Swedish Certification Body for IT Security

Certification Report - Nexus CM8

Issue: 1.0, 2020-Mar-20

Authorisation: Jerry Johansson, Lead certifier , CSEC

Table of Contents

1 Executive Summary

The TOE is the two software components: Nexus Certificate Manager v.8.0.0, and Nexus OCSP Responder v.6.0.2, which form a Certificate Authority (CA), i.e. a system for issuing X.509 certificates. The TOE issues X.509 certificates, maintains revocation lists, and responds to certificate status requests.

Both TOE components need a Java Run-time Environment, and an operating system, which can be contained in a virtual machine or run directly on server hardware. The TOE has built-in cryptographic support but it is intended to use a separate Hardware Security Module for cryptographic functions. Database functionality is also needed.

The ST claims demonstrable conformance to the Certificate Issuing and Management Components Protection Profile [CIMC].

The evaluation has been performed by atsec information security AB in their premises in Danderyd, Sweden, to some extent in the developer's premises in Hägersten, Sweden, and was completed on the 4th of March 2020.

The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 5, and the Common Methodology for IT Security Evaluation, version 3.1, release 5. The evaluation conforms to evaluation assurance level EAL 4, augmented by ALC_FLR.2.

atsec information security AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. atsec information security AB is is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target [ST], and have been reached in agreement with the requirements of the Common Criteria and the Common Methodology for the evaluation assurance level EAL 4 + ALC_FLR.2.

2 Identification

Certification Identification	
Certification ID	CSEC2017002
Name and version of the certified IT product	Nexus Certificate Manager version 8.0.0 Nexus OCSP Responder version 6.0.2
Security Target Identification	Nexus CM8 Security Target, Technology Nexus Secured Business Solution AB, 2020-03-02, document version 1.0
EAL	EAL 4 + ALC_FLR.2
Sponsor	Technology Nexus Secured Business Solution AB
Developer	Technology Nexus Secured Business Solution AB
ITSEF	atsec information security AB
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
QMS version	1.23.1
Scheme Notes Release	14.0
Recognition Scope	CCRA, SOGIS, EA/MLA
Certification date	2020-03-20

3 Security Policy

The TOE provides the following security services:

- Roles
- Identification and Authentication
- Access Control
- Certificate Registration
- Certificate Revocation (CRL and OCSP validation)
- Certificate Profile Management
- OCSP Profile Management
- Certificate Revocation List Profile Management
- Key Management: Key Storage, Key Destruction and Key Export
- Remote Data Entry and Export
- Security Audit

3.1 Roles

The TOE users are known collectively as Officers. There are three general types of Officers:

- Administration Officers who are responsible for administering the security policies of the TOE (i.e. setting up CA policies, auditing, etc.)
- Registration Officers who are responsible for registering users, issuing certificates, revoking certificates, etc.
- Authentication Officers who only have restricted rights, such as establishing TLS connection between a client application and the CM server, listing of certificates and forwarding of certification requests signed by a Registration Officer.

The TOE enables configuration of officer roles on a fine-grained level for restricting officers to perform specific tasks, e.g. audit tasks. For the complete list of tasks that can be assigned to different types of Officers please refer to section 7.1.2 "Roles" of the Security Target [ST].

3.2 Identification and Authentication

Identification and authentication of Officers is accomplished by use of certificates, i.e. PKI based signed challenges and requests. All requests received by the CM server are first handled by the Request Manager component. The Request Manager authenticates the connecting Officer and during this process a client/server authenticated TLS session is established between the CM Server and the CM client. The Officer uses a private authentication key for this purpose.

For OCSP clients, they can be identified and authenticated by the OCSP Responder when TLS is enabled, or by enforcing use of signed OCSP client requests. Note however it is configurable whether client authentication is required for the OCSP Responder to accept and reply to OCSP requests.

3.3 Access Control

For each request received by the CM, the Access Manager component ensures that the authorization level of Officers, once authenticated, are suitable for all given requests (i.e. registration requests, revocation requests, etc.). All other components rely upon the Access Manager to perform these checks.

