CSEC

Swedish Certification Body for IT Security

Certification Report - Dencrypt Server System 5.0

Issue: 1.0, 2021-Jul-09

Authorisation: Ulf Noring, Lead Certifier , CSEC

SWEDAC · ACKREDITERING ·
Accred. no. 1917
Certification of
Products
ISO/IEC 17065

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is Dencrypt Server System version 5.0, build 5.0.0.122. The Dencrypt Server System consists of the following software components:

- Dencrypt Certificate Manager (DCM)
- Dencrypt Provisioning Server (DPS)
- Dencrypt Control Center (DCC)
- Dencrypt Database (DDB)
- Dencrypt Communication Server (DCS)
- Dencrypt Server Bridge (DSB)
- Debian Linux 8
- Apache, PHP, Laravel, MySQL and their dependencies

The TOE is the server part of the Dencrypt Communication Solution, a VoIP and messaging solution for iPhone clients.

The main security features of the TOE are:

- Administration:
  - Identification and authentication of administrators
  - Administrative roles and privileges associated with those role
  - Management functions, for managing the DCA clients and TOE itself
  - Auditing and audit review
- Secure provisioning of clients
- Trusted channel to clients
- Trusted channel to service access
- Provisioning to end users of new configurations and central managed phone books
- Key generation and certificate issuing and a certificate authority
- Secure bridge to another Dencrypt Server System
- Encryption of push notifications
- TCP tunnelling for voice or video communication

The TOE is delivered as an ISO image containing the TOE (Dencrypt developed server system components, the Debian Linux operating system, the Apache server, PHP, the Laravel framework, the MySQL database, and the dependencies for these software components.) The delivery, installation and initial configuration is performed by Dencrypt employees or by personnel that have been trained to perform delivery and installation on behalf of Dencrypt. Guidance is provided in two manuals:

- Operational User Guide v. 5.0
- Preparative Guide v. 5.0

The TOE claims conformance to the EAL2 package of security assurance requirements, augmented with ALC_FLR.2. It does not claim conformance to any Protection Profile (PP).

Five threats, seven OSPs and eleven assumptions are specified in chapter three in the security target [ST].

The evaluation has been performed by atsec information security AB in their premises in Danderyd, Sweden. The evaluation was completed on 2021-06-22. The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version. 3.1 release 5.

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 also accredited by the Swedish accreditation body according to ISO/IEC 17025 for Common Criteria.

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 the Common Methodology for evaluation assurance level EAL 2 augmented by ALC_FLR.2. The technical information in this report is based on the Security Target [ST] and the Final Evaluation Report (FER) produced by atsec information security AB.

The certification results only apply to the version of the product indicated in the certificate, and on the condition that all the stipulations in the Security Target are met. This certificate is not an endorsement of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification	
Certification ID	CSEC2020003
Name and version of the certified IT product	Dencrypt Server System 5.0, build 5.0.0.122
Security Target Identification	Security Target for Dencrypt Server System version 5.0, 2021-06-11, version 0.17
EAL	EAL 2 + ALC_FLR.2
Sponsor	Dencrypt A/S
Developer	Dencrypt A/S
ITSEF	atsec information security AB
Common Criteria version	3.1 revision 5
CEM version	3.1 revision 5
QMS version	1.25
Scheme Notes Release	18.0
Recognition Scope	CCRA, SOGIS, EA/MLA
Certification date	2021-07-09

3 Security Policy

The TOE has the following security functionality:

- Identification & authentication, administrative roles and access control
- Audit generation and protection
- Management functions
- Secure provisioning of clients
- Update of configuration
- Secure communication channel (TLS)
- Encrypted push notifications
- Service access channel
- Key generation and certificate management
- Key distribution to support client data-at-rest security

For detailed information on the security functionality, see chapter 7 of the [ST].

