Swedish Certification Body for IT Security

Certification Report

Entrust Certificate Authority 10.1 and

Entrust Certificate Authority Administration 10.1

Issue: 1.0, 2023-apr-13

Authorisation: Jerry Johansson, Lead certifier , CSEC

Table of Contents

1 Executive Summary

The TOE is:

- Entrust Certificate Authority 10.1 and
- Entrust Certificate Authority Administration 10.1,

which are the two central components of an X.509 certificate/ePassport authoring public key infrastructure system. The TOE is software only.

During the evaluation, the operational environment has provided necessary support for the TOE, as outlined in chapter 8 of this document. Notably, Hardware Security Modules (HSMs) in the operational environment have been used.

The ST does not claim conformance to any PP.

The Security Target contains eight threats, two Organisational Security Policies (OSPs) and seven assumptions, which have been considered during the evaluation.

The evaluation has been performed by Combitech AB in their premises in Växjö and Stockholm, Sweden, with the assistance of EWA Canada Ltd. in their premises in Ottawa, Canada. The evaluation was completed on the 29th of March 2023.

The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, revision 5.

Combitech AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. Combitech AB is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation. EWA-Canada Ltd. operates as a Foreign location for Combitech AB within scope of the Swedish Common Criteria Evaluation and Certification Scheme.

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 evaluation assurance level: EAL 4 + ALC_FLR.2

The technical information in this report is based on the Security Target (ST) provided by the developer and the Final Evaluation Report (FER) produced by Combitech AB.

As specified in the security target of this evaluation, the invocation of certain cryptographic primitives has been included in the TOE, while the implementation of these primitives is located in TOE environment. Therefore the invocation of these cryptographic primitives has been in the scope of this evaluation, while correctness of the implementation of these cryptographic primitives has been excluded. Users of this product are advised to select cryptographic modules for the operational environment where the implementation of the cryptographic primitives has been verified by a trusted third party.

2 Identification

Certification Identification	
Certification ID	CSEC2018008
Name and version of the certified IT product	Entrust Certificate Authority 10.1 and Entrust Certificate Authority Administration 10.1
Security Target Identification	Entrust Certificate Authority 10.1 and Entrust Certificate Authority Administration 10.1 Security Target
EAL	EAL 4 + ALC_FLR.2
Sponsor	Entrust Corporation
Developer	Entrust Corporation
ITSEF	Combitech AB and EWA-Canada Ltd.
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
QMS version	2.3
Scheme Notes Release	20.0
Recognition Scope	CCRA, SOGIS, and EA/MLA
Certification date	2023-04-13

3 Security Policy

- Security Audit
- Identification and Authentication
- Security Management
- Remote Data Entry and Export
- Certificate Management
- Certificate Revocation
- Key Management

3.1 Security Audit

The ECA component of the TOE generates audit records for all security-relevant events. ECA can be configured to select which audit records are generated based on various attributes. For each event, the TOE records the date and time, the type of event, the subject identity, and the outcome of the event. The audit trail is protected from unauthorized modification and will detect changes to the audit records. The TOE also implements timestamps to ensure reliable audit information produced.

3.2 Identification and Authentication

Before any action, each user is identified with a login name or subject identity, and authenticated with either (a) a password or (b) a certificate and the associated private key. Each authorized user is associated with a subject identity, assigned role and specific permissions that determine access to TOE features.

3.3 Security Management

The ECAA component of the TOE provides GUI-based remote administration, separate from the command line interface.

The TOE implements roles that are used to control what operations users are allowed to perform on the TOE. All of the management functions are restricted according to the role assigned to the user or administrator.

The security management functions provided by the TOE include the ability to manage user accounts and roles, administer system configuration, view the audit records, configure the security audit functionality, certificate registration, certificate status change, PKI configuration, Certificate profile management, Revocation profile management, and Certificate Revocation List management.

ECA also enforces an access control policy on the ECA system data associated with the key and certificate functions performed by the ECA.

3.4 Remote Data Entry and Export

The TOE provides the ability to assure the identity of parties exchanging data using digitally signed certificates and revocation lists. This includes generating and verifying evidence of the identity of the originator of information.

The operational environment is configured to provide a TLS tunnel to protect communications between the TOE components (the ECA and ECAA) using the ASH protocol. Communications with the database are over TLS provided by the ODBC driver, where the ODBC driver is part of the operational environment.

