Jabra Engage 65 and Jabra Engage 75 with Embedded Software v4.2.0 Security Target

Contents

1 Document Introduction

This document is a Common Criteria Security Target (ST) for Jabra Engage 65 and Jabra Engage 75 with Embedded Software v4.2.0. The ST is authored in accordance with Common Criteria Version 3.1 Revision 5.

1.1 References

[CC Part1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model. April 2017 Version 3.1 Revision 5 CCMB-2017-04-001.

[CC Part 2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components. April 2017 Version 3.1 Revision 5 CCMB-2017-04-002.

[CC Part 3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components. April 2017 Version 3.1 Revision 5 CCMB-2017-04-003.

[EN 300 175-7] Final draft ETSI EN 300 175-7 V2.4.0 (2011-12), European Standard Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 7: Security features

1.2 Acronyms and Abbreviations

Term	Explanation
AC	Authentication Code
AES	Advanced Encryption Standard
AU	Australia
CPU	Central Processing Unit
DCK	Derived Cipher Key
DECT	Digital Enhanced Cordless Telecommunications (or Digital European Cordless Telecommunications)
DLC	Data Link Control Layer
DSAA	DECT Standard Authentication Algorithm
DSAA2	DECT Standard Authentication Algorithm #2
DSAA2-256	DECT Standard Authentication Algorithm #2 with 256-bit output
DSC	DECT Standard Cipher
DSC2	DECT Standard Cipher #2
DSC2-256	DECT Standard Cipher #2 with 256-bit key
EAN	European Article Number
EMEA	Europe, Middle East, Africa
ETSI	European Telecommunications Standards Institute

FP	DECT Fixed Part
HK	Hong Kong
IC	Integrated Circuit
JP	Japan
K	Authentication Key shared between the Base Station and a Headset
KS	Session Authentication Key
KS'	Reverse Authentication Key
MAC	Media Access Control Layer (or: Message Authentication Code)
NA	North America
N/A	Not Applicable
NWK	Network Layer
NZ	New Zealand
OTA	Over the Air
PC	Personal Computer
PDF	Portable Document Format
PP	DECT Portable Part (or: Common Criteria Protection Profile)
PHL	Physical Layer
RES1	Value computed and transmitted by PP
RES2	Value computed and transmitted by FP
RS	Value transmitted by FP in authentication protocol
RSA	Rivest-Shamir-Adleman
SG	Singapore
SHA-256	Secure Hash Algorithm w/256 digest length
SKU	Stock Keeping Unit
UAK	Unique Authentication Key
UK	United Kingdom
UPC	Universal Product Code
UPI	User Personal Identity
USB	Universal Serial Bus
VoIP	Voice Over Internet Protocol

2 ST Introduction

This Section is the Security Target Introduction. It states the ST Identification and TOE Identification, followed by TOE Overview and TOE Description.

2.1 ST Identification

The ST Identification is as follows:

ST Title	Jabra Engage 65 and Jabra Engage 75 with Embedded Software v4.2.0 Security Target
ST Version	Revision M
ST Date	July 28, 2022

2.2 TOE Identification

The TOE Identification is as follows:

TOE Name	Jabra Engage 65 and Jabra Engage 75 with Embedded Software v4.2.0
TOE Guidance	Jabra Engage 65 and Jabra Engage 75 with Embedded Software v4.2.0 Common Criteria Guidance Supplement Rev. B

2.3 TOE Overview

This section is the TOE Overview. It summarises the usage and major security features of the TOE, states the TOE Type and identifies all hardware, software and firmware which are not parts of the TOE, but which are required by the TOE.

2.3.1 Usage and Major Security Features of the TOE

This section states the usage of the TOE and introduces the major security features. It commences with a brief overview of DECT and DECT security followed by an identification of the key DECT security processes. This is followed by an introduction of the TOE use case. The TOE user interface is described following the introduction of the use case. Finally, the section concludes by an overview of the security features implemented in the TOE.

2.3.1.1 DECT and DECT Security Overview

The TOE is a DECT (Digital Enhanced Cordless Telecommunications[1]) Base Station and Headset. The Base Station acts as a DECT Fixed Part (FP) and the Headset acts as a DECT Portable Part (PP). The Base Station and the Headset consist of hardware and software and together implement a secure mechanism for users to take phone calls using wireless headsets. The TOE ensures that

[1] Historically also referred to as Digital European Cordless Telecommunications

each Base Station and Headset is successfully authenticated and that all data streams between successfully authenticated Base Stations and Headsets are strongly encrypted.

Authentication prevents attackers from successfully masquerading as legitimate Base Stations and Headsets. Strong encryption prevents attackers and listening devices operating on their behalf from tapping the air interface and deducing the content of communication from the DECT data streams between legitimate Base Stations and Headsets.

DECT is defined in the European Telecommunication and Standards Institute (ETSI) standard family ETSI EN 300 175 V2.8.1. Security protocols are defined in Part 7 of the standard [EN 300 175-7]. The DECT standards include definitions for protocols at the Physical (PHL) layer, Media Access Control (MAC) layer, Data Link Control (DLC) layer, and Network (NWK) layer for a FP to communicate with one or more PP. In case of the TOE, the FP are the Base Stations and the PP are wireless Headsets which together allow secure, hands-free DECT calls.

DECT security protocols define mutual authentication of a Base Station and the Headsets, and encryption and decryption of data streams between them. Mutual authentication protocol implements a NWK Layer DSAA2 Challenge-Response authentication protocol using a Unique Authentication Key (UAK) established by a Base Station and Headset during a coupling of the two. A one-time authentication key K is established and used by each party to prove their knowledge of K by computing an encrypted response to a random challenge sent by the other party.

DSAA2 protocol also establishes a Derived Cipher Key (DCK) which is used for generating a key stream for encrypting at the MAC layer all data streams between the authenticated parties. The encryption is in accordance with a DSC2 protocol.

DECT standards support custom protocols to replace DSAA2 and DSC2. This allows higher levels of security on critical applications but may prevent interoperability of devices implementing standard protocols and those implementing custom protocols.

Earlier versions of the DECT standard included a weaker DSAA standard for mutual authentication and a DSC protocol using a proprietary encryption algorithm. Both are considered obsolete and insecure and should not be used.

DECT Security standards support optionally authentication of the user by a manually entered authentication data. This requires that a terminal device supports entry of the authentication data through a suitable input device. The TOE does not support user authentication.

2.3.1.2 DECT Security Processes

DECT Security standards define a number of processes by which key security features needed for DSAA2 and DSC2 are implemented. These are used by the TOE with the exception of some 128-bit quantities being enhanced to 256-bit quantities as described in Sect. 2.3.1.3.