For each OCSP request received by the OCSP Responder, the OCSP client is authorized by matching its certificate to the content of a trust store or by matching the subject name to a table of authorized clients.

3.4 Certificate Registration

Signed certificate requests (and/or certificate orders) are received by the CM via the Request Manager component over a TLS channel. The Request Manager is responsible for distributing the incoming request to the other factory components. Once the authorization of the requesting Officer has been successfully verified by the Access

Manager, the factory component that received the request performs the requested operation, including certificate and subject data registration for individual certificate issuance or smart card batch production.

3.5 Certificate Revocation (CRL and OCSP validation)

Signed certificate revocation requests are received by the Request Manager over a TLS channel, which ensures that the TOE does not accept revocation requests through channels that are not secure and does not accept requests that are not signed by an authorized Officer. Revocation requests are processed by the Request Factory components (in this case the CRL Factory and Revocation Factory) and result in the certificate status being changed in the CM database (CMDB). Subsequent to certificate revocation, the CRL is updated/the certificate is added to the CRL. The TOE enables certificate revocation and generation of CRLs according to X.509 and allows OCSP responses according to RFC 6960.

3.6 Certificate Profile Management

The TOE enables certificate profiles to be configured in accordance with ISO/ITU X.509, RFC 5280, RFC 5755 (attribute certificates), Card Verifiable Certificates specifications, IEEE 1609.2, ISO 9796-2 (Tachograph certificates), RFC 6962 (Certificate Transparency Precertificates), and RFC 4889 (PGP certificates). Certificate profile

configuration is performed by Administrator Officers, who specify the acceptable values of the certificate’s fields and extensions.

3.7 OCSP Profile Management

The TOE enables OCSP responder profiles to be configured in accordance with RFC 6960. OCSP profile configuration is performed by Administrators, who specify acceptable values, fields and types in OCSP responses.

3.8 Certificate Revocation List Profile Management

The TOE enables certificate revocation list profiles to be configured in accordance with ISO/ITU X.509, RFC 5280 and RFC 5755. Certificate revocation list profile management is performed by Administration Officers by using CRL formats and CRL procedures.

3.9 Key Management: Key Storage, Key Destruction and Key Export

The TOE relies on FIPS 140-2 validated (or CC EAL 4+ evaluated) Hardware Security Modules (HSMs) for key management. CIMC keys (e.g. CA keys, CIS log signing keys, PIN encryption and decryption keys, TLS keys and OCSP responder keys) are generated and stored in one or more HSMs. If certificate subject private keys are to be archived, they are stored in encrypted form in the CMDB and the encryption is achieved by using an HSM and Key Encryption Keys (KEKs).

Cryptographic keys in the HSMs are destroyed by the HSMs in accordance with the FIPS 140-2 cryptographic key destruction method to ensure that an untrusted entity cannot use a trusted entity's key after the TOE's usage of the key ends.

The TOE ensures that electronically distributed private and secret keys are only exported from the TOE in encrypted form. The keys are exported to either a smart card or to a PKCS#12 soft certificate. The smart card is protected by a PIN. For a PKCS#12 soft certificate, the private key is encrypted with a password by using a FIPS 140-2 validated evaluated HSM.

Please note that the HSM(s) are not part of the TOE, but the TOE environment.

3.10 Remote Data Entry and Export

The TOE enables secure data entry for certificate creation, registration, revocation, keys, PIN/PUK and other data, and supports secure export of certificates, keys, and PIN/PUK. This is achieved through an HTTPS mutually authenticated connection, which is validated and auditable at all times.

The TOE exports certificate status information to various LDAP directories and HTTP servers according to the CA policy distribution rules, which is also secured through a mutually authenticated connection (LDAPS or HTTPS). The CM distributes CILs (Certificate Issuing Lists which contain all certificates issued by the signing CA) and CRLs to the OCSP Responder.

