THALES

MLS Voice Terminal
MVT

Security Target

Classification	Document Title	Radical – Business Id	Revision	DTC	Language	Entity Cage Code	Thales Cage Code	PAGE
UNCLASSIFIED	**MLS Voice Terminal MVT Security Target**	**3AQ 32627 AAAA**	**007-lite**	**938**	**[EN]**	**N4244**	**0026**	**1 of 43**

THALES

DOCUMENT CHANGE HISTORY

Revision	Date	Description
007	15 Dec 2023	Official document version for CC evaluation.
007-lite	14 Feb 2024	Document development revisions omitted for lite version. Document sanitized according to "*CCRA ST sanitising for publication*" ("*CCDB-2006-04-004.pdf*", www.commoncriteriaportal.org › supdocs › CCDB-2006-04-004).

	–	001	002	003	004	005	006	007
Written by		**HS**	**HS**	**HS**	**HS**	**HS**	**HS**	**HS**
Checked by	QA Manager	**TT**	**TT**	**TG**	**TTA**	**TTA**	**TTA**	**TTA**
Approved by	PDA	**ES**	**ES**	**ES**	**ES**	**ES**	**ES**	**ES**

THALES

Table of Contents

1. SECURITY TARGET INTRODUCTION (ASE_INT)

1.1 Security Target reference

(1) The Security Target is consistent with Common Criteria as specified in ref. [2], [3] and [4].

(2) The following table identifies the Security Target (ST).

Item	**Identification**
ST title	MLS Voice Terminal MVT Security Target
ST reference	3AQ 32627 AAAA 938 EN
ST version	(see footer)
ST author	Thales Norway AS

1.2 TOE reference

(1) The following table identifies the Target Of Evaluation (TOE)

TOE Name	MLS Voice Terminal
TOE Version	1.1.10
TOE Assurance Level	EAL4 augmented with ALC_FLR.3
TOE Developer	Thales Norway AS
CC Identification	Version 3.1 Revision 5

Product id.	Variant code (4 characters)		Version
	Customer id. (3 char.)	Export regulation (1 char.)	
3AQ 32627	<A-Z . A-Z . A-Z>	<A-Z>	x.x.x

Example: 3AQ 32627 AAAB version 1.1.10

1.3 Referenced documents

Ref	Id	Title
[1]	AC/35-D/2001-REV2	NATO Security Committee - Directive on Physical Security Note: replaces C-M(55)15(Final), Enclosure C.
[2]	[CCPART1]	Common Criteria for Information Technology Security Evaluation, April 2017, Version 3.1 revision 5, Part 1 (also known as part 1 of the ISO/IEC 15408 Evaluation Criteria).
[3]	[CCPART2]	Common Criteria for Information Technology Security Evaluation, April 2017, Version 3.1 revision 5, Part 2 (also known as part 2 of the ISO/IEC 15408 Evaluation Criteria).
[4]	[CCPART3]	Common Criteria for Information Technology Security Evaluation, April 2017, Version 3.1 revision 5, Part 3 (also known as part 3 of the ISO/IEC 15408 Evaluation Criteria).
[5]	[MVG-ST]	TNOR Guards Security Target (EAL4 ST for MVG)

1.4 TOE overview

1.4.1 General

(1) The TOE is the MLS Voice Terminal (MVT) which provides a secure voice handling module inside Operator Terminals (OCP) in a MLS Voice System (MVS).

(2) The TOE works together with the MLS Voice Guard [MVG-ST] to tunnel a lower classified voice stream from the OCP to a lower classified network via an MVG.

(3) The TOE makes sure that the operator behind the OCP has clear information about the classification level of the network the microphone is connected to.

(4) The TOE also makes sure that the operator has information whether any neighbouring OCPs have microphones connected to a lower classified network, thereby take measures when speaking classified information; e.g. speak lower.

(5) For the purpose of component re-use and to simplify security certification, the system architecture is separated into two main parts:

(a) The Voice Application(s)

(b) The secure voice handling part, MLS Voice Platform

(6) The main purpose of the TOE is to provide the capabilities required to handle all voice presented at the OCP and to perform the required separation of voice data (VoIP) at different

classification levels. The OCP is physically connected to the highest classified network. The TOE tunnels different classified voice data to corresponding networks via MLS Voice Guard (MVG) in a secure way.

(7) The operators typically have a multi-level operator terminal (OCP) hosting a VoIP application. VoIP connections can be made to other similar (multi level) OCPs or to standard VoIP applications (single level) on different security levels.

(8) The OCP consists of the Voice Application SW providing the communication logic and HMI (except the HMI for the security indicators which are controlled by the MVT), and the MVT SW providing the security certified SW for the audio handling in the OCP. The audio is handled by the MVT only.

