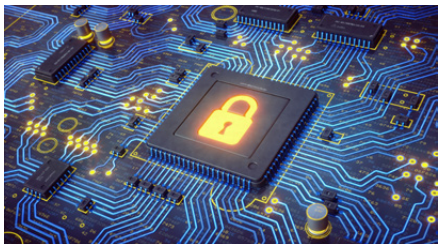
Horus metapki

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



Dans un contexte de dématérialisation des échanges internes ou 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. Atos, 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 (VPN - 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 identités numériques matérialisées par une paire de clés asymétrique (une clé publique et une clé privée) et des certificats fournis par une Autorité de Certification (AC) qui associent un identifiant à chaque identité publique.

Metapki supporte une ou plusieurs AC, 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 AC. La solution comporte des services de séquestre et de recouvrement de clés lorsque cela est requis.

Acteur européen de la sécurité

Atos fournit des services de conseil, de formation et de support afin définir le meilleur moyen pour intégrer la solution dans les applications du système d'information (exemple : SSO).

Atos propose également l'hébergement de la solution metapki dans ses centres d'infogérance hautement sécurisés.

SÉCURITÉ CERTIFICATION SÉCURITÉ CERTIFICATION

Common Criteria Certification
EAL3 + ALC FLR.3, AVA VAN.3
ANSSI-CC-2012/81

Standard Qualification
N° 400/ANSSI/SDE/PSS/BQA

Trusted partner for your **Digital Journey**

Atos

Metapki est accessible au moyen d'interfaces web personnalisées, permettant ainsi aux utilisateurs équipés d'un navigateur web standard d'accéder à l'ensemble des fonctions.

Metapki intègre les modules fonctionnels suivants

- 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. L'information est rendue disponible aux applications au moyen des Listes de Révocation de Certificats (LRC) et/ou d'un répondeur 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 pour les certificats utilisés pour la confidentialité des données.

Chaque module fonctionnel peut être dupliqué. L'enchaînement logique des modules est défini dans un workflow afin de mettre en œuvre le processus organisationnel retenu pour la gestion du cycle de vie des certificats.

Metapki intègre en option les services fonctionnels suivants

- Gescard un service de gestion, de personnalisation graphique, de personnalisation électrique et de déblocage des supports cryptographiques (cartes à puce, clés USB).
- Vericert un service de validation de certificats, pour vérifier la validité d'un certificat en accord avec une politique de validation.

Metapki comprend des mécanismes de sécurité renforcés

- L' accès à tous les modules fonctionnels de metapki est contrôlé. Les opérateurs agissant en tant que gestionnaires doivent être authentifiés de manière forte (c.à.d. 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 un module donné peuvent être consultés par des opérateurs bénéficiant d'une autorisation.
- Les communications entre les modules fonctionnels 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). Atos intègre différents types de HSM, fournis par Atos ou par des tiers.

Normes et spécifications techniques

Matériels et logiciels requis pour le serveur hébergeant metapki	
Serveurs physiques	Plateforme 32/64 bits équipée de 4 Go de RAM & de 10 Go d'espace disque minimum, 2 ports Ethernet
Machines virtuelles	VMWare, HyperV
Systèmes d'exploitation	RedHat 6 et 7 (32 ou 64 bits) / SUSE SLES 11 et 12 (32 ou 64 bits) / CentOS 6 et 7 (32 ou 64 bits)
Serveur LDAP	Les AC publient les certificats et/ou les LCR dans un annuaire
Serveur de courriel	Envoi des courriels possibles à chaque étape du cycle de vie des certificats
Station de travail pour les utilisateurs de metapki	
Navigateurs	Internet Explorer version 8 et supérieur, Firefox ou Chrome
Systèmes d'exploitation	Windows XP (Service Pack 3) / Windows 7
Java Runtime Environment	1.7 et 1.8
Carte a puce	
Toute carte disposant d'une interface d'accès PKCS#11 et en particulier les suivantes : CardOS, Gemalto ID PRIME MD840, Gemalto IAS TPC, Gemalto Classic TPC IM, Gemalto Cyberflex Access 64k v2, Morpho vpsID SmartCard Ux, ActivIdentity ActivCard 64K V2C	
HSM	
Tout HSM disposant d'une interface d'accès PKCS#11 et en particulier les suivants : Trustway Crypt2pay profil protect, Trustway Proteccio®, Utimaco, Adyton	

Exigences techniques
Plateforme Linux (c.à.d RedHat, CentOS ou SuSE)
Composants Open source internationaux fournis avec metapki : Apache, OpenSSL, PostgreSQL et PHP
Serveur LDAP : lorsque les AC publient les certificats et/ou les LCR
Serveur de courriel SMTP : lorsque metapki envoie des notifications en accord avec le cycle de vie des certificats

Normes et standards
• Format des certificats conforme à l'ITU-T X.509v3 et au RFC 5280 • Protocole d'enrôlement de certificats : SCEP , CMP (RFC 2510 et RFC4210), CCEP • Profils des certificats conformes à ETSI TS 101 862, Netscape et Microsoft • Informations de Révocation conformes à l'ITU-T X.509v2 LCR et au protocole OCSP (RFC 2560) • Format d'échange de clés : PKCS#12 • Format des demandes de certificats : PKCS#10, SPARC • Connectivité : LDAP, HTTPS, SMTP • Interface HSM : PKCS#11

Veuillez trouver plus d'information sur
https://atos.net/fr/produits/cybersecurite/digital-identities/metapki

CT_180608_LPM_F-Horus_metapki-fr6