3.11 Security Audit

The TOE uses two logs for security auditing:

- Audit Log contains signed requests from the Officers that can change the configuration or state of any policy object or certificate.
- CIS log records the signing of certificates, CILs and CRLs by the Certificate Issuing System (CIS). Log entries are signed by a system key and chained to the previous record. The chained signature of the CIS Log enables detection of any modifications of the CIS Log and by that alerting Officers operating the Administrator Workbench (AWB).

If the storage space for the Audit Log or the CIS Log would be exhausted, the auditing will stop and no further certificate management request will be accepted until the storage space has been cleaned up or extended.

Review of the Audit and CIS Logs is performed by an Administration Officer that has the role of ’Audit tasks’. The Officer uses the AWB to request and search for the log records to be displayed.

4 Assumptions and Clarification of Scope

4.1 Assumptions

The Security Target [ST] makes eleven assumptions on the usage of the TOE.

A.Auditors Review Audit Logs

Audit logs are required for security-relevant events and must be reviewed by the Auditors.

A.Authentication Data Management An authentication data management policy is enforced to ensure that users change their authentication data at appropriate intervals and to appropriate values (e.g., proper lengths, histories, variations, etc.) (Note: this assumption is not applicable to biometric authentication data.)

A.Competent Administrators, Operators, Officers and Auditor

Competent Administrators, Operators, Officers and Auditors will be assigned to manage the TOE and the security of the information it contains.

A.Cooperative Users

Users need to accomplish some task or group of tasks that require a secure IT environment. The users require access to at least some of the information managed by the TOE and are expected to act in a cooperative manner.

A.CPS

All Administrators, Operators, Officers, and Auditors are familiar with the certificate policy (CP) and certification practices statement (CPS) under which the TOE is operated.

A.Disposal of Authentication Data

Proper disposal of authentication data and associated privileges is performed after access has been removed (e.g., job termination, change in responsibility).

A. Malicious Code Not Signed

Malicious code destined for the TOE is not signed by a trusted entity.

A.Notify Authorities of Security Issues

Administrators, Operators, Officers, Auditors, and other users notify proper authorities of any security issues that impact their systems to minimize the potential for the loss or compromise of data.

A.Social Engineering

General users, administrators, operators, officers and auditors are trained in techniques to thwart social engineering attacks.

A.Operating System

The operating system has been selected to provide the functions required by this CIMC to counter the perceived threats identified in this PP.

A.Communications Protection

The system is adequately physically protected against loss of communications i.e., availability of communications.

A.Physical Protection

The TOE hardware, software, and firmware critical to security policy enforcement will be protected from unauthorized physical modification.

4.2 Clarification of Scope

The Security Target contains fourteen threats, which have been considered during the evaluation.

T.Administrative errors of omission Administrators, Operators, Officers or Auditors fail to perform some function essential to security.

Clarification: Functions essential to security are the management functions that are described in Table 2 under FMT_MOF.1 (iteration 2).

T.Administrators, Operators, Officers and Auditors commit errors or hostile actions

An Administrator, Operator, Officer or Auditor commits errors that change the intended security policy of the system or application or maliciously modify the system's configuration to allow security violations to occur.

Clarification: Changes to the security policy are changes in security management functions behaviour as described in Table 2 under FMT_MOF.1 (iteration 2).

T.User abuses authorization to collect and/or send data User abuses granted authorizations to improperly collect and/or send sensitive or security-critical data.

Clarification: Sensitive or security-critical data is any information that authorized users will be given access to that may not be disclosed to other parties. While it cannot be prevented for authorized users, access to any information as part of the operation of the TOE will be audited. This is described in Table 1 under FAU_GEN.1 Audit data generation (iteration 2) in rows "Local Data Entry", "Remote Data Entry", "Data Export and Output".

T.User error makes data inaccessible User accidentally deletes user data rendering user data inaccessible.

T.Critical system component fails

Failure of one or more system components results in the loss of system critical functionality. Threat agent in this case is the CIMC hardware. Adverse action can be compromise of the security of the CIMC and/or relying party systems that rely on the PKI objects such as certificates, CRLs, or OCSP Responses.

