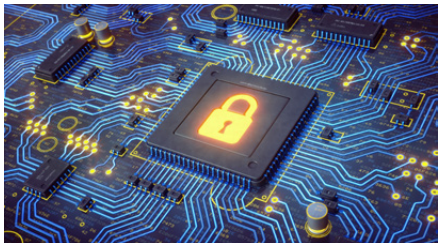
Horus metapki

For managing certificates creating and managing secure identities



Information system security is an essential issue for organisations moving to paperless exchanges, whether for internal communications or for relationships with partners and customers. Electronic certificates respond to this need as they allow applications to support security services such as user authentication, non-repudiation of transactions, and confidentiality of data exchanges. Atos, a European actor in IS security, provides metapki, a complete solution to create electronic certificates and manage their life cycle.

Keeping control of security

Electronic certificates may be used to support:

- Strong authentication for users with smart cards or USB tokens (two factor authentication)
- Strong authentication for web servers (SSL/TLS)
- Strong authentication for VPN (Virtual Private Networks)
- Electronic signature to provide integrity and non-repudiation of transactions
- Data confidentiality for data in transit or in storage

Users and applications are provided with one or more digital identities materialized by key pair (a public key and a private key) and certificates, generated by a Certification Authority (CA), that associate the registered user or application with the digital identity.

Metapki supports one or more Certification Authorities that may be independent, or subordinate CA.

A whole range of security profiles for public certificates is supported by metapki. For each profile, the registration process may be tailored to the specific needs of the organisation and integrated with the existing IS.

A workflow manager handles the registration process in order to minimise the time to produce and manage the certificates through the use of one or more Local Registration Authorities (LRA).

Accompanying growth

As a European security leader, Atos has metapki's modularity and sales conditions enable the smooth deployment of a solution tailored to the organisation's needs: new types of certificate, new management processes, new organisational units and new Certification Authorities may be added as required. The solution includes key escrow and key recovery when requested.

A European actor in IS security

Atos provides consultancy services for defining the best way to integrate metapki into the IS, as well as for making use of certificates in applications (e.g. SSO-single sign-on). Atos provides the training and the support.

Metapki components may be hosted in secure data centres managed by Atos.

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 is managed through the use of customised web interfaces, allowing full deployment for users using standard web browsers.

Keeping control of security metapki supports the following functional modules

- Certification Authorities generating public key certificates with pre-defined profiles in accordance with certification policies
- Registration Authorities and/or Local Registration Authority (RA and/or LRA), for registering users or modules and checking their credentials
- Revocation Services for revoking certificates before the end of their validity period. Information is available for applications using either Certificate Revocation Lists (CRL) and/or servers using the On-line Certificate Status Protocol (OCSP responders)
- Publication Services, for distributing keys and certificates to certificate holders and optionally making certificates available to Relying Parties
- Key Escrow and Key Recovery Services for certificates used for confidentiality purposes

Each functional module can be duplicated. The logical sequence of modules is defined in a workflow to execute the organisational process used to manage the lifecycle of certificates.

Metapki supports the following optional services

- A Card Management System (GesCard) for managing smart cards: customisation, PIN unblocking...
- A validation authority (VeriCert) for checking the validity of a certificate according to a validation policy.

Metapki includes strong internal security mechanisms

- Access to all metapki functional modules is controlled. Operators and administrators must be authenticated using strong authentication (with smart card or USB token)
- Access is though front office functions, back office functions are separate
- All actions related to the management of certificates are recorded in a database accessible only by authorised operators. All events are logged
- Communications between functional modules and information stored in the database are all protected. Sensitive information is enciphered
- Private keys and public keys are protected using Hardware Security Modules (HSM). Atos supports different kinds of HSM, either provided by Atos or by third parties.

Standards and technical specifications

Hardware and Software for metapki Hosting	
Physical Servers	32/64 bits platform with at least 4 Go of RAM, 10 Go of available disc memory, 2 Ethernet ports
Virtual Machines	VMWare, HyperV
Operating Systems	RedHat 6 and 7 (32 or 64 bits) / SUSE SLES 11 and 12 (32 or 64 bits) / CentOS 6 and 7 (32 or 64 bits)
LDAP Server	CAs publish the certificates and/or the LCR in a LDAP directory
Mail Server	Email sending is possible for each step of certificates life cycle
Working station for metapki users	
Navigators	Internet Explorer 8 version and later, Firefox, Chrome
Java Runtime Environment	1.7 et 1.8
Smart Card	
All smart cards with PKCS#11 interface and particularly: 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	
All HSM with PKCS#11 interface and particularly: Bull crypt2pay profil Protect, Bull TrustWay Proteccio®, Utimaco, Adyton	

System requirements
Linux Platform (e.g. RedHat, CentOS or SuSE)
Open source international components delivered with metapki: Apache, OpenSSL, PostgreSQL and PHP
LDAP Server: when the CA publishes certificates and/or LCR in a directory
SMTP Mail Server: when metapki sends notifications related to the management of certificates

Norms and standards
• Certificate compliance with ITU-T X.509v3 and RFC 5280 • Certificate enrollment protocols: SCEP, CMP (RFC 2510 et RFC4210), CCEP • Certificate profile compliance with ETSI TS 101 862, Netscape and Microsoft • Revocation information compliance with ITU-T X.509v2 LCR and OCSP Protocol (RFC 2560) • Certification request format: PKCS#10, SPKAC • Key exchange format: PKCS#12 • Connectivity: LDAP, HTTPS, SMTP • HSM interface: PKCS#11

Find out more about us
atos.net/en/products/cyber-security/digital-identities/metapki

CT_180608_LPM_F-Horus_metapki-en7