



Chiffrement
Authentification
Signature
Dématérialisation
Gestion des Clés

MetaPKI, la PKI d'entreprise

La sécurité du Système d'Information est un enjeu essentiel pour l'entreprise et plus encore depuis l'ouverture et l'intégration des S.I. entre eux. Les certificats électroniques apportent une réponse à ce besoin, avec en particulier le chiffrement des échanges et l'authentification des utilisateurs. Bull, acteur européen de la sécurité, propose MetaPKI, une solution complète pour créer et gérer le cycle de vie des certificats électroniques.

Garder la maîtrise de sa sécurité

La dématérialisation des échanges interentreprises et les applications de l'e-administration se généralisent et imposent de nouvelles règles de sécurité. Le certificat électronique, qui repose sur les technologies de PKI (Public Key Infrastructure ou Infrastructures à Clé Publique) permet de signer un document en attestant de l'identité de l'expéditeur tout en garantissant l'intégrité et la confidentialité des données.

Sa finalité :

- l'authentification forte des utilisateurs à partir de cartes à puces ou clés USB ;
- la signature électronique pour assurer l'intégrité et la non répudiation des échanges ;
- le chiffrement des données.

Les solutions de PKI sont conçues pour réaliser la gestion sécurisée des clés en apportant des fonctions de génération, de diffusion et de révocation des clés et des certificats. Les techniques reposent aujourd'hui sur la cryptographie

asymétrique. Chaque utilisateur doit être équipé d'un couple de clés (publique et privée), ce qui nécessite une bonne maîtrise de leur diffusion, dans un contexte de confiance.

Accompagner la croissance

MetaPKI gère l'ensemble du cycle de vie du certificat depuis l'enregistrement des utilisateurs jusqu'au support de la solution. Sa modularité et son mode de commercialisation permettent de disposer d'une solution très évolutive, adaptable aux nouveaux besoins de l'entreprise. La solution permet aussi d'exploiter pleinement les multiples fonctions offertes par la cryptographie à clé publique.

Bull, acteur européen de la Sécurité

Leader européen de la sécurité intégrée, Bull a développé une expertise unique de la sécurité des S.I., conjuguant un savoir faire de conseil et d'intégrateur et la maîtrise des technologies de souveraineté.



Architect of an Open World™

Une solution de sécurité complète

MetaPKI intègre les différentes entités fonctionnelles et de services

- **AC, l'Autorité de Certification**, pour générer les certificats en associant l'identité d'une personne ou d'un système à un couple de clé et à un certificat électronique ;
- **AE, l'Autorité d'Enregistrement**, pour l'inscription et la vérification de l'identité des utilisateurs ;
- **SP, le Service de Publication des certificats** pour la diffusion des clés vers les référentiels et les utilisateurs,
- **AEA, Autorité d'Enregistrement Administrative** ;
- **AEL, Autorité d'Enregistrement Locale** ;
- **SA, Service d'Administration** ;
- **SR, Service de Recouvrement**.

Chaque entité :

- est dupliquée et répartie pour reproduire l'organisation et implémenter les Politiques de Certification de l'Entreprise ;
- dispose d'une interface dédiée et personnalisée pour s'adapter à vos besoins et s'intégrer à votre S.I.

MetaPKI comprend des mécanismes de sécurité renforcés

Contrôle d'accès aux différentes entités et services

Tous les opérateurs sont déclarés et chaque opérateur dispose d'un certificat d'authentification qui peut être stocké sur une carte à puce. Les droits d'accès sont gérés avec le Service d'Administration. Tous les accès sont contrôlés et tracés.

Communications sécurisées entre entités via des messages de type PKCS#7 (S/MIME)

Chaque message est stocké dans la base de données. L'ensemble des messages constitue un dossier complet.

Intégration d'un composant cryptographique matériel (HSM)

- pour renforcer la protection des clés de l'Autorité de Certification et/ou des clés privées des entités (AC, AE, AEL, ...)
- pour générer les bi-clés ;
- pour accélérer les communications SSL.

MetaPKI implémente les normes et standards au niveau des interfaces et protocoles

- X.509 v3 pour les certificats ;
- PKCS#11 pour accéder aux ressources cryptographiques ;
- PKCS#12 pour la génération de certificats en central ;
- PKCS#10 et SPKAC pour les demandes de certificats ;
- LDAP pour l'accès à l'annuaire ;
- HTTP et HTTPS pour l'utilisation, l'administration et la publication web.

Un environnement technique ouvert

MetaPKI est développé par Bull sur des composants techniques Open-Source (Linux, Apache, Open-ssl, PostgreSQL et PHP) et est qualifié sur les principales distributions Linux (RedHat, Debian, SuSE et Mandriva).

Bull s'appuie sur l'ensemble de ses compétences sécurité et services et propose :

- la fourniture de l'ensemble des composants de l'infrastructure de confiance ;
- la définition, la mise en place et l'intégration de la solution ;
- l'accompagnement au changement et la formation ;
- le support ;
- l'hébergement sur les centres hautement sécurisés de Bull.

Cadre d'usage et cycle de vie du certificat

