Flexible multitenant public key infrastructure (PKI) platform

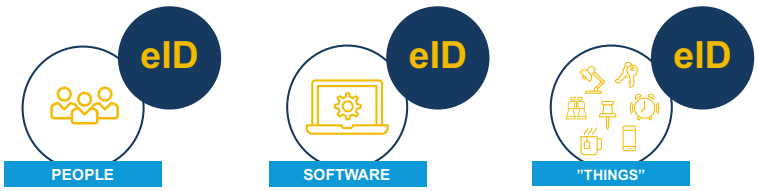
Nexus Certificate Manager combines secure innovation with flexibility, offering leading features such as multitenancy. It manages the full life cycle of electronic identities (eID) for consumers, citizens, employees, mobile services and for internet of things (IoT), in nearly any format and for any application across networks and systems.

Convenience
Complete suite for building trust, including certificate life cycle management, OCSP responder and timestamping services

Freedom
Managing Identities for people, software and things

Certificate Manager is trusted by numerous banks, enterprises, mobile network operators, defense organizations, device manufacturers all over the world; and issues eIDs for millions of users and things.

Create, manage and use



Digitalization

For this era of digitalization, with its explosion of mobile services and IoT, PKI provides a generic security mechanism that is inevitable for numerous applications. PKI provides people, software and things with an eID. It then provides the means for managing and validating these during their life cycle.

Certificate Manager is an easy to scale, high-security platform for issuing, managing and validating any sort of PKI-based eID. Compliance with standards assures that eIDs can be used across applications from different vendors in a large-scale federated environment.

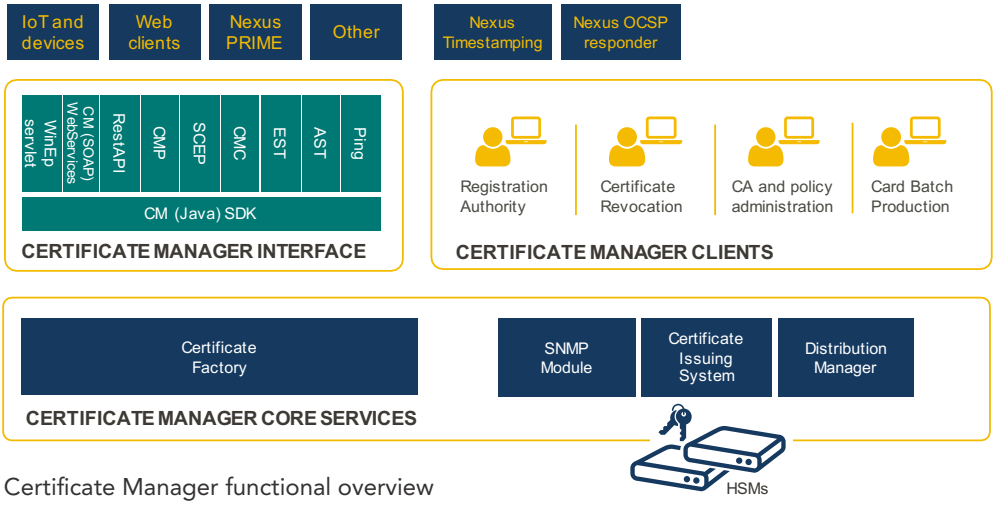
Key features

- Certificate Authority and life cycle management of certificates.
- Compliance with established PKI standards for certificates, revocation lists, smart cards and certificate management interfaces.
- Separation between core certificate authority (CA) functionality and remote administrative clients.
- All configuration changes must be signed by two security officers, to avoid unauthorized manipulation.
- Certificate lifecycle management for LTE Backhaul components including support for all relevant certificate enrolment protocols. Interoperability tested devices from Cisco, Ericsson, Nokia, Juniper and others.
- Managed cloud or on-premises installation.

All-round PKI platform

Certificate Manager offers a comprehensive all-round PKI platform designed for:

- **Bank and insurance** customers, to give credentials to access private accounts, close contracts and conduct electronic transactions.
- **Retailer** customers, to give credentials to purchase goods over internet.
- **Mobile Operators'** to secure their LTE Backhaul.
- **Enterprise** employees, to log in to the corporate network over the desktop, VPN or smart phone, securing emails or accessing data in cloud services, workflows and digital signatures.
- **Citizens'** eIDs, to use for safe e-government services, cross-border identification and strong authentication.
- Routers, firewalls and **Machines** to establish encrypted and integrity protected TLS, IPSec and WiFi communication.
- **Trust Service Providers**, to support different types and sizes of certificate customers with appropriate value for money solutions.



