HASHLOGIC
security solutions

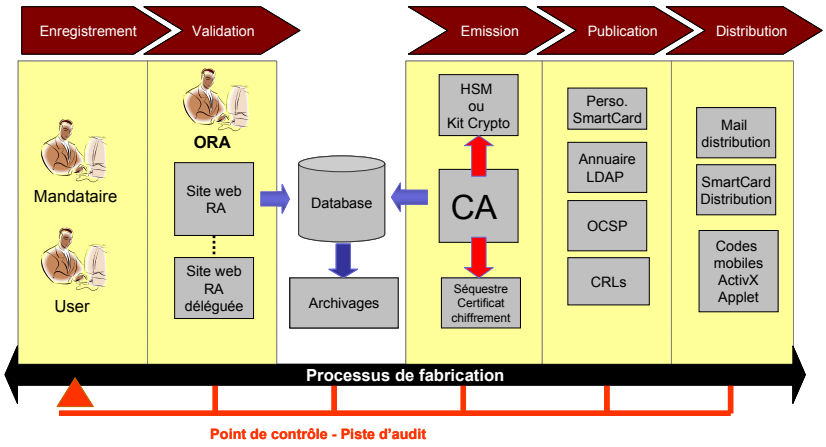
Version 1.0 de Janvier 2007

PKI Server

Une solution simple, performante et économique

Les projets ayant besoin d'une infrastructure PKI sont souvent freinés soit par le coût d'acquisition des logiciels, soit par leur coût d'intégration, soit par les bouleversements qu'engendre sur le SI le déploiement de la PKI.

HASHLOGIC bouleverse tous les préjugés en proposant une solution simple, performante et économique.



La plate-forme HASHLOGIC est fondée principalement sur des composants Open Source pour supporter l'intégration de nouveaux composants.

Respect des standards :

x509v3, CRL, OCSP, SCEP mais aussi les standards RSA : PKCS#7, PKCS#10, PKCS#11, PKCS#12.

Portabilité :

La technologie Java utilisée pour développer le logiciel garantit sa portabilité sur tout OS supportant une JVM : Windows, Linux, Solaris, AIX, HP-UX .

Environnement spécifique :

Le logiciel peut fonctionner avec tout type d'annuaire d'entreprise : Ldap, Active Directory, etc., ainsi qu'avec tout type de serveur mail.

En bref …

L'infrastructure logicielle et matérielle offre les moyens techniques permettant d'assurer l'ensemble des tâches relatives à la gestion du cycle de vie des certificats :

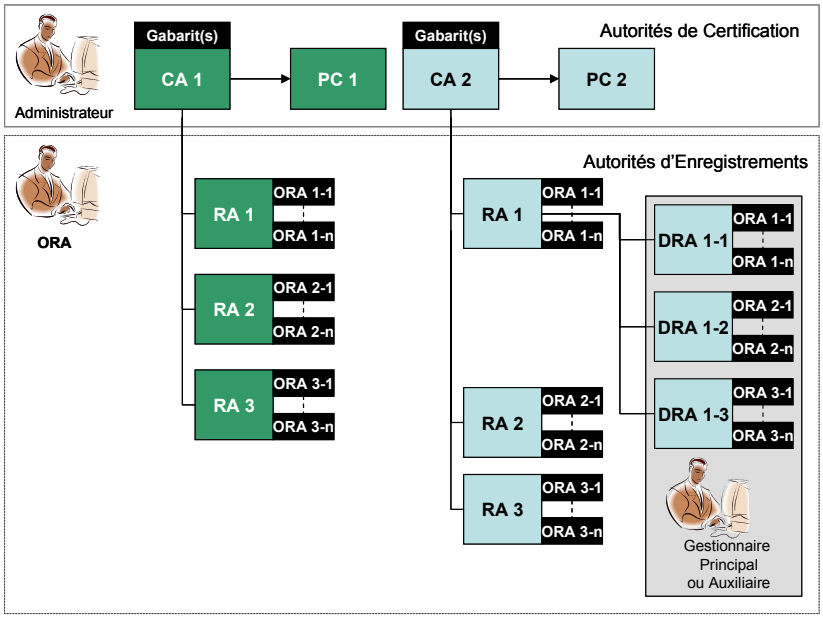
- Enregistrement des demandes de certificats à travers une autorité d'enregistrement principale ou déléguée
- Génération des bi-clés par l'utilisateur ou en back office (HSM ou software)
- Génération des certificats lors des demandes de certification
- Séquestre des certificats de chiffrements
- Distribution des clés et des certificats sous forme logicielle ou support matériel (carte à puce, token, …)
- Publication des certificats dans un Annuaire public
- Enregistrement des demandes révocations
- Publication des Listes de Certificats Révoqués (LCR)
- Répondeur OCSP
- Journalisation des évènements
- Archivage

Un modèle organisationnel souple et évolutif …

Le modèle organisationnel permet de distinguer les différents rôles :

- demandeur du certificat,
- Mandataire,
- Opérateur,
- Administrateur,

… de manière à rester ouvert à toutes les configurations potentielles des clients.