(9) A Voice Application part can be tailored to many different roles and is not subject to security certification. It constitutes the business logic of one of several possible voice applications and will typically contain the user interface (GUI).

(10) The MLS Security Manager (MSM) performs configuration of security parameters in MVT and it is responsible to receive security events and fetch security audit log.

1.4.2 Major security features of the TOE

(1) The main security features of the TOE are:

- Security indication to the operator.
- Neighbour security status indication.
- Tagging of outgoing microphone voice data according to security indication such that the MVG securely can make decisions on whether data can pass to the lower level supported by the MVG.
- Checking of incoming voice data tagging for proper handling according to security level.

1.4.2.1 Security levels and security groups (policies)

The MLS Voice System shall support several security levels. These security levels may be seen as parallel security groups typically to represent different security policies.

1.4.3 Required non-TOE SW

(1) Separation kernel

(2) OCP Voice Application

The OCP Voice Application SW can be any application which interfaces a user API to the MVT.

(3) The MLS Security Management (MSM) as relevant for the MVT TOE

(4) Voice Recorder (VoIP)

Centralised IP based recording service.

1.4.4 Required non-TOE HW

(1) OCP HW platform

(2) MLS Voice Guard (MVG)

1.5 TOE description

The MVT (TOE) is a building block in the operator terminal (OCP) of a MLS Voice System (MVS) that provides security related functions

The MVS is intended for use in military operation sites. The Operator Terminal (OCP) is used by the operators for voice communications to other echelons and authorities connected at different security levels.

The MVS provides voice communications for several security levels to operators in the operation sites, between operators and external military and civilian networks and between operators and radios where that is required. The system is designed to provide a continuous 24/7/365operation.

1.5.1 Definition of TOE perimeter

(1) The TOE is the part of the OCP implementing the core security functions (MVT) which must be highly trusted. The TOE is defined in section 1.2 “TOE reference”.

(2) The MLS Voice Terminal (MVT) provides the security related functionality that is used by the Voice Application on the OCP.

1.5.2 MLS Voice Terminal as part of MLS Voice System

(1) The MVT (TOE) and the MLS Voice Guard (MVG), plus the corresponding MLS Security Manager (MSM), together constitute the MLS Voice Platform (MVP).

(2) The MVP, in which the TOE is the part in the OCP, provides the capability to establish voice connections on different security levels from the same OCP. The MVP is common to all applications. It separates and isolates all the security related functions. MVP is further divided into three parts:

(a) MLS Voice Terminal, this TOE (MVT)

(b) MLS Voice Guard (MVG)

(c) MLS Security Management (MSM)

(3) The network with the highest security level is connected to a lower classified network. In effect,the MVP tunnels differently classified voice data from the OCP to networks of corresponding classifications in a secure way.

(4) The users can receive audio in voice connections from one or more security levels simultaneously, while each user can transmit audio from the microphone according to security levels of the active voice connections. The OCP HMI displays the current security level(s) for the microphone audio, and the user must be trained to communicate information according to the displayed security level(s).

(5) The MVG is the physical gateway between the internal (highest) security level and the external lower security level.

(6) All audio streams are integrity protected according to their security level by the MVT (TOE).

(7) There are specific MLS Voice Guards (MVGs) that handle the voice connections (VoIP) to the lower security levels. The MVG provides an automatic and controlled flow of information between two domains that may operate under different security policies. No information is allowed to pass from one of the domains to the other unless the Security Policy of the MVG explicitly allows it to pass.

1.5.3 Separation kernel

(1) The MVT runs on top of a separation kernel.

1.5.4 MVT (TOE) configuration (by the MSM)

(1) Each MVT can be assigned a subset of security levels.
(2) The MVT can be configured with keys and policy rules.

1.5.5 The TOE HW and platform

(1) The TOE is SW only. The TOE is typically hosted on COTS hardware.

1.5.6 The TOE SW

(1) The TOE performs the security functions for security indication and audio handling.

1.5.6.1 Microphone security status indication

(1) The main security function of the OCP is to display the security levels that apply to the active (TX) connections

(2) The OCP user has to look at the screen to be sure which information can be exchanged on the active voice connections. It is a manual and operational decision to only exchange information that is according to the displayed security levels (or any information with lower classification).

(3) The OCP can have several active voice connections with different security levels, but the security levels displayed are the lowest security level within each security group (policy) that has active (TX) connections.

1.5.6.2 Sending audio packets for recording

(1) The transmitted and received audio for each individual MVT is sent to a centralised Voice Recorder.

(2) The recording connection is set up using the highest security level since this connection will include audio from the highest security level.