T.Flawed code

A system or applications developer delivers code that does not perform according to specifications or contains security flaws. Threat agent in this case is the TOE developer. Adverse action can be compromise of the security of the CIMC and/or relying party systems that rely on the PKI objects such as certificates, CRLs, or OCSP Responses.

T.Malicious code exploitation

An authorized user, IT system, or hacker downloads and executes malicious code, which causes abnormal processes that violate the integrity, availability, or confidentiality of the system assets. Threat agent could be an authorized user, TOE itself, or an unauthorized user. Adverse action can be compromise of the security of the CIMC and/or relying party systems that rely on the PKI objects such as certificates, CRLs, or OCSP Responses.

T.Message content modification

A hacker modifies information that is intercepted from a communications link

between two unsuspecting entities before passing it on to the intended recipient. Threat agent is an unauthorized user. Adverse action can be compromise of the security of the CIMC and/or relying party systems that rely on the PKI objects such as certificates, CRLs, or OCSP Responses.

T.Disclosure of private and secret keys

A private or secret key is improperly disclosed. Threat agent is the authorized user or erroneous protocol. Adverse action can be compromise of the security of the CIMC and/or relying party systems that rely on the PKI objects such as certificates, CRLs, or OCSP Responses.

T.Modification of private/secret keys A secret/private key is modified. Threat agent is the authorized user or erroneous protocol. Adverse action can be compromise of the security of the CIMC and/or relying party systems that rely on the PKI objects such as certificates, CRLs, or OCSP Responses.

T.Sender denies sending information

The sender of a message denies sending the message to avoid accountability for sending the message and for subsequent action or inaction. Threat agent is a subscriber to CIMC. Adverse action can be reduced trust in CIMC.

T.Hacker gains access

A hacker masquerades as an authorized user to perform operations that will be attributed to the authorized user or a system process or gains undetected access to a system due to missing, weak and/or incorrectly implemented access control causing potential violations of integrity, confidentiality, or availability. Threat agent is the unauthorized user. Adverse action can be compromise of the security of the CIMC and/or relying party systems that rely on the PKI objects such as certificates, CRLs, or OCSP Responses.

T.Hacker physical access

A hacker physically interacts with the system to exploit vulnerabilities in the physical environment, resulting in arbitrary security compromises. Threat agent is the unauthorized user. Adverse action can be compromise of the security of the CIMC and/or relying party systems that rely on the PKI objects such as certificates, CRLs, or OCSP Responses.

T.Social engineering

A hacker uses social engineering techniques to gain information about system entry, system use, system design, or system operation. Threat agent is the unauthorized user. Adverse action can be compromise of the security of the CIMC and/or relying party systems that rely on the PKI objects such as certificates, CRLs, or OCSP Responses.

Please note that the threats are taken from the [PP], so the references to Table 1 and 2 refers to the [PP].

The Security Target contains two Organisational Security Policies (OSPs), which have been considered during the evaluation.

P.Authorized use of information

Information shall be used only for its authorized purpose(s).

P.Cryptography

FIPS-approved or NIST-recommended cryptographic functions shall be used to perform all cryptographic operations.

5 Architectural Information

Section 1.4 in the [ST] provides a detailed description of the components in the TOE and in the TOE environment.

6 Documentation

For proper configuration and operation of the TOE in the evaluated configuration, the following documentation is available:

TECH	Technical Description Certificate Manager 8.0.0
INSTALL	Installation Guide Certificate Manager 8.0.0
ADM	CA Administrator's Guide Certificate Manager 8.0.0
REG	Registration Officer's Guide Certificate Manager 8.0.0
SYS	System Administrator's Guide Certificate Manager 8.0.0
CCCG	CC Configuration Guide Certificate Manager 8.0.0
OCSP	Nexus OCSP Responder Reference Guide 6.0.2

7 IT Product Testing

7.1 Developer Testing

The developers tested the TOE automatically, on four TOE configurations including two windows versions and two Linux versions, on two Java platforms, and using a PKCS#11 interfaced HSM emulator. The developer tests cover all TSFI, SFRs and all subsystems.

