CSEC

Swedish Certification Body for IT Security

Certification Report - Dencrypt Connex 6.0

Issue: 1.0, 2021-Jul-09

Authorisation: Ulf Noring, Lead Certifier , CSEC

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is Dencrypt Connex, version 6.0 for Apple iOS, build 6.0.0.4.

The TOE is an application for iPhone that offers encrypted mobile voice, video and message communication within well-defined user groups. Although the application is available for both iPhone and Android, only the iPhone version is evaluated.

The main security features of the TOE and its operational environment are:

- Encrypted end-to-end voice and video communication (Secure Call)
- Encrypted messages (Secure Messaging)
- Encrypted group calls
- Secure Individual phone book
  - Centrally managed (TOE environment)
  - Distributed seamlessly to user devices
  - Supports individual groups settings
  - Supports individual emergency contacts
- Encrypted communication is restricted to administrator defined groups
- Supports secure provisioning to set up a new DCA installation
- Supports its own key-pair generation
- Secure data-at-rest storage of credentials and data
- Encrypted push notifications
- TCP tunnelling for voice or video communication

The TOE is provided and installed using Apple's App Store. The App Store delivery mechanism operated by Apple is assumed to be trusted and secure. The TOE can also be provided using Apple's Volume Purchase Program (VPP), where the app is installed via an MDM. Note that the TOE is delivered in an unprovisioned state. Provisioning is started by the Dencrypt administrator by adding the user to the Dencrypt Communication Solution and directory (part of the TOE environment). After that the administrator will send an invitation message e.g. by email to the user's handset. The invitation message has a link to the web server. The user shall tap the link which starts the TOE. The link can also be encoded in a QR code which the phone can scan to load the link into the TOE. The TOE parses the link, fetches the provisioning data from the Dencrypt Provisioning Server (part of the TOE environment) and installs the data.

Guidance is provided in two manuals:

- Operational user guide Dencrypt Connex v. 6.0.0.4
- Dencrypt Connex v. 6.0.0.4 Preparative guide

The TOE claims conformance to the EAL4 package of security assurance requirements, augmented with ALC_FLR.2. It does not claim conformance to any Protection Profile (PP).

Three threats, eight OSPs and nine 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 2021-06-24. 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 and by observing a site visit and performing testing oversight. 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 4 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.

As specified in the Security Target of this evaluation, the invocation of the random number generator (RNG) has been included in the TOE, while the implementation of the RNG has been located in TOE environment (Apple iOS). Therefore the invocation of cryptographic primitives has been in the scope of this evaluation, while correctness of implementation of cryptographic primitives been excluded from the TOE. Correctness of implementation is assumed by the Security Target as stated in A.KEYS: "It is assumed that random bits provided by the underlying platform are of good quality and have sufficient entropy."

Users of this product are advised to consider their acceptance of this assumption regarding the correctness of implementation of the RNG.

2 Identification

Certification Identification	
Certification ID	CSEC2020005
Name and version of the certified IT product	Dencrypt Connex 6.0.0.4
Security Target Identification	Security Target for Dencrypt Connex version 6.0, 2021-03-31, version 0.14
EAL	EAL 4 + 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:

- Secure initialisation
- Update of TOE settings, phonebook and certificate
- Secure voice and video
- Secure messaging
- Data-at-rest protection
- Secure communication channel (TLS)
- Encrypted push notifications
- TCP tunnelling of secure calls

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

3.1 Secure initialisation

This security function provisions a Dencrypt Connex client with user credential, Dencrypt Server System (DSS) domain and signed certificate. The provisioning starts by the administrator adding the user to the DSS. Afterwards, the administrator provides an invitation link (which can also be encoded as a QR-code) to the user in a secure way. This link points to the web server of the Dencrypt Provisioning Server (DPS). The user shall tap the invitation link or scan the QR code which starts the TOE. The TOE parses the link, fetches the provisioning data from the DPS and installs the provisioning data. The provisioning data is then deleted from the DPS, i.e. the link can be used only once. Additionally, the link is only valid for a limited time after the link has been provided.