1.5.6.3 Neighbour security status

(1) The neighbour security status is used to inform the operator about possible low security microphone connections on the operator positions defined to be neighbours.

2. CONFORMANCE CLAIMS (ASE_CCL)

2.1 CC conformance claim

Conformance	Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, [CCPART2] Part 3: Security Assurance Components, [CCPART3]
Assurance level	EAL4 augmented with ALC_FLR.3 (Systematic flaw remediation)

2.2 PP and Package conformance claims

(1) The Security Target has no Protection Profile claims.

3. SECURITY PROBLEM DEFINITION (ASE_SPD)

3.1 General

(1) This section provides the statement of the Security Problem Definitions, which identifies and explains:

- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects.
- Known and presumed threats countered by either the TOE or by the security environment.
- Organisational security policies to which the TOE must comply.

3.2 Assumptions

(1) The following conditions are assumed to exist in the operational environment.

A.PHYSICAL	The MVS is installed in a physical protected area, minimum approved for the highest security level of information handled in the system.
A.TRAINING	All OCP users are trained in the correct use of the MVS facilities.
A.CLEARANCE	All OCP users have a minimum clearance for the highest security level of information handled in the system, and is authorised for all information handled by the system.
A.MAN.AUTHORISED	Only users with special authorization are allowed to do configuration and management of the system including TOE.
A.MVS.COM	The LANs in the MVS shall not be used for other communication than voice and signalling for call handling and system internal management communication. Attached networks must be logically or physically separated, and must be approved for the security level the MVT is operating on. The LANs used for MVS may be utilised for other data traffic, i.e. the MVS may be installed in an existing data network. Care must be taken to only expose the MVG to MVS related traffic (by means of data flow control such as firewall, VLAN etc.) isolating the voice related traffic from/to MVS devices and software through the MVG.
A.USAGE	The MVT in the MVS is installed according to the installation guidelines for the MVS.
A.AUDIT	The TOE environment retrieves the audit records of the TOE, provides secure storage of audit records and performs security violation analysis.
A.MVT.ALARM	The TOE environment must contain an instantiation of the MLS Management System (MSM) for receiving and presenting Security Events from the TOE.

A.HARDENING	TOE will be running in a virtualized and hardened software architecture to meet all general and relevant cyber security requirements.

3.3 Threats

3.3.1 General

(1) This section identifies the assets, threat agents and threats.

3.3.2 Identification of assets

(1) The assets that TOE shall protect as specified in this Security Target are the following:

.

AS.NON_RELEASABLE_INFORMATION	Higher classified voice data that shall not be released to lower classified networks.

3.3.3 Identification of threat agents

TA.INTERNAL	Personnel which have authorised access to the operations site and which has intent to perform unauthorised actions. These persons may be trained specially to perform their unauthorised actions. They may bring unauthorised software into the site and may be able to load it. They may be supported by entities with unlimited resources.
TA.EXTERNAL	Personnel which do not have access to the operations site and which has the intent to divulge classified information. These persons may have unlimited resources.
TA.USER	OCP users with no intent to perform unauthorised actions. They may unintentionally perform unauthorised actions.
TA.TECHNICIAN	Technicians with no intent to perform unauthorised actions. They may unintentionally perform unauthorised actions.
TA.MALFUNCTIONS	System malfunctions. System malfunctions to be considered are limited to single point of failure.

3.3.4 Threats

T.CONN.SEC.NON-SEC	Classified information on a secure channel may be transferred to a lower classified channel than intended.

Threat agents	TA.TECHNICIAN, and/or TA.MALFUNCTIONS. In addition the following must be present: TA.EXTERNAL
Asset	Classified information
Unwanted outcome	Unauthorised personnel get access to classified information.
Attack methods	1. A technician (TA.TECHNICIAN) unintentionally configure or install the TOE in a way which transfer information on secure channels (i.e. classified information) to a lower classified channel than intended. The classified information is picked up from this channel by persons (TA.EXTERNAL) outside the physically protected area. 2. A malfunction (TA.MALFUNCTIONS) in the TOE implies that information on secure channels (i.e. classified information) is transferred to a lower classified channel than intended. The classified information is picked up from this channel by persons (TA.EXTERNAL) outside the physically protected area.
T.WRONG.SEC.IND	System malfunctions may give the OCP user a wrong indication of whether the microphone is channelled to a specific security level. The OCP user may then speak classified information on a lower classified network than intended.
Threat agent	TA.USER, TA.MALFUNCTIONS combined with TA.EXTERNAL
Asset	Classified information
Unwanted outcome	Unauthorised personnel get access to classified information.
Attack method	System malfunctions (TA.MALFUNCTIONS) gives the OCP user (TA.USER) an indication that the microphone is not connected to a lower classified network, while in reality it is. The OCP user then speaks classified on a higher level than expected. The classified information is picked up by the microphone and transmitted on a lower classified network. The classified information is picked up by persons (TA.EXTERNAL) outside the physically protected area.
T.ACOUSTIC.PICK-UP	Microphones connected to a lower classified channel may pick up higher classified speech.
Threat agent	TA.USER combined with TA.EXTERNAL
Asset	Classified information
Unwanted outcome	Unauthorised personnel get access to classified information.
Attack method	When the microphone is connected to a lower classified channel, and a person in the room (TA.USER) speaks higher classified information, then the information can be picked up by the microphone and transmitted on a lower classified channel than intended. The higher classified information is picked up from the lower classified channel by persons (TA.EXTERNAL) outside the physically protected area.

