

NetGuard Certificate Manager

The Nokia NetGuard Certificate Manager (NCM) is composed of software, as well as highly available and secure hardware to manage the digital certificates. Based on a trusted certification authority, the NCM manages digital identities in a standardized and secure way.

NCM is widely deployed in 4G mobile networks where base stations and small cells are located in unsecured areas, and where a secured connection to the backbone network is required. Deployment is not limited to mobile networks. NCM can be used to enable the safe authentication of users, devices, applications and systems in the Enterprise and Internet of Things (IoT) domain as well without the need for tokens, passwords, or other non-standardized authentication schemes. The distributed architecture allows for NCM deployments with active certificates scaling up to 100M+.

Key features and benefits

Features	Benefits
Provides certificates for any sort of standardized encrypted communication (IPsec, TLS, SSH).	• Qualified for devices and applications using IPsec protocol as defined by 3GPP • Validated with Nokia radio products • Proven with various IT systems and applications using TLS and SSH
Simplifies the exchange and management of certificates.	• Certificates are automatically downloaded using authenticated exchanges. • Designed and tested to support a full PKI up to 6 levels. • Easily managed by either a graphical user or command-line interface.
Increases interoperability by using standard management protocols.	• Supports all major certificate enrollment and validation protocols. • Complies with various PKI-related RFC and 3GPP standards.
Ensures service continuity with high availability.	• Fully redundant architecture provides carrier-grade reliability (99.99 percent availability).

Technical specifications

Certificate management

Online certificate life-cycle management

- Fully customizable automation of Certification Authority (CA) and Registration Authorities (RA) policy rules
- Multiple CA hierarchies and RAs within an installation
- Web-based self-enrolment with customizable web enrollment pages
- RA with smart card and USB token personalization option
- Automatic CA renewal
- Manual and online cross-certification
- Online key backup and recovery
- CA private key storage in Hardware Security Module (HSM)

Revocation

- Periodic Certificate Revocation List (CRL) publishing
- Per-revocation CRL publishing
- Self-revocation based on pre-shared key (PSK)
- Online Certificate Status Protocol (OCSP) responder service with whitelist checking and HSM support

Architecture

- Modular architecture: Front-end PKI services and back-end certificate engine
- Clustering of multiple back-end certificate engines with geo-redundant deployment option
- Duplication of front-end PKI services
- Online and offline CA deployment options
- Secure communication between system components

Deployment modes

- Bare metal on COTS HP hardware
- Virtualized (VMware ESXi, OpenStack, Nokia CloudBand)

Directory integration

- Certificate and CRL publishing to standard LDAP directory or HTTP server
- Flexible publishing schemas
- Support for Microsoft Active Directory
- TLS protection of LDAP publishing
- LDAP authentication

Administration

- Web administration UI with role-based access control
- Support for dual control and separation of duties
- Restriction of access to specific CAs and operations
- Integrity-protected event logging and audit trail
- SNMP support for monitoring and statistics

Compliance

- EU Directive on Electronic Signatures (1999/93/EC)
- EU/ETSI qualified certificates
- 3GPP CMP profile
- ICAO Doc 9303, Part 12 - Public Key Infrastructure for Machine Readable Travel Documents

Security

- PKI-white and blacklist support
- Protocol conformity checks
- Certificate request validation
- Access control/local firewalling
- Dual admin control

Protocols and algorithms

Enrollment, publishing and management protocols

- Certificate Management Protocol (CMPv2)
- Simple Certificate Enrolment Protocol (SCEP)
- Enrollment over Secure Transport (EST)
- RESTful API (HTTP)
- Web-form-based PKCS #10 certification requests
- Web browser enrolment
- Online Certificate Status Protocol (OCSP)
- Lightweight Directory Access Protocol (LDAP)
- Hypertext Transfer Protocol (HTTP)

Supported formats

- X.509v3 certificate profile
- X.509v2 CRL format
- PKCS#1 RSA
- PKCS#6 extended certificate syntax (selectively)
- PKCS#7 envelopes
- PKCS#8 password-protected private keys
- PKCS#9 attribute types (selectively)
- PKCS#10 certification requests
- PKCS#12 Personal Information Exchange Syntax
- Certification Request Message Format (CRMF)

Supported 3GPP standards

- TS 33.210
- TS 33.310
- TS 33.401

Interfacing with Hardware Security Modules (HSM)

- PKCS #11 crypto API
- Supports Thales HSM

Security protocols

- Transport Layer Security (TLS)

Public-Key algorithms

- RSA (up to 8192 bits)
- ECC (secp256r1, secp384r1 and secp521r1)

Hash algorithms

- SHA-1
- SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512)

Symmetric algorithms

- AES 128/256-bit
- 3DES



About Nokia

We create the technology to connect the world. Only Nokia offers a comprehensive portfolio of network equipment, software, services and licensing opportunities across the globe. With our commitment to innovation, driven by the award-winning Nokia Bell Labs, we are a leader in the development and deployment of 5G networks.

Our communications service provider customers support more than 6.4 billion subscriptions with our radio networks, and our enterprise customers have deployed over 1,300 industrial networks worldwide. Adhering to the highest ethical standards, we transform how people live, work and communicate. For our latest updates, please visit us online www.nokia.com and follow us on Twitter [@nokia](https://twitter.com/nokia).

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

© 2020 Nokia

Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Product code: SR2009046880EN CID: 200770