CM 7.16.1 requirements and interoperability

This article provides a list of supported platforms, formats, and third party products, for use with Nexus Certificate Manager. All listed hardware and software can be used in supported configurations of the product.

> ⚠ Listed third party hardware and software has been verified with the current or a previous version of Nexus Certificate Manager.

Expand/Collapse All

This article is valid for Nexus Certificate Manager 7.16.1.

Related information

- Nexus Personal Desktop
- Nexus PRIME

Requirements

- Key Generation System, KGS
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows 7, 8.1, 10
- CM Clients
  - Windows XP SP3
  - Windows Vista SP1
  - Windows 7, 8.1, 10
  - Windows Server 2012 R2, 2016
  - Red Hat Enterprise Linux 6/7
  - CentOS 6/7
- CM Server
  - Windows Server 2012 R2
  - Windows Server 2016
  - Red Hat Enterprise Linux 6/7
  - CentOS 6/7

- Microsoft SQL Server Express and Enterprise editions:
  - 2008 SP2, 2008 R2, 2012 SP4, 2016.
- Oracle Express and Enterprise editions:
  - 10g, 11g. 12c when upgraded from 11g
- PostgreSQL:
  - 9.5

- CM Server
  - Oracle Java SE JRE 8u151 (64 bit) or a later 1.8-release
- CM Clients
  - Oracle JRE 8u151 (32 or 64 bit) or a later 1.8-release

CM Web Services and Protocol Gateway servlets run on Apache Tomcat version 8.

Nexus Personal Desktop is middleware for use on CM clients, for officer smart card authentication and personalization of smart cards:

- CM clients and CM SDK on Windows: Nexus Personal Desktop 4.28.2.
- CM clients and CM SDK on RedHat: Nexus Personal Desktop 4.28.2.

Interoperability

Formats and standards

- X.509/RFC 3280/RFC 5280/RFC 6818 certificates, configurable profiles
- X.509/RFC 3281 attribute certificates
- Common PKI (alias ISISMTT) v2.0 private extensions, private attributes and optional SigG-Profile
- Card Verifiable Certificates (CVC) according to Gematik specification Electronic Health Card, Part 1, v2.0.0 (Dec. 2007). Generations G0, G1 and G2. CPI types: 3, 4, 21, 22 and 70. CV certificates must be issued over CM SDK.
- Tachograph certificates
- Certificate Transparency Precertificate, RFC 6962
- PKIX and ETSI Qualified Certificates
- OpenPGP V4 keys and certificates
- Extended Validation certificates
- Swedish eID certificate profile as defined by the Swedish e-identification board

- X.509/RFC3280/RFC5280 CRL
- Full and delta CRL
- Direct and indirect CRL
- Partitioning according to revocation reasons
- Immediate CRL issuing option: besides the regular issuing, a CRL can be generated immediately at revocation of a certificate

A Nexus proprietary format used by CM to inform the Nexus OCSP Responder about issued or activated certificates to enable the non-issued concept of RFC 6960 and for activation of user certificates. The CIL format is similar to CRL in structure and is signed alike by the CA.

The following types of CILs are provided:

- Complete CIL
- Size segmented CILs
- Delta CIL

Support for precertificates according to RFC 6962, Certificate Transparency, with version 1 Signed Certificate Timestamps (SCTs) and Log servers.

- CA signatures: RSA, RSASSA-PSS, DSA
  Key lengths as supported by HSM (e.g. RSA 1024 - 16384 bit). Algorithms: SHA-1, SHA-256, SHA-384, SHA-512, RipeMD-160
- CA signatures: EC, Prime field based ECDSA algorithms with named curves as supported by HSM, hash functions as above
- End user keys: RSA, 1024-4096 bits (soft tokens and on smart card/token type)
- End user keys: EC, Prime field based ECDSA algorithms with arbitrary curve parameters (only on smart cards). Certificates for ECDSA keys can be requested only via CM SDK

In addition to using the standard CM clients for certificate enrollment can third party devices, clients and servers enroll for certificates directly by support of any of the following protocols:

- **SCEP** - Simple Certificate Enrollment Protocol, draft-nourse-scep-23
- **CMP** - Certificate Management Protocol, RFC 4210, RFC 421
- **CMC** - Certificate Management over CMS, RFC 5273
- **EST** – Enrollment over Secure Transport, RFC 7030
- **EST-coaps** – EST over coaps, IETF draft
- **CM SDK** – CM Software Development Kit
- **SOAP** – Web Services
- **WinEP** - Windows certificate auto enrollment using Windows certificate templates

- Operational logs and signed audit logs
- Ping-request for system health checks
- SNMP v1, v2c, v3
- Syslog

- PKCS#12 v1.1, according to RFC 7292
- PGP, OpenPGP V4 keys and certificates

Smart cards

Smart card support as provided in middleware used by card personalization software, for example CM clients, Nexus PRIME, and SmartAct.

Currently available cards supported by Nexus Personal Desktop:

- Atos CardOS 4.4, 5.0, 5.3
- Gemalto IDClassic 340
- Gemalto IDPrime MD 840 Nexus Profile. Gemalto product name: ENT_Nexus_IDPrime MD 840_PPR. PDM-Customer Item: C1105591 A

The smart cards must be prepared with the card profiles delivered with CM, in accordance with ISO /IEC 7816-15:2004.

