Swedish Certification Body for IT Security

Certification Report - Dencrypt Server System 2.0

Issue: 1.0, 2017-nov-20

Authorisation: Imre Juhász, Lead Certifier , CSEC

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is the Dencrypt Server System version 2.0. The TOE is software only and consists of a Voice over Internet Protocol server and management components that are part of the Dencrypt Communication Solution. The Dencrypt Server System provides secure provisioning, management and secure communication establishment.

The TOE consists of the following components:

- Dencrypt Certificate Manager (DCM), version 1.0.90
- Dencrypt Provisioning Server (DPS), version 1.0.163
- Dencrypt Control Center (DCC), version 3.0.69
- Dencrypt Database (DDB), version 1.0.59
- Dencrypt Communication Server (DCS), version 1.0.434

The TOE is delivered as an ISO image. Dencrypt is responsible for installation and therefore needs access to the customer's IT environment either physically or by a VPN connection. In the VPN case Dencrypt will first provide the customer with an installation USB containing the ISO image. The TOE user can verify the TOE software version by using the web interface to the Dencrypt Control Center.

The TOE is dependent on several 3rd-party components in order to provide the security functionalities. The 3rd-party components consist of Debian Linux operating system, Apache server, PHP, Laravel framework and MySQL database.

There are ten assumptions and five organisational security policies made at the ST regarding the secure usage and environment of the TOE. The TOE relies on these being met in order to be able to counter the four threats in the ST. The assumptions, organisational security policies and the threats are described in chapter 4 Assumptions and Clarification of Scope.

The evaluation has been performed by atsec information system AB at their premises in Danderyd, Sweden. The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 4, and the Common Methodology for IT security Evaluation, version 3.1, release 4. The evaluation was performed at the evaluation assurance level EAL2, augmented by ALC_FLR.2 Flaw reporting procedures.

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 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 evaluation assurance level:

EAL 2 + ALC_FLR.2.

The evaluation was completed on 2017-10-22. The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version 3.1 release 4.

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	CSEC2016012
Name and version of the certified IT product	Dencrypt Server System version 2.0
Security Target Identification	Security Target for Dencrypt Server System version 2.0, version 1.1
EAL	EAL 2+ augmented with ALC_FLR.2
Sponsor	Dencrypt A/S
Developer	Dencrypt A/S
ITSEF	atsec information security AB
Common Criteria version	3.1 release 4
CEM version	3.1 release 4
QMS version	1.20.5
Recognition Scope	CCRA, SOGIS, EA/MLA
Certification date	2017-11-21

3 Security Policy

The TOE consists of five security functions. Below is a short description of each of them. For more information, see Security Target [ST]:

- Audit generation and protection
- I&A, administrative roles and access control
- Management functions
- Update of configuration
- Secure communication channel (TLS)
- Sevice access channel
- Key generation and certificate management

3.1 Audit generation and protection

The Dencrypt Control Center generates a log event for all events that change the state of the server system components, login attempts and error messages from HTTPS requests to server system components. The logs are stored in the database with the setting that no queries can delete or modify entries in that database table. The logs are overwritten after a specified period of time.

3.2 I&A, administrative roles and access control

Administrators can access the TOE web interface through a HTTPS connection. Administrators have to identify and authenticate themselves using passwords before access is given. The defined administrator roles are User Admin, Company Admin, System Admin and Service Access. Each role is associated with certain privileges and the roles are hierarchical.

3.3 Management functions

The management functions available to the administrator depend on the role assigned. The TOE provides the several management functions, e.g. edit profile, user administration, administrator roles & permissions, view log, system management, etc.

3.4 Update of configuration

The TOE updates Dencrypt Talk clients with new phone books whenever there is a change of users or groups in the Dencrypt Database. If the configuration of the Session Initiated Protocol (SIP) server in the Dencrypt Communication Server has changed, the Update of configuration clients will also be updated with new settings for the Dencrypt Talk app. This is achieved by using a subscription based notification mechanism.

3.5 Secure communication channel (TLS)

The TOE does not initiate any outside connection, but it can accept and establish a secure channel coming from either the Dencrypt Talk client or the web browser of the administrator. The following secure channels are established:

- Secure SIP connection
- Mutually authenticated secure HTTPS connections
- Server side authenticated secure HTTPS connections

When Dencrypt Communication Server or Dencrypt Certificate Manager receives a TLS connection request from a client, it fetches the latest certification revocation list from the Dencrypt Database and uses it to check the validity of the client certificate.

3.6 Sevice access channel

OpenSSH (SSH v2) provides secure service access to the command line interface of the TOE.

