



Nexus Certificate Manager

THE WORLD'S LEADING SERVICE PROVIDERS OF LARGE PUBLIC KEY INFRASTRUCTURE (PKI) RELY ON CERTIFICATE MANAGER TO SUPPLY ELECTRONIC IDENTITIES AND SMART CARDS TO THE GROWING POPULATION OF SERIOUS E-SERVICE USERS. BASED ON YEARS OF PKI EXPERIENCE, NEXUS CERTIFICATE MANAGER PROVIDES A TRUSTWORTHY, OPEN, STANDARDS-BASED SYSTEM FOR THE PRODUCTION AND ADMINISTRATION OF ELECTRONIC CREDENTIALS.

Enables development and operation of PKI

Nexus Certificate Manager offers increased functionality and security to its users, and remains the industry's most effective tool for PKI deployment. Nexus Certificate Manager is designed for largescale 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. The solution enables its customers to develop and operate high-availability PKI.

Provides Platform for Secure E-services

Nexus Certificate Manager provides a trustworthy, open, standards-based system for the production and administration of electronic credentials. Nexus Certificate Manager combines all the necessary tools for the creation and management of digital certificates by Certification Authorities (CAs). Providing standards-based PKI security for user authentication and electronic signatures, the product enables customers to offer e-business services without compromising security, thereby fulfilling the five principal security

goals for commercial transactions:

- Confidentiality
- Integrity
- Authentication
- Nonrepudiation
- Authorisation

For large-scale public deployments, Certificate Manager is the principal choice of governments, TSPs, telecommunication operators and financial organisations.

Protecting end-user security

Protecting the end-user's private key is essential to the integrity of a PKI. The highest degree of protection available against malicious use is offered by a physical cryptographic token such as a smart card or a USB device. These tokens are used to store keys that never can be retrieved, duplicated or tampered with.

Nexus Certificate Manager uniquely offers support for both soft and the widest possible set of physical tokens as a principal part of the CA solution. It employs common, open standards such as the PKCS #12, and ISO 7816-15 for token storage, allowing supplier independence within a common client application interface.

Scalability, performance and reliability

Nexus Certificate Manager's CA hosting capabilities contain unmatched scalability features. Certificate Manager is able to scale from the internal electronic ID deployment of small corporations, up to hundreds of hosted CAs, and manage millions of certificates with a proven ability to issue certificates at very high rates. This performance is unsurpassed, meeting even the advanced demands of large public trust service providers. A specially developed and supported high-availability configuration assures the uninterrupted service of the central certificate management facilities.

Interoperability and industry standards

Nexus Certificate Manager is designed to operate in a multi-vendor, multi-application environment, regardless of the source of equipment or software involved. Emphasis is given to the use of open standards, and interfaces, to ensure interoperability with other CA vendor software, application software, and industry frameworks

Focused on technical security requirements

By being committed to provide PKI products that fulfill requirements on trustworthiness as described by electronic signature legislation, Nexus Certificate Manager is the basis for law compliant service providers around the world. For our customers seeking conformance, and accreditation in accordance with the European electronic signature legislation, Nexus Certificate Manager offers the best possible foundation by meeting, and exceeding the requirements for compliance with the ETSI/CEN Workshop Agreement 14167-1.

These requirements are focused on providing all the technical security requirements for the trustworthy systems that a Certification Service Provider needs to deploy.

Key Archiving and Recovery

The need to recover keys is sometimes essential for corporations that uses public key technique for confidentiality. The Key Ar-

chiving and Recovery services make it possible to archive, and recover user's private encryption keys, in a distributed manner, without putting the overall system security at risk. This facilitates for a corporation to implement routines for lost or broken smart cards. The Key Archiving and Recovery functionality in Certificate Manager is completely integrated in terms of access conditions for operators, log, and audit, user interface, and software development kit.

CA Hosting

CA Hosting enables the deployment of multiple virtual CAs on a single platform. Each CA can be defined with different policies, operator groups, certificate, and smart card procedures, certificate distribution and more. This is critical in a TSP environment where the demands of multiple customers must be satisfied. Different policy rules can be created for each application, in order to comply with different Certificate Policies (CP), and Certification Practice Statements (CPS).