3.1 I&A, administrative roles and access control

Administrators can access the TOE using a web interface. An HTTPS connection is established from the web browser to the web server of the TOE. Administrators have to identify and authenticate themselves using passwords before administrative access is given.

Each administrator will be assigned a role, either User Admin, Company Admin, System Admin or Service Access. Each role is associated with certain privileges and the roles are hierarchical. This means Company Admin has more privileges than User Admin, System Admin has more privileges than User Admin and Company Admin, and so on. The Service Access role has highest privilege and is intended for system maintenance and updates.

The MySQL database in the DCC holds permission tables that explicitly specify which administrators can access which companies. For every request from the administrator's browser, the TOE checks the role of the administrator and performs a permission evaluation before serving the request.

3.2 Audit generation and protection

The DCC generates a log event for all events that change the state of the server system components. In addition to server state change, the log also audits TOE login attempts (both successful and unsuccessful) and error messages from HTTPS requests to server system components. This log is stored in the MySQL database with the setting that no queries can delete or modify entries in that database table. To ensure that audit is always active, there is a log cycle, where logs are overwritten after a specified period of time. For each audit event, the log records the date and time of the event, type of event, subject identity (if applicable), outcome (success or failure) of the event and additional information specific to the event type.

3.3 Management

The management functions available to the administrator depend on the role assigned. The TOE provides the following management functions:

- Edit users, groups, departments and emergency contacts
- Visualization of statistics
- Browser Verification
- Company Administration
- Administrator Roles & Permissions
- View Log
- Servers, Certificates & Systems (Read)
- Servers, Certificates & Systems (Modify)
- Dencrypt Server Bridge management

3.4 Secure provisioning of clients

Provisioning starts by the administrator adding the user to the TOE. This will trigger the creation of an invitation link which points to the web server of the Dencrypt Provisioning Server (DPS). The link can be encoded into a QR code which a user can scan into the client using the iPhone native camera QR scan functionality. The invitation link contains a random string of 30 characters and must be provided to the user in a secure way, i.e. the link is not disclosed during transmission to anyone else than the intended user. When accessing the link a TLS connection with server authentication is established to protect provisioning data against disclosure and modification. The link is available for a limited time and once accessed the link and the provisioning data will be removed from the DPS.

3.5 Update of configuration

The TOE updates the client with new phone books whenever there is a change of users or groups in the Dencrypt Database (DDB). If the configuration of the SIP server in the TOE has changed, the clients will also be updated with new settings for the client. This is achieved by the client polling the TOE for updates.

3.6 Secure communication channel (TLS)

The TOE does not initiate any outside connection with the client, but it can accept and establish a secure channel coming from the client or from the web browser of the administrator. The TOE can initiate and accept connections via the Dencrypt Server Bridge to a different instance of the TOE. The following secure channels are established:

● Secure SIP connection between client and the SIP server on the Dencrypt Communication Server (DCS), which is a mutually authenticated TLS connection

● Secure HTTPS connection between client and web server on the DCS, which is a mutually authenticated TLS connection

● TLS tunnel channel between client and web server on the DCS, which provides tunnelling of voice or video communication over TCP and TLS 1.2

● Secure TLS connection between the TOE and another trusted

Instance of the TOE, to enable sharing of phonebook data and forwarding of calls

- Secure HTTPS connection between client and web server on the Dencrypt Provisioning Server, which is a TLS connection with server side authentication only
- Secure HTTPS connection between web browser of the administrator and the TOE, which is a TLS connection with server side authentication only.

For the Dencrypt Server Bridge, a TLS connection can be established to a separate TOE instance to enable calls between different systems. Initially, this connection is used to exchange the metadata and phonebook data to make the calls. SIP call initialisation and messages to users belong to a different domain are forwarded by the TOE DCS to the DCS on the other system. In this scenario the DCS can also act as a TLS client. In addition to providing the secure channel it also verifies the identity of the remote system via certificate validation.