The TOE implements CMP to protect the transfer of keys and certificates between its own components and between the TOE and the trusted external entities, such as administrative client applications and end entity client applications. To protect communications from modification and disclosure, the TOE also implements TLS v1.2 between:

- ECA and directory (LDAP over TLS)
- ECAA and directory (LDAP over TLS)
- ECA and XAP clients (XAP, a protocol which transfers information over HTTPS)

3.5 Certificate Management

The TOE generates certificates and establishes proof of possession before providing the certificate to the end user. The TOE is able to implement certificate definitions that comply with the specification provided by an Administrator.

3.6 Certificate Revocation

ECA generates and issues X.509 version 2 Certificate Revocation Lists. ECA can also publish certificate and certificate revocation information to an Online Certificate Status Protocol (OCSP) responder.

3.7 Key Management

The ECA component of the TOE makes use of the Cryptographic Module (CM) to perform the following cryptographic functionality:

- Key generation
- Encryption, decryption, hashing, keyed-hash message authentication, random number generation, signature generation and verification
- Entropy is collected and used to support seeding
- Critical Security Parameters (CSPs) are protected so that they are not directly viewable in plaintext and stored internally.
- CSPs are cleared when no longer in use

The CM also protects all private and secret key material using cryptographic mechanisms. The ECA protects public keys stored in the database against unauthorized modification.

The ECA component of the TOE uses that same CM to manage CSPs and implements deletion procedures to mitigate the possibility of disclosure or modification of CSPs.

4 Assumptions and Clarification of Scope

4.1 Assumptions

The Security Target [ST] makes seven assumptions on the TOE environment:

A.Administrators Review Audit Logs

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

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

Competent administrative users will be assigned to manage the TOE and the security of the information it contains.

A.CPS

All administrative users are familiar with the certificate policy (CP) and certification practices statement (CPS) under which the TOE is operated.

A.Operating System

The operating system has been selected to provide the following functions required by this PKI to counter the perceived threats as identified in this ST: identification and authentication, process isolation and separation, reliable time stamps, file system access controls, enforcement of a TLS tunnel for ASH protocol communications.

A.Tunnel

The operational environment will protect the ASH protocol communications between ECA and ECAA from modification and disclosure. The operational environment will also protect the ODBC communications between ECA and the database from modification and disclosure.

A.Physical Protection

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

4.2 Clarification of Scope

The Security Target contains eight threats, which have been considered during the evaluation:

T.Administrators commit errors or hostile actions

An administrative user 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.

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.

T.Critical system component fails

Failure of one or more system components results in the loss of system critical functionality.

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.

T.Disclosure of private and secret keys

A private or secret key is improperly disclosed. The threat agent is an authorized user or erroneous protocol. An adverse action can be compromise of the security of the PKI and/or relying party systems that rely on PKI objects such as certificates or CRLs.

T.Modification of private/secret keys

A secret/private key is modified. The threat agent is an authorized user or erroneous protocol. An adverse action can be compromise of the security of the PKI and/or relying party systems that rely on PKI objects such as certificates or CRLs.

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.

T.Social engineering

A hacker uses social engineering techniques to gain information about system entry, system use, system design, or system operation.

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

The TSF shall exclusively rely on verified cryptographic primitives to perform all cryptographic operations.

5 Architectural Information

The TOE architecture is described in detail in the [ST] sections 1.4.1 and 1.4.4.

6 Documentation

For proper installation and configuration into the evaluated configuration, the following guidance documents are available:

Entrust Certificate Authority 10.1, Operations Guide, v3.0

Entrust Certificate Authority Administration 10.1, User Guide, v2.0

Entrust Certificate Authority 10.1, Installation Guide, v2.0

Entrust Certificate Authority 10.1 Deployment Guide, v2.0

Entrust Certificate Authority 10.1 Database Configuration Guide, v 3.0

Entrust Certificate Authority 10.1 Directory Configuration Guide, v2.0

Entrust Certificate Authority 10.1 Common Criteria Supplemental Guide, v1.0

Entrust ePassport Solutions Guide 4.10, v3.0

7 IT Product Testing

7.1 Developer Testing

The developer has tested the TOE in 5 test configurations, composed using the following IT products in the operational environment:

ECA operating systems

- Microsoft Windows Server 2019
- Microsoft Windows Server 2022
- RedHat Enterprise Linux 7.9
- RedHat Enterprise Linux 8.5

ECAA operating systems

- Microsoft Windows Server 2019
- Microsoft Windows Server 2022
- Microsoft Windows 10, 64 bit
- Microsoft Windows 11, 64 bit

HSMs/Clients

- Entrust nShield Connect XC 12.60.15 with Security World Client 12.81.2)
- Thales Luna K7 Network HSM (firmware 7.3.3) with
  Thales Luna HSM Universal Client 10.4

Databases

- PostgreSQL 14
- EDB Postgres Advanced Server 14
- Oracle 19c
- Microsoft SQL Server 2019

Directories

- Synchronoss Directory Server 8.1.0
- Active Directory Domain Services (Windows Server 2019)
- Active Directory Lightweight Directory Services (Windows Server 2022)

OCSP responder

- Entrust KeyOne Validation Authority 4.0

Smartcard/token

- Thales SafeNet eToken 5110 CC/FIPS with
  Thales SafeNet Authentication Client v10.8 (R6)

Each of the 5 configurations was tested with good coverage/depth of the security functionality. The testing was performed in April-June 2022. All results were as expected.

