune clé secrète n'est stockée sur le poste de l'utilisateur

Aucune clé secrète n'est conservée en mémoire de manière résidente sur le poste de l'utilisateur et aucune clé chiffrée présente sur le Web Key Server ne peut être déchiffrée.

Utilisation d'un clavier virtuel pour la saisie des codes

Suivant la politique de sécurité, l'utilisateur peut être contraint de saisir son code confidentiel à travers un clavier virtuel afin de parer à des attaques de type keylogger.

Web Key Server

Evaluation des risques

Le protocole de sécurité a été développé dans l'optique où un attaquant peut être un simple utilisateur connecté à Internet ou un exploitant, gestionnaire, administrateur du serveur ayant accès à toutes les données stockées en base de données. Le protocole est construit de telle façon que seule la personne connaissant le code confidentiel peut déchiffrer une clé privée.

Risques potentiels		Les parades du Web Key Server
Attaque sur le poste client	**(1)** KeyLogger ou robots spécifiques	Clavier virtuel ou Empreinte digitale ou badge de proximité
	Screenlogger	Déplacement aléatoire du clavier virtuel - Empreinte digitale - badge de proximité
	Dump Memory (mémoire vive) pour tenter de récupérer les clés privées.	**(2)** Risque résiduel négligeable
	vol, copie, destruction, compromission des certificats	Sans objet. Aucune information sensible n'est stockée sur le Poste Client.
Attaque en testant toutes les combinaisons du code Pin pour un compte utilisateur		Pour un compte l'estimation est de 2^{62} secondes. Trois tentatives avant blocage du compte utilisateur.
(3) Attaque de type man-in-the-middle ou de type sniffing		Communication sécurisée à l'aide du protocole SSL V3.
		Les communications avec le Web Key Server sont chiffrées.
(4) Attaques sur le serveur Web Key Server		Toutes les données stockées sur le serveur sont chiffrées. Seuls les utilisateurs peuvent déchiffrer leurs clés privées.

(1) Key Logger

Dans l'hypothèse où l'option a été activée au niveau de la politique de sécurité, l'identification de l'utilisateur vis-à-vis du Web Key Server repose sur :

a) Clavier virtuel : la saisie du code confidentiel devra se faire obligatoirement sur le clavier virtuel.

b) Badge de proximité : l'unicité du badge permet l'identification (exemple BlueLoc)

c) Empreinte digitale : la lecture de l'empreinte digitale

(2) Dump Memory

Les clés privées chiffrées contenues dans le coffre fort d'un utilisateur (situées sur le serveur) sont téléchargées en mémoire vive de l'ordinateur. Lors d'une opération d'authentification, de signature ou de déchiffrement, la clé privée chiffrée est déchiffrée puis utilisée pour réaliser l'opération, puis automatiquement détruite. La clé privée est donc présente dans la mémoire vive pendant quelques millisecondes.

Pour tenter de récupérer la clé privée, il est donc nécessaire de « dumper » la mémoire vive de l'ordre de 512 Mo à une fréquence suffisamment élevée pour espérer capturer les données.

Ensuite, les données devront être analysées pour tenter de localiser les fragments de la clé privée afin de l'extraire et la reconstituer.

(3) "Sniffing" ou "Man In The Middle"

Le Poste Client établit avec le Web Key Server une communication permettant l'authentification du Web Key Server. Toutes les communications entre le poste client et le Web Key Server sont chiffrées.

(4) Attaques sur le serveur Web Key Server

Toutes les clés privées des utilisateurs sont stockées chiffrées. Une personne ayant accès aux données stockées sur le serveur devra réaliser une attaque par force brute pour compromettre un seul compte.

Web Key Server

Les caractéristiques techniques

Caractéristiques du Provider HASHLOGIC

Système d'exploitation :
Windows 2000, XP, Vista

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

Langues :
Français et Anglais.

Interfaces :
PKCS#11 et CSP de Microsoft

Algorithmes :
Génération de clés RSA jusqu'à 2048 bits ; Algorithmes AES, DES (3DES), DSA, SHA-1, MD5 ;

Certificats :
X.509v3 (RFC 3279, RFC 3280)

Compatible avec tous les Progiciels compatibles avec les interfaces PKCS#11 et CSP Microsoft

	Navigateur	Messagerie	VPN	Progiciels
Produits Microsoft	IE 5+	OutLook OutLook Express		Microsoft Office
Produits Open Source	Netscape 4.7+, Mozilla1.5+, Firefox 1.0+	Netscape 4.7+, Mozilla 1.5+, Thunderbird 1.0+		
Autres		Lotus Notes	Cisco, CheckPoint, …	Sign & Crypt, AnySign, Adobe, …

Le Provider HASHLOGIC se base sur la configuration de Windows pour déterminer la présence et le paramétrage d'un proxy.

Caractéristiques de Web Secure Server

Système d'exploitation :
Windows 2000, 2003, XP, Linux, JRE 1.4.1 de SUN.

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

Stockage des données :
compatible JDBC, LDAP, Active Directory

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 :
SSL V3,

Codages :
ASN 1, PEM, DER

Contraintes de disponibilité :
Cluster pour gérer le "load balancing" ou pour s'intégrer avec tout autre load balancer

Librairie Web services :

Le Web Key Server propose des web services notamment pour la création des comptes utilisateurs, le chargement de certificats ou la génération de certificats par les utilisateurs, …