3.7 Encrypted push notifications

The TOE supports importing an encryption key from the client during client provisioning. The key is used for encrypting push notifications to the client, as the push notifications are sent via a third party vendor and not through a direct TLS channel between the client and the TOE.

3.8 Service access channel

The TOE supports SSH connections for remote service access.

3.9 Key generation and certificate management

As part of the installation of the Dencrypt Server System, the Dencrypt Certificate Manager (DMC) generates a 4096-bit RSA key pair and obtains a certificate signed by the root CA. This certificate and the root certificate are installed on Key generation and certificate management the DCM. The DCM is thus made ready to issue certificates to both clients and system servers. client users can access the functionality of the DCM via the DCS or DPS. When a new client user is created and accesses the provisioning link, the client will generate a local 3072-bit RSA key pair and submit a

Certificate Signing Request (CSR) to the DCM via the DPS. The DCM will then sign the certificate with its own RSA private key if the supplied invite ID is valid and distribute the client certificate and provisioning data to the DCA.

For server certificates, each server generates by itself a 4096-bit RSA key pair, creates a CSR and sends it to the DCM. The DCM signs and returns the certificate to the server. Administrators in Service Access role can renew the certificates for the DPS, DCM, DCS and DCC.

3.10 Key distribution to support client data-at-rest security

The TOE provides support for data-at-rest functionality of the client by storing and providing an encrypted AES key to the client. The client generates the key to encrypt its stored files. As a measure to protect its data-at-rest in the event of compromise of its underlying hardware, it then encrypts this key and submits it to the TOE. Only the Key Encryption Key is stored locally by the client, ensuring that its storage can only be decrypted after a valid connection and authentication by the TOE. The TOE must as such import, store and distribute this key to the client.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The Security Target [ST] makes four assumptions on the usage of the TOE:

A.NOEVIL

It is assumed that administrators are given privileges they are authorized for, and that they are competent, non-hostile and follow all their guidance; however, they are capable of error.

A.REVIEW

It is assumed that audit trails are regularly analysed for misuse and security incidents.

A.LINK

It is assumed the link, possibly encoded as a QR code, used for provisioning is provided to the correct DCA user and not being disclosed to anyone else.

A.USER

It is assumed that the DCA users are trustworthy and trained to perform their actions in accordance with their instructions and security policies.

4.2 Environmental Assumptions

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

A.NETWORK

It is assumed that the underlying hardware of the TOE and local network is dedicated to the TOE usage and function.

A.PHYSICAL

The TOE is physically protected, i.e. no unauthorised persons have physical access to the TOE and its underlying system. This includes the administrators that only can access the TOE via the local network or through a trusted VPN connection.

A.TIME

It is assumed that the IT environment will provide a reliable time source to the TOE and the TOE environment.

A.WORKSTATION

It is assumed that administrators are performing administration from computers that are well-configured, located in a secure environment and are not exposed to other users or potential attackers.

A.TRUSTANCHOR

It is assumed that a trust anchor is provided and will be used for TLS connections by the DCAs, administrator browsers and other DSS for validation of TOE certificates when connecting to the TOE.

A.FIREWALL

It is assumed that the IT environment provides a firewall or other suitable means to protect the TOE from untrusted networks.

A.CROSS-SYSTEM

It is assumed that separate DSS which the TOE connects to via the DSB to enable cross-system functionality are trusted and operated in a secure manner.

4.3 Clarification of Scope

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

T.COMMUNICATION

An external attacker reads or manipulates information transmitted between the TOE and components that are outside of the trusted network. This affects both user and TSF data.

T.MASQUERADE

An external attacker gain read or write access to information or resources that are held by the TOE including user data, phone books, audit information or any other TSF data.

T.UNAUTH

An administrator may by accident access data or use management functions for which they have not been authorised to, to read, modify or destroy security critical TSF data or tamper with the TSFs.

T.UNDETECTED

An external attacker may attempt to compromise the assets without being detected. This threat includes a threat agent causing audit records to be lost, deleted or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attacker's actions.

