

## OpenTrust™ PKI



### **La base de la Confiance Electronique pour la gestion des identités digitales des utilisateurs, des composants réseau et des applications**

#### **La PKI leader du Marché**

- Gestion complète et intégrée du cycle de vie des identités digitales associées aux utilisateurs, aux composants réseau et aux applications
- Une solution limitant les coûts de possession, reconnue et largement adoptée par le marché
- Nombreux connecteurs disponibles (WS/SOAP) simplifiant l'intégration au SI
- Une solution ouverte, modulaire et évolutive
- Gestion centralisée ou décentralisée des paires de clés
- Support intégré de multiples Autorités de Certification associées à différents usages
- Gestion intégrée du cycle de vie des certificats numériques dans l'infrastructure IT
- Architecture modulaire procurant souplesse et simplicité d'exploitation

#### **Le Principal**

L'accélération du développement technologique est accompagnée en parallèle par une cybercriminalité de plus en plus sophistiquée qui menacent les infrastructures informatiques des entreprises dans le monde. Cela a conduit à la nécessité de mettre en œuvre rapidement des solutions de sécurité plus abouties pour contrer efficacement ces nouveaux risques tous les jours plus complexes à déjouer.

OpenTrust PKI est une solution ouverte, modulaire et hautement évolutive conçue pour répondre à ce besoin. Cette solution innovante et éprouvée du marché est l'un des principaux produits OpenTrust pour la construction d'un écosystème de confiance.

OpenTrust PKI crée, distribue et gère les identités numériques des utilisateurs ou des devices au sein d'une infrastructure de confiance. Il supervise la gestion complète des certificats dans les infrastructures informatiques, compatible avec tout type de cartes à puce ou tokens qui intègre un certificat X.509 et une paire de clés.

L'architecture modulaire de OpenTrust PKI permet de s'intégrer à des applications uniques ou multiples, la gestion des certificats et des clés peut être gérée au choix en centralisé ou en décentralisé.

Mis en œuvre en interne OpenTrust PKI répond point par point au concept de PKO défini et recommandé par le Gartner Group.

OpenTrust PKI s'intègre simplement à l'infrastructure informatique existante des entreprises et bases de données grâce à sa conception et son architecture ouvertes. Il gère le cycle de vie des identités numériques de toutes les entités, les utilisateurs, des dispositifs ou des applications dans les systèmes informatiques et par conséquent constitue la base d'un écosystème de confiance.

Déjà déployée et utilisée quotidiennement par des millions d'utilisateurs, OpenTrust PKI est la solution leader du marché et est d'un faible coût total de possession.

Avec un rapide retour sur investissement et des connecteurs standards vers les autres composants informatiques du système, OpenTrust PKI permet de mettre en place de manière progressive et aisées tout niveau de sécurité avancé pour la gestion de toutes les entités numériques, les utilisateurs, les devices ou les applications, au sein de l'infrastructure informatique.

Les solutions de sécurité OpenTrust ont déjà été adoptées par de très nombreuses entreprises multinationales ou par des administrations et des gouvernements. OpenTrust PKI est devenue la solution leader du marché et est reconnue comme une solution d'authentification forte facile à mettre en œuvre et à intégrer.

### ***OpenTrust PKI, une solution globale pour construire votre environnement de confiance***

#### ***Mobilité & Ecosystème***

- Authentification utilisateur
- Chiffrement de fichiers et courrier électronique,
- Accès via un portail VPN/SSL

#### ***Infrastructure IT***

- Authentification forte 802.1x et IPSec (postes de travail, téléphones IP, PDA, Smartphones, serveurs...),
- Protection de vos serveurs (SSL)

#### ***Applications & Processus***

- Signature électronique de vos documents
- Authentification des processus et applications Horodatage

#### ***Avantages de la Solution***

- Gestion complète du cycle de vie des certificats et des autorités de certifications
- Modulaire, ouverte et respectant les standards
- Architecture SOA (connecteur SOAP) pour mieux s'intégrer dans votre SI
- Intégration native dans les architectures Microsoft (auto-enrôlement)
- Réversibilité (dépôt officiel des codes sources à l'APP)
- Facilité de déploiement, d'administration et d'exploitation
- Adaptée aux déploiements les plus larges
- Impératif de minimisation du coût de possession intégré dès la conception du logiciel (concept *Simplicity by Design*)

#### ***Modules Intégrés***

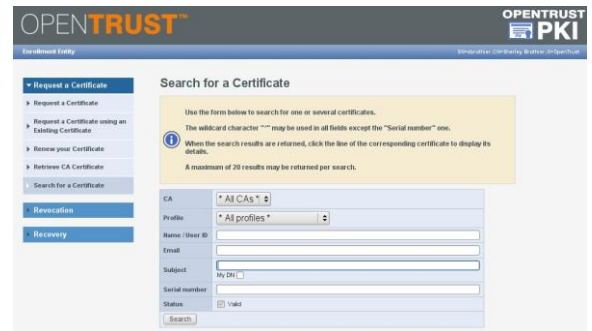
- Autorité de certification racine en ligne ou hors ligne
- Gestion d'autorités de certification multiples
- Sauvegarde et recouvrement des clés de chiffrement
- Serveur OCSP
- Moteur de workflow sécurisé
- Entités d'enrôlement
- Connecteurs SCEP, CMC et SOAP
- Publication multiple des certificats et CRLs

