Swedish Certification Body for IT Security

Certification Report - Dencrypt Talk App

Issue: 1.0, 2017-nov-21

Authorisation: Imre Juhász, Lead Certifier , CSEC

Table of Contents

1 Executive Summary 3

2 Identification 4

3 Security Policy 5
3.1 PROVISIONING – Secure initialisation 5
3.2 SECURE MANAGEMENT 5
3.3 SECURE MESSAGING 5
3.4 CHANNEL – Secure communication channel (TLS) 5

4 Assumptions and Clarification of Scope 6
4.1 Usage Assumptions 6
4.2 Environmental Assumptions 6
4.3 Clarification of Scope 6

5 Architectural Information 8
5.1 Dencrypt Talk subsystems 9

6 Documentation 10

7 IT Product Testing 11
7.1 Developer Testing 11
7.2 Evaluator Testing 11
7.3 Penetration Testing 12

8 Evaluated Configuration 13

9 Results of the Evaluation 14

10 Evaluator Comments and Recommendations 16
10.1 The certifier comments and recommendations 16

11 Glossary 17

12 Bibliography 18

Appendix A Scheme Versions 19
A.1 Scheme/Quality Management System 19
A.2 Scheme Notes 19

1 Executive Summary

The Target of Evaluation (TOE) is the Dencrypt Talk version 4.2.794 for the iPhone. The TOE is a VoIP application for iPhone that offers end-to-end encrypted mobile voice communication and encrypted live chat within well-defined user groups.

The TOE is delivered to the user as an in-house app by the Mobile Device Management system under control of the organization deploying the TOE. The user installs and configures the app by following the instructions given in the user documentation.

The TOE is dependent on the mobile device hardware (iPhone) and iOS software on which the TOE is installed, the Dencrypt Server System and any standard mobile device management system.

There are eight assumptions and six organisational security policies made in 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 three threats in the ST. The assumptions, organisational security policies and the threats are described in chapter 3 Security problem definition.

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 EAL4, 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 4 + ALC_FLR.2.

The evaluation was completed on 2017-10 10. 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

2 Identification

Certification Identification	
Certification ID	CSEC2016008
Name and version of the certified IT product	Dencrypt Talk version 4.2.794 for the iPhone
Security Target Identification	Security Target for Dencrypt Talk, version 1.0
EAL	EAL 4+ 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 four security functions. Below is a short description of each of them. For more information, see Security Target [ST]:

- Provisioning - Secure initialisation
- Secure Management
- Secure Messaging
- Secure Channel

3.1 PROVISIONING – Secure initialisation

The Dencrypt Server System administrator adds the user to the Dencrypt Server System and then provides an invitation link to the user. This link must be provided in a secure way to the user, i.e. the link is not disclosed during transmission to the TOE user, and the link is only valid for a limited time after the link has been provided.

3.2 SECURE MANAGEMENT

When registered to the Dencrypt Server System the client will subscribe for changes of network settings. This allows the TOE to keep its local settings in sync with the server system's settings. The TOE downloads network settings as soon as the checksum of its local settings differs from the settings checksum advertised by the Dencrypt Server System. The same mechanism applies to keep the phone book up-to-date. The TOE user cannot change any phone book entries or make encrypted calls from a dialpad:

The TOE will generate by itself an RSA 3072-bit private-public key pair and send its public key with a certificate signing request to the Dencrypt Server System which signs it and delivers the client certificate.

3.3 SECURE MESSAGING

A secure communication channel between two TOE handsets can be placed through an extended Voice-over-IP system (VoIP) which encrypts the voice data. The core elements of the Session Initiated Protocol (SIP) VoIP system are the SIP clients and the SIP server. The SIP server is the signaling center of the communication system. The SIP transmissions are protected by mutually authenticated TLS. Dencrypt Talk's live chat messages uses SIP messaging as transportation protocol where the chat text is encrypted. Both call's and live chat keys originate from the same encryption keys. Once the call or live chat ends, all the keys are destroyed (overwritten with zeros).

3.4 CHANNEL – Secure communication channel (TLS)

The TOE can establish a secure channel between the TOE and the Dencrypt Server System components. All TLS connections are initiated by the TOE. For TLS 1.2 mutual authentication, the TOE has a 3072-bit RSA key pair while each server component has a 4096-bit RSA key pair. So the TOE shall verify server signature by using the server system's 4096-bit RSA public key.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

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

A.ADMIN: It is assumed that the TOE administrators (i.e. the administrators using the Dencrypt Server System) are trustworthy and trained to perform the actions required by them for the management and maintenance of the Dencrypt Server System.