T.BRIDGE

An external attacker could intercept or manipulate user and TSF data sent between two DSS via the DSB.

The Security Target contains seven Organisational Security Policies (OSPs) which have been considered during the evaluation:

OSP.MANAGE

The TOE shall provide the authorized administrators with the means to manage the TSFs and the DCAs associated with the TOE installation.

OSP.SERVICE

The TOE shall provide the authorized secure service access to manage the TSFs and the TOE installation.

OSP.ACCOUNT

Administrators shall be accountable for the actions they conduct by generating and maintaining sufficient audit records for the actions.

OSP.PROVISIONING

The TOE must provide a secure provisioning process that can be used for any remote users without access to the secure local network.

OSP.CA

The TOE must be able to generate its own private-public keys and generate its own certificates as well as sign certificates for DCAs.

OSP.CLIENTKEY

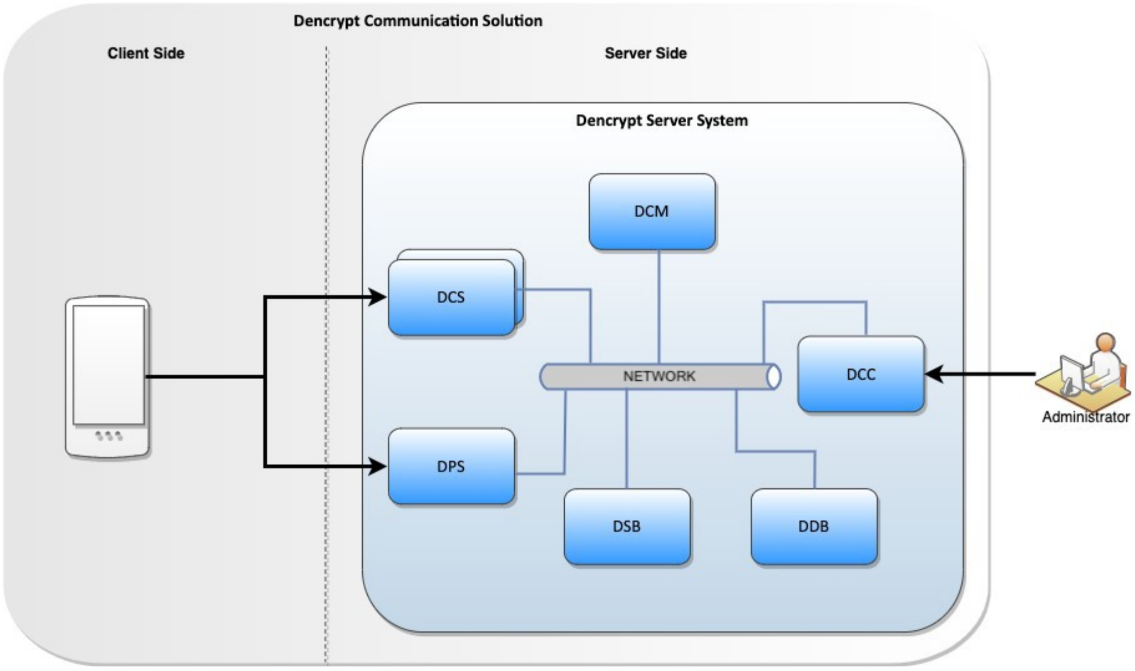
The TOE must be able to distribute previously encrypted keys to authenticated clients on request, to support data-at-rest protection for the DCA.

OSP.TUNNEL

The TOE must provide a tunnelling service to enable voice or video communication to the DCA over TCP by tunnelling the connection over TLS 1.2.

5 Architectural Information

The TOE consists of six parts, as can be seen in the below figure:



The parts are:

- Dencrypt Communication Server

The Dencrypt Communication Server (DCS) provides the connections and communication services to the client:

  - SIP Server – necessary for the clients to establish voice or video communication between two or more clients. Also provides routing for messaging.
  - Lime server – provides the key-exchange functionality to initiate secure message communication.
  - Tunnel server - provides a server to tunnel voice or video communication over TCP.