7.2 Evaluator Testing

The evaluators used a variant of the developer's configurations for the repeated developer testing, the independent testing and for the penetration testing.

The evaluators performed a substantial amount of developer tests, as well as complementary independent tests. The testing was performed in August-September 2022. All results were as expected.

7.3 Penetration Testing

The evaluators used a variant of the developer's configurations for the penetration testing. The evaluators performed a vulnerability scan with Nessus.

The testing was performed in October 2022. All results were as expected.

The vulnerability database search was last performed on the 24th of March 2022.

8 Evaluated Configuration

8.1 Tested configurations of the TOE

The tested configurations of the TOE are:
- Entrust Certificate Authority 10.1 (ECA) and
- Entrust Certificate Authority Administration 10.1 (ECAA)

has been installed with the following license codes:
- Enterprise (X.509)
- CVCA for Foreign DVs (EAC / ePassport)
- CVCA for Domestic DVs (EAC / ePassport)
- DV for Inspection Systems (EAC / ePassport)

and with support from the operational environment by:

ECA operating systems
- Microsoft Windows Server 2019
- Microsoft Windows Server 2022
- RedHat Enterprise Linux 7.9
- RedHat Enterprise Linux 8.5

ECAA operating systems
- Microsoft Windows Server 2019
- Microsoft Windows Server 2022
- Microsoft Windows 10, 64 bit
- Microsoft Windows 11, 64 bit

HSMs/Clients
- Entrust nShield Connect XC (firmware 12.60.15) with Security World Client 12.81.2
- Thales Luna K7 Network HSM (firmware 7.3.3) with Thales Luna HSM Universal Client 10.4

Databases
- PostgreSQL 14
- EDB Postgres Advanced Server 14
- Oracle 19c
- Microsoft SQL Server 2019

Directories
- Synchronoss Directory Server 8.1.0
- Active Directory Domain Services (Windows Server 2019)
- Active Directory Lightweight Directory Services (Windows Server 2022)

OCSP responder
- Entrust KeyOne Validation Authority 4.0

Smartcard/token
- Thales SafeNet eToken 5110 CC/FIPS with Thales SafeNet Authentication Client v10.8 (R6)

8.2 Functionality excluded from the evaluated configuration

The following TOE functionality is excluded and not enabled/utilized in the evaluated configuration:

- Proto-PKIX (SEP) - a proprietary protocol that handles certificate requests from legacy applications
- Autologin
- Database backup, which is only available with the embedded database that is not included in the evaluated configuration
- Cross-certification and subordinate CAs when using an Active Directory Domain Services

Administrative guidance will instruct administrators to not use the following features of the TOE. Use of the following TOE functionality is not permitted in the evaluated configuration and must not be used by administrators:

- CA migration functionality – provides the ability to migrate an existing CA from non-TOE software. This includes importing private keys and revocation lists.
- Move user functionality - allows for end-users to be moved from one TOE CA to a different TOE CA. This includes importing and exporting of private keys.
- Archive user functionality - allows archiving end-users that are not currently being used from the ECA database to an archive file.
- Smart Energy Profile 2 CAs
- Constructs used to store and protect the digital identities and certificates created by ECA (such as Entrust profiles)
- Online cross-certification is excluded from the evaluated configuration. (Note: Offline cross-certification is included in the evaluated configuration.)
- Online subordinate CA creation is excluded from the evaluated configuration. (Note: Offline subordinate CA creation is included in the evaluated configuration.)
- XAP user registration password functionality is excluded from the evaluated configuration. (This functionality allows a 'registration password' to be specified for a user. XAP provides an operation for matching a user-specified password against the known registration password that is stored in the database.)
- Use of an Entrust-supplied embedded PostgreSQL database is excluded from the evaluated configuration.
- Use of the ASH protocol by client systems other than ECAA
- Use of entropy in certificate validity dates
- Ability to view pre-10.0 audits
- Ability to archive audits from the DB
- Ability to repair revocation lists and user reference numbers
- Use of User attribute certificates
- Use of ECAA bulk commands
- Use of Entrust profiles for administrative users (.epf)
    - In the evaluated configuration, administrators must not use ECAA to create Entrust profiles for administrative users or for end users. Instead,

administrators should use ECAA to create all such credentials on a PKCS #11 tokens.