T.TEMPEST	Electromagnetic emanations may divulge classified information.
Threat agent	TA.EXTERNAL possibly in combination with TA.INTERNAL
Asset	Classified information
Unwanted outcome	Unauthorised personnel get access to classified information.
Attack method	Information on secure channels (i.e. classified information) is electromagnetically emanated onto a lower classified channel than intended. The higher classified information is picked up from the lower classified channels by persons (TA.EXTERNAL) outside the physically protected area.
T.UNAUTHORISED.USE	Authorised persons may perform unauthorised use of the operator position applications and management system inside the operation site.
Threat agent	TA.INTERNAL or TA.USER. In addition the following must be present TA.EXTERNAL.
Asset	Classified information
Unwanted outcome	Unauthorised personnel get access to classified information.
Attack method	Authorised persons may perform intentionally (TA.INTERNAL) or unintentionally (TA.USER) unauthorised use of the operator position applications and management system inside the operation site. The threat is that this may lead to transfer of higher classified information onto lower classified channels. The higher classified information is picked up from the lower classified channel by persons (TA.EXTERNAL) outside the physically protected area.
T.INFORMATION_LEAK	Classified information may be transferred to a lower classified channel than intended due to a network based attack.
Threat agent	TA.EXTERNAL
Asset	Classified information
Unwanted outcome	Unauthorised personnel get access to classified information.
Attack method	TA.EXTERNAL may carry out a network-based attack against a traffic interface or released objects in order to obtain AS.NON_RELEASABLE_INFORMATION.
T.OBJECT_TAMPERING	The integrity of the higher classified voice data objects (AS.NON_RELEASABLE_INFORMATION) may be modified such that they may be released to lower classified networks by means of the MVG.
Threat agent	TA.INTERNAL. In addition the following must be present TA.EXTERNAL.

Asset	Classified information
Unwanted outcome	Unauthorised personnel get access to classified information.
Attack method	TA.USER or TA_INTERNAL may modify security related information associated with AS.NON_RELEASABLE_INFORMATION to make the MVG release them. Example: A TA.USER that is not allowed to release information from the TOE via the MVG may append an invalid authentication tag to an information object to circumvent the MVG release policy.

3.4 Organisational security policies

P.COUPLING	Audio coupling of higher classified communications onto active lower classified channels at operator consoles shall be avoided in accordance with ref. [1], paragraphs 35 and 37.
P.ACCOUNTABILITY	The TOE shall provide the capability to make available information regarding the occurrence of security relevant events. The authorized subjects of the TOE shall be held accountable for their actions within the TOE.
P.CRYPTOGRAPHY	The TOE shall use approved and validated methods for cryptographic operations, (i.e. signature validation, and hashing.
P.MINIMAL_POSTURE	The Administrator shall ensure that only strictly required services and applications are running on the TOE.

