

Product: Nexus Certificate Manager

Version: 7.0

Availability date: 1st March 2009

Document version: 1st March 2009

About this document

This product release bulletin reports about the current, generally available release 7.0 of the Nexus Certificate Manager product. It provides information about architectural changes, and about new and discontinued features.

Interoperability Information

Platform:

Windows 2003 Server R2, Windows 2008 Server, Red Hat Enterprise Linux 5

Support for other Linux distributions upon request.

Database Engine:

Microsoft SQL Server 2005 SP3, Oracle 10g

Support for MySQL upon request.

Java VM:

CM Server & Clients: Java SE Runtime Environment (JRE) 6 Update 12

CM SDK client (including custom applications using the SDK): JRE 6 Update 12

Nexus Personal:

Nexus Personal 4.10

Internet Browser:

WebRA CMC/RegUtil Server: Microsoft Internet Explorer v7

WebRA EUI Server: Microsoft Internet Explorer v7, Mozilla Firefox 3

Discontinued features

Discontinued platforms:

Red Hat Linux 4

CPM DB, KAR DB

In CM 7.0 the content of the card production database (CPM DB) and the key archiving database (KAR DB) has been integrated into CM DB.

LCM API

The LCM API has been removed from the CM product. Customers using the LCM-API are advised to migrate to CM SDK or CM Web Services. Nexus Professional Services offer assistance for migration projects.

WebRA - SCEP Registration, Application and Claim modules

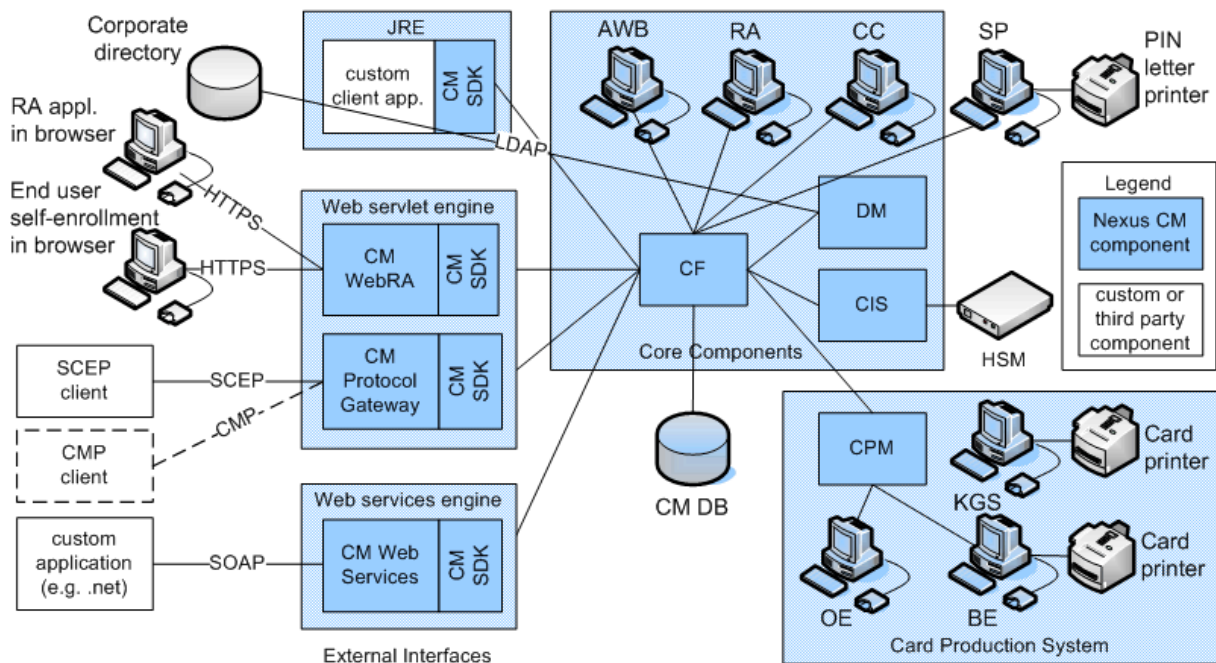
The former 'SCEP Registration' module in the WebRA has been removed. The SCEP registration is implemented now in the RA client, which adds strong authentication, request signature, batch registration and auditing capability to the former registration functionality.

The WebRA modules 'Application' and 'Claim' have been removed. These functions will be replaced by the Credential Life-cycle Manager (CLM) component in a later CM v7 release.

New features in this release

Architecture overview

The overall architecture of CM 7.0 is illustrated in the diagram below. Most CM v6 server and client components are retained in their original form and remain nearly unaltered. Only the WebRA modules 'SCEP registration', 'Application' and 'Claim' have been removed. The new web-based components are CM Protocol Gateway and CM Web Services (CM WS).



CM 7.0 architecture overview

All new CM web components use the CM SDK to access the CM server. WebRA and Protocol Gateway are implemented as Java servlets and run in a web servlet engine. CM Web Services is implemented as XML-based Web Services on Sun JAX-WS framework. The WSDL description of the service is published in the product documentation to enable customers implementing their own Web Service based applications.

CM Protocol Gateway

The CM Protocol Gateway module supports certificate management protocols, such as SCEP, CMC or CMP. The Protocol Gateway services are implemented as Java servlets and run in a web servlet engine. Currently, Nexus tests exclusively on a Tomcat servlet engine. The Protocol Gateway module is offered as licensable add-on option to CM. The CM SDK server is included in this license.