The DECT Security processes are the following:

- A11 Process and A21 Process are used for deriving the session authentication keys (KS and KS') from Authentication Key K and Random Challenge (RS) as described in Sect. 4.5.3 of [EN 300 175-7].
- A12 Process and A22 Process are used for computing the Derived Cipher Key (DCK) the Response (RES1 or RES2) to an authentication challenge using KS or KS' as described in Sect. 4.5.3 of [EN 300 175-7].
- B1 Process is used for deriving the Authentication Key K from the Unique Authentication Key (UAK) or Authentication Code (AC) as described in Sect. 4.5.2 of [EN 300 175-7].
- B2 Process is used for deriving the Authentication Key K from a combination of the Unique Authentication Key (UAK) and User Personal Identity (UPI) as described in Sect. 4.5.2 of [EN 300 175-7].
- Key Stream Generation (KSG) Process is used for generating a key stream from the Derived Cipher Key (DCK) as described in Sect. 4.5.4 of [EN 300 175-7]

2.3.1.3 TOE Use Case

The overall use case of the TOE is illustrated in Figure 1. Wireless Headsets are coupled with Base Stations. Once the coupling is completed, two Headsets coupled to different Base Stations may be used for establishing a secure one-to-one DECT call through the Base Stations. Users may roam within the coverage area of the Base Station.

DECT security protocols protect the over-the-air communication between the Base Stations and Headsets. Security of the call is achieved through the establishment of a UAK which a Headset establishes when physically coupled with a Base Station. Over the air coupling is not supported. The UAK is used for mutual authentication of the Base Station and a Headset and for the establishment of a DCK over the air at a later time.

Mutual authentication of the Base Station and Headsets ensures that any malicious device attempting to masquerade as a legitimate Headset or Base Station shall be detected. Encryption of the call ensures that any party listening to the air interface either within the premises or within the proximity of the premises where the wireless communication propagates shall not be able to disclose the content of the communication between Base Stations and Headsets.

The TOE implements 256-bit enhancements to DSAA2 and DSC2. As this reduces the interoperability of the TOE with non-TOE Base Stations and Headsets, the Base Stations and Headsets constituting the TOE are not to be used with non-TOE Base Stations or Headsets.

The enhancements are the following:

- DSAA2 protocol is enhanced to use 256-bit challenges with 32-bit responses for authentication and for generation of a 256-bit DCK. The protocol is otherwise identical to the standard DSAA2. The enhanced DSAA2 shall be called DSAA2-256 in this Security Target.

- DSC2 is enhanced to use a 256-bit DCK for encryption and decryption of data streams between a Base Station and a Headset. The 256-bit DCK is derived from 128 bits of UAK (hence, offering the security strength of 128 bits). Otherwise it is identical to the standard DSC2 protocol. The enhanced DSC2 shall be called DSC2-256 in this Security Target.

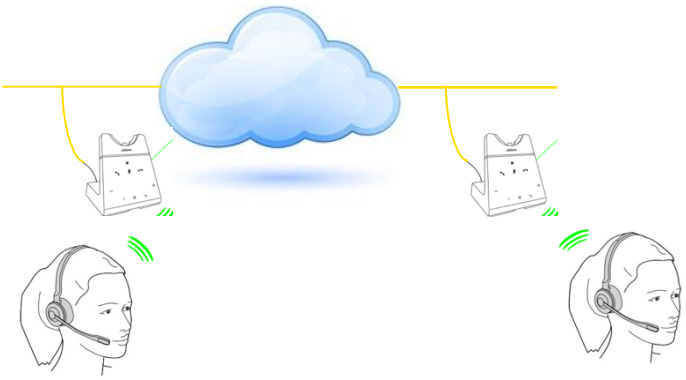

Figure 1 The Use Case of the TOE

Base Stations and the Headsets incorporate a Dialog Semiconductors DA14495A Integrated Circuit (IC). The TOE embedded software is executed on the CPU of the IC and utilises the non-deterministic hardware random number generator and hardware implementation of DSAA2-256 and DSC2-256.

DECT standards allow authentication of users through manual entry of the user authentication data prior to the allowing of the handset to register with a Base Station. As the terminals for the TOE are Headsets without user input devices other than voice, the TOE does not implement user authentication.

TOE Software resides in the memories of the Base Stations and Headsets and is associated with a digital signature computed by the manufacturing environment. The developer may issue software upgrades for the TOE. The software upgrade mechanism verifies the authenticity of each software upgrade by verifying the signature associated to the upgrade.

2.3.1.4 TOE User Interface

The Base Station may be a Jabra Engage 65 or Jabra Engage 75. The Base Stations are illustrated in Figure 2. The two are functionally similar but differ in the physical interface. Jabra Engage 65 has buttons for controlling the calls while Jabra Engage 75 has a touch pad. Further, Jabra Engage 75 has a display while Jabra Engage 65 does not. The presence of a display and touch pad allows broader configuration option from the Base Station.

Figure 3 Jabra Engage 65 (left) and Jabra Engage 75 (right) Base Stations

The Headset form factors are identical for models compatible with Jabra Engage 65 and Jabra Engage 75 but the software differs to handle the differences in the Base Station interfaces. There are three TOE Headset form factor variants: Convertible, Mono and Stereo. The variants differ in a way they are worn by the user. They are illustrated in Figure 3. Functionally each headset variant is identical and runs identical software. The difference is in form factor only.

Figure 2 Convertible (left), Mono (middle) and Stereo (right) Headset

The TOE Base Station may be connected to a Management PC for administration through a USB connection. A properly connected Management PC may be used for administering Base Stations and those Headsets which are physically coupled to a Base Station. The Management PC runs Jabra Direct software for interacting with the TOE. Jabra Direct may run as a stand-alone software or it may be connected to the Jabra Xpress enterprise software for managing a large set of Base Stations and Headsets. Neither the Management PC, Jabra Direct nor Jabra Xpress are part of the TOE.

2.3.1.5 TOE Security features overview

The TOE implements DSAA2-256 and DSC2-256. DSAA2-256 implements mutual authentication of the Base Station and a Headset and establishment of a 256-bit symmetric DCK between the two. DSC2-256 implements 256-bit Advanced Encryption Standard (AES) using a key stream derived from the DCK for encrypting and decrypting the data stream between Base Stations and Headsets.

When a Headset is coupled physically with a Base Station, the two establish a UAK which is used for deriving the mutual authentication key K. The TOE is not intended for roaming applications and only uses authentication key K instead of the authentication session keys KS and KS' defined in [EN 300 175-7]. Key K is used by each party to encrypt the random challenged received from the other party. Successful verification of the encrypted response assures a party of the other party being in possession of a valid K.