A.SINGLEUSER: It is assumed that the TOE is under the physical control of a single authorized user.

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

4.2 Environmental Assumptions

A.APPS: It is assumed that only approved, benign applications are running on the handset where the TOE is running.

A.BACKEND: It is assumed that the underlying hardware, firmware (BIOS and device drivers) and software of the server system used by the TOE are working correctly and have no undocumented security critical side effect on the TOE. Furthermore, the server system is operated in a physically secure and well managed environment.

A.HANDSET: It is assumed that the functions in the TOE environment related to memory management, program execution, access control and privilege management provided by the underlying iOS of the handset and the SIM card, work correctly and have no undocumented security critical side effects on the security functions of the TOE.

A.KEYS: It is assumed that random bits provided by the underlying platform are of good quality and have sufficient entropy.

A.PROVISIONING: It is assumed that the operational environment ensures that the web link is not predictable, only active for a limited time and that access to the link is limited to one attempt only. It is also assumed that the operational environment provides the link to clients in a secure way so that the link is not disclosed to any potential attacker. Note: The link might be disclosed for the user's organisation, e.g. the link might be in cleartext on the organisation's local mail server.

4.3 Clarification of Scope

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

T.DATA: An unauthorized user or attacker will gain access to user credentials, TOE settings or phone book entries to which they are not authorized.

T.MASQUERADE: A user within a closed user group is masquerading, pretending to be another user to mislead the receiver that a secure voice call or a secure chat is originating from another user belonging to the phone book of that user group.

T.TRAFFIC: An attacker (including network operators) may gain access (disclosure or modification) to secure voice or chat conversations between users within a closed user group.

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

OSP.CLOSED: The TOE shall ensure that secure calls and secure chats are restricted to parties defined into the phone book held by the TOE.

OSP.FORWARD: The TOE must be able to prevent an unauthorized user that obtains a handset to decrypt previously transmitted traffic (voice or chat) that has been encrypted using the obtained handset.

OSP.PRIVATEKEY: The TOE must be able to generate its own private-public key pairs.

OSP.MANAGE: The TOE shall allow secure provisioning and remote update of certificates and phone book.

OSP.PHONEBOOK: The TOE must ensure that the phone book cannot be changed locally.

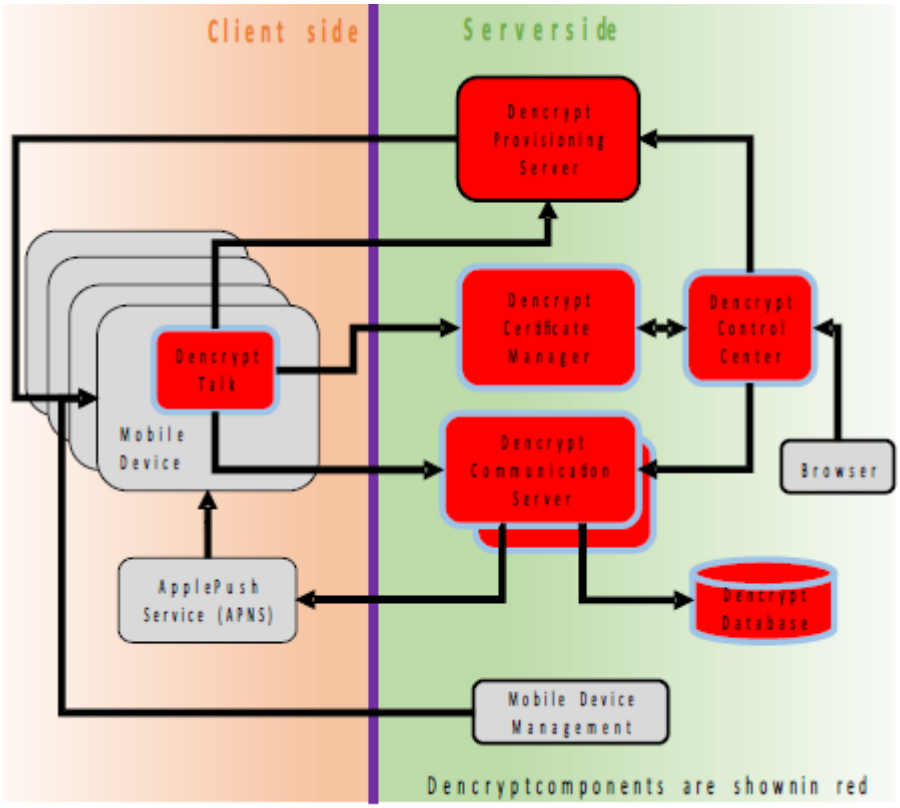
OSP.UPTODATE: The TOE must ensure that the phone book held by the TOE is up-to-date.