4. SECURITY OBJECTIVES (ASE_OBJ)

4.1 TOE IT security objectives

O.ALARM.FAILURE	If a failure is detected in the TOE, the TOE shall raise an alarm to the MSM as well as a local alarm to the user.
O.CROSS-TALK	To prevent unacceptable acoustic cross-talk, the TOE shall ensure the following: • When using handset, higher classified channels shall be disconnected from the audio outputs when the voice transmission is activated and the microphone is connected to a lower classified channel to prevent unacceptable acoustic cross-talk of voice from higher classified channels to lower classified voice channels. • When using headset, it is assumed that it will provide sufficient attenuation to avoid the risk for crosstalk. Audio output remains active on headset ears even if headset mic is active on a lower level. • The microphone(s) shall be disconnected from lower classified channels when voice transmission is not activated. • The loudspeaker shall not be connected to higher classified (configurable) channels. Remark to the term “unacceptable acoustic cross-talk”: The headsets and the use of the headsets shall prevent unacceptable acoustic cross-talk between earpiece and microphone of the headsets. The TOE shall cover all other potential cases of acoustic cross-talk of voice from secure channels to non-secure voice channels via audio devices connected to the TOE.
O.SEC.ATTRIBUTES	The TOE shall ensure that only secure (valid) values are accepted for security attributes that are received from the environment.
O.SEC.NON-SEC	Only voice data destined for a lower security level shall be tagged according to the Security Indicator. This way the MVG can take the right decisions and avoid transfer of higher classified voice channels to lower classified voice channels. I.E. any information shall only be transmitted on an equal or higher classification level.
O.SELF.TEST	Security critical functions shall be tested by a combination of power-up tests, periodic tests and/or continuous tests.
O.TX.STATUS	The OCP user shall unambiguously be made aware whether the microphone is connected to a channel to a lower security level.
O.NEIGHBOUR	Each OCP user shall be made aware of ongoing transmissions to lower classification levels on the neighbouring OCPs.
O.AUDIT	The TOE shall create audit records of security relevant events and send these to the management system.

O.RECORDING	The TOE shall send selected transmitted and received audio channels to the centralised Voice Recorder.
O.TRAFFIC_DATA_INTEGRITY	The TOE shall validate the integrity of the received and transmitted audio. The TOE shall validate Authentication Tags.

4.2 Environment IT security objectives

OE.AUDIT	The security management system (MSM) will receive auditable events from the TOE (O.AUDIT) and provide facilities to securely store the audit data and present them for authorised management operators.
OE.MAN.ACCESS	Special authorisation is required to grant access to handle configuration and management of the MVS.
OE.MAN.ALARM	The security management system (MSM) shall receive alarms from the TOE and present them for the management operator.
OE.RECORDING	The audio stream from the OCP shall be recorded by a centralized recording system provided by the TOE environment.
OE.TIME_SOURCE	The TOE environment provides NTP time service.
OE.NETWORK	The TOE Environment will ensure the network and platforms used for the security domains are protected according to the sensitivity and integrity protection required for the information contained within the domains. The network and platforms shall protect MVT from unauthorised users and applications.
OE.SRTP_KEYS	The TOE environment (MSM) will generate and distribute SRTP keys to the TOE. The MSM uses approved and validated methods for cryptographic operations.

4.3 Environment non-IT security objectives

NOE.ACCESS.CTRL	Only authorised persons shall be given physical access to the MVS.
NOE.AUDIT	Authorised users of the audit facilities must ensure that the audit facilities are used and managed effectively. On particular, audit logs should be inspected on a regular basis, appropriate and timely action should be taken on the detection of breaches of security, or events that are likely to lead to a breach in the future. Also, the audit logs should be archived in a timely manner to ensure that the machine does not run out of audit log data storage space.
NOE.CLEARANCE	All OCP users shall have a minimum clearance and/or authorisation for the maximum-security level of information handled in the system.
NOE.INSTALL	The responsible for the TOE must ensure that the MVS including the TOE are installed accordingly to the installation guidelines for the MVS.
NOE.MAN.TRAIN	The MVS managers are fully trained to use and interpret the management application for the TOE.
NOE.NEIGHBOURS	Each OCP user shall be made aware of ongoing lower classified transmission on the neighbouring OCPs (O.NEIGHBOUR). Operational procedures, not technical solutions, shall regulate concurrent use of higher and lower classified conversations to prevent acoustic cross-talk of higher classified conversations to be transmitted on lower classified communication channels.
NOE.PHYS. PROT	The MVS site shall have physical protection sufficient for the security level of the information handled by the system.
NOE.USER.TRAIN	The OCP users are fully trained to use the MVS and interpret the security indications from the TOE.

4.4 Security objectives for the TOE rationale

Threats/ Assumptions / Objectives	P.COUPLING	P.ACCOUNTABILITY	P.CRYPTOGRAPHY	P.MINIMAL_POSTURE	T.CONN.SEC.NON-SEC	T.WRONG.SEC.IND	T.OBJECT_TAMPERING	T.INFORMATION_LEAK	T.ACOUSTIC.PICK-UP	T.TEMPEST	T.UNAUTHORISED.USE	A.MVT.ALARM	A.PHYSICAL	A.TRAINING	A.CLEARANCE	A.MAN.AUTHORISED	A.MVS.COM	A.USAGE	A.AUDIT	A.HARDENING
O.ALARM.FAILURE					x	x														
O.AUDIT		x									x									
O.CROSS-TALK	x				x				x											
O.TRAFFIC_DATA_INTEGRITY			x				x	x												
O.NEIGHBOUR									x											
O.RECORDING		x									x									
O.SEC.ATTRIBUTES											x									
O.SEC.NON-SEC	x		x		x															
O.SELF.TEST					x	x														
O.TX.STATUS						x														
OE.AUDIT		x									x								x	
OE.MAN.ACCES											x					x				
OE.MAN.ALARM					x							x								
OE.RECORDING		x									x									
OE.TIME_SOURCE		x																x		
OE.NETWORK				x	x		x			x			x							x
OE.SRTP_KEYS			x																	
NOE.ACCESS.CTRL								x					x		x					
NOE.AUDIT		x									x								x	
NOE.CLEARANCE															x					
NOE.INSTALL				x	x			x		x			x	x			x	x	x	x
NOE.MAN.TRAIN					x									x						
NOE.NEIGHBOURS									x											
NOE.PHYS.PROT								x					x							
NOE.USER.TRAIN					x	x					x			x						