- Dencrypt Certificate Manager

  Dencrypt Certificate Manager (DCM) is the central point for TLS certificates in the system. Once provisioning has taken place, all connections between the DCA and DSS use mutually authenticated TLS connections. The required TLS certificates are issued by the DCM via the following procedure: The client or server generates the private/public key pair and creates a CSR. The CSR is sent to the DCM which signs the CSR if permitted. The DCM provides the certificate back to client/server for employment. All communication between the DCM and the DCA take place via the DCS, except during provisioning where it takes place via the DPS.

- Dencrypt Control Center

  The user management is performed using the Dencrypt Control Center (DCC). The user management means creating/deleting/revoking users and groups, as well as adding and removing users from these groups. The DCC offers a web interface that is accessible using a web browser from the administrator's local machine.

- Dencrypt Provisioning Server

  The Dencrypt Provisioning Server (DPS) is used to initialise clients with user credentials, DCS URL and respond to the Certificate Signing Request (CSR) sent from the client to set up its certificate. During provisioning, the client is provided with a HTTPS web link for the initialisation. The link can also be encoded into a QR code which the app can scan. The link is provided in a secure way as part of the TOE
- Dencrypt Server Bridge

  The Dencrypt Server Bridge (DSB) introduces functionality to make Dencrypt Calls between users on two different DSS. It enables Secure Phonebook synchronization between systems and routing of SIP or messaging data between systems. The connection between two DSS are protected by a TLS channel. The DSB ensure that this connection is authenticated.
- Dencrypt Database
  The Dencrypt Database (DDB) provides the database services for the DCS. It keeps the user data and most meta data e.g. call statistics.

6 Documentation

The following documentation comprise the TOE guidance:

PREGUIDE	Preparative guide & hosting requirements Dencrypt Server System 5.0
OPGUIDE	Operational User Guide Dencrypt Server System 5.0

7 IT Product Testing

7.1 Developer Testing

The developer uses both automated and manual tests. In total 198 tests were executed to test the TOE and most of them were automated. All TSF has been tested. The developer has provided the results of all test cases that were performed and the source code of the automated tests. All tests were successful.

7.2 Evaluator Testing

The evaluators observed when the developer ran all automated developer tests. The evaluator performed a subset of developer manual tests. Totally 186 developer tests were executed. The evaluator also examined the source code of a sample of automated developer tests to verify that they test what they claim. The evaluator further performed extra audit and certificate revocation tests created by the evaluator. All security functionality defined in the ST has been tested. The subset of developer tests re-run by the evaluator went successfully. All evaluator tests were also performed successfully.

7.3 Penetration Testing

The evaluator performed TCP and UDP port scans of the TOE interfaces from the Internet to detect any potential attack surfaces. The evaluator also performed tests on provisioning and TLS. None of the performed penetration tests revealed any applicable vulnerability in the TOE.

8 Evaluated Configuration

The IT environment must provide the following:

- Mobile devices (iPhones with iOS) where the Dencrypt Connex App is installed.
- The virtual or physical amd64 or x86_64 server systems to host and run the TOE components.
- Mail server to send new client user invitations.
- Push server used for sending notifications to clients. For this evaluation of the client on iOS, Apple Push Notification (APN) is used.
- NTP Server to provide correct time to the TOE components.
- An administrative client and browser for the TOE administrator to manage the TOE.
- A firewall or other suitable means to protect the TOE from untrusted networks.
- Physical protection for the underlying hardware of the TOE
- A physically protected local network dedicated to TOE usage and functions
- A trust anchor that will be used for TLS connections by clients, administrator browsers and other DSS for validation of TOE certificates when connecting to the TOE.
- A DNS server to serve DNS records from pertaining to the TOE

[PREGUIDE] can be downloaded from Dencrypt's website and contains an extensive set of detailed instructions for making sure the IT environment is ready for the TOE. It is highly recommended to consult [PREGUIDE] to make sure the IT environment fulfils the TOE IT environment requirements before purchasing the TOE.