Certificate Manager functional overview

Validation platform

Nexus validation platform, Nexus Online Certificate Status Protocol (OCSP) Responder, is tightly integrated in the Certificate Manager platform, including multitenancy. All responses are digitally signed for integrity protection. Hardware security modules (HSM) are supported.

Nexus OCSP Responder is available as a stand-alone component or as a part of a complete Certificate Manager package.

Time stamping

The Certificate Manager platform includes time stamping capabilities with HSM support and integration towards external Network Time Protocol (NTP) servers. Nexus Timestamp Server is available as a stand-alone component or as a part of a complete Certificate Manager package.

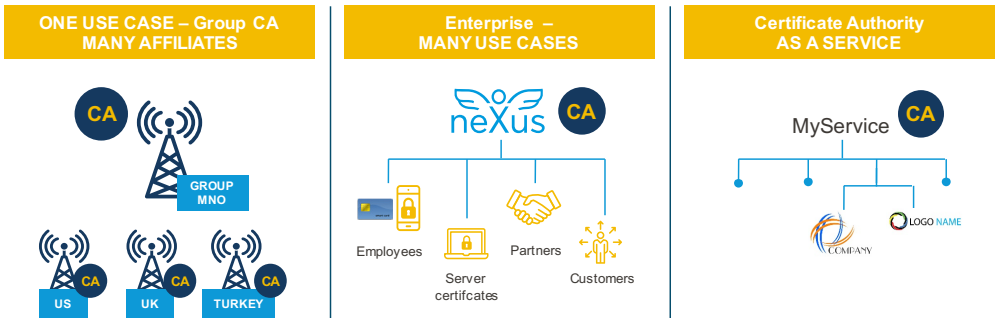
Complete life cycle management

The platform has highly flexible registration, issuing and revocation processes. These include:

- enrollment interfaces
- generation and publication of certificates and revocation lists to directories and archiving and recovery of OCSP responder keys
- smart card and PIN letter production in batch mode
- CA, policy, user and access management over GUI
- cross certification

Safe with multitenancy

A single instance of Certificate Manager can run multiple CAs for many client organizations and use cases. Each CA can be managed with clean separation of individual policies, issuing and maintenance processes, and separate groups of policy administrators in one platform.



Multitenancy use cases

Reliability, scalability and availability

Certificate Manager has been verified in critical, large-scale, multi-CA deployments. High availability and performance scaling can be enabled with a traditional active-passive cluster or multiple active-active nodes. Multiple HSM instances are supported for high availability of keys and for separation of keys among tenants.

Security

Based on a Common Criteria evaluated security architecture, Certificate Manager conducts strong user authentication and fine-grained, role-based access control for performing certificate management tasks for users and CAs. It is a market-proven technology that suits high-security deployments, and can be adapted to almost any role concept and certificate policy. All relevant administrative operations are logged in a tamper-evident audit log.

Migration

Many different systems may be used to issue digital certificates across an organization, because of different departmental requirements, or the lack of a common policy. Certificate management is fast becoming an important issue, and a central issuance solution maintained by dedicated PKI personnel gives much better control than a distributed one. Another case where migration is needed, is when old CA products are being discontinued and need to be replaced.

Certificate Manager enables integration of CAs into one multi-CA platform. Nexus migration tool can be used to import external CA and user certificates, certificate revocation lists (CRLs), and archived keys from legacy CA products. Existing HSMs can be moved and connected to Certificate Manager. The operation can then continue in a seamless way with Certificate Manager as the single platform.

Specification

- Support for certificate enrollment protocols Simple Certificate Enrollment Protocol (SCEP), Certificate Management Protocol (CMP) and Enrollment over Secure Transport (EST).
- Compliance with EU regulation eIDAS and Swedish e-legitimationsnämnden EID2.
- Timestamp capabilities complying with IETF RFC 3161 and ETSI TS 101 861 standards.
- Nexus Timestamp Server and Nexus OCSP Responder, available as stand-alone components or parts of a complete CM package.
- Common Criteria EAL4+ to be completed during 2017.
- Support for HSM and smart card products from major vendors, for example, Thales, SafeNet, Utimaco, Bull, and IBM.
- Platform support: Windows and Red Hat Linux.
- Database support: SQL Server, Oracle, and PostgreSQL.