Nokia 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 used in the security domain. Based on a trusted certification authority, the NCM manages the entire lifecycle of a digital identity in a standardized and secure way. Its primary use is for 4G mobile networks where base stations and small cells are deployed in an unsecured area, and where a secured connection to the backbone network is required.

In that context, the IPsec protocol is used for securing data exchanges with the Security Gateway—the Nokia 7750 Service Router—and requires digital certificates for the purpose of identification. The NCM simplifies and secures this process by setting up a public key infrastructure (PKI), according to the 3GPP TS 33.210, 33.310, and 33.401 standards. It allows certificates to be securely and automatically enrolled to the base stations.

For the Internet of Things (IoT), the NCM can be used to enable the safe authentication of users, devices, applications and systems without the need for tokens, passwords, or other non-standardized authentication schemes. The distributed architecture allows NCM deployments of active certificates scaling up to 100M+.

Benefits and features

| Prevents security issues, where an unsecured backhaul connects base stations to the RAN (leased line, public network, or public places with easily accessible equipment). | • Implements the IPsec protocol, as required by the 3GPP specification.  
• Fully validated with Nokia radio products |
|---|---|
| Simplifies the exchange and management of certificates when using the IPsec protocol. | • 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).  
• Geo-redundancy offers autonomous site loss recovery. |
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

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/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)
• RESTfulAPI (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)

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