Autorités de certification (CA)

L'Administrateur dispose des moyens techniques pour créer

- des Autorités de Certifications (CA) et des sous autorités de certification,
- définir les gabarits de certificats et créer des Autorités d'Enregistrement (RA).

Autorités d'enregistrement (RA)

Une Autorité d'Enregistrement est créée par l'administrateur du serveur, qui lui attribue un label et des règles de gestions (moyens mise en œuvre pour enregistrer et valider les demandes de certificats, mode de distribution des certificats, etc).

L'autorité d'enregistrement est indépendante de l'autorité de certification. Elle est gérée par un ou plusieurs Opérateurs d'Enregistrement (ORA).

L'opérateur (ORA) a les droits pour une politique donnée de créer, renouveler ou révoquer des certificats, et créer des Autorités d'Enregistrement déléguées.

Autorités d'enregistrement Déléguées (DRA)

L'Autorité d'Enregistrement déléguée est créée par le gestionnaire principal de l'Autorité d'Enregistrement à laquelle elle se rattache. Elle est régie par les mêmes règles que son autorité.

Une Autorité d'Enregistrement Déléguée assure elle-même l'enregistrement de ses utilisateurs finaux.

Chaque RA déléguée a un ou plusieurs Gestionnaires principaux et un ou plusieurs Gestionnaires Auxiliaires. Ils ont les droits pour une politique donnée de créer ou révoquer des certificats.

Obtention d'un certificat

Le processus de création des certificats est une étape critique et essentielle dans la PKI.

Les seules personnes habilitées à délivrer des certificats sont les ORA.

Pré-enregistrement …

La demande de certificat s'effectue en ligne sur le site web RA à l'aide d'un navigateur standard par l'utilisateur ou par un Mandataire.

La demande consiste à renseigner un formulaire web pour pré enregistrer la demande de certificat.

Un contrôle strict par authentification du certificat du RA, est soumis à cette demande.

Validation …

L'ORA est informé par mail des demandes de certificat en instance de validation.

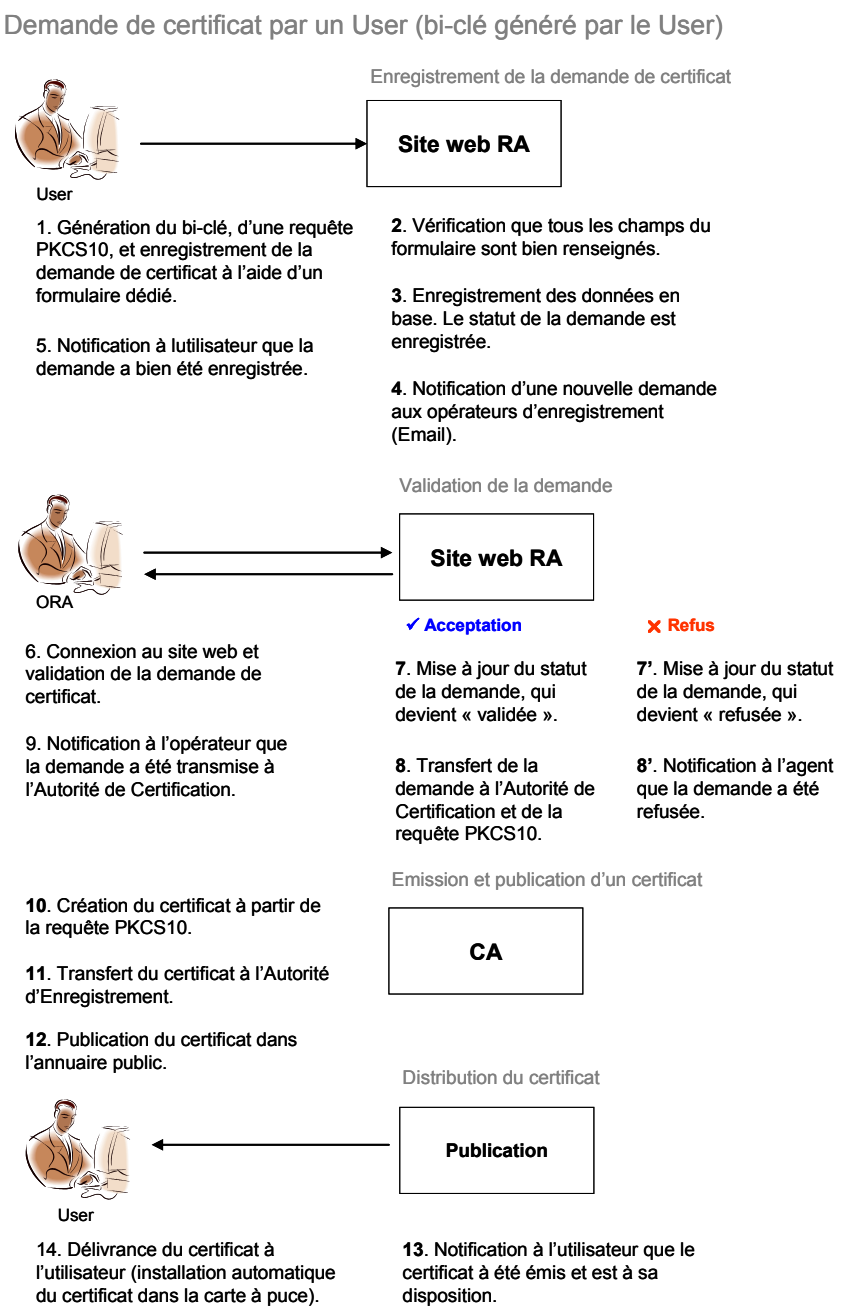
L'Opérateur utilise sa carte à puce pour accéder à la console d'administration à l'aide de son navigateur via un canal sécurisé en SSL v3.