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 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 assurance classes and components are summarised in the following table:

Assurance Class Name / Assurance Family Name	Short name (including component identifier for assurance families)	Verdict
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
Derived security requirements	ASE_REQ.2	PASS
TOE summary specification	ASE_TSS.1	PASS
Life-cycle support	ALC	PASS
Use of a CM system	ALC_CMC.2	PASS
Parts of the TOE CM Coverage	ALC_CMS.2	PASS
Delivery procedures	ALC_DEL.1	PASS
Flaw reporting procedures	ALC_FLR.2	PASS
Development	ADV	PASS
Security architecture description	ADV_ARC.1	PASS
Security-enforcing functional specification	ADV_FSP.2	PASS
Basic design	ADV_TDS.1	PASS
Guidance documents	AGD	PASS
Operational user guidance	AGD_OPE.1	PASS
Preparative procedures	AGD_PRE.1	PASS
Tests	ATE	PASS
Evidence of coverage	ATE_COV.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing - sample	ATE_IND.2	PASS
Vulnerability Assessment	AVA	PASS
Vulnerability analysis	AVA_VAN.2	PASS

10 Evaluator Comments and Recommendations

None.

11 Glossary

CEM	Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within a evaluation and certification scheme
ST	Security Target, document containing security requirements and specifications , used as the basis of a TOE evaluation
TOE	Target of Evaluation
DSS	Dencrypt Server System
DCM	Dencrypt Certificate Manager
DPS	Dencrypt Provisioning Server
DCA	Dencrypt Connex Application
DCC	Dencrypt Control Center
DDB	Dencrypt Database
DCS	Dencrypt Communications Server
DSB	Dencrypt Server Bridge

12 Bibliography

12.1 General

CC Combination of CCp1, CCp2, CCp3, and CEM (see below)

CCp1 Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1, revision 5, April 2017, CCMB-2017-04-001

CCp2 Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1, revision 5, April 2017, CCMB-2017-04-002

CCp3 Common Criteria for Information Technology Security Evaluation, Part 3:, version 3.1, revision 5, April 2017, CCMB-2017-04-003

CEM Common Methodology for Information Technology Security Evaluation, version 3.1, revision 5, April 2017, CCMB-2017-04-004

ST Security Target for Dencrypt Server System version 5.0, Dencrypt A/S, 2021-06-22, document version 0.17

SP-002 SP-002 Evaluation and Certification, CSEC, 2020-11-30, document version 32.0

SP-188 SP-188 Scheme Crypto Policy, CSEC, 2020-11-03, document version 10.0

12.2 Documentation

PREGUIDE Preparative guide & hosting requirements Dencrypt Server System 5.0, Dencrypt A/S, 2020-12-15, document version 1.4

OPGUIDE Operational User Guide Dencrypt Server System 5.0, Dencrypt A/S, 2020-12-15, document version 1.1

Appendix A Scheme Versions

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

A.1 Scheme/Quality Management System

Version	Introduced	Impact of changes
1.25	2021-06-17	None
1.24	2020-11-19	None
1.23.2	2020-05-11	None
1.23.1	Application	Original version

A.2 Scheme Notes

Scheme Note	Version	Title	Applicability
SN-15	3.0	Demonstration of test coverage	Clarify demonstration of test coverage at EAL3.
SN-18	3.0	Highlighted Requirements on the Security Target	Clarifications on the content of the ST.
SN-22	3.0	Vulnerability Assessment	Vulnerability assessment needs to be redone if 30 days or more has passed between AVA and the final version of the final evaluation report.
SN-28	1.0	Updated procedures application, evaluation and certification	Evaluator reports should be received in two batches.