Table 4-1 Mapping of Objectives to Threats and Assumptions

4.4.1 General

(1) As can be seen from Table 4-1, at least one objective, either TOE or environment, as applicable meets all threats and assumptions. The coverage of the threats and assumptions countered by the TOE is discussed in the subsections below.

4.4.2 P.COUPLING

(1) The TOE controls the separation of higher and lower classified information and the information flowing from the audio interfaces to/from the higher and lower classified networks (O.SEC.NON-SEC) via and by means of the MVG. The audio handling on the TOE will block higher classified information to the audio outputs, when there is a possibility that lower classified microphones may pick up classified information (O.CROSS-TALK).

4.4.3 P.ACCOUNTABILITY

(1) The TOE generates auditable events (O.AUDIT) to be received and recorded by the security management system (MSM) (OE_AUDIT, NOE_AUDIT). Such logged events may be used for later investigations into security incidents in the MVS. Auditable events are time tagged with a reliable time source (OE.TIME_SOURCE).

(2) The TOE will send selected transmitted and received audio channels to the centralised Voice Recorder (O.RECORDING, OE.RECORDING). Such recordings may be used for later investigations into security incidents in the MVS.

4.4.4 P.CRYPTOGRAPHY

(1) The TOE are using the following approved and validated methods for cryptographic operations:

- Hash-based Message Authentication Code (HMAC SRTP authentication), Keyed-Hashing for Message Authentication (for Authentication Tags) to ensure voice data integrity (O.TRAFFIC_DATA_INTEGRITY, O.SEC.NON-SEC).

(2) The TOE receives SRTP keys from the TOE environment (OE.SRTP_KEYS) by means of the MSM.

4.4.5 P.MINIMAL_POSTURE

(1) By running in a virtualized and hardened software architecture (OE.NETWORK) and by following the installation guidelines (NOE.INSTALL), ensures that only strictly required services and applications are running on the TOE and in the external services connected to the TOE.

4.4.6 T.CONN.SEC.NON-SEC

(1) The TOE is installed accordingly to the installation guidelines for the MVS (NOE_INSTALL), and operates on a sufficiently protected network and platforms (OE.NETWORK). It controls the separation of lower and higher classified information and the information flowing from the audio interfaces to/from the higher/lower classified networks (O.SEC.NON-SEC) via and by means of the MVG. The audio handling on the TOE will block higher classified information to the audio outputs, when there is a possibility that microphones connected to lower classified channels may pick up higher classified information (O.CROSS-TALK). The TOE will eliminate the threat that higher classified information can exist on the loudspeaker that could be picked up by microphones connected to lower classified channels (O.CROSS-TALK). A failing in domain separation will be detected during power-up and/or normal operation (O.SELF.TEST). A local alarm indication is given by detection of software failure (O.ALARM.FAILURE). The alarm is reported to the security management system (MSM) which will raise an alarm to the management operator (OE.MAN.ALARM). All users of MVS are fully trained to use, handle and interpret the MVS equipment (NOE.USER.TRAIN), (NOE.MAN.TRAIN).

4.4.7 T.WRONG.SEC.IND

(1) The OCP user shall always have a clear indication whether the microphone is connected to a channel to a lower security level (O.TX.STATUS). If voice data is sent from a module which is not according to the security indicator to the OCP user (O.SELF.TEST), the TOE will block the signals from the microphone to the non-secure network. A local alarm is always given by detection of software failure (O.ALARM.FAILURE). All OCP users are fully trained in the correct use and interpretation of the TOE (NOE.USER.TRAIN).

4.4.8 T.OBJECT_TAMPERING

(1) The TOE prevents object tampering attacks through use of Authentication Tags (O.TRAFFIC_DATA_INTEGRITY).