3.7 Key generation and certificate management

The Dencrypt Certificate Manager 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 the Dencrypt Certificate Manager. When a new Dencrypt Talk user is created the Dencrypt Control Center requests a temporary certificate from the Dencrypt Certificate Manager. This temporary certificate is used together with other provisioning data, when provisioning a new Dencrypt Talk client.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The Security Target makes ten assumptions on the operational environment of the TOE.

A.NOEVIL: It is assumed that administrators 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.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.LINK It is assumed the link used for provisioning is provided to the correct Dencrypt Talk user and not being disclosed to anyone else.

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

4.2 Environmental Assumptions

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

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

A.TRUSTANCHOR: It is assumed that a trust anchor is provided and will be used for TLS connections by the Dencrypt Talk clients and administrator browsers for validation of TOE certificates when connecting to the TOE.

4.3 Clarification of Scope

The Security Target contains four 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.

The Security Target contains five 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 Dencrypt Talk applications associated with the TOE installation.

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

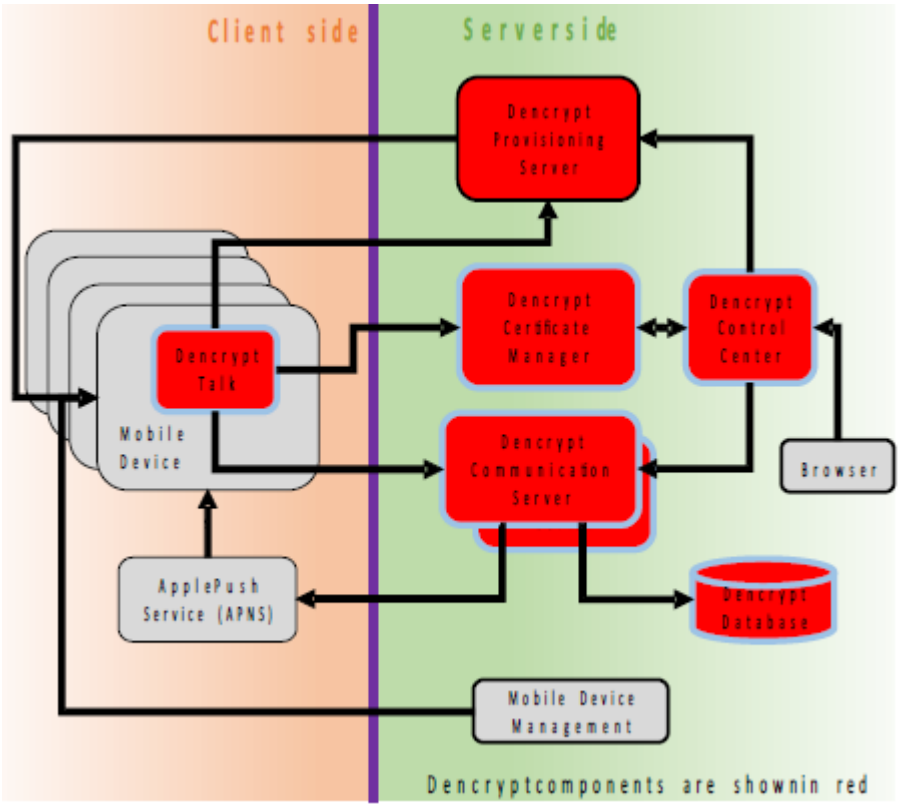
OSP.ACCOUNT: Administrators shall be accountable for the actions they conduct by generating and maintaining sufficient audit records for the actions.

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 Dencrypt Talk clients.

5 Architectural Information

The TOE is part of the Dencrypt Communication solution and consists of the server system version 2.0 components. The TOE consists of server components that are necessary to support provisioning, management and call establishment for end-to-end voice encryption and encrypted live chat between iPhones. The whole Dencrypt Communication Solution is shown in the picture below. The components that are marked red are those developed by Dencrypt. On the Server side, in addition to Dencrypt developed components, certain 3rd party components are required to provide security functionalities. These 3rd party components include Debian Linux operating system, Apache server, PHP, Laravel framework and MySQL database.



Dencrypt Provisioning Server

The Dencrypt Provisioning Server is used to initialise clients with user credentials. The clients are provided with a HTTPS web link for the initialisation. The link is provided in a secure way as part of the TOE environment. The HTTPS web link points to the web server of the DPS that is only reachable within a safe environment.

Dencrypt Communication Server

The Dencrypt Communication Server provides the SIP Services that are necessary for the clients to establish voice and live chat communication between two or more clients.

Dencrypt Database

The Dencrypt Database provides the database services for the DCS. It keeps the user data and most meta-data e.g. call statistics.