DSAA2-256 and DSC2-256 as well as the underlying cryptographic primitives and the random number generation are implemented in hardware on the IC.

The TOE also allows the Management PC to read out the hardware Stock Keeping Unit (SKU) to help administrator in ensuring that the hardware identity stored on the TOE memory is correct and identical to the identity printed in the sticker attached to the TOE hardware. TOE software implements self-checks to verify the correct functioning of the hardware random number generator prior to accepting the quantities from it.

TOE Software resides on the memories of the IC and is associated to a 2048-bit RSA digital signature of a SHA-256 message digest of the TOE software. The message digest and the digital signature are computed at the software production environment. The digital signature is used for verifying the authenticity of the software upgrades loaded on the TOE. Only upon successful verification shall the TOE accept the upgraded software. When requested by the Management PC, the TOE shall produce a diagnostic report which includes a code indicating the type of the latest reason for a failure to boot up.

The Management PC can be used for configuring the TOE and for upgrading the TOE software when an upgrade is available. The Headset must be docked to the Base Station in order for the Headset software to be upgraded. The software upgrade is protected with a digital signature. The digital signature is verified at the upgrade and once the TOE is first booted up after a software update. Failure to verify the signature of the updated software will cause the TOE to boot up with the current software. Upon successful verification of the digital signature the TOE shall overwrite the boot image with the upgraded software.

2.3.2 TOE Type

The TOE is hardware and software for implementing a secure DECT Base Station and a secure DECT Headset. The Base Station acts as a DECT FP and the Headset acts as a DECT PP. Together, the Base Station and the Headset implement secure Over the Air communication mechanism.

2.3.3 Non-TOE Hardware, Software and Firmware required by the TOE

The following hardware, software and firmware are required by the TOE but are not part of the TOE:

- The TOE requires a Management PC for configuration and software upgrade. The Management PC must run Jabra Direct management software. The management PC is connected to the TOE physically over a USB port but is not part of the TOE.
- Jabra Direct management software running on the Management PC is not part of the TOE. Neither is the Jabra Xpress which may run in addition to Jabra Direct.
- The TOE requires a telephone handset connected to a telephone network or a PC running Voice over IP (VoIP) software and connected to a network. The TOE does not implement the calling software and hardware but must be connected to an external device for the calls.

2.4 TOE Description

This section is the TOE Description. The physical scope of the TOE and the logical scope of the TOE are stated. This section also states the features of the TOE which are not included in the certified configuration.

2.4.1 Physical Scope of the TOE

The Physical scope of the TOE consists of the TOE Hardware, TOE Software and the TOE Security Guidance.

2.4.1.1 TOE Hardware

TOE Hardware consists of the Base Station hardware and of the Headset hardware. Each Base Station and Headset includes an Integrated Circuit (IC) which is wired to other components. Cryptographic functions of the TOE are implemented on the IC. The IC is the DA14495A Multi Level Modulation 1.9GHz DECT transceiver by Dialog Semiconductors.

There are two variants of the Base Station hardware: Jabra Engage 65 and Jabra Engage 75.

Headset hardware comes in three different variants (Convertible, Mono and Stereo) for each Base Station. Base Station and Headset variants are also configured to the DECT regions to ensure that the correct bandwidth is used in accordance with the regional regulations.

Jabra Base Stations and Headsets share identical Stock Keeping Unit (SKU), European Article Number (EAN) and Universal Product Code (UPC) numbers. The SKU can be read out by Jabra Direct software for verification.

Jabra 65 Engage hardware variants are identified as follows:

Region	SKU	Model	EAN	UPC
EMEA	9553-553-111	Jabra Engage 65 Mono	5706991019681	706487017257

	9555-553-111	Jabra Engage 65 Convertible	5706991019728	706487017295
	9559-553-111	Jabra Engage 65 Stereo	5706991019827	706487017394
NA	9553-553-125	Jabra Engage 65 Mono	5706991019704	706487017271
	9555-553-125	Jabra Engage 65 Convertible	5706991019742	706487017318
	9559-553-125	Jabra Engage 65 Stereo	5706991019841	706487017417
UK, HK, SG, AU, NZ	9553-553-117	Jabra Engage 65 Mono	5706991019698	706487017264
	9553-553-117-1[2]	Jabra Engage 65 Mono[3]	5706991021769	N/A
	9555-553-117	Jabra Engage 65 Convertible	5706991019735	706487017301
	9559-553-117	Jabra Engage 65 Stereo	5706991019834	706487017400
JP	9553-553-136	Jabra Engage 65 Mono	5706991019711	706487017288
	9555-553-136	Jabra Engage 65 Convertible	5706991019759	706487017325

Jabra 75 Engage hardware variants are identified as follows:

Region	SKU	Model	EAN	UPC
EMEA	9556-583-111	Jabra Engage 75 Mono	5706991019681	706487017257
	9555-583-111	Jabra Engage 75 Convertible	5706991019728	706487017295
	9559-583-111	Jabra Engage 75 Stereo	5706991019827	706487017394
NA	9556-583-125	Jabra Engage 75 Mono	5706991019704	706487017271
	9555-583-125	Jabra Engage 75 Convertible	5706991019742	706487017318
	9559-583-125	Jabra Engage 75 Stereo	5706991019841	706487017417
UK, HK, SG, AU, NZ	9556-583-117	Jabra Engage 75 Mono	5706991019803	706487017370
	9555-583-117	Jabra Engage 75 Convertible	5706991019773	706487017349
	9559-583-117	Jabra Engage 75 Stereo	5706991019865	706487017431

TOE Hardware is delivered either by the retailer in person or drop shipped from a distribution centre by courier with parcel tracing.

2.4.1.2 TOE Software

TOE Software consists of the embedded software running in the Base Station and of the embedded software running in the Headset. Different software runs in Jabra Engage 65 and Jabra Engage 75 but all software releases are parallel, i.e. each software component has an identical version number:

Jabra Engage 65 Base Station embedded software is version 4.2.0

Jabra Engage 75 Base Station embedded software is version 4.2.0

[2] UK Only

[3] High Density model

Jabra Engage 65 Headset embedded software is version 4.2.0

Jabra Engage 75 Headset embedded software is version 4.2.0

The software is delivered installed on Base Stations and Headsets.

2.4.1.3 TOE Guidance

TOE Guidance is the Common Criteria Guidance Supplement document provided for the users of the TOE to be followed in all use. It is identified by document name and document version. The exact name and version of the TOE Guidance are given in Sect. 2.2.

The Guidance is delivered to the users as a PDF document via the Jabra secure web site.