L'Opérateur est chargé de contrôler la validité des données.

Si les données sont correctes, l'Opérateur valide la demande et enclenche la fabrication d'un certificat.

En revanche, s'il considère que les données ne sont pas valides, il refuse la demande de certificat.

Le demandeur est alors informé par mail dans lequel la cause du rejet est indiqué.



Révocation d'un certificat

Le processus de révocation s'établit en plusieurs étapes :

- demande de révocation par le détenteur du certificat ou une autre personne (Mandataire)
- enregistrement de la demande de révocation
- révocation effective par l'Autorité de certification
- publication dans la liste de révocation

Demande de révocation

Le détenteur de certificat peut demander la révocation de son certificat auprès de l'Autorité responsable de son enregistrement pendant les heures ouvrées.

Toute demande de révocation est soumise à la vérification de l'identité du demandeur et doit mentionner la cause de révocation.

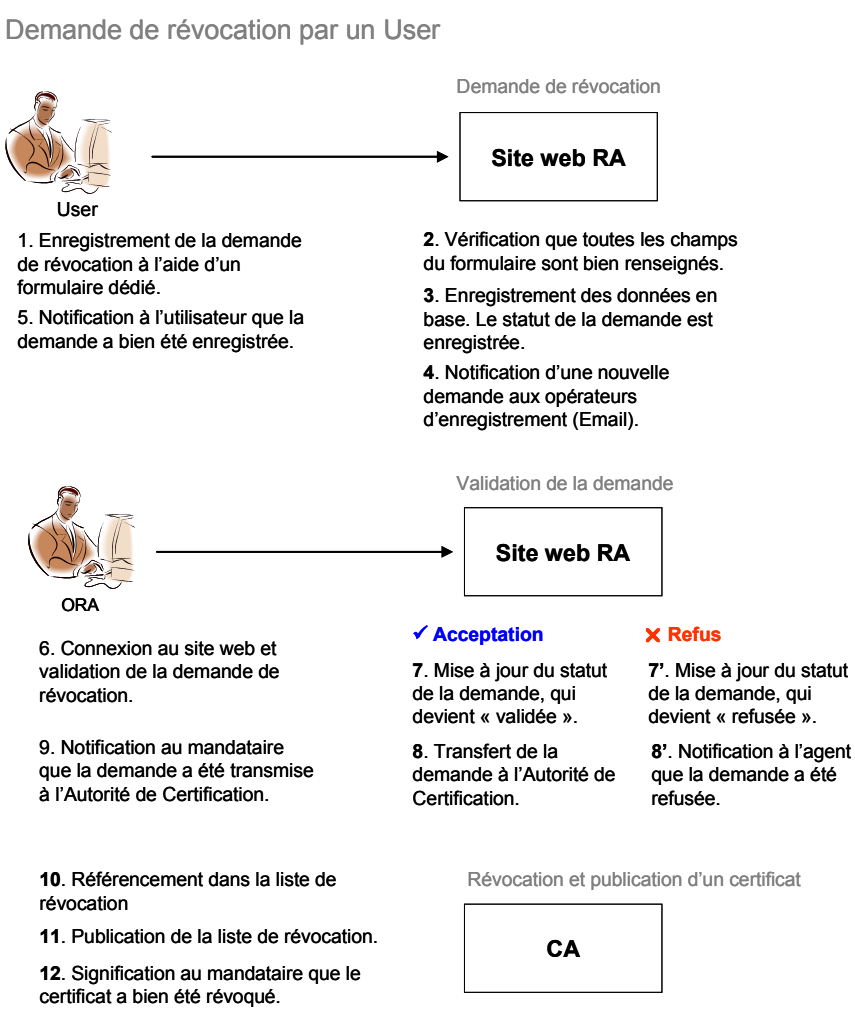
Il dispose également d'un service de révocation accessible 24h/24 via une interface web. Cette interface permet de demander la révocation d'un certificat après que le détenteur s'est authentifié à l'aide de la « pass-phrase ».