5 Architectural Information

The Dencrypt Talk is a component in the Dencrypt Communication Solution. The TOE is an application, running on an iPhone. It is a VoIP client providing end-to-end voice encryption and live chat between iPhones. The main security features of the TOE and its operational environment are:

- Encrypted end-to-end voice calls over VoIP (Secure Call)
- Encrypted live chat (Secure Live Chat)
- Encrypted group calls
- Secure Individual phone book
  - Centrally managed (TOE environment)
  - Pushed seamlessly to user devices
  - Supports individual groups settings
- Encrypted calls are restricted to the phone book
- Support secure provisioning to set up a new Dencrypt Talk installation
- Support its own key-pair generation

The Dencrypt Communication Solution consists of Dencrypt Talk (the TOE) and the Dencrypt Server System, which contains: a Dencrypt Communication Server (a SIP server), a Dencrypt Database Server (provides database services to DCS), a Dencrypt Certificate Manager (signs server and client certificates), a Dencrypt Provisioning Server (provisions clients) and a Dencrypt Control Center (provides administrator interface). Only the Dencrypt Talk is part of the TOE. The other parts are not within the scope of the TOE, but are considered as necessary parts of the TOE environment. The Dencrypt Server System is specified in another Security Target and subject to a separate evaluation and certification.



5.1 Dencrypt Talk subsystems

The Dencrypt Talk is an application running on iOS and consists of four subsystems.

5.1.1 User interface

The user interface offers a graphical interface which manages the in- and output displayed to user of the application.

5.1.2 Controller

The controller provides the API to access Dencrypt Talk´s VoIP functionality. It also includes phonebook storage and handling, PKI management and chat handling as well.

5.1.3 Secure Signal Handler

The Secure Signal Handler is responsible for the signaling between Dencrypt Talk and the Dencrypt Server System.

5.1.4 Secure Media Handler

The Secure Media Handler manages the media data of the end-user. Thus, the subsystem manages the audio real-time data stream between two Dencrypt Talk applications.

6 Documentation

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

- Operational User Guide Dencrypt Talk v. 4.2 (iOS)
- Preparative Guide Dencrypt Talk v. 4.2 (iOS)

7 IT Product Testing

The testing was conducted on iPhone 5C using iOS version 10.3.3.

7.1 Developer Testing

Test Effort

The developer uses both automated and manual tests. Two automated test systems are used for testing the TOE. All tests, both automated and manual, contain a test description. The manual tests also describe the expected outcome of the tests.

Test approach

The developer demonstrated that all test cases ran successfully. The developer tests cover all SFRs, interfaces, and subsystems. The developer conducted extensive testing, 181 tests, to test the complete Dencrypt Communication Solution (Dencrypt Talk and Dencrypt Server system). Two automated test systems, Calabash and Client TLS, were used. The tests include both positive and negative tests.

Test configuration

The developer performed the tests on the TOE installed on three iPhones, the TOE running in the simulated environment and some tests were performed on a special build of the TOE. The developer also performed several entropy tests. These tests are executed on a special build of the TOE in order to be able to read out the keys.

7.2 Evaluator Testing

The developer provided the evaluator with the results of all test cases, the source code of the automated tests, as well as the associated low-level log files from the entropy tests. All evaluator tests were performed successfully. The testing of the TOE was conducted on

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 also modified two automated tests from different test suites to verify that the outcome of the test changed to the new expected outcome. The evaluator also performed a negative test.

Test approach

The independent testing covered every security function, without striving for exhaustive testing. All automated developer tests and a sample of the manual developer tests were selected by the evaluators to re-run. The tests were selected so that each TSFI, subsystem and SFR was tested. The evaluators performed both manual and automated developer tests along with several entropy tests created by the developer.

Test configuration

The evaluators executed a sample of the developer tests. The evaluator preformed a subset of the tests at the developer's site as well at the evaluation facility in Sweden.

7.3 Penetration Testing

The evaluator performed six penetration tests. None of the performed penetration tests revealed any exploitable vulnerability in the TOE.