2.4.2 Logical Scope of the TOE

The logical scope of the TOE includes the key security features the TOE implements. Each one is listed and summarised in the following.

Security feature	Description
Component authentication	The TOE implements a NWK layer DSAA2-256 Challenge-Response mutual authentication and key generation protocol for Base Stations and Headsets. DSAA2-256 is identical to the standard DSAA2 authentication except it uses larger random challenges and produces a 256-bit Derived Cipher Key (DCK). Successful authentication is required for the Headset to register with a Base Station. DSAA2-256 protocol is implemented on the IC of the TOE. The random quantities are generated within the IC implementing a non-deterministic random number generator. The correct functioning of the random number generator is checked for quality prior to the acceptance of the produced quantities. When the Headset is physically coupled with the Base Station, the two exchange a 256-bit Unique Authentication Key (UAK). When establishing a connection at a later time, the Base Station and the Headset use the UAK to compute a shared 256-bit authentication key K and the 256-bit DCK. Authentication key K is used for computing the response to a random challenged issued by the other party in accordance with the [EN 300 175-7]. The party receiving the response verifies it and if the verification succeeds, accepts the other party as authentic. Otherwise, the connection request is rejected.
Data Stream Confidentiality	Upon successful mutual authentication of the Base Station and the Headset using DSAA2-256, a shared 256-bit DCK is established between the two. The TOE implements a DSC2-256 protocol to encrypt the data

	stream between the Base Station and the Headset at the MAC layer. DSC2-256 differs from the standard DSC2 in that instead of a 128-bit DCK and 128-bit AES, the key stream used for data stream encryption is generated from a 256-bit DCK and used with 256-bit AES. The key stream is derived from DCK and used for encrypting the data stream with AES in accordance with the DSC2-256 conventions. Base Station and the Headset incorporate an IC supporting hardware implementation of DSC2 and for the cryptographic algorithms used for cryptographic operations.
TOE Authenticity	The TOE has a printed label containing the SKU of the TOE. The same SKU is stored in the memory of the TOE during manufacturing. Users may use the Management PC to read out the SKU from the memory and compare it to the label to ensure that the two are identical. The TOE software is distributed with a SHA-256 message digest which is digitally signed using a 2048-bit RSA private key. The signature computation takes place at the manufacturing site using a dedicated manufacturing private RSA key. The corresponding public key is stored on the TOE and is used to verify the integrity and authenticity of the TOE software upgrades. In case of the signature verification failing, the TOE shall not replace the boot image with the upgraded software but boots up with the non-upgraded software. If the signature verification succeeds, the TOE overwrites the boot image with the upgraded software and boots up. The TOE stores the type of failure which caused the latest boot up failure and the user may use the Management PC to generate a diagnostic report which includes the type of the failure.
Secure upgrade	To ensure that all discovered security and other flaws are effectively mitigated, the TOE allows upgrading of the software once deployed. Software upgrade is implemented through a management PC and a SHA-256 digest of each software upgrade is digitally signed by the manufacturer using a 2048-bit RSA private key. The corresponding public key is stored in the TOE and is used by the TOE to verify the integrity and authenticity of the software upgrade. In case of a failure to verify the digital signature, the TOE shall boot up with an un-upgraded software.

2.4.3 Items Outside the Scope of the TOE

The following features and characteristics are not included in the certified configuration or are not implemented by the TOE:

- The following protocols are considered insecure and are not used in the certified configuration of the TOE:
  - Bluetooth,
  - Over the Air (OTA) Pairing of a Headset and Base Station,
  - Headset conference mode
- The TOE implements DECT DSAA and DECT DSC protocols which are considered obsolete and insecure. This is required for interoperability. However, DSAA and DSC shall not be used in the certified configuration.
- The TOE does not implement user authentication. The terminal is a Headset with no user interface device which could be used for manually entering the authentication data of a user.
- The TOE does not implement a trusted channel or a trusted path between itself and a Management PC. The TOE does not implement roles and does not require the administrator to successfully authenticate to the TOE. Instead, the configuration of the TOE and updating of a TOE software must take place in a secure environment by known, trusted administrators using a trusted Management PC.

3 Conformance Claims

3.1 Conformance Claims statement

The ST and the TOE claim conformance to Common Criteria v3.1 Release 5 Part 1, Common Criteria v3.1, Release 5 Part 2, and Common Criteria v3.1 Release 5 Part 3.

Common Criteria v3.1 Release 5 Part 1 is fully identified in [CC Part 1], Common Criteria v3.1 Release 5 Part 2 in [CC Part 2] and Common Criteria v3.1 Release 5 Part 3 in [CC Part 3].

The ST is CC Part 2 conformant.

The ST is CC Part 3 conformant.

The ST claims conformance to the following Protection Profiles and Packages: None.

The ST claims package-augmented conformance to the following: Evaluation Assurance Level EAL2 Augmented with ALC_FLR.1.

3.2 Conformance Claims Rationale

The ST does not claim conformance to any Protection Profile. Therefore, the Conformance Claims Rationale is not applicable.

4 Security Problem Definition

This section states the assumptions, threats and organisational security policies applicable to the TOE.

4.1 Assumptions

There are no assumptions applicable to the TOE.

4.2 Threats

The following threats are applicable to the TOE.

Threat ID	Threat Description
T.MASQUERADE	An attacked with physical access to the vicinity of the TOE succeeds in violating the authenticity of the parties communicating using the TOE by constructing an illegitimate Base Station which succeeds in establishing a connection with a legitimate Headset, or by constructing an illegitimate Headset which succeeds in establishing a connection with a legitimate Base Station. Successfully constructing an illegitimate Base Station or a Headset would allow the attacker to masquerade as a legitimate TOE part and join a call protected by the TOE.
T.EAVESDROP	An attacker with physical access to the vicinity of the TOE succeeds in violating the confidentiality of the data communicated between a Base Station and a Headset by recording unencrypted communication and relaying or replaying it to the attacker.
T.WEAK_CRYPTO	An attacker with physical access to the vicinity of the TOE succeeds in violating the confidentiality of the data communicated between a Base Station and a Headset by recording communicating between the two and successfully cryptoanalysing it to disclose the content of the communication.
T.TOE_TAMPER	An attacker with physical access to the TOE or to the Management PC succeeds in violating the authenticity of the TOE software by tampering with the software in order to modify the executables without detection. This would allow the attacker to modify the software or bypass the security functions and mechanisms of the TOE or to create additional functions not present in an authentic TOE.

4.3 Organisational Security Policies

The following Organisational Security Policies are applicable to the TOE.