SCEP server

The SCEP server is available in CM 7.0. More SCEP protocol elements (commands) are supported than in former CM versions. A more user-friendly installation procedure is provided. Upon a SCEP request a certificate will be enrolled only if:

- the SCEP client device is registered in CM and
- the registration record is flagged 'active' and
- all other conditions defined in the SCEP protocol are fulfilled.

CMP server

CMP has been developed with additional proprietary extensions for the German health card (eGK) project. The CMP module can be added to the product on customer request.

CMC server

A new CMC server is planned for CM 7.1. The CMC/RegUtil module of the WebRA can be used in CM 7.0.

CM Web Services

The CM Web Services module (CM WS) is implemented as XML-based Web Services on Sun JAX-WS framework. Registration officer functions are available over this web interface. The WSDL description of the service is published in the product documentation to enable customers implementing their own Web Services based applications. The CM WS module is offered as licensable add-on option to CM. The CM SDK server is included in this license.

Not all CM SDK functions are supported in CM 7.0. In this version all requests are signed by a virtual registration officer (VRO) at the CM WS server side. A complete coverage of SDK functions, individual officer signatures and SSL communication are planned in CM 7.1. It is at current time not foreseen to expose AWB functions over CM WS.

CM server improvements

Java version

The server components deploy JRE 6 Update 12.

CM protocol improvements

Changes in TCP protocol

A new protocol between CM server and native CM clients has been introduced in CM 7.0. The new protocol is based on HTTP and needs only one (configurable) port connection. CM 7.0 clients deploy the new protocol, if connecting to the server. For the ease of upgrading systems in a distributed environment, the CM 7.0 server also supports the CM 6.7 protocol, i.e. it is backwards compatible with CM 6.5...6.7 clients.

CM client improvements

General Purpose Input View (GPIV)

The General Purpose Input View (GPIV) has been introduced in CM 6.6 and can be used in the native RA client for creating certificate, soft token, smart card, and token requests from an imported list of registration records. The GPIV has been extended in this release so that it can import request records not only from CSV files, but also from an LDAP directory. The GPIV is also able to search and to list data records into CSV files.

SCEP registration

Before the SCEP server can respond to certificate requests with a certificate, the SCEP client device must be registered. SCEP devices need to be registered over the native RA client. The registration may have a configurable validity period. A SCEP device registration can be entered via the 'order' tab of the RA client. All registration requests must be signed and can later also be audited via AWB.

The registration can take place in two different modes:

- Single registration: using a preconfigured input view, it is possible to register SCEP devices on-by-one.
- Batch registration: using a preconfigured input view (GPIV) and CSV file format, it is possible to import registration records from a file and register multiple records with one single PIN entry by the administrator.

Each registration record can be edited later and can be set 'active' or 'closed', enabling or disabling thus the certificate enrolment.

Using the preconfigured input view and CSV file format, it is also possible to list all available registration records to a file.

Java version

The native CM clients as well as the CM SDK client deploy JRE 6 Update 12.

Upgrade information

Upgrade packages

Besides a complete installation package for CM 7.0, upgrade packages are available for former CM versions 6.5 and later. We recommend customers to use Nexus Professional Services to assist the upgrade and subsequent system verification tests. We strongly recommend creating a backup of the database and all configuration data, and exercising the upgrade procedure in test systems before upgrading production systems.

Functional backward compatibility

In the current release 7.0, the former CM server and client functions are retained and remain nearly unaltered, i.e. all functions, objects, configuration settings etc. that were available in version 6.5...6.7 are also available in version 7.0.

Database compatibility

The CM 7.0 database is not be compatible with the database scheme of CM 6.7. In particular, the content of the former CPM DB has been integrated into CM DB. CPM DB and KAR DB can be dropped after the upgrade. SQL upgrade scripts are provided in the respective upgrade package for former CM versions 6.5 and later.

CM server compatibility

The Java run-time environment has to be upgraded to version 6 (i.e. JRE 6) before installing CM 7.0 server components.

CM client compatibility

CM 7.0 is shipped with native CM client and SDK client components, which use a new HTTP based protocol to connect to the CM server. For the ease of upgrading distributed systems, CM 7.0 server also supports the CM 6 protocol over a separate port during a migration phase, i.e. it is backwards compatible with CM 6.5...6.7 clients, including the SDK client, but excluding the AWB client. An AWB 6.5...6.7 client can only be used to view the current configuration, but it cannot be used to change or create any key, CA or policy object. The client backwards compatibility option needs to be enabled in cm.conf.

Native CM clients as well as the CM SDK client deploy JRE 6 Update 12.

CM SDK compatibility

There are no changes to the Java interface of SDK, so custom Java applications, working with CM SDK 6.5 or later, do not require code changes to fit CM SDK 7.0. In this way, client applications can be easily updated to CM 7.0. During a migration phase, customers may also use the CM SDK 6.5...6.7 client in conjunction with CM 7.0 SDK server.

How to contact us

Please contact your sales representative for pricing information or to get a copy of the new version. A free, fully functional evaluation version can be requested too by new customers.

To provide feedback or to suggest product enhancements, please send an email to productmanagement@nexussafe.com. If you have questions about the product or this bulletin, do not hesitate to contact us. General information is available at: <http://www.nexussafe.com>.

Best regards,

Nexus Product Management

Technology Nexus AB

Box 47057

100 74 Stockholm

SWEDEN

productmanagement@nexussafe.com