

L'enregistrement, la création et la gestion d'identités sûres



MetaPKI, pour gérer les certificats

Dans un contexte de dématérialisation des échanges internes ou des échanges avec leurs clients ou leurs partenaires, la sécurité du Système d'Information (SI) est un enjeu essentiel pour les organisations. Les certificats électroniques permettent aux applications d'intégrer des services de sécurité tels que l'authentification des utilisateurs, la non répudiation des transactions ou la confidentialité des échanges de données. Bull, acteur européen de la sécurité, propose MetaPKI, une solution complète pour créer des certificats électroniques et gérer leur cycle de vie.

Garder la maîtrise de la sécurité.

Les certificats électroniques peuvent être utilisés pour assurer :

- l'authentification forte des utilisateurs à l'aide de deux facteurs : carte à puce ou clé USB et PIN;
- l'authentification forte des serveurs web (SSL/TLS);
- l'authentification forte des réseaux privés virtuels (VPNs - Virtual Private Networks);
- les signatures électroniques pour assurer la non répudiation des transactions;
- la confidentialité des données échangées ou stockées.

Chaque utilisateur ou application peut recevoir une ou plusieurs paires de clés (une clé publique et une clé privée) et des certificats fournis par une Autorité de Certification (AC) qui associent un identifiant à chaque clé publique.

MetaPKI supporte une ou plusieurs ACs, indépendantes ou subordonnées, ainsi qu'une gamme de profils de certificats. Pour chaque profil, le processus d'enregistrement peut être personnalisé afin de répondre aux besoins spécifiques des organisations et d'être intégré au SI existant.

Le processus d'enregistrement est géré par un outil collaboratif utilisant une ou plusieurs Autorités d'Enregistrement Locales afin de réduire au minimum le temps de production et de gestion des certificats électroniques.

Accompagner la croissance.

La modularité de MetaPKI et son mode de commercialisation permettent de disposer d'une solution souple et évolutive, adaptée aux besoins de l'entreprise: nouveaux types de certificats, nouveaux processus de gestion, nouvelles organisations des services, nouvelles ACs. La solution comporte des services de séquestre et de recouvrement de clés pour les clés de déchiffrement.

Bull, acteur européen de la sécurité.

Bull fournit des services de conseil, de formation et de support afin de définir le meilleur moyen pour intégrer la solution dans les applications du SI. (ex: SSO). Bull propose également l'hébergement de la solution MetaPKI dans ses centres d'infogérance hautement sécurisés.

SERVICES DE SECURITE



Architect of an Open World™

Une solution pour des applications sûres

MetaPKI est géré au moyen d'interfaces web personnalisées, permettant ainsi aux ordinateurs équipés d'un navigateur web standard d'accéder à l'ensemble des fonctions.

MetaPKI intègre les entités fonctionnelles suivantes :

- Autorité de Certification (AC), chargée de générer les clés et les certificats électroniques sur la base de profils préalablement définis et en accord avec les politiques de certification;
- Autorité d'Enregistrement(AE), qui peut être locale ou non, pour l'inscription et la vérification de l'identité des porteurs de certificats (personnel ou équipements informatiques);
- Service de Révocation pour révoquer les certificats avant la fin de leur validité, au moyen de Listes de Révocation de Certificats (LRCs) et/ou de serveurs supportant le protocole OCSP (RFC 2560).
- Service de Publication pour la diffusion des clés et des certificats aux porteurs et, en option, l'accès aux certificats pour les tiers.
- Service de séquestre et recouvrement des clés, en option, pour les certificats utilisés pour la confidentialité des données.

Chaque entité fonctionnelle est gérée au moyen de rôles dont la relation avec le personnel est définie par l'organisation.

MetaPKI intègre en option les entités fonctionnelles suivantes :

- GesCard, un service de gestion de cartes pour la personnalisation et le déblocage des cartes à puce;
- Service de Validation de Certificats (SVC), pour vérifier la validité d'un certificat par rapport à une politique de validation.

MetaPKI comprend des mécanismes de sécurité renforcés :

- L'accès à toutes les entités fonctionnelles de MetaPKI est contrôlé. Les opérateurs agissant en tant que gestionnaires doivent être authentifiés de manière forte (i.e. un PIN et une carte à puce ou une clé USB);
- Toutes les actions concernant la gestion des certificats sont archivées dans une base de données. Tous les certificats liés à une entité donnée peuvent être consultés par des opérateurs bénéficiant d'une autorisation.
- Les communications entre les entités fonctionnelles sont protégées. Toutes les informations stockées dans une base de données sont protégées.
- Les clés privées et publiques, sont protégées par un HSM (Hardware Security Module). Bull intègre différents types de HSMs, fournis par Bull ou bien des tiers.

Normes et standards:

- Format des certificats conforme à l'ITU-T X.509v3 et au RFC 5280;
- Référentiel Général de Sécurité créé par l'article 9 de l'ordonnance n°2005-1516 du 8 décembre 2005 (RGS_A);
- Profils des certificats conformes à ETSI TS 101 862, Netscape et Microsoft;
- Informations de Révocation conformes à l'ITU-T X.509v2 CRL et au protocole OCSP (RFC 2560);
- Demandes de certificat: PKCS#10, SPKAC;
- Format d'échange de clés : PKCS#12;
- Connectivité : LDAP, HTTPS, SMTP;
- Interface HSM : PKCS#11;

Exigences techniques:

- Plateforme Linux (e.g. RedHat ou SuSE);
- Composants Open Source internationaux fournis avec MetaPKI: Apache, OpenSSL, PostgreSQL et PHP;
- Serveur LDAP : quand l'AC publie un certificat et/ou une CRL dans un annuaire;
- Serveur mail SMTP : quand MetaPKI envoie des consignes pour la gestion des certificats.