#### ***Caractéristiques Techniques***

- Intégration native aux environnements *Microsoft*: Active Directory, multi-domaine, multi-forêt, fonctions d'auto-enrôlement (utilisateurs, postes, serveurs, contrôleurs de domaine)
- Support des annuaires LDAPv3
- Gestion des CRLv2 et du protocole OCSP
- Interface d'administration et d'utilisation de type Web
- Haute-disponibilité de l'architecture de confiance
- Connecteur SOAP RA et EE pour l'intégration du cycle de vie des certificats dans les applications tierces

### Console D'administration

- Entièrement graphique
- Module de Gestion avancée des logs
- Gestion complète des profils et gabarits de certificats et du paramétrage
- Gestion fine et complète des droits des opérateurs de sécurité
- Traçabilité des opérations



### Plates-formes supportées

- RedHat Enterprise Linux 4
- Novell SUSE Linux Enterprise Server 9

### Equipement Supportés

- Cards/Tokens: Oberthur, Aladdin, Gemalto, Giesecke & Devrient, Vasco
- HSM: nCipher, SafeNet, Utimaco, Bull, Banksys

### Standards et Protocoles

- X509v3, S/MIME, LDAPv3, PKCS#1, #5, #7, #8, #10, #11, #12, SSLv3, TLSv1, RFC 2459, 3280, 3161

### Algorithmes Supportés

- Algorithmes Asymétriques: RSA (up to 8192 bits)
- Algorithmes De Hachage: SHA-1, SHA-256, SHA- 512, MD2, MD4, MD5, RMD160
- Autre algorithmes: (symmetric et compression): Blowfish, DES, 3DES, IDEA, RC2, RC4, RC5, AES

### Nos Références

OpenTrust™ équipe déjà de nombreux grands comptes et administrations.

#### Administration

CEA, La Poste, INSERM, SwissArmy, French Ministry of Finance, French Ministry of Agriculture, Cetrel in Luxembourg...

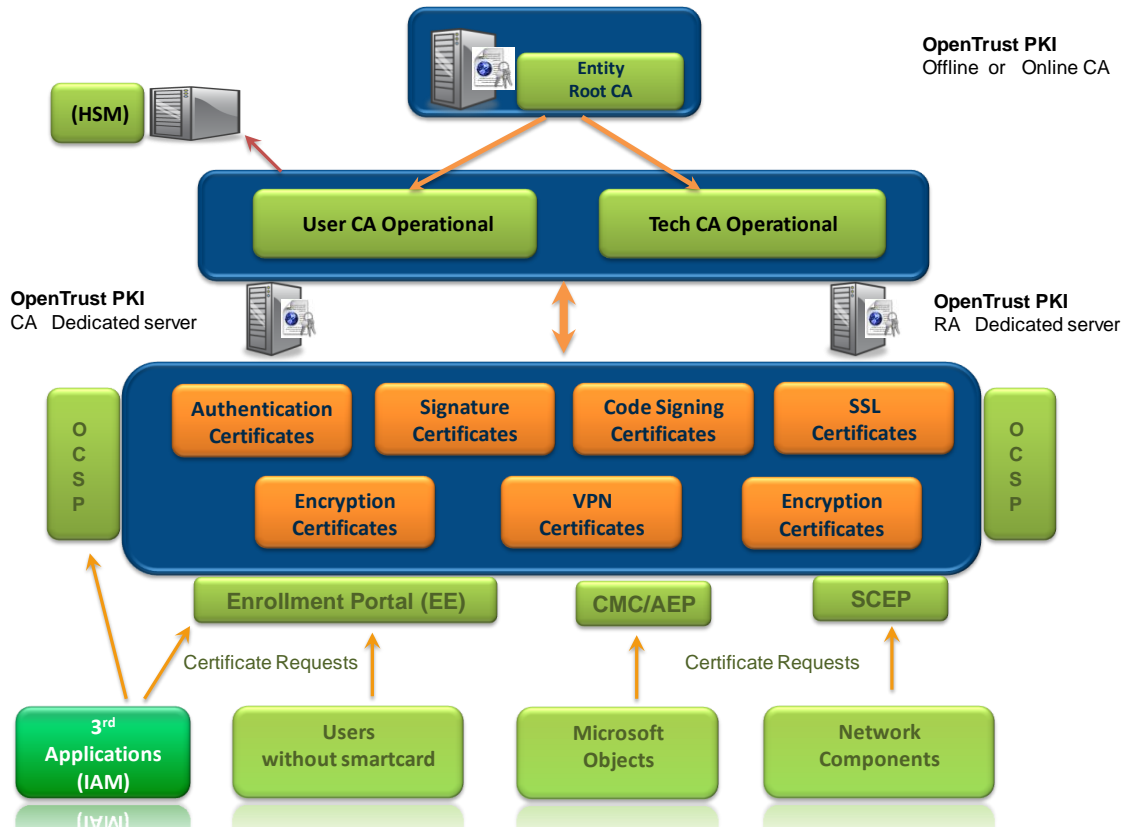
#### Banque et Assurance

LCL, GMF Assurances, Bred, CNCE, Banksys, National Bank Of Belgium, SPF-Finance, AGF, SMAM, Gan...

#### Industrie et Services

Total, Renault, Nissan, Alstom, Sanofi Aventis, Pixid, Michelin, Areva, Technip, Faurecia, Thalès, Mobistar...

## OpenTrust PKI Architecture



General            Info@OpenTrust.com  
Phone:            +33 1 444 20000  
Fax:                +33 1 444 20001  
Marketing        Marketing@OpenTrust.com  
Sales              Sales@OpenTrust.com