(2) When the TOE is connected to security domains that do not provide integrity protection of information objects, it is the responsibility of the TOE Environment to offer the appropriate protection (OE.NETWORK).

4.4.9 T.INFORMATION_LEAK

(1) Information leaks are mitigated through a compartmentalized TOE implementation. Audio data are protected against modification through authentication tags (O.TRAFFIC_DATA_INTEGRITY). Further, the TOE Environment ensures the configuration is correct (NOE.INSTALL, NOE.ACCESS.CTRL, NOE.PHYS.PROT).

4.4.10 T.ACOUSTIC.PICK-UP

(1) When there is a possibility that microphones connected to lower classified channels on the TOE may pick up higher classified information (O.CROSS-TALK), the audio handling on the TOE will block higher classified information to the audio outputs,. The TOE will eliminate the

threat that higher classified information can exist on the loudspeaker that could be picked up by microphones connected to lower classified channels (O.CROSS-TALK). To prevent acoustic pick up from neighbouring OCP users, each OCP user is made aware of ongoing lower classified transmission on the neighbouring OCPs (O. NEIGHBOUR, NOE.NEIGHBOURS). The TOE will minimise the risk that microphones connected to lower classified channels can pick up higher classified information by blocking the microphone when not used (O.CROSS-TALK).

4.4.11 T.TEMPEST

(1) Depending on the installation environment, following the installation guidelines (NOE.INSTALL, OE.NETWORK), the TOE SW may be required to run in TEMPEST approved hardware implementations avoiding electromagnetic leakage of classified information from the TOE.

4.4.12 T.UNAUTHORISED.USE

(1) Users need special authorisation to handle the configuration and management part of the MVS (OE.MAN.ACCES), and received security attributes are checked by the TOE (O.SEC.ATTRIBUTES). The voice from the OCP will be recorded (O.RECORDING , OE.RECORDING) and actions being logged (O.AUDIT, OE.AUDIT, NOE.AUDIT) such that unauthorised use can be exposed. All OCP users are fully trained in the correct use and interpretation of the TOE (NOE.USER.TRAIN).

4.4.13 A.MVT.ALARM

(1) The TOE Environment provide an MSM instance for collecting and handling alarms (OE.MAN.ALARM).

4.4.14 A.PHYSICAL

(1) The MVS including the TOE must be installed accordingly to the installation guidelines (NOE.INSTALL, OE.NETWORK). Only authorised persons shall be given physical access to the MVS (NOE.ACCESS.CTRL). The TOE must be installed in a physical protected area, minimum approved for the highest security level of information handled in the system (NOE.PHYS.PROT).

4.4.15 A.TRAINING

(1) All users of MVS are fully trained to use, handle and interpret the MVS equipment (NOE.USER.TRAIN), (NOE.MAN.TRAIN). The technicians should be trained to install the MVS including the TOE accordingly to the installation guidelines (NOE.INSTALL).

4.4.16 A.CLEARANCE

(1) Only authorised persons shall be given physical access to the MVS (NOE.ACCESS.CTRL). All OCP users have the minimum clearance and/or authorisation for the maximum-security level of information handled in the system (NOE.CLEARANCE).

4.4.17 A.MAN.AUTHORISED

(1) Special authorisation is required to grant access to handle configuration and management of the MVS (OE.MAN.ACCESS).

4.4.18 A.MVS.COM

(1) The MVS including the TOE must be installed accordingly to the installation guidelines (NOE.INSTALL).

4.4.19 A.USAGE

(1) The MVS including the TOE must be installed accordingly to the installation guidelines (NOE.INSTALL, OE.TIME_SOURCE).

4.4.20 A.AUDIT

(1) All audit data is stored in a secure way and authorised users ensures that the logs are maintained and inspected on a regular basis, and ensures that proper action is taken on any breaches of security (OE.AUDIT, NOE.AUDIT). The audit functionality is put outside the TOE (NOE.INSTALL).

4.4.21 A.HARDENING

(1) The TOE is running in a virtualized and hardened software architecture to meet general requirements for Cyber security (NOE.INSTALL, OE.NETWORK).

5. EXTENDED COMPONENTS DEFINITION (ASE_ECD)

(1) The following explicit components have been included in this Security Target because the Common Criteria components were found to be unsuitable as stated.

5.1 Explicit Functional Components

Explicit Component	Identifier	Rationale
FAU_GEN_EXT.1	Audit data generation	This extended component is necessary to describe that the TOE does not produce auditable events at start-up and shutdown of the audit functions.

6. SECURITY REQUIREMENTS (ASE_REQ)

6.1 General

(1) This section contains the functional requirements that are provided by the TOE and the IT environment. These requirements consist of functional components from Part 2 of the Common Criteria (CC), extended with explicitly stated requirements.