Enregistrement de la demande

Les responsables ayant autorité pour prendre en compte et valider une demande de révocation sont les opérateurs ORA pour l'Autorité d'Enregistrement et les Gestionnaires Principaux ou Auxiliaires pour les Autorités d'Enregistrement Déléguées. L'identification de la demande peut se faire :

- En face-à-face à l'aide d'une carte d'identité ou tout document pouvant identifier de manière sûre le demandeur.
- Par téléphone, le responsable identifie le demandeur par un questionnaire
- A l'aide d'une « pass-phrase », celle-ci étant propre à chaque propriétaire d'un certificat.

Le traitement de la révocation est un processus automatique. Aussi, la demande est enregistrée de manière quasi-immédiate.



Révocation effective

L'Autorité de Certification est l'unique entité autorisée à révoquer définitivement un certificat. Elle traite les demandes de révocations à l'aide de procédures automatiques afin que soit publié le certificat dans la liste de révocation. La révocation sera effective lors de la prochaine publication de la CRL.

Publication

La CRL est publiée automatiquement à une fréquence paramétrée au niveau du module logiciel CA, dans une plage pouvant prendre toutes les valeurs possibles exprimées en minutes. En cas d'extrême urgence, il est possible de forcer manuellement la publication d'une CRL.

Recouvrement

Le produit permet de faire le séquestre des clés de chiffrement des utilisateurs.

Mise sous séquestre d'un certificat de chiffrement

Lorsque les bi-clés et certificats sont produits de façon centralisée sur le serveur, un module de séquestre permet de conserver de manière sécurisée les bi-clés et certificats produits.
Pour ce faire, un fichier au format PKCS12 contenant le bi-clé et le certificat est créé et chiffré à l'aide d'un certificat de séquestre.

Extraction d'un certificat de chiffrement

Pour extraire un bi-clé et un certificat de chiffrement sous séquestre, le Gestionnaire habilité doit disposer du certificat de séquestre (certificat généré lors de l'activation de la Politique de Sécurité).
Le bi-clé et le certificat sont alors regroupés dans un fichier au format PKCS12 stocké sur le poste du Gestionnaire.

Publication

La publication permet de rendre disponibles les certificats de clés publiques émis, à l'ensemble des utilisateurs de ces certificats.

Mode de publication

L'accès aux certificats de clés publiques s'effectue via un annuaire de type X.500 à l'aide du protocole LDAP.
Sur le serveur Web, une procédure automatique et périodique, vérifie la mise à jour de la CRL et la rend disponible et accessible par un lien URL en http.

Procédure de publication

La publication d'un certificat est subordonnée au respect de la procédure de traitement des demandes. Les certificats sont publiés dès leur émission.

Purge des annuaires

Un mécanisme de purge automatique peut être activé permettant de supprimer tous les certificats périmés de la base de données et de l'annuaire notamment les certificats révoqués dont la date est périmée.

Logs

Le produit dispose d'un système de logs permettant un suivi précis de toutes les opérations effectuées.
Toutes les opérations de traitement des demandes de certificats à chaque étape du processus sont enregistrées et tracées.

Librairie APIs

Le Server PKI propose un ensemble de webservices accessibles par les applications web ou non web pour l'intégration des services PKI.

L'utilisation des webservices est réservée à des applications (serveur) déclarées sur le PKI Server.

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

Espace disque
L'espace disque nécessaire au Serveur est de 300 Mo.

Horodatage
L'horodatage des fichiers et des preuves repose sur l'horloge système du serveur.

Synchronisation temporelle
L'horloge système du serveur doit être régulièrement surveillée pour corriger toute dérive. (Synchronisé temporellement à l'aide du protocole NTP).

Administration
Le Serveur dispose d'une console d'administration accessible par un navigateur en https.

Supervision
Redirection des alarmes, des logs à destination des exploitants vers l'outil de supervision lorsque l'accès à la base de données est impossible.

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, …