



# Nexus Certificate Manager

Certificate Manager is the world's probably most flexible, multi-tenant PKI platform for enterprises, state departments, defense, and service providers from the PKI specialist Nexus. It issues electronic IDs (digital certificates) for consumers of corporate, Internet or mobile services and for components of IT infrastructure, in nearly any format and for any applications across networks and systems.

**PUBLIC KEY CRYPTOGRAPHY** is one of the most practical innovations of the 20th century's mathematics with tremendous impact on computer security technology. Public Key Infrastructures (PKI) provide a highly scalable security infrastructure for safe identification, authentication, confidentiality and data integrity while communicating or consuming electronic services. In the era of global communication and the explosion of Internet and mobile services, PKI provides a generic security mechanism for numerous applications and is inevitable in specific application areas.

PKI provides the users with electronic identities (eID) and provides means for managing and validating them during their lifecycle. The eIDs can be considered the users' passports while accessing remote resources, communicating, collaborating across corporate and public networks or conducting high-value electronic transactions.

Nexus Certificate Manager is the world's probably most comprehensive and most flexible PKI platform. It provides a highly scalable, high-security platform for issuing, managing and validating any sort of PKI-based electronic IDs, so-called digital certificates: user certificates, smart cards, smart hardware tokens, software tokens, certificates for desktop computers, servers, routers, VPN gateways, network devices, and embedded systems. Standard compliance ensures the

## What is a digital certificate?

A digital certificate comprises:

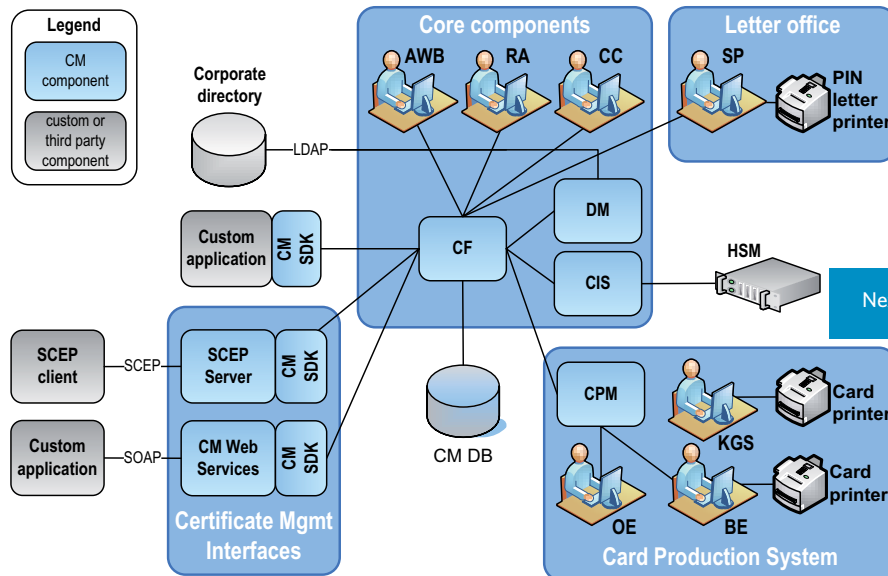
- certificate owner's identity data,
- certificate owner's unique public key,
- certificate validity period,
- and
- digital signature of the CA, approving the binding between the above.

usage of the eIDs across applications from different vendors in a large scale federated environment. Nexus Certificate Manager can be adopted to any security policies, eID formats, data source and directories. The build-in key management, card management and PIN printing capabilities enable its use as a cost-efficient single-platform eID solution. Trust Service Providers benefit from multi-tenancy: certification services of many client organizations can be managed on the same system with safe separation of user and policy data. Nexus Certificate manager is trusted by numerous large governmental agencies, defense organizations, banks and enterprises all over the world and issues eID for millions of users.





