

Creating and managing secure identities



MetaPKI for managing certificates

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. Bull, 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 VPNs (Virtual Private Networks);
- Electronic signatures 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 key pairs (a public key and a private key) and public key certificates, generated by a Certification Authority (CA), that associate the registered user or application with the public key.

MetaPKI supports one or more Certification Authorities, that may be independent, or subordinate CAs.

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

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, new Certification Authorities may be added as required. The solution includes key escrow and key recovery for confidentiality keys.

Bull, European actor in IS security

Bull 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). Bull provides the training and the support. MetaPKI components may be hosted in secure data centres managed by Bull.

SECURITY SERVICES

A solution enabling secure applications

MetaPKI is managed through the use of customised web interfaces, allowing full deployment on personal computers using standard web browsers.

MetaPKI supports the following functional entities:

- 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 entities and checking their credentials.
- Revocation Services for revoking certificates before the end of their validity period using either Certificate Revocation Lists (CRLs) and/or OCSP responders (servers using the On-line Certificate Status Protocol).
- Publication Services, for distributing keys and certificates to certificate holders and optionally making certificates available to Relying Parties (RP).
- Key Escrow and Key Recovery Services for certificates used for confidentiality purposes (optional).

Each functional entity is managed through the use of roles. The organisation defines the relationship between individuals and roles.

MetaPKI supports the following optional entities:

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

MetaPKI includes strong internal security mechanisms:

- Access to all MetaPKI functional entities 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 entities 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). Bull supports different

kinds of HSMs, either provided by Bull or by third parties.

MetaPKI implements norms and standards for interfaces and protocols:

- Certificate format compliance with ITU-T X.509v3 and RFC 5280.
- Certificate profile compliance with : ETSI TS 101 862, Netscape and Microsoft.
- Revocation information compliance with ITU-T X.509v2 CRL and OCSP Protocol (RFC 2560).
- Certification request format: PKCS#10, SPKAC.
- Key exchange format: PKCS#12.
- Connectivity: LDAP, HTTPS, SMTP.
- HSM interface: PKCS#11.

System Requirements:

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