Third-party software

Certificate Manager supports directory servers compliant with LDAPv3 and X.500 for retrieving user data, publication of certificates and CRLs.

Certificate Manager is tested and commonly used with, but not limited to, the following directory servers:

- Atos DirX Directory
- ApacheDS
- Microsoft Active Directory
- OpenLDAP

MDM software that supports SCEP can request certificates for registered devices.

Nexus has explicitly verified the following software:

- MobileIron
- VMware AirWatch

Third-party hardware

Certificate enrolment for firewalls and network equipment using SCEP is based on version: draft-nourse-scep-23.

The following devices are explicitly verified:

- Cisco – current SCEP compatible IOS and ASA versions
- Fortinet FortiGate firewall series with up-to-date firmware

A PKCS#11 compliant device can be used for handling of CA key pairs, system keys, protection of archived keys, and for key generation.

The following devices are explicitly verified:

- AEP Systems Sureware Keyper, FIPS 140-1 level 4
- Atos Bull Trustway Proteccio NetHSM
    - Note: Only verified with CIS, not with CCM and KAR.
- DocuSign ARX PrivateServer
- Gemalto SafeNet ProtectServer Internal - Express 2
- Gemalto SafeNet ProtectServer External 2
- Gemalto SafeNet Luna CA3, FIPS 140-1 lvl 3
- Gemalto SafeNet Luna CA4, FIPS 140-2 lvl 3
- Gemalto SafeNet Luna SA 4.4, FIPS 140-2 lvl 3
    - Note: Since SafeNet Luna disallow key export when in FIPS mode, enable non-FIPS mode for use with CM KAR, Key Archiving and Recovery.
- Gemalto SafeNet Luna SA 5.0, FIPS 140-2 lvl 3
    - Note: Since SafeNet Luna disallow key export when in FIPS mode, enable non-FIPS mode for use with CM KAR, Key Archiving and Recovery.
- Gemalto SafeNet Luna G5
- IBM 4758, FIPS 140-1 level 3 and 4
- Thales nShield Connect+, FIPS 140-2 level 3
- Thales nShield Solo+, FIPS 140-2 level 3
- Thales nShield Edge
- Thales WebSentry PCI, FIPS 140-1 level 4
- Thales WebSentry Ethernet, FIPS 140-1 level 4
- Utimaco CryptoServer Security Server CS 10/50 LAN/PCI, FIPS 140-2 level 3 (level 4 for physical)
- Utimaco CryptoServer Security Server Se 10/50/400/1000 LAN/PCI, FIPS 140-2 level 3

PIN decryption is not allowed using a FIPS mode HSM.

Stackers used for smart card handling with KGS.

- Fischer Electronicsysteme GmbH
- Zeitcontrol MKW Professional.

Mass production of cards with card printers is enabled in Registration Authority and Batch Explorer clients by using the Nexus Card SDK. Card SDK enables card printing and feeding of cards, while Nexus Personal handles chip personalization.

- Printer models as supported by the Nexus Card SDK. The printer must be equipped with a smart card chip coupler that can be accessed over USB from the client computer. A PC /SC driver has to be installed on the client.
- A license for Nexus Card SDK must be purchased separately.

Printers using a vendor provided driver is expected to work with CM Secure Printer for PIN letters. Dot matrix printers, capable of printing on 3-layer PIN envelopes, which have been explicitly tested:

- Tally T2340/24
- EPSON LQ-300, 300+II

Laser printers can be used for printing PIN letters equipped with a removable PIN protection label.

Readers for personalization of cards and for using smart card based CM officers with the CM clients.

- PC/SC compliant card readers.
- PC/SC 2.01 Part 10 compliant PIN-pad readers
- HID/Omnikey 6121 Mobile USB smart card reader (to be used with smart cards in SIM format).

Equipment that supports SCEP or CMP can request certificates after being registered in CM.

The following devices are explicitly verified:

- Airspan AirHarmony 1000 ENB (CMP)
- Airvana/Commscope OneCell (CMP)
- Alcatel Lucent 9412 (CMP)
- CISCO 7600 Series Routers with SAMI (CMP)
- Ericsson RBS6000 (SCEP)
- Ericsson RBS6201 (CMP)
- Huawei ENB (CMP)
- Huawei Femtocell BTS3202H, 3202E (CMP)
- Juniper SRX (SCEP)
- Nokia Networks ENB (CMP)
- Nokia Networks Flexi Zone micro (CMP)

High availability

Different types of high availability techniques can be used with the CM core components Certificate Factory (CF) and Certificate Issuing System (CIS):

- Active/passive dual-node hardware cluster using clustering software supported by the OS: Microsoft Windows Server Failover Clustering and Red Hat Cluster High Availability.
- Active/active, unlimited number of active nodes behind a load balancer. This alternative provides performance scalability in addition to HA.
- High Availability functionality as provided in virtualization software solutions, for example, VMware vSphere HA.