OSP ID	OSP Description
OSP.PHYSICAL	The organisation using the TOE must define a policy which states the requirements for the physical space in which the TOE may be used and stored. The requirements must be consistent with the risk management practices of the organisation. The requirements for the physical space must include the space in which the TOE may be used to prevent unauthorised parties from overhearing conversations protected by the TOE, and the storage and use of the Management PC so that it may not be accessed by parties not authorised to manage the TOE.
OSP.ADMIN	The organisation using the TOE has in place a policy stating the requirements for skills and competence for the parties authorised to manage the TOE from the Management PC and a process for ensuring that each authorisation is approved and recorded, and that all authorised administrators receive the necessary training for managing the TOE.
OSP.DIRECT	The organisation using the TOE has in place a policy stating that only Jabra Direct software may be used in managing the TOE. Jabra Xpress is allowed in association with Jabr Direct if authorised by the organisation. The responsibility for ensuring that the version of Jabra Direct used is up to date and the necessary security and other patches are installed in the Management PC is defined and delegated, and the conformance with the policy is monitored. Corrective action is taken in case of any deviation is detected.

5 Security Objectives

Security objectives for the TOE and security objectives for the environment of the TOE are stated in this section.

5.1 Security Objectives for the TOE

The following security objectives are enforced by the TOE.

Objective ID	Objective Description
O.AUTHENTICATION	The TOE implements strong mutual authentication between the Base Station and each Headset to ensure that any attempted masquerading as a legitimate Base Station or Headset fails with an overwhelming probability.
O.COMMSEC	The TOE encrypts the data stream a Base Station and each Headset to ensure that the content of the communication remains illegible to anybody except legitimate Base Stations and Headsets.
O.CRYPTO	The TOE only uses strong cryptographic algorithms and primitives, and all parameters used in the cryptographic protection of the communication are of high cryptographic quality. The TOE ensures that only cryptographically secure random challenges are used in the DSAA2-256 protocol.
O.TOE_INTEGRITY	The TOE implements a mechanism to verify the integrity of the TOE software when the TOE software is upgraded. The TOE shall accept an upgrade if an integrity and authentication verification of the upgrade fails. The TOE also implements basic audit mechanisms to assist users in the verification of the TOE hardware and software.

5.2 Security Objectives for the Environment of the TOE

The following security objectives are stated for the environment of the TOE.

OSP ID	OSP Description
OE.PHYSICAL	The TOE is only used in a physical space which is sufficiently likely to prevent unauthorised parties from overhearing conversations protected by the TOE. The Management PC is stored in a manner which prevents access by unauthorised parties.

OE.ADMIN	Each administrator authorised to manage the TOE is individually authorised for the role when shown to possess the necessary skills and competences. The authorisation is in accordance with a well-defined policy and is recorded in a manner which allows auditing of the decisions. Each administrator has received the training necessary to administer the TOE in a proper manner.
OE.DIRECT	Only the Jabra Direct software is used for managing the TOE.

5.3 Security Objectives Rationale

This section provides the Security objectives rationale. The security objectives are first traced to the elements in the security problem definition. The tracing is followed by a justification of the tracing.

5.3.1 Tracing of Security Objectives to Assumptions, Threats and OSPs

The tracing of the security objectives to the assumptions, threats and organisational security policies applicable to the TOE is given in the following.

SPD Element	O.AUTHENTICATION	O.COMMSEC	O.CRYPTO	O.TOE_INTEGRITY	OE.PHYSICAL	OE.ADMIN	OE.DIRECT
T.MASQUERADE	X						
T.EAVESDROP		X					
T.WEAK_CRYPTO	X	X	X				
T.TOE_TAMPER				X			
OSP.PHYSICAL					X		
OSP.ADMIN						X	
OSP.DIRECT							X

5.3.2 Justification of the tracing

O.AUTHENTICATION concerns with the two parts of the TOE mutually authenticating each other in a manner which prevents illegitimate parties from successfully establishing themselves as authentic parts of the TOE. This objective is fulfilled if threat of illegitimate parties masquerading as legitimate parties (T.MASQUERADE) is prevented from occurring, and the cryptographic primitives

- specifically generation of random quantities - are of sufficient quality, i.e. attackers are prevented from exploiting weak cryptographic primitives to gain access to the TOE communication (T.WEAK_CRYPTO).

O.COMMSEC concerns with the communication security, i.e. encryption and decryption of the data streams between successfully authenticated Base Stations and Headsets. Upon successful mutual authentication, the two parties establish a cryptographic key which is used for generating a key stream used for encrypting and decrypting the data stream between the Base Station and the Headset. This ensures that the threat of external parties succeeding in eavesdropping of the communication (T.EAVESDROP) is prevented from occurring. Encrypting the data using a strong DSC2-256 also ensures that the used cryptographic primitives are of sufficient cryptographic strength and, therefore, prevents T.CRYPTO from occurring.

O.CRYPTO concerns with the cryptographic strength of the primitives used by the TOE to protect communication between Base Stations and Headsets. Only using strong cryptographic primitives ensures that any practical number theoretical attacks against the cryptographic functions implemented in the TOE will fail with an overwhelming probability. This prevents threat T.CRYPTO from occurring in practice.

O.TOE_INTEGRITY concerns with ensuring that the Integrity of the TOE is protected from tampering. The TOE does not implement tamper-evident or tamper-proof hardware but protects the TOE software from modification by ensuring that the authenticity and integrity of the TOE software can be verified. The TOE also ensures that the users can verify the hardware versions of the TOE and that random quantities are verified for quality prior to use by the TOE software. These mechanisms jointly ensure that any modification of the TOE shall be detected with an overwhelming probability and prevent threat T.TOE_TAMPER from occurring.

OE.PHYSICAL concerns with ensuring that the TOE is used and stored in accordance with the physical security policies of the organisation. This ensures that the residual risk of eavesdropping is prevented from occurring in accordance with the risk assessment of the organisation using the TOE. This ensures that OSP.PHYSICAL is enforced in the organisation using the TOE.

OE.ADMIN concerns with ensuring that only trusted and sufficiently trained individuals are authorised to administer the TOE. This ensures that OSP.ADMIN is enforced in the organisation using the TOE.

OE.DIRECT concerns with ensuring that only Jabra software is used for administering the TOE. The administration software must be Jabra Direct, but the organisations may additionally use Jabra Xpress for the administration of large numbers of TOEs depending on the security policies in place. This ensures that OSP.DIRECT is enforced in the organisation using the TOE.

6 Security Requirements

This section states the security requirements for the TOE. The security functional requirements are defined with reference to CC Part 2 and to Sect. 6. The security assurance requirements are defined with reference to a well-defined evaluation assurance package EAL2 augmented with ALC_FLR.1 defined in CC Part 3.