3.2 Update of TOE settings, phonebook and certificate

This security function keeps the TOE's local settings in sync with the server system's settings. Whenever the TOE is running and registered on the Dencrypt Communication Server (DCS), the TOE downloads network settings as soon as the checksum of its local settings differs from the settings checksum advertised by the DCS. The same mechanism applies to keep the phone book up-to-date.

Although the TOE user is the single individual that is authorized to use the TOE, the user cannot change any phone book entries or make calls from a dial-pad. Besides, the mobile's built-in phone book is kept completely separate from the Dencrypt Connex application (DCA)'s phone book.

During provisioning, the TOE generates by itself an RSA 3072-bit private-public key pair and sends, via the DPS, its public key with a certificate signing request (CSR) to the Dencrypt Certificate Manager (DCM) which signs it and delivers the client certificate. This is to ensure that the private key never must leave the TOE. The client creates a new private key and CSR if the client certificate expires soon (e.g. within the next 12 months). This CSR is submitted to the DCM via the DCS, since the DPS is only used during provisioning.

3.3 Secure voice and video

The secure communication channel between two handsets, the TOE and the other instance of the TOE goes as followed: Dencrypt's secure call extends a Voice/Video over IP (VoIP) system by a patented Dynamic Encryption for voice and video data. Dencrypt's VoIP system employs the Session Initiation Protocol (SIP), Secure Real-time Transmission Protocol (SRTP) and DTLS-SRTP standard components that are partly modified to integrate dynamic encryption.

For secure calls, DTLS-SRTP uses Elliptic Curve Diffie-Hellman key exchange to establish a common secret and authenticate the call. Additionally, both DCAs exchange their client certificates over the peer-to-peer connection. The fingerprints of the certificates are sent over the call setup channel through the DSS. To mitigate a Man-in-the-middle (MitM) attack, the fingerprint calculated from the exchanged certificate has to match with the fingerprint signalled through the DSS. The common secret is then used to derive a 256-bit key and 128-bit salt which are fed into SRTP's key derivation function (KDF). Besides, Key Boosting is used to create a common Dynamic Encryption key which is used for both AES and the S-box seed. Once the SRTP session ends all the keys are destroyed (overwritten with zeros)

Secure calls and messages can only be initiated to users within the caller’s phone book. All the content, i.e. SRTP stream for audio/video and text data for messaging, are dynamically encrypted.

3.4 Secure messaging

The Secure Messaging is provided by the LIMEv2 protocol, which in turn is based on the Signal Protocol. Additionally the message encryption has been modified via Dencrypt’s Dynamic Encryption and Key Boosting, which are the same implementation as for Secure Calls. The DCA primarily generates Diffie-Hellman keypairs and uploads its public keys to the DSS. Extended Triple Diffie-Hellman (X3DH) is used to establish the initial shared secret. After that, Double Ratchet computes the symmetric key for the Dynamic Encryption of the messages. The algorithm ratchets the symmetric key for each message to ensure Perfect Forward Secrecy (PFS). After a message is received and decrypted, the related keys are erased.

3.5 Data-at-rest protection

The TOE dynamically encrypts the databases that store the chat history and the LIMEv2 keys. The same Dynamic Encryption key decrypts both databases and the key is constant but unique for each TOE.

At the end of provisioning the TOE generates two 640-bit keys. One (Storage Key) will be used for Dynamic Encryption of the storage, while the other (Device Key) will be used as a Key Encryption Key using XOR. The encrypted Storage Key is submitted to the DSS and will not be stored by the TOE, it is downloaded and only kept in RAM. After a message is received and decrypted using the LIMEv2 protocol it is encrypted via storage encryption before being stored on the device. The cleartext data (messages and attachments) will only be stored in RAM. This approach ensures that neither the device nor the server system becomes a point-of-alack. In case of a lost or stolen device, the TLS certificate is revoked and the device cannot connect to the server system to fetch the encrypted Storage Key

3.6 Secure communication channel (TLS)

The TOE can establish a secure channel between the TOE and DSS components. All TLS connections are initiated by the TOE. The secure SIP connection between the TOE and the SIP server on the DCS uses mutually authenticated TLS 1.2, with RSA signature, AES 256-bit encryption and SHA-384 hashing. The HTTPS connection to the web server on the DPS also uses TLS 1.2, with RSA signature, AES 256-bit encryption and SHA-384 hashing. However, in this case the TOE is not authenticated to the DPS. This is only performed once during the provisioning and the link is only valid for a limited time after it has been provided.