All test results were as expected.

The testing was performed in the developer's premises in Hägersten, Sweden.

7.2 Evaluator Testing

The evaluators tested the TOE on one configuration, with a PKCS#11 interfaced HSM. The evaluators re-ran 42 of the developer's test cases, modified and ran 4 test cases using the developer's automated test platform. The evaluators also ran 8 independently designed test cases.

All test results were as expected.

The tests were performed in the developer's premises in Hägersten, Sweden.

7.3 Penetration Testing

The evaluators penetration tested the TOE on one TOE configuration, with a PKCS#11 interfaced HSM. NMAP port scans and a Nessus vulnerability scan were made.

All test results were as expected.

The tests were performed in the developer's premises in Hägersten, Sweden.

8 Evaluated Configuration

The evaluated configuration of the TOE is Nexus Certificate Manager version 8.0.0 and Nexus OCSP Responder version 6.0.2, installed and operated in accordance with the documentation listed in chapter 6 of this document.

OpenJDK Runtime Environment AdoptOpenJDK 11.0.2

During the testing, the following Java Runtime Environments were used:

- Oracle Java 11
- Adopt Open JDK 11,

the following operating systems were used:

- Windows 2012
- Windows 2016
- CentOS 7
- Open SUSE LEAP 15,

and the following PKCS#11 interfaced crypto modules:

- Utimaco Security Server HSM simulator v. 4.30.0
- nCipher nShield F2 500+ v. 11.72.02.

9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target [ST] for an attack potential of Enhanced-Basic.

The certifier reviewed the work of the evaluator and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluators overall verdict is PASS.

The verdicts for the respective assurance classes and components are summarised in the following table:

Assurance Class/Family	*Short name*	*Verdict*
Development	ADV	PASS
Security Architecture	ADV_ARC.1	PASS
Functional Specification	ADV_FSP.4	PASS
TOE Design	ADV_TDS.3	PASS
Implementation Representation	ADV_IMP.1	PASS
Guidance Documents	AGD	PASS
Operational User Guidance	AGD_OPE.1	PASS
Preparative Procedures	AGD_PRE.1	PASS
Life-cycle Support	ALC	PASS
CM Capabilities	ALC_CMC.4	PASS
CM Scope	ALC_CMS.4	PASS
Delivery	ALC_DEL.1	PASS
Development Security	ALC_DVS.1	PASS
Life-cycle Definition	ALC_LCD.1	PASS
Flaw Remediation	ALC_FLR.2	PASS
Tools and Techniques	ALC_TAT.1	PASS
Security Target Evaluation	ASE	PASS
ST Introduction	ASE_INT.1	PASS
Conformance Claims	ASE_CCL.1	PASS
Security Problem Definition	ASE_SPD.1	PASS
Security Objectives	ASE_OBJ.2	PASS
Extended Components Definition	ASE_ECD.1	PASS
Security Requirements	ASE_REQ.2	PASS
TOE Summary Specification	ASE_TSS.1	PASS
Tests	ATE	PASS
Coverage	ATE_COV.2	PASS
Depth	ATE_DPT.1	PASS
Functional Tests	ATE_FUN.1	PASS
Independent Testing	ATE_IND.2	PASS
Vulnerability Assessment	AVA	PASS
Vulnerability Analysis	AVA_VAN.3	PASS

10 Evaluator Comments and Recommendations

None.

11 Certifier Comments and Recommendations

The [CIMC] PP requires that a FIPS 140-2 validated HSM in the operational environment is used for the cryptographic functionality in the PP and ST. The TOE is a software only product, and it is the user's responsibility to select a validated HSM.

The cryptographic FCS_CKM.1 and FCS_COP.1 SFRs are placed in the operational environment, but during the evaluation, all these cryptographic SFRs were tested against independent reference implementations. This was done to verify that the TOE actually supports, and correctly calls, all claimed algorithm variants and key lengths.