The statement of security functional requirements utilizes operations as defined for each applicable security functional requirement in CC Part 2 and Sect. 6. The notation for identifying the operations is as follows:

Iteration is identified by repeating the identifier of the security functional requirement with a string indicating a specific iteration separated from the SFR identification by a slash (e.g. FCS_COP.1/DSC2-256).

Refinement is identified by a) indicating in square brackets in bold font any added text, in form of [**Refinement: added text**] and b) indicating any removed words using ~~overstrike~~ font. Whenever a refinement is used, the rationale and justification of the refinement is given immediately after the statement of the security requirement.

Selection is identified by indicating the selected values in [**square brackets using bold font**].

Assignment is identified by indicating the assigned values in [***square brackets using bold, italic font***].

Application notes may be added after the formal statement of the security requirements to assist the reader in understanding the specific security requirement in the context of this particular TOE.

The wording and capitalisation in the statements of security functional requirements is exactly as in [CC Part 2].

6.1 Statement of Security Functional Requirements

6.1.1 Class FAU: Security audit

6.1.1.1 Security audit data generation (FAU_GEN)

6.1.1.1.1 FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

~~a) Start-up and shutdown of the audit functions;~~

~~b) All auditable events for the [**not specified**] level of audit; and~~

c) [***Type of last error that caused a boot failure***].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) ~~Date and time of the event,~~ type of event, ~~subject identity (if applicable), and the outcome (success or failure) of the event~~; and

~~b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [***No other information***].~~

Rationale: The TOE implements an audit function to store the error that caused the latest failure to boot. There is no audit trail generated as per several IT Security products implementing more rich sets of audit functions. There is also no explicit start and stop of the audit function as audit is not a separate process but writing the type of error is coded into the TOE software when handling failures to boot up. The TOE does also not store the time of the event - calendar time is not implemented in the TOE and sequential or equivalent time is not applicable as the audit log only stores the single entry. The statement of the SFR is refined to precisely reflect the implementation of the audit function in the TOE.

6.1.1.2 Security audit review (FAU_SAR)

6.1.1.2.1 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [***Jabra Direct software***] with the capability to read [***Type of last error that caused a boot failure***] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Application note: The user to interpret the information is Jabra technical support personnel working off-line to investigate the failure.

6.1.2 Class FCS: Cryptographic support

6.1.2.1 Cryptographic key management (FCS_CKM)

6.1.2.1.1 FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [***DSAA2-256***] and specified cryptographic key sizes [***256 bits***] that meet the following: [***256-bit enhanced ETSI EN 300 175 V2.8.1***].

6.1.2.2 Cryptographic operation (FCS_COP)

6.1.2.2.1 FCS_COP.1 Cryptographic operation

FCS_COP.1.1/DSC2-256 The TSF shall perform [***Encryption and decryption of data streams between a Base Station and Headset***] in accordance with a specified cryptographic algorithm [***DSC2-256***] and cryptographic key sizes [***256 bits***] that meet the following: [***256-bit enhanced ETSI EN 300 175 V2.8.1***].

FCS_COP.1.1/SHA-256 The TSF shall perform [***Hash computation of TOE software***] in accordance with a specified cryptographic algorithm [***SHA-256***] and cryptographic key sizes [***none***] that meet the following: [***FIPS PUB 180-4***].

FCS_COP.1.1/RSA The TSF shall perform [***TOE software upgrade digital signature verification***] in accordance with a specified cryptographic algorithm [***RSA***] and cryptographic key sizes [***2048 bits***] that meet the following: [***PKCS#1 v2.2***].

6.1.3 Class FDP: User data protection

6.1.3.1 Stored data integrity (FDP_SDI)

6.1.3.1.1 FDP_SDI.2 Stored data integrity monitoring and action

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for [***TOE Software upgrade integrity failure***] on all objects, based on the following attributes: [***TOE Software upgrade digital signature***].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [***Reject the TOE software upgrade***].

6.1.4 Class FIA: Identification and authentication

6.1.4.1.1 FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [***DSAA2-256***].

6.1.5 Class FMT: Security management

6.1.5.1 Specification of Management Functions (FMT_SMF)

6.1.5.1.1 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

- ***Upgrading TOE software,***
- ***Generating a diagnostics report,***
- ***Reading TOE software version,***
- ***Reading TOE hardware SKU,***
- ***Configuration of the TOE***

].

6.1.6 Class FPT: Protection of the TSF

6.1.6.1 Fail secure (FPT_FLS)

6.1.6.1.1 FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [

- ***TOE Software upgrade digital signature verification failure,***
- ***Random number generator failure***

].

6.1.6.2 TSF self test (FPT_TST)

6.1.6.2.1 FPT_TST.1 TSF testing

FPT_TST.1.1 The TSF shall run a suite of self tests [

- **periodically during normal operation**,
- **at the conditions** [***When upgrading TOE Software***]

] to demonstrate the correct operation of [[***TOE Software upgrade, Random Number Generator***]].

~~**FPT_TST.1.2** The TSF shall provide authorised users with the capability to verify the integrity of [[***none***]].~~

~~**FPT_TST.1.3** The TSF shall provide authorised users with the capability to verify the integrity of [[***none***]].~~

Rationale: The TOE does not implement user authentication and does not maintain roles. Consequently, there are no users that can verify the integrity of the TOE Software or the random number generator. Instead, both are verified without user intervention: The TOE software upgrade is verified prior to the boot image being overwritten with the issued upgrade, and the random number generator is verified when executing the DSAA2-256 and DSC2-256 protocols requiring random quantities. As there is no Parts of the TSF or TSF Data that may be verified for integrity by any type of a user, FPT_TST.1.1 and FPT_TST.1.2 are considered unnecessary and is refined away.

6.2 Security Assurance Requirements

Security assurance requirements for the TOE constitute the evaluation assurance package EAL2 augmented with ALC_FLR.1 and are fully defined with reference to CC Part 3. The security assurance requirements constituting EAL2 augmented with ALC_FLR.1 are the following:

- Assurance Class ADV: Development

- ADV_ARC.1 Security architecture description
    - ADV_FSP.2 Security-enforcing functional specification
    - ADV_TDS.1 Basic design
- Assurance Class AGD: Guidance documents
    - AGD_OPE.1 Operational user guidance
    - AGD_PRE.1 Preparative procedures
- Assurance Class ALC: Life-cycle support
    - ALC_CMC.2 Use of a CM system
    - ALC_CMS.2 Parts of the TOE CM coverage
    - ALC_DEL.1 Delivery procedures
    - ALC_FLR.1 Basic flaw remediation
- Assurance Class ASE: Security Target evaluation
    - ASE_CCL.1 Conformance claims
    - ASE_ECD.1 Extended components definition
    - ASE_INT.1 ST introduction
    - ASE_OBJ.2 Security objectives
    - ASE_REQ.2 Derived security requirements
    - ASE_SPD.1 Security problem definition
    - ASE_TSS.1 TOE summary specification
- Assurance Class ATE: Tests
    - ATE_COV.1 Evidence of coverage
    - ATE_FUN.1 Functional testing
    - ATE_IND.2 Independent testing – sample
- Assurance Class AVA: Vulnerability assessment
    - AVA_VAN.2 Vulnerability analysis

6.3 Security Requirements Rationale

This section presents all the security requirements rationales.