Test effort

Vulnerability testing was performed against the TOE interfaces that are accessible to a potential attacker. The evaluator also performed traffic analysis during voice call and live chat between TOEs. Several tests using modified provisioning links were also executed.

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 also modified the behavior of the TOE environment, e.g. provisioning link and Apple Push Notification Service, in order to verify that no unexpected behavior was identified.

Test configuration

The TOE and the TOE environment was configured according to the ST, Preparative Guide Dencrypt Talk v. 4.2 (iOS) and Operational User Guide Dencrypt Talk v. 4.2 (iOS) The evaluator also used Macbook Pros with Xcode and Wireshark installed to intercept and analyze network traffic.

8 Evaluated Configuration

The IT environment must contain the following:

- Multiple mobile devices (iPhone) where the TOE is installed. At least iPhone version 5C and iOS version 10.
- The Dencrypt Server System version 2.0.
- A standard Mobile Device Management system.

The SIP VoIP system is designed for the usage over an IP network, i.e. Dencrypt Communication Solutions can be deployed where an IP network connection exits but is limited to Dencrypt Communication Solution users.

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	
Production support, acceptance procedures and automation	ALC_CMC.4	Pass
Problem tracking CM coverage	ALC_CMS.4	Pass
Delivery procedures	ALC_DEL.1	Pass
Identification of security measures	ALC_DVS.1	Pass
Well-defined development tools	ALC_TAT.1	Pass
Flaw reporting procedure	ALC_FLR.2	Pass
Development	ADV	
Security Architecure description	ADV_ARC.1	Pass
Complete functional specification	ADV_FSP.4	Pass
Implementation representation of the TSF	ADV_IMP.1	Pass
Basic modular design	ADV_TDS.3	Pass
Guidance documents	AGD	
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Tests	ATE	
Analysis of coverage	ATE_COV.2	Pass
Testing: basic design	ATE_DPT.1	Pass
Functional testing	ATE_FUN.1	Pass

Independent testing - Sampling	ATE_IND.2	Pass
Vulnerability assessment	AVA	
Focused vulnerability analysis	AVA_VAN.3	Pass

10 Evaluator Comments and Recommendations

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

10.1 The certifier comments and recommendations

The ST claims that the TOE is an application for the iPhone. The TOE is dependent on the underlying operating system of iOS and hardware of the iPhone as expressed by A.HANDSET. The TOE is also dependent on the Dencrypt Server System version 2.0, certifier at EAL2+, as expressed by A.BACKEND.

As the mobile device industry pushing new hardware and both OS versions and updates in a high pace, any application dependent on the OS and the hardware needs to be updated regularly. As the threat landscape is shifting at a high pace, the current security level of the mobile devices can swiftly change, as new potential vulnerabilities that could affect the TOE or its underlying platform are regularly discovered. The certifier notes that for many scenarios a reasonable policy would be to keep products up to date with the latest version of the firmware/software. However, the benefit of installing firmware/software updates must be balanced with the potential risks that such changes might have unexpected effect on the behavior of the evaluated security functionality.

The certification conducted at EAL4 augmented with ALC_FLR.2 indicates the developer's intention to maintain and update the TOE in order to keep it relevant over time. The testing of the TOE has been conducted by the evaluator on iOS version 10.3.3. The certifier would strongly recommend that only iPhones versions upgradable to iOS version 11 to be used.

The TOE is depending on the iPhone for the generation of random numbers. The TOE uses the Yarrow algorithm implemented in iOS as pseudorandom number generator.

11 Glossary

BIOS	Basic Input/Output System
CC	Common Criteria
CEM	Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations
DCS	Dencrypt Communication Server
DCM	Dencrypt Certificate Manager
DPS	Dencrypt Provisioning Server
DCC	Dencrypt Control Center
EAL	Evaluation Assurance Level
FER	Final Evaluation Report
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
PKI	Public Key Infrastructure
SIM	Subscriber Identity/Identification Module
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
VoIP	Voice over Internet Protocol

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]	Security Target for Dencrypt Talk, Dencrypt A/S, document Version 1.0, 2017-09-11
[CCConfigGuide]	Operational User Guide Dencrypt Talk, Dencrypt A/S, Version 4.2(iOS), 2017-08-31
[UserGuide]	Preparative Guide Dencrypt Talk, Dencrypt A/S, Version 4.2(iOS), 2017-08-31

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