The following TOE functionality is allowed, but does not interfere with the security functionality and was not tested during the CC certification:

- entDerEncoder utility
- High Availability (support for multiple CA nodes, also known as an Entrust CA cluster) and Listener Service
- Use of ECAA with multiple ECAs

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 evaluators 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 Glossary

ASH	Administration Service Handler
CA	Certification Authority
CC	Common Criteria
CEM	Common Methodology for Information Technology Security
CM	Cryptographic Module
CMP	IETF PKIX Certificate Management Protocol
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSCA	Country Signing Certification Authority
CV	Card Verifiable
CR	Change Request
DV	Document Verifier
ECA	Entrust Certificate Authority
ECAA	Entrust Certificate Authority Administration
FER	Final Evaluation Report
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
LDAP	Lightweight Directory Access Protocol
NIST	National Institute of Standards and Technology
OR	Observation Reports
PP	Protection Profile
SAR	Security Assurance Requirements
SER	Single Evaluation Report
SFR	Security Functional Requirements
ST	Security Target, document containing security requirements and specifications , used as the basis of a TOE evaluation
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions

12 Bibliography

ST — Entrust Certificate Authority 10.1 and Entrust Certificate Authority Administration 10.1 Security Target, Entrust Corporation, 2023-Jan-25, document version 1.1, FMV ID 18FMV7159-24

OP — Entrust Certificate Authority 10.1, Operations Guide, Entrust Corporation, May 2022, document version 3.0, FMV ID 18FMV7159-17

UG — Entrust Certificate Authority Administration 10.1, User Guide, Entrust Corporation, May 2022, document version 2.0, FMV ID 18FMV7159-17

INST — Entrust Certificate Authority 10.1, Installation Guide, Entrust Corporation, May 2022, document version 2.0, FMV ID 18FMV7159-17

DEP — Entrust Certificate Authority 10.1 Deployment Guide, Entrust Corporation, May 2022, document version 2.0, FMV ID 18FMV7159-21

DB — Entrust Certificate Authority 10.1 Database Configuration Guide, Entrust Corporation, May 2022, document version 3.0, FMV ID 18FMV7159-21

DIR — Entrust Certificate Authority 10.1 Directory Configuration Guide, Entrust Corporation, May 2022, document version 2.0, FMV ID 18FMV7159-21

CCSup — Entrust Certificate Authority 10.1 Common Criteria Supplemental Guide, Entrust Corporation, 2022-Nov-02, document version 1.0, FMV ID 18FMV7159-17

ePASS — Entrust ePassport Solutions Guide 4.10, Entrust Corporation, May 2022, document version 3.0, FMV ID 18FMV7159-17

CCpart1 — Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1, revision 5, April 2017, CCMB-2017-04-001

CCpart2 — Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1, revision 5, April 2017, CCMB-2017-04-002

CCpart3	Common Criteria for Information Technology Security Evaluation, Part 3, version 3.1, revision 5, April 2017, CCMB-2017-04-003
CC	CCpart1 + CCPart2 + CCPart3
CEM	Common Methodology for Information Technology Security Evaluation, version 3.1, revision 5, April 2017, CCMB-2017-04-004
EP-002	EP-002 Evaluation and Certification, CSEC, 2021-10-26, document version 34.0

Appendix A Scheme Versions

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme have been used.

A.1 Quality Management System

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was registered 2018-10-09:

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
QMS 1.23.2	valid from 2020-05-11
QMS 1.24	valid from 2020-11-19
QMS 1.24.1	valid from 2020-12-03
QMS 1.25	valid from 2021-06-17
QMS 2.0	valid from 2021-11-24
QMS 2.1	valid from 2022-01-18
QMS 2.1.1	valid from 2022-03-09
QMS 2.2	valid from 2022-06-27
QMS 2.3	valid from 2023-01-26

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 system. The changes between consecutive versions are outlined in “Ändringslista CSEC QMS 2.3”.

The certifier concluded that, from QMS 1.21.4 to the current QMS 2.3, there are no changes with impact on the result of the certification.

A.2 Applicable Scheme Notes

SN-15 Testing

SN-18 Highlighted Requirements on the Security Target

SN-22 Vulnerability assessment

SN-25 Use of CAVP-tests in CC evaluations

SN-27 ST requirements at the time of application for certification

SN-28 Updated procedures for application, evaluation and certification

SN-31 New procedures for site visit oversight and testing oversight