12 Glossary

CA	Certification Authority
CC	Common Criteria, standard for IT security evaluations
CEM	Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations
CIL	Certificate Issuance List
CIMC	Certificate Issuing Management Components
CIMS	Certificate Issuing Management System
CP	Certification Policy
CPS	Certification Practise Statement
CRL	Certificate Revocation List
EAL	Evaluation Assurance Level
HSM	Hardware Security Module
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within a evaluation and certification scheme
OCSP	On-line Certificate Status Protocol
OSP	Organisational Security Policy
PKI	Public Key Infrastructure
PP	Protection Profile
RA	Registration Authority
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target, document containing security requirements and specifications , used as the basis of a TOE evaluation
TOE	Target of Evaluation
X.509	CCITT standard for public key certificates

13 Bibliography

ST	Nexus CM 8 Security Target, Technology Nexus Secured Business Solutions AB, 2020-03-02, document version 1.0
CCCG	CC Configuration Guide Certificate Manager 8.0.0 , Technology Nexus Secured Business Solutions AB, 2019-07-02, document version A
TECH	Technical Description Certificate Manager 8.0.0, Technology Nexus Secured Business Solutions AB, 2019-04-26, document version A
INSTALL	Installation Guide Certificate Manager 8.0.0, Technology Nexus Secured Business Solutions AB, 2019-04-26, document version A
ADM	CA Administrator's Guide Certificate Manager 8.0.0, Technology Nexus Secured Business Solutions AB, 2019-04-26, document version A
REG	Registration Officer's Guide Certificate Manager 8.0.0, Technology Nexus Secured Business Solutions AB, 2019-04-26, document version A
SYS	System Administrator's Guide Certificate Manager 8.0.0, Technology Nexus Secured Business Solutions AB, 2019-04-26, document version A
OCSP	Nexus OCSP Responder Reference Guide 6.0.2, Technology Nexus Secured Business Solutions AB, 2019-10-24
CIMCPP	Certificate Issuing and Management Components Protection Profile, 2011-08-11, document version 1.5
CCpart1	Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1 revision 5, CCMB-2017-04-001
CCpart2	Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1 revision 5, CCMB-2017-04-002
CCpart3	Common Criteria for Information Technology Security Evaluation, Part 3, version 3.1 revision 5, CCMB-2017-04-003

CC	CCpart1 + CCpart2 + CCpart3
CEM	Common Methodology for Information Technology Security Evaluation, version 3.1 revision 5, CCMB-2017-04-004
SP-002	SP-002 Evaluation and Certification, CSEC, 2019-09-24, document version 31.0

Appendix A Scheme Versions

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was received and registered 2017-03-20:

QMS 1.20.2	valid from 2017-02-27
QMS 1.20.3	valid from 2017-04-24
QMS 1.20.4	valid from 2017-05-11
QMS 1.20.5	valid from 2017-06-28
QMS 1.21	valid from 2017-11-15
QMS 1.21.1	valid from 2018-03-09
QMS 1.21.2	valid from 2018-03-09 SIC!
QMS 1.21.3	valid from 2018-05-24
QMS 1.21.4	valid from 2018-09-13
QMS 1.21.5	valid from 2018-11-19
QMS 1.22	valid from 2019-02-01
QMS 1.22.1	valid from 2019-03-08
QMS 1.22.2	valid from 2019-05-02
QMS 1.22.3	valid from 2019-05-20
QMS 1.23	valid from 2019-10-14
QMS 1.23.1	valid from 2020-03-06

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management sys-tem.

The changes between consecutive versions are outlined in "Ändringslista CSEC QMS 1.23.1".

The certifier concluded that, from QMS 1.20.2 to the current QMS 1.23.1, there are no changes with impact on the result of the certification.

A.1 Relevant Scheme Notes

The following Scheme Notes have been considered during the evaluation:

- Scheme Note 15 Demonstration of test coverage
- Scheme Note 18 Highlighted Requirements on the Security Target
- Scheme Note 22 Vulnerability assessment