3.7 Encrypted push notifications

Apple requires the TOE to indicate to the user immediate feedback for incoming mobile push. This leaves TOE no time to connect to DSS to get hold of the incoming caller ID. The SIP caller ID is placed encrypted in the mobile push. This ensures that only the intended DCA recipient can read the caller ID, even though the push message is sent via the system of a different vendor. The TOE generates and submits an AES push encryption key at the end of provisioning. The key is also stored by the TOE and used to decrypt incoming push notifications. AES CFB is used instead of Dynamic Encryption since DSS has no Dynamic Encryption capabilities. There is no integrity protection since the push notification is sent through Apple via TLS.

3.8 TCP tunnelling of secure calls

The TOE also supports tunnelling of voice and video traffic over TCP and TLS 1.2. Voice and video are normally sent over UDP via SRTP, however, this tunnelling service will allow the TOE to instead use TCP and TLS 1.2 to tunnel the call traffic. The DSS provides a tunnel server to which the TOE can connect to enable this. Whether the tunnel is enabled or not by default depends on the settings as specified on the server, but this setting can be changed on the TOE. While the tunnel provides the TLS encryption, this is not security relevant since the tunnelled traffic is still protected by SRTP.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

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

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

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

A.ADMIN

It is assumed that the TOE administrators (i.e. the administrators using the DSS) are trustworthy and trained to perform the actions required by them for the management and maintenance of the DSS.

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.

A.APPSTORE

It is assumed that the operational environment provides a secure delivery mechanism for the TOE operated by a trusted third party. For the TOE which runs on the iPhone iOS operating system, this is the built in App Store operated by Apple.

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. This involves data sent between the TOE and the DSS, including push notifications.

T.MASQUERADE

A user within a closed user group is masquerading, pretending to be another user to mislead the receiver that a secure voice or video call, or a secure message 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, video or messaging conversations between users within a closed user group.

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

OSP.CLOSED

The TOE shall ensure that secure calls and secure messages are restricted to parties defined by the phone book on the TOE of the calling party.

OSP.FORWARD

The TOE must be able to prevent an unauthorized user that obtains a handset to decrypt previously transmitted traffic (voice, video or message) that has been encrypted using the obtained handset. Any encryption keys used for the transmitted traffic must be erased.

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.