6.3.1 Security Requirements Dependency Rationale

Dependencies of the security functional requirements applicable to the TOE and their fulfilment are stated in the following.

SFR	Dependencies	Fulfilment
FAU_GEN.1	FPT_STM.1 Reliable time stamps	Not fulfilled by the TOE. The audit function does not store time stamp of the latest audit event as explained in the rationale of the refinement of the statement of the SFR. Therefore, the dependency of FAU_GEN.1 to FPT_STM.1 is not applicable and is not fulfilled by the TOE.
FAU_SAR.1	FAU_GEN.1 Audit data generation	FAU_GEN.1 by the TOE
FCS_CKM.1	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/DSC2-256 by the TOE FCS_CKM.4 is not fulfilled by the TOE. There are no explicit functions that will overwrite the values of cryptographic parameters but the memories allocated to the parameters are deallocated by the TOE software.
FCS_COP.1/DSC2-256	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1 by the TOE FCS_CKM.4 is not fulfilled by the TOE. There are no explicit functions that will overwrite the values of cryptographic parameters but the memories allocated to the parameters are deallocated by the TOE software.
FCS_COP.1/SHA-256	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Not fulfilled by the TOE. None of the dependencies are applicable. SHA-256 is a cryptographically secure hash function and does not use cryptographic keys. Therefore, neither the generation, distribution nor destruction of the cryptographic keys is applicable and, consequently, cannot be fulfilled by the TOE.
FCS_COP.1/RSA	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	Not fulfilled by the TOE. None of the dependencies are applicable. RSA is used by the TOE for the verification of the digital signature of the TOE software. Verification is done using a public key of the developer stored in the TOE during the manufacturing of the TOE. The public key is

	FCS_CKM.4 Cryptographic key destruction	neither destroyed nor updated during the life-time of the TOE. Therefore, none of the dependencies are applicable and are not fulfilled by the TOE.
FDP_SDI.2	No dependencies.	N/A
FIA_UAU.4	No dependencies.	N/A
FMT_SMF.1	No dependencies.	N/A
FPT_FLS.1	No dependencies.	N/A
FPT_TST.1	No dependencies.	N/A

6.3.2 Tracing of security objectives to Security Functional Requirements

The security functional requirements stated for the TOE are traced to the security objectives for the TOE in the following.

SFR	O.AUTHENTICATION	O.COMMSEC	O.CRYPTO	O.TOE_INTEGRITY
FAU_GEN.1				X
FAU_SAR.1				X
FCS_CKM.1	X		X	
FCS_COP.1/DSC2-256		X	X	
FCS_COP.1/SHA-256			X	X
FCS_COP.1/RSA			X	X
FDP_SDI.2				X
FIA_UAU.4	X			
FMT_SMF.1				X
FPT_FLS.1	X			X
FPT_TST.1	X			

6.3.3 Justification of the Tracing

O.AUTHENTICATION concerns with the mutual authentication of Base Stations and Headsets and, upon successful authentication, establishment of a shared session key between the two. The two parties engage in a mutual authentication protocol and the TOE keeps track of the success. The IC of the TOE generates random quantities using a non-deterministic random number

generator seeded by a hardware entropy source. The TOE tests the random number generator output prior to the accepting the random quantities required for the authentication protocol (FPT_TST.1). If the random quantities do not meet the randomness requirements, the TOE shall reboot in an attempt to restore a secure state (FPT_FLS.1). The TOE also ensures that the memories allocated to the cryptographic keys and random quantities are released and shall not be reused in subsequent runs of the DSAA2-256 protocol (FIA_UAU.4). Upon successful mutual authentication, the Base Station and Headset establish a mutual symmetric cryptographic key in accordance with the DSAA2-256 standard. This is formally state in FCS_CKM.1. Jointly these SFRs ensure that O.AUTHENTICATION is fully enforced by the TOE.

O.COMMSEC concerns with the cryptographic protection of data streams between Base Stations and Headsets. The cryptographic protocol and algorithms for encrypting and decrypting the data streams must be of sufficient quality. The TOE ensures sufficient protection by implementing DSC2-256 encryption and decryption of the data stream as stated in FCS_COP.1/DSC2-256. DSC2-256 uses key streams derived from a symmetric key established by the DSAA2-256 authentication and key exchange protocol. The random quantities are produced by the IC. Once the key is no longer used, it shall be released. All communication between the Base Stations and Headsets requires successful authentication of the communicating parties. However, the authentication is based on the UAK key established by the Headsets and Base Stations when docked. Establishment of the UAK is not protected by the DSC2-256 protocol as well as management actions taking place when the Headset is docked to the Base Station are allowed to take place prior to the authentication and session key establishment taking place. These SFRs ensure that data stream communication takes place and is correctly implemented, i.e. that the TOE enforces O.COMMSEC.

O.CRYPTO concerns with ensuring that high quality cryptographic primitives are used in all security functions and mechanisms of the TOE requiring cryptographic algorithms. The cryptographic algorithms implemented by the TOE include

- mutual authentication of Base Stations and Headsets and establishment of session keys between them in accordance with DSAA2-256 using a non-deterministic random number generator implemented within the IC(FCS_CKM.1),
- Encryption and decryption of data streams between Base Stations and Headsets in accordance with DSC2-256 (FCS_COP.1/DSC2-256),
- computation of a SHA-256 message digest for the TOE software (FCS_COP.1/SHA-256), and
- verification of the digital signature of the TOE software using RSA with 2048-bit keys (FCS_COP.1/RSA).

Jointly, these security requirements ensure that only high quality cryptographic primitives are used by the TOE. This ensures that any cryptanalytical attacks against the cryptographic primitives used by the TOE will fail with an overwhelming probability. This ensures that the TOE enforce security objective O.CRYPTO.