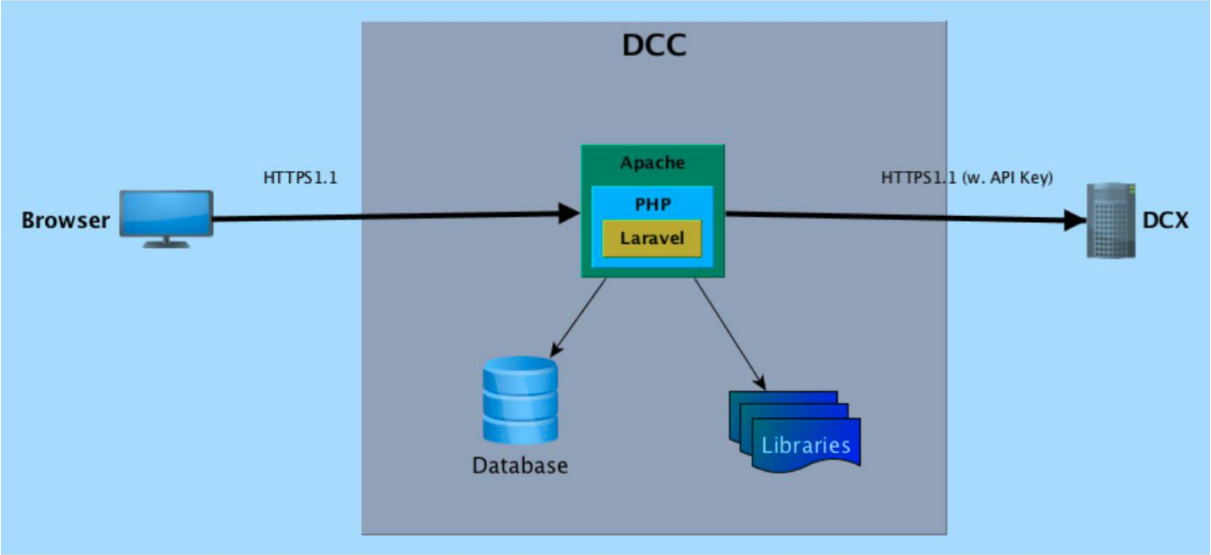
Dencrypt Control Center

The user management is performed using the Dencrypt Control Center. This includes creating/deleting 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 Certificate Manager

Dencrypt Certificate Manager is the central point for TLS certificates in the system. Once provisioning has taken place, all connections between Dencrypt Talk and Dencrypt Server System use mutually authenticated TLS connections.

All the backend servers are installed with a turnkey Linux distribution which includes, among other things, Debian Linux operating system, Apache server and PHP. Debian Linux, Apache and PHP are part of the TOE. The DCC has two additional components that are also part of the TOE: the Laravel framework and the MySQL database.



6 Documentation

The physical scope of the TOE also includes the following guidance documentation:

- Operational User Guide, Dencrypt Server System v. 2.0
- Maintenance Guide, Dencrypt Server System v. 2.0
- Preparative Guide & Hosting Requirements, Dencrypt Server System v. 2.0
- Acceptance Test & Handover, Dencrypt Communication Solution, Dencrypt Server System v. 2.0, Dencrypt Talk v. 4.2

7 IT Product Testing

7.1 Developer Testing

The following 3rd party components are included in the TOE during testing:

- Turnkey Linux LAMP Stack v14.1 (Debian 8.2 Jessie)
- Appache 2.4.10
- PHP 5.6.30
- MySQL 5.5.54-0

Test Effort

The developer conducted extensive testing using both automated and manual tests. Five automated test systems are used for testing the TOE, the automated tests are written in PHP and Python. Each test, both automated and manual test, contains a description, and for manual tests are also steps described which contains the expected outcome of the test.

Test approach

The developer demonstrated that all test cases ran successfully. The developer tests cover all SFRs, interfaces, and subsystems. The developer used in total 181 tests to test the complete Dencrypt Communication Solution (Dencrypt Talk and Dencrypt Server system). The tests include both positive and negative tests.

7.2 Evaluator Testing

The developer provided the evaluator with the results of all test cases. The testing environment consisted of Dencrypt Server System (TOE), iPhones running Dencrypt Talk, and TLS server configured with different TLS settings (used for negative testing).

Test effort

The evaluators executed a large subset of the developer tests, both automated and manual tests. The evaluator also examined the source code of the automated developer test in order to verify the test claims. The evaluator further created and performed extra SSH tests.

Test approach

The independent testing followed the CEM guidance to test every security function, without striving for exhaustive testing. All automated developer tests were selected by the evaluators to re-run. The tests were selected so that each TSFI, subsystem and SFR was tested. All security functionality defined in the ST has been tested.