OSP.STORAGE

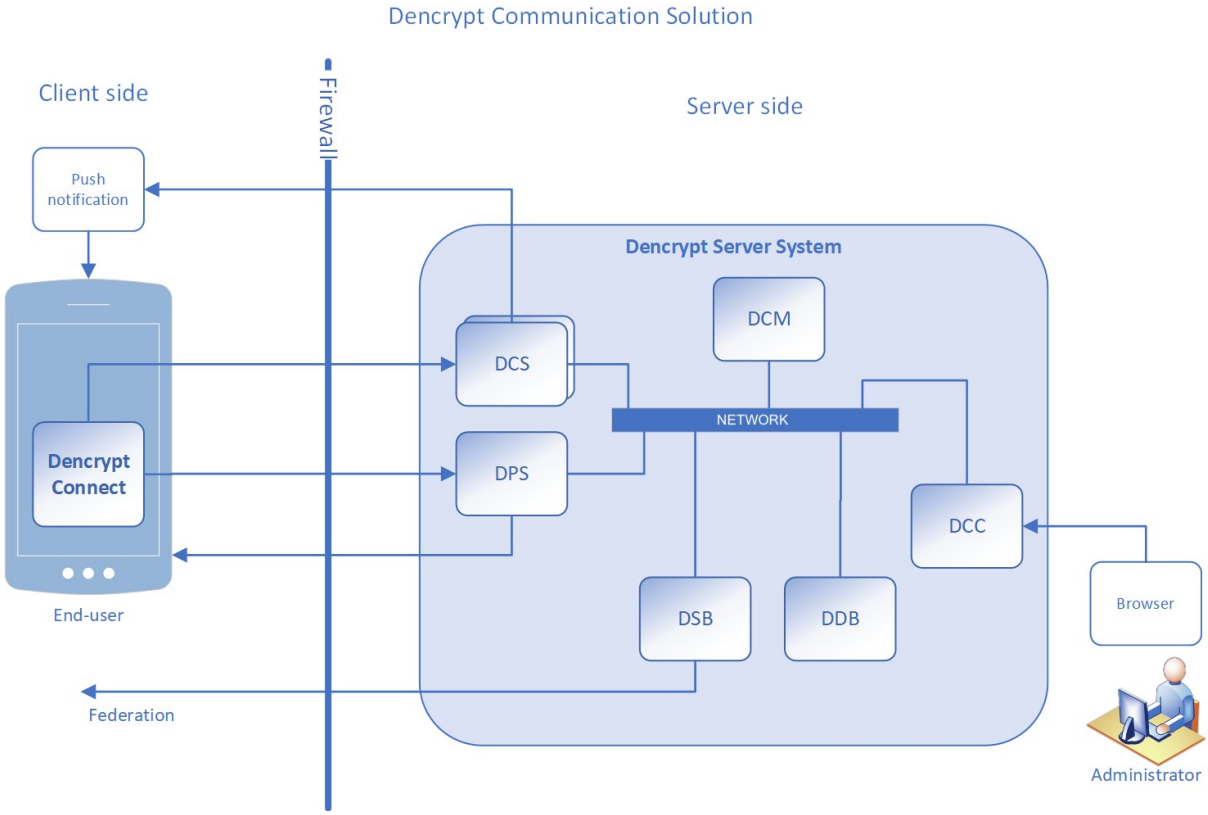
The TOE must use cryptography to protect the confidentiality of data stored on the device. The data involves both DCA data, messages and message attachments. The data must only be accessible if the user can authenticate to the DSS.

OSP.TUNNEL

The TOE must support tunnelling of voice or video communication over TCP by tunnelling the connection over TLS 1.2.

5 Architectural Information

The TOE, i.e. Dencrypt Connex, is an app running on iPhone. It is part of the Dencrypt Communication Solution that provides mobile devices with secure end-to-end voice, video and message communication within closed user groups that are centrally managed. The Dencrypt Communication Solution also contains the server side system - Dencrypt Server System (DSS). The TOE relies on the DSS for provisioning, call signaling, messaging, and management of phone book, but only the Dencrypt Connex application is in the scope of this evaluation. The figure below shows the TOE and its interactions with the server side within the Dencrypt Communication Solution.



6 Documentation

The following documentation comprise the TOE guidance:

PREGUIDE	Dencrypt Connex v. 6.0.0.4 Preparative guide
OPGUIDE	Operational user guide Dencrypt Connex v. 6.0.0.4

7 IT Product Testing

7.1 Developer Testing

The developer uses both automated and manual tests. In total 130 tests were executed to test the TOE. Among them, there are 5 manual tests, 10 design checks (only code review is performed) and the rest are automated. Each test, both automated and manual test, contains a description. For manual tests the test steps are described which contain the expected outcome of the test, e.g. "Accept call and check that transmission, e.g. audio works". For automated tests, the steps are described in the code which the evaluator has examined.

The testing approach of the developer was to demonstrate that all test cases ran successfully and that all ST claims, interfaces, and subsystems are verified by the tests.

Doctest C++ testing framework, Python, GnuTLS server and TCL/TK are used for testing. For automated tests, some are limited to a specific functionality that does not require any interaction with DSS. For tests that require DSS, both mocked VoIP/Chat transmission engine and fully functional DSS are used, and the tests with mocked engine are more extensive.

The tests include both positive and negative tests, e.g. test case "DC-TLS-WrongCipher: Negative TLS test: Wrong ciphersuite" has the following description: "Testing that connection fails when server insists on wrong algorithm".

The developer performed the tests on the actual TOE installed on the iPhone and on the TOE running in a simulated environment.

The tests were either executed on TOE installed on iPhone or in a simulated environment on Mac. The TOE was configured (provisioned) to use the servers in the test environment. The developer also performed manual/semi-automatic test of dynamic encryption by making a separate build to test against reference implementation.