## PRODUCT SHEET



Nexus Certificate Manager is the general-purpose Certificate Authority platform, which supports the issue and life-cycle management of PKI-based credentials, such as:

- citizens' electronic identities (eIDs) used for safe cross-border identification and strong authentication at on-line governmental services
- bank and insurance customers' credentials to access private accounts, close contracts and conduct electronic transactions
- retailer customers' credentials to purchase goods over Internet
- members of collaboration networks; for accessing shared remote resources and exchanging highly confidential material
- corporate employees logging in to the corporate network over desktop, VPN or smart phone

- cloud service customers accessing confidential data and dedicated applications hosted at a remote cloud service provider
- computers of a network domain for authentication by the domain controller
- routers and firewalls to establish encrypted and integrity protected communication channels.

### Comprehensive, all-round CA platform

Nexus Certificate Manager is designed for large-scale public electronic ID deployment by governments, trust service providers (TSPs), telecommunication operators and financial institutions as well as medium-scale deployments used within corporations and organisations.

Nexus Certificate Manager comprises all functionality that is needed for a Certificate Authority (CA): highly flexible registration, issuing and revocation processes, enrolment interfaces, generation and publication of





## PRODUCT SHEET

certificates and revocation lists to directories and OCSP responders, key archiving and recovery, smart card and PIN letter production in batch mode, CA, policy, user and access management over GUI, and cross certification.

### One platform for all PKI applications

Nexus Certificate Manager is capable to handle any number of Certificate Authorities with individual policies, individual issuing and maintenance processes, and separate groups of policy administrators. The flexibility of configuration enables implementing almost any policies and issuing workflows, and connecting to any computing environment. Standard interfaces support certificate issue and lifecycle management triggered by external systems and the automatic delivery of certificates.

Certificates can be used for desktop and VPN login, strong user authentication, data and email encryption, document signatures, legal digital signatures, encrypted ITSec and WiFi communication, machine domain authentication and many more.

### Comply with standards and 3rd party vendors

Nexus Certificate Manager complies with established PKI standards for certificates, revocation lists, smart cards and certificate management interfaces. This ensures that your CA can service enrolment requests from standards compliant clients and produces certificates that are understood and can be validated by compliant applications in large scale, multi-vendor application environments. HSM and smart card products of major vendors are supported.



Nexus Certificate Manager exceeds compliance requirements

### Save with multi-tenancy

A single instance of Nexus Certificate Manager can run CAs of many client organizations can be managed on the same platform with clean separation of user data and access rights.

### Rely on Common Criteria EAL3+ evaluated security architecture

Nexus Certificate Manager conducts strong user authentication and fine-grained, role-based access control for performing certificate management tasks for users and CAs. For each transaction, user commitment signatures are requested and logged in the temper-resistant audit trail. Subsystems communicate over encrypted, integrity protected channels. Sensitive data, like keys, PIN, are always encrypted while transmitting or storing.





## PRODUCT SHEET

Nexus Certificate Manager is Common Criteria EAL3+ evaluated and complies with the European Signature Directive and the German Signature Act. The market-proven technology suits high-security deployments and can be adopted to almost any role concept and certificate policy.

### **Cross-platform support**

Nexus Certificate Manager can be run on Windows and Red Hat Linux and supports multiple databases including SQL Server, Oracle, and MySQL.

### **Reliability, scalability and availability**

Nexus Certificate Manager has been verified in critical, large-scale, multi-CA deployments. It is possible to run all services on one host with high performance. The system can be further scaled up by distributing processes among several host servers. High availability can be supported with an active-passive clustered configuration, including multiple HSM instances.

### **The bottom line**

PKI is the best available technology for authentication, encryption, integrity protection and digital signatures in large scale, federated applications and provides a generic security infrastructure. Digital certificates are the user's electronic IDs to access resources, consume services or conduct high-value transactions. Nexus Certificate Manager provides a



highly secure, standards-based, scalable, multi-tenant, high performance, platform agnostic solution for trusted third parties that want to offer certification services or for organizations that want a cost-efficient, flexible in-house CA solution.