O.TOE_INTEGRITY concerns with ensuring that the TOE only operates when the integrity and authenticity of the TOE is ensured. To ensure that the critical parts of the TOE are checked for integrity, the TOE ensures that the digital signature of the TOE software is verified prior to accepting the TOE software upgrade (FCS_COP.1/SHA-256, FCS_COP.1/RSA, FDP_SDI.1) and the random number generator tested for correct functioning prior to the use (FPT_TST.1). If any of the two fails, the TOE shall require a reboot and possibly manual intervention until the problems are resolved (FPT_FLS.1). In case of a failure to boot up, the TOE stores the last reason for a failure in an audit record (FAU_GEN.1) and allows the Jabra Direct software to generate a diagnostic report including the reason (FAU_SAR.1). The diagnostic report may concern the Base Station or a Headset. Requesting a diagnostic report is a well-defined management function and, together with other management functions, constitute a well-defined management interface to the TOE (FMT_SMF.1). Management of the Headset is only allowed when physically docked to the Base Station. Jointly these SFRs ensure that the TOE implements sufficient measures to ensure authenticity of itself and that necessary protective measures are taken if any violation of authenticity and integrity is detected. Jointly they ensure that the TOE fully enforces O.TOE_INTEGRITY.

6.3.4 Justification for the Security Assurance Requirements

The security assurance requirements selected for the TOE constitute a well-defined evaluation assurance package EAL2 augmented with ALC_FLR.1. As such, the selected security assurance requirements are in accordance with [CC Part 3] and constitute an internally consistent set of security assurance requirements.

7 TOE Summary Specification

The following gives for each SFR stated in Sect. 6.1 a rationale describing how the TOE implements that SFR.

SFR	Rationale
FAU_GEN.1	The TOE implements an audit function which stores the code for the error that caused the latest failure to boot. Only a single entry is stored, whenever a new failure to boot occurs, the existing audit record is overwritten. The audit function for the latest reason for a failure to boot is always on and there is no management function to switch it on and off. The TOE does not implement a meaningful time which means that there is no meaningful representation of a date and time which could be stored with the audit record.
FAU_SAR.1	The error causing the latest failure to boot is stored as a code which can be read from the TOE by the Jabra Direct software. The code is used by the developer for debugging the TOE software (even if occurring when the TOE is operational) and is not for general debugging use. Therefore, the code can only be interpreted by the developer's technical personnel.
FCS_CKM.1	When a Headset and a Base Station are physically coupled, they may engage in a mutual authentication and key generation protocol. Upon successful mutual authentication, the base station and a headset engage in a key generation protocol which results in a creation of a 256-bit Derived Cipher Key (DCK). The protocol is a standard DECT protocol (i.e. as stated in ETSI EN 300 175 V2.8.1) with an enhancement which allows generation of a 256-bit instead of a 128-bit DCK. The DCK is used for encrypting all traffic between the base station and the headset.
FCS_COP.1/DSC2-256	As part of the mutual authentication protocol, a 256-bit DCK is established between a Base Station and a Headset. Subsequent communication between the Base Station and the Headset is encrypted using the DSC2-256 protocol at the DECT MAC layer in accordance with [EN 300 175-7]. DSC2-256 differs from the standard DSC2 defined in ETSI EN 300 175 V2.8.1 in that instead of a 128-bit DCK and 128-bit AES, the key stream used for encrypting the data stream is generated from a 256-bit DCK and used with 256-bit AES. Both the Base Station and the Headset incorporate a Dialog Semiconductor DA14495A IC. AES used in DSC2-256 is implemented on the IC with the exception of the KeyExpansion stage which also uses software implementation.
FCS_COP.1/SHA-256 FCS_COP.1/RSA	The TOE software is distributed with a SHA-256 message digest which is digitally signed using a 2048-bit RSA private key. The signature computation takes place at the manufacturing site using a dedicated manufacturing private RSA key. The corresponding public key is stored on the TOE and is used to verify the integrity and authenticity of the TOE software upgrades. The TOE leverages the DA14495A IC for computing the SHA-256 value of the software and then performs the 2048-bit RSA computation for verifying the signature. RSA is implemented in software.

FDP_SDI.2	When the TOE software is upgraded, an upgrade is downloaded together with a 2048-bit RSA key of the upgrade (see FCS_COP.1/SHA-256 and FCS_COP.1/RSA). The software upgrade is stored in the memories of the TOE and once the TOE boots up, the signature of the firmware is verified. If the verification succeeds, the TOE shall replace the software with the upgraded software. If the verification fails, the TOE shall boot up with the old software.
FIA_UAU.4	The TOE implements a DSAA2-256 mutual authentication protocol between a Base Station and a Headset. The authentication uses a challenge-response exchange which allows both parties to verify the authenticity of the other party. Once the challenge is used, the memory are used for storing it shall be immediate deallocated by the TOE software. This ensures that the TOE does not use the same challenge twice but requires each authentication to occur with a fresh challenge.
FMT_SMF.1	The TOE implements a limited user interface which in turns restricts the management interface available to the users. The following management functions are implemented and are available to all users of the TOE: – Upgrading TOE software, – Generating a diagnostics report, – Reading TOE software version, – Reading TOE hardware SKU, and – Configuration of the TOE.
FPT_FLS.1	The TOE implements two types of self-tests: – Verification of the correct functioning of the random number generator prior to the generation of any random quantities, and – Verification of the software upgrade authenticity prior to the upgrading of the software. The IC of the TOE implements a suite of health-tests for the random number generator prior to each use of the random quantities. If any of the health-tests fails, the random number generator shall not produce output which ensures that no poor quality random quantities are used by the TOE. If the verification of the firmware upgrade fails, the TOE ensures a secure state by not installing the upgrade but booting up using the old software instead.

8 Revision History

Maintenance interval: None.

Rev	Date	Editor	Reviewer(s)	Description
A	2021.05.04	Teron Labs	N/A	Initial version
B	2021.05.05	Teron Labs	N/A	Initial internal comments
C	2021.05.11	Teron Labs	N/A	Teron Labs internal
D	2021.05.12	Teron Labs	Erling Skjoldbord	Second internal review
E	2021.05.19	Teron Labs	Erling Skjoldbord, Anthony Baldwin	First developer review
F	2021.05.19	Teron Labs	N/A	Updated document ownership
G	2021.10.06	Teron Labs	N/A	Added TOE Summary Specification
J	2022.03.28	Teron Labs	N/A	Addresses observations EFT-T025-EOR-ASE 1.3.
K	2202.03.28	Teron Labs	N/A	Addresses Observations EFT-T025-EOR-ASE 1.4
L	2022.06.25	Teron Labs	N/A	Addresses Observations EFT-T025-EOR-ASE 1.5
M	2022.07.28	Teron Labs	N/A	Addresses Observations EFT-T025-EOR-ASE 1.7