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 re-ran all developer tests (130 tests), both automated and manual tests. The evaluators also observed when the developer ran an extra test to verify the inner and outer AES operations within Dynamic Encryption. The evaluator also examined the source code of a sample of automated developer test to verify that they test what they claim. The evaluator further performed two Evaluator Tests: one negative test where she tested if the provisioning link was usable after the valid time window had expired; and the other where she intercepted a chat message to verify it is end-to-end encrypted.

The developer's testing environment was used, which consisted of iPhones running Dencrypt Connex (TOE), Dencrypt Server System, and a Mac computer running automated tests. All security functionality defined in the ST has been tested.

The evaluators tested all security functions for appropriate coverage and depth; since the evaluators already determined that the developer testing sufficiently exercised all interfaces and TSF subsystems, the evaluators did not need to exhaustively test all interfaces and subsystems.

The tests re-ran by the developer and the extra Dynamic Encryption test ran by the developer, both under the evaluators' observation, went successfully. All evaluator tests were also performed successfully.

7.3 Penetration Testing

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

The evaluator analyzed the developer design, the implementation representation and guidance documentation in order to identify the attack surface of the TOE. The evaluator came to the conclusion that the attack surface consists of the external network interfaces, i.e., data that are sent or received on these interfaces. The evaluator also used publicly documented vulnerabilities in CVE database and used general search engines. The analysis of potential attack surfaces was performed according to the ISO/OSI layer model, i.e., for TLSv1.2, SRTP, DTLS etc. connections.

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

8 Evaluated Configuration

The TOE is an iPhone application and thus requires an iPhone to run.

The IT environment must provide the following:

- The mobile device hardware (iPhone) and iOS software on which the TOE is installed. This includes the App Store application included in iOS, which is used for the delivery mechanism.
- The DSS with DPS, DCC, DCM, DDB, DSB and DCS, as well as any standard MDM system in the case that the DCA is distributed using Apple's VPP.

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 (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.4	PASS
Parts of the TOE CM Coverage	ALC_CMS.4	PASS
Delivery procedures	ALC_DEL.1	PASS
Developer Security	ALC_DVS.1	PASS
Flaw reporting procedures	ALC_FLR.2	PASS
Life-cycle definition	ALC_LCD.1	PASS
Tools and Techniques	ALC_TAT.1	PASS
Development	ADV	PASS
Security architecture description	ADV_ARC.1	PASS
Security-enforcing functional specification	ADV_FSP.4	PASS
Implementation representation	ADV_IMP.1	PASS
Basic design	ADV_TDS.3	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.2	PASS
Depth	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing - sample	ATE_IND.2	PASS
Vulnerability Assessment	AVA	PASS
Vulnerability analysis	AVA_VAN.3	PASS

10 Evaluator Comments and Recommendations

None.

10.1 Certifier Comments

Dencrypt's Dynamic Encryption, used to protect voice and video calls, messaging and local storage in the TOE, is based on 256-bit AES in GCM mode with several steps added as described in chapter 7.3.1 in the [ST]. For the purposes of this certification, the security provided by Dynamic Encryption is considered to be at least that of 256-bit AES in GCM mode.

As the mobile device industry pushes new hardware, OS versions and updates at a high pace, any application dependent on the OS and hardware needs to be updated regularly. As the threat landscape is shifting at a high pace, the current security level of mobile devices can swiftly change, since new potential vulnerabilities that could affect the TOE or its underlying platform are regularly discovered. While the Common Criteria certificate is only valid for version 6.0.0.4 of the Toe, and though the evaluator has not found any vulnerabilities in the TOE, it is possible that the developer will release security updates at a later date. The certifier notes that while updating the application or its environment will put it outside of the evaluated configuration, 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 effects on the behaviour of the evaluated security functionality.

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 Connex version 6.0, Dencrypt A/S, 2021-03-31, document version 0.14

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 Dencrypt Connex v. 6.0.0.4 Preparative guide, Dencrypt A/S, 2020-12-15, document version 2.13

OPGUIDE Operational user guide Dencrypt Connex v. 6.0.0.4, Dencrypt A/S, 2020-12-15, document version 1.2

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 EAL4.
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.