IDnomic PKI

Trusted digital identities for all IT use cases

Establishing a highly secure process to restrict access, authenticate the identity of users and devices, and most important, verifying the integrity of documents and communications handled every day, represents a major challenge for any organization. IDnomic PKI enables all public and private entities to establish and maintain a trustworthy networking environment by issuing digital identities for strong authentication, data encryption and digital signature.

In line with your business growth

.IDnomic ID PKI is a world leading solution, which provides a powerful and advanced Public Key Infrastructure (PKI) software suite to secure all digital processes by delivering electronic certificates for users and devices.

Based on X.509v3 standards, it enables the deployment of trusted IT infrastructures, and manages the lifecycle of electronic certificates and their associated issuing Certificate Authorities, thus simplifying greatly the identity management process.

Its architecture is based on a modular approach that combines a high level of flexibility for evolutive needs with an ergonomic and modern design, bringing easy-to-use interface for customers and helps you to address every step of your digital transformation project, adapted to your business needs.

Covering a wide range of digital identity use cases, IDnomic PKI suite is available "On Premises" installed at the customer sites, or in a "Software as a Service" cloud-based mode, delivered through our high security datacenters.

IDnomic PKI can be combined with other IDnomic modules and especially:
Certificate Lifecycle Management (CLM)
Credential Management System (CMS)
Timestamping Application (TSA)
Digital Signature

Focusing on highest security, IDnomic PKI has been Commonn Criteria EAL4+ (CC) certified. Our teams of consultants and experts deliver extensive support to help you address every step of your digital transformation project.
Leverage our experience to define, upgrade or ensure the compliance of your security solutions for users, machines, objects, documents, and transactions.

Delivering trust and security to all digital transformation use cases

Atos

IDnomic PKI – a modular solution

ID CA (Certification Authority)

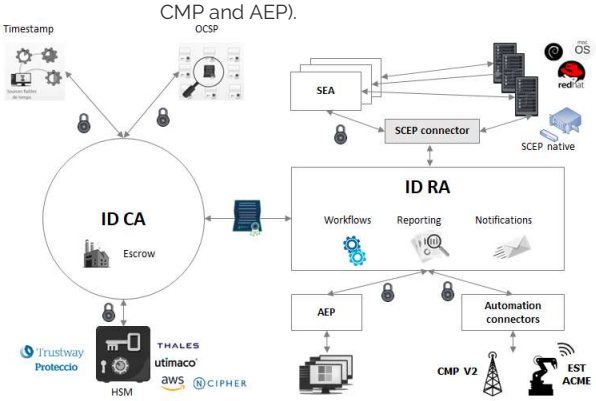
Central entity, in charge of the construction of trusted digital identities. It is responsible for the creation, organization and management of Certification Authorities and the production of certificates.

ID RA (Registration Authority)

This module manages the lifecycle of certificates and defines the different workflows associated to certificate profiles and their delivery modes. It addresses all machine use cases and supports multiple enrollment protocols (ACME, EST, SCEP, CMP and AEP).

ID OCSP (Online Certificate Status Protocol)

Provides real time proof of the validity status of a digital certificate (revoked, suspended, active).
This component comes in addition to Certificate Revocation Lists (CRL) natively supported by IDnomic PKI.



Benefits for our customers

IDnomic PKI provides several decisive functional advantages for trusted digital identity management.

- Modern, ergonomic design – ease to deploy, configure, maintain and use
- High performance oriented, yet extremely scalable – Manage 1000 to 100 million certificates
- Highest proven security – Common Criteria EAL 4+ certification
- Multi-tenant by design – Deploy, Configure and manage several PKIs independently with one software instance
- On Premises or Cloud – deployments adapted to your needs and operational capacities
- Configuration export *- to ease the transition from a pre-production to production environment
- Capacity to use certificate linters following CAB/FORUM recommendations
- Support of a large variety of enrollment protocols (EST, SCEP, ACME, CMP)

Standards and technical specifications

Norms and standards

- Certificate format compliance: X.509v3, RFC 5280 and RFC 3739
- Certificate requests: PKCS#10, CSR, SPKAC
- Signature algorithms RSA (1024 - 4096) , (RSA PKCS#1 v1.5, RSA PSS PKCS#1 v2.1), ECDSA (192-521)
- Hash algorithms SHA-224, SHA-256, SHA-384, SHA-512, SHA-256 MGF1, SHA-384 MGF1, SHA-512 MGF1
- Certificate content : UTF8, T61, printable, email, SAN (RFC822, UPN), etc.
- PKCS#11 for interfacing with a Hardware Security Module (HSM)
- Connectivity: LDAP, HTTPS, SMTP
- Dedicated interfaces for users and third-party applications:
- SOAP Connector.
- ACME, CMP, SCEP, EST Protocol.
- WCCE / CMC Protocol through the Auto Enrollment Proxy (AEP)
- Certificate revocation compliance: CRL X.509v2 and OCSP (RFC 2560) Local credentials

Compliance

- RGS certified considering all certificates usage and for all its classifications (1, 2 and 3). LSTI N° 8029-1318-V3.0 / EN319411-1 V1.1.1
- eIDAS compliant: obtaining Certificate LSTI N° 8029-1318-V3.0.
- CC EAL 4+ Certification:

System requirements

Operating System Redhat, SUSE or Rocky Linux

Java Development Kit (JDK) installed

The product is fully integrated with Open-Source components:

- Apache, PostgreSQL, PHP,
- Tomcat, Keycloak, Ansible

Find out more about us atos.net/en/solutions/cyber-security/trusted-digital-identities