Centralized policies and process management

Each company or organisation planning a CA system has security requirements unique to their business. In order to tailor the PKI for each application, policies, issuing processes, and certificate formats can be customised through a centralised management tool with an intuitive and scalable graphical user interface. Some of the management capabilities are:

- Multiple Root CA
- Multiple Virtual CA
- Cross-Certification
- Policies and procedures
- Certificate formats
- Distribution
- User roles
- Auditing

Comprehensive management tools for end-user credentials

Nexus Certificate Manager is delivered with a full range of tools for registration authorities and helpdesks, covering smart card and soft token management as well as the issuing, publication, suspension, restoration and revocation of certificates. Registration scenarios scale from webbased self-enrolments, to face-to-face enrolments, immediate smart card allocation, to bulk registration and centralised, high-volume card production.

Integration with External Systems and Data

To enable customers and partners to integrate their own tools, the CM Software Development Kit (CM SDK) exposes all the capabilities of Certificate Manager for certificate issuing, publication, suspension, reinstatement and revocation.

The same strong authentication and access management based on electronic signatures used in the standard tools is automatically deployed in all applications of this SDK.

The SDK protects investments by facilitating the use of existing data, for example, by integrating with a human resource system where the intended certificate holders are registered.

Smart card personalisation

The smart card personalisation functionality included in Nexus Certificate Manager supports different models of personalisation. A range of systems for personalisation of corporate, governmental and nationwide general purpose electronic ID-cards are also covered.

Both electrical and graphical personalisation is supported. Nexus Certificate Manager can be supplied with one or more card production workstations.

These workstations interface with card personalisation equipment, and enable distributed processes for card personalisation, including card surface printing and distribution support.

The card-production workstation permits outsourcing of card production, and seamless integration with existing third-party cardproduction facilities.

Nexus Certificate Manager has extensive support for most major PKI enabled smartcards, out of the box. Customer unique card contents and support for new smart cards can easily be added.

Secure printing

The production of electronic identities presents the need for a separate channel for shared secrets, i.e PIN codes. The Secure Printer facility offers a complete solution for secure and decentralized distribution of sensitive data. Features include splitting of PIN codes, pre-printed PIN letters and a capability to manage batches of print jobs.

Administrative security

Actions performed by all types of operator are always digitally signed and securely logged, providing a tamper-resistant audit trail. All communication between operators and the central servers is based on SSL v3 using strong authentication and encryption.

Operators of Nexus Certificate Manager use individual smart cards, permitting different levels of access to system functions and procedures. For administrative operations, the 4-eye principle is consistently employed.

Key features and options:

- Realises the complete electronic ID production process, from key generation and smart card profiling to the distribution of PIN codes to the end user
- Provides keys and certificates for software such as browsers, and Web servers, for smart cards, VPN devices, etc.
- Supports a variety of cryptographic algorithms including RSA, DSA, ECC, SHA, and IPE-MD
- Supports CA Hosting with Virtual CA
- Scalable, with the ability to issue over 40,000 certificates per hour
- Integrated management of smart cards and USB tokens from such vendors as Aladdin, Gemalto, (Axalto, Gemplus, and Setec) G&D, Sagem Orga and Siemens
- Distributed or single-process card production including electrical card personalisation and surface printing
- Designed for compliance to electronic signature legislation worldwide
- Centralised or distributed management of policies and procedures
- Generates any X.509 certificate format including IETF RFC 3280, S/MIME, SSL/TLS and SigG
- Supports WTLS CA and certificates for Wireless PKI (WPKI)
- Supports the PKCS #12 and ISO/IEC 7816-15 standards for token storage
- Supports all LDAP v3 directories
- Full support for key archiving and recovery
- Optional support for certificate lifecycle protocols such as CMC, XKMS and SCEP
- Supports PKCS #11 and JCE based Hardware Security Modules (HSMs) such as SafeNet (Éracom), nCipher, and Thales
- Windows and Linux platforms supported
- Support for Card Verifiable Certificates, HPC version 2.1 and Gematic
- Microsoft SQL and Oracle database engines supported
- Supports Tachograph certificates for recording

contact@nexussafe.com

www.nexussafe.com

Sweden

Headquarters:
Technology Nexus AB
Box 47057
100 74 Stockholm
Phone: +46 8 655 39 00

Germany

Nexus Technology GmbH
Kantstraße 13
10623 Berlin
Phone: +49 30 206 14 15 0

Sweden

Technology Nexus AB
Nämndemansgatan 3
431 33 Mölndal
Phone: +46 31 720 60 00

France

Nexus Technology SAS
112 ter, rue Cardinet
75017 Paris
Phone: +33 1 40070606



Providing safety in a digital world