7.3 Penetration Testing

The evaluator performed penetration tests revealing no applicable vulnerability in the TOE.

Test effort

Vulnerability testing was performed against the interfaces of the systems included in the TOE. The tests were directed towards the IPv4 TCP and UDP ports of these systems. Also, the provisioning and TLS functionality establishment was examined.

Test approach

The evaluator analyzed the developer design, the implementation representation and guidance documentation in order to identify the attack surface of the TOE. The evaluator also used publicly documented vulnerabilities in CVE database and used general search engines. The evaluator performed TCP and UDP port scans of the TOE interfaces from the internal network to detect any potential attack surfaces. The evaluator also performed tests on provisioning and TLS.

8 Evaluated Configuration

The IT environment must contain the following:

- Multiple mobile devices (iPhone) where the Dencrypt Talk App is installed.
- A standard Mobile Device Management system.
- The hardware and software components (excluding the TOE components) that are delivered as part of the ISO image where the TOE is installed. 3rd party components required to provide security functionalities:
  - Turnkey Linux LAMP Stack v14.1 (Debian 8.2 Jessie)
  - Appache 2.4.10
  - PHP 5.6.30
  - MySQL 5.5.54-0
- An administrative client and browser for the TOE administrator to manage 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 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 assurance classes and components are summarised in the following table:

Assurance Class Name / Assurance Family Name	Short name	Verdict
Security Target Evaluation	ASE	
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	
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 procedure	ALC_FLR.2	Pass
Development	ADV	
Security Architecure description	ADV_ARC.1	Pass
Security-enforcing functional specification	ADV_FSP.2	Pass
Basic design	ADV_TDS.1	Pass
Guidance documents	AGD	
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Tests	ATE	
Evidence of coverage	ATE_COV.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - Sampling	ATE_IND.2	Pass
Vulnerability assessment	AVA	
Vulnerability analysis	AVA_VAN.2	Pass

10 Evaluator Comments and Recommendations

The evaluators have no remaining comments, observations, or recommendations.

11 Glossary

CC	Common Criteria
CEM	Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations
DCC	Dencrypt Control Center
DCS	Dencrypt Communication Server
DCM	Dencrypt Certificate Manager
DDB	Dencrypt Database
DPS	Dencrypt Provisioning Server
EAL	Evaluation Assurance Level
FER	Final Evaluation Report
HTTPS	Hypertext Transfer Protocol Secure
iOS	Apple iPhone Operating System
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within a evaluation and certification scheme
MDM	Mobile Device Management
SIP	Session Initiated Protocol
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

12 Bibliography

[CCp1]	Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1, revision 4, September 2012, CCMB-2012-09-001
[CCp2]	Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1, revision 4, September 2012, CCMB-2012-09-002
[CCp3]	Common Criteria for Information Technology Security Evaluation, Part 3:, version 3.1, revision 4, September 2012, CCMB-2012-09-003
[CEM]	Common Methodology for Information Technology Security Evaluation, version 3.1, revision 4, September 2012, CCMB-2012-09-004
[SP-002]	Evaluation and Certification, SP-002, Issue: 26.0, 2017-06-27, FMV/CSEC
[ST]	ST Security Target for Dencrypt Server System, Dencrypt A/S, document Version 1.1, 2017-10-11
[AcceptTest]	Acceptance Test & Handover Dencrypt Communication Solution Dencrypt Server System v. 2.0 Dencrypt Talk v. 4.2, Dencrypt A/S, 2017-09-21
[DCC-Guide]	Operational User Guide Dencrypt Server System v. 2.0 Version 1.2, Dencrypt A/S, Version 1.2, 2017-09-05
[Maint-Guide]	Maintenance Guide Dencrypt Server System v. 2.0, Dencrypt A/S, Version 1.1, 2017-09-04
[Pre-Guide]	Preparative Guide & Hosting Requirements Dencrypt Server System v. 2.0, Dencrypt A/S, Version 1.5, 2017-10-25

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

<a complete list of QMS versions valid from the registered application date to the certification date, the date it was introduced, and a comment on the impact on the certification. Note that the required information is available in "Ändringslista" for the latest version – e.g. from the S-disk.>

Version	Introduced	Impact of changes
1.20.5	2017-06-26	*None*
1.20.4	2017-05-11	*None*
1.20.3	2017-04-24	*None*
1.20.2	2017-02-27	*None*
1.20.1	2017-01-12	*None*
1.20	2016-10-20	Original version

A.2 Scheme Notes

Scheme Note	Title	Applicability
SN-15	Demonstration of test coverage	ATE
SN-18	Highlighted Requirements on the Security Target	ASE