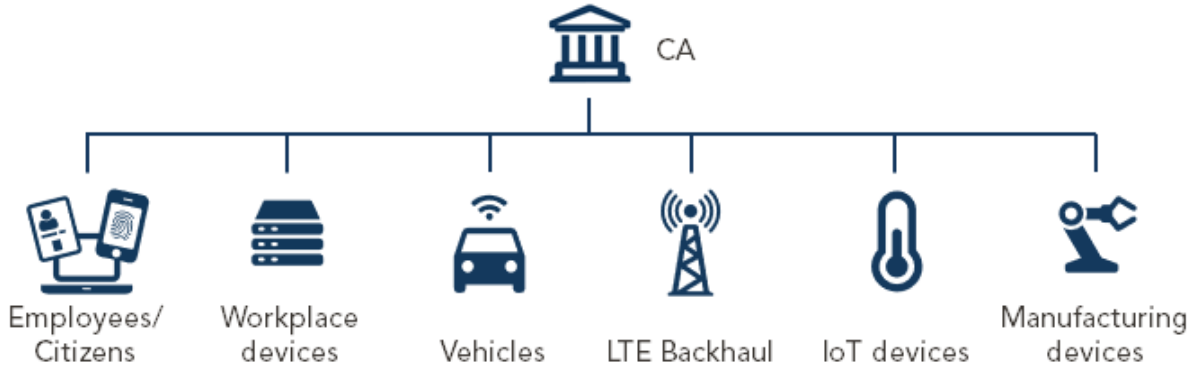
Certificate Manager overview

This article includes updates for Certificate Manager 8.10.



Certificate Manager use cases

Smart ID Certificate Manager (CM) is a flexible, scalable, and high-security certificate authority (CA) software. Certificate Manager supports a wide range of certificate enrollment protocols, which enables you to issue, manage, and validate certificate-based electronic identities (eIDs) for people, infrastructure, software and devices. The component can be used for customized operations on-premises or in a hosted environment. Core certificate authority (CA) functionality is separated from remote administrative clients. Additionally, CM can establish Signing Authorities, SA, with HSM based key and trusted signing certificate, similar to how a CA operates when signing certificates. This allows clients using the CM REST API to request signing of arbitrary data by the SA, e.g. for code signing.

Issue and manage certificate-based digital identities

A public key infrastructure (PKI) provides a generic security mechanism that enables for example strong authentication, email encryption, digital signing, secure IoT applications and secure vehicle-to-everything communication. PKI provides people, software and devices with a digital identity, and provides the means for managing and validating these during their lifecycle.

Certificate Manager is an easy to scale, high-security platform for issuing, managing and validating certificates for consumers, citizens, employees, communication services, software and equipment. Compliance with standards assures that eIDs can be used across networks and applications from different vendors in a large-scale federated environment.

Store certificates on multiple bearers

The eID certificates and keys can be stored on different bearers, for example smart cards, mobile phones, network equipment, computers, soft tokens, HSMs, and IoT devices. Third-party products can be integrated with CM via a number of different interfaces, such as EST, SCEP and ACME. Compliance with these and other standards assures that eIDs can be used across applications from different vendors in large-scale environments.

Manage complete lifecycle of certificates

Certificate Manager handles the lifecycle of user's digital identities, for example Initial enrollment of a user, revocation and renewal of credentials. Revoked certificates are listed in certificate revocation lists (CRLs) and periodically distributed to services such as an external LDAP directory or the Nexus OCSP Responder. Instant update of revocation status to the OCSP Responder is possible by immediate issuance of a delta CRL when a certificate is revoked. Activation, or white-listing, of certificates is done in the OCSP Responder by use of Certificate Issuance Lists.

A user's private keys that are used for encryption of data, for example for S/MIME use, can be encrypted and archived in the CM database. If a smart card with the encryption key is lost, the key can be recovered, which means that loss of encrypted data can be avoided. Key archiving and recovery is sometimes referred to as key escrow.

Ensure high performance and scalability

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.

Use an allround PKI platform

Smart ID Certificate Manager is a part of Nexus' comprehensive PKI solutions designed for various use cases, such as these:

- Workforce - to securely access Windows and company applications, encrypt emails and sign documents digitally.
- IoT - to secure connected devices with automated processes
- Connected vehicles - to protect vehicle-to-everything (V2X) communication.
- Mobile operators - to secure their LTE Backhaul.
- Manufacturing industry - to protect devices with digital identities and issue factory certificates.
- Workplace devices - to secure routers, firewalls and machines.
- Trust Service Providers - to support all kinds of certificate customers.

These solutions can be combined with other Nexus Smart ID solutions, such as Digital identities and Digital access.

Manage multiple CAs and tenants

It is possible to operate multiple logical Certification Authorities (CAs) on the same instance of Certificate Manager and each CA can operate with its own set of policies. These CAs can be organized in one or more sub-ordinate hierarchies and if required also with cross-certification between CAs.

Certificate Manager is multitenant, which means that several different client organizations can use the same software instance to implement several parallel, private eID solutions to a reduced cost. Logically isolated administration domains enable organizations to use their own separate domains of users, CAs and policies with a separate thread of the audit trail.

Migrate CAs for consolidation

To manage all certificate issuing in one system, external CAs can be migrated into Certificate Manager, including user certificates, certificate revocation lists (CRLs), and archived keys from legacy CA products. Existing HSMs can be moved and connected to Certificate Manager.

Protect CA keys with HSM

Certificate Manager creates, uses, and deletes CA keys. For highest security is Hardware Security Modules recommended to use for creating and protecting the CA keys for production use. Certificate Manager handles all necessary operations automatically under the control of the CA administrators and enables several HSM's to be used in parallel by different tenants and purposes. For training and testing purposes can Certificate Manager be used without a Hardware Security Module to manage the CA keys.

Enforce CA policies

A CA operates within a framework of legal and social responsibilities, which must be addressed through a CA policy. A CA policy is established to provide guidelines for operating the PKI and govern the issuing of certificates. A CA policy normally includes a Certification Practice Statement (CPS), a Certificate Policy, and Liability and legal conditions. Certificate Manager implements, supports and enforces CA policies. For definition of the operational policies in CM, a dedicated administrative client is used, the Administrator's Workbench client.

Rely on proven security

Certificate Manager is Common Criteria EAL4+ certified according to the international standard Common Criteria EAL4+ for Information Technology Security Evaluation (CC). Nexus' organization complies with ISO 27001 and TISAX (Trusted Information Security Assessment Exchange).

Certificate Manager itself is protected with PKI, using dedicated roles to log in, manage and operate the system. CM follows the four-eye principle, which means that all policy changes must be signed by two security officers. The signature of policy configuration allows a trustful auditing of configuration updates and integrity protection to avoid unauthorized manipulation of settings.

Specification

- Support for multiple interfaces and certificate enrollment protocols, including SCEP, ACME, CMP, CMC, EST, EST-coaps, Rest API.
- Nexus Timestamp Server and Nexus OCSP Responder are available as stand-alone components or parts of a solution
- REST API available for customized integrations with third-party applications
- The CM WEB UI provides common registration authority functions: certificate request and revocation, statistics dashboard, IoT device registrations, search and filters for list of various certificate properties.
- Compliance with EU regulation eIDAS and PSD2
- Support for vehicle-to-everything (V2X) communication by support for IEEE 1609.2, ETSI
- Common Criteria EAL4+ certified and complying with ISO 27001 and TISAX

- Support for various HSMs, LTE backhaul networks and smart card products from major vendors

For more information on the supported interfaces, standards and specifications, see Certificate Manager requirements and interoperability.