6.2 TOE Security Functional Requirements

6.2.1 Security audit

FAU_ARP.1(1)	**Security alarms**
FAU_ARP.1.1(1)	The TSF shall take [assignment: *an action to raise a local alarm*] upon detection of a potential security violation.
	Dependencies: FAU_SAA.1
FAU_ARP.1(2)	**Security alarms**
FAU_ARP.1.1(2)	The TSF shall take [assignment: *an action to raise an alarm to the security management system (MSM)*] upon detection of a potential security violation.
	Dependencies: FAU_SAA.1

6.2.2 Audit data generation

FAU_GEN_EXT.1	**Audit data generation**
FAU_GEN_**EXT**.1.1	The TSF shall be able to generate an audit record of the following auditable events: a) None; b) All auditable events for the [selection: *not specified*] level of audit. c) [assignment: *All auditable events listed in Table 6-1* and *Voice streams sent to central voice data recorder if recording has been enabled*]
FAU_GEN_**EXT**.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, [assignment: *none*].
	Dependencies: FPT_STM.1

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN_EXT.1	None	None
FAU_ARP.1	Minimal: Actions taken due to potential security violations.	Relevant metadata
FCS_COP.1	Minimal: Success and failure, and the type of cryptographic operation.	Relevant metadata
FTP_ITC.1	Minimal: Failure of the trusted channel functions. Minimal: Identification of the initiator and target of failed trusted channel functions.	Relevant metadata.
FPT_TDC.1	Basic: Detection of modified TSF data.	Relevant metadata
FDP_IFC.2	None	None
FDP_IFF.1	None	None
FMT_MOF.1	Basic: All modifications in the behaviour of the functions in the TSF.	Relevant metadata
FMT_MSA.1	Basic: All modifications of the values of security attributes.	Relevant metadata
FMT_MSA.2	Minimal: All offered and rejected values for a security attribute.	Relevant metadata
FMT_MSA.3	Basic: All modifications of the initial values of security attributes.	Relevant metadata
FPT_FLS.1	Basic: Failure of the TSF.	Relevant metadata
FPT_TST.1	Basic: Execution of the TSF self tests and the results of the tests.	None
FTP_TRP.1	None	None

Table 6-1 Auditable events

6.2.3 Cryptographic support

FCS_COP.1	Cryptographic operation (cryptographic hashing)
FCS_COP.1.1	The TSF shall perform [assignment: *cryptographic hashing services*] in accordance with a specified cryptographic algorithm [assignment: *SHA-256*] and cryptographic key sizes [assignment: *message digest sizes 256 bits (truncated to the first 10 bytes)*] that meet the following: [assignment: *FIPS PUB 180-4 [FIPS-180*].

	Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4.

6.2.4 Inter-TSF trusted channel

FTP_ITC.1	**Inter-TSF trusted channel**
FTP_ITC.1.1	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit [selection: *the TSF*] to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for [assignment: *sending/receiving voice data to/from MVG,* *SRTP Authentication Tag is generated and added to the transmitted audio stream, and verified according to the security level of the received audio stream.* *All audio streams are handled according to the defined security level* *Received audio packets without an Authentication Tag are assigned the highest security level*].
	Dependencies: (none)

6.2.5 Protection of the TSF

FPT_TDC.1	**Inter-TSF basic TSF data consistency**
FPT_TDC.1.1	The TSF shall provide the capability to consistently interpret [assignment: *SRTP Authentication Tags*] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2	The TSF shall use [assignment: *rules defined for the communication channel (RFC3711 SRTP)*] when interpreting the TSF data from another trusted IT product.
	Dependencies: (none)

6.2.6 User data protection

FDP_IFC.2	**Complete Information Flow Control**

FDP_IFC.2.1	The TSF shall enforce the [assignment: *information flow control SFP*] on [assignment: *the following subjects:* • *TOE higher classified domain functions and* • *TOE lower classified domain functions* *for the following information:* • *potentially higher classified audio streams and* • *lower classified audio streams*] and all operations that cause that information to flow to and from subjects covered by the SFP. Note: The TOE *information flow control SFP* includes the policy statement to reject unacceptable messages attempted transmitted from the higher classified domain to lower classified channels, thus potentially to lower classified domains via the MVG.
FDP_IFC.2.2	The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.
	Dependencies: FDP_IFF.1
FDP_IFF.1	**Simple security attributes (information flow control)**
FDP_IFF.1.1	The TSF shall enforce the [assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: Subjects : Incoming Audio streams, Outgoing Audio stream Attributes : Current Security Level, Incoming Streams' Security Level].
FDP_IFF.1.2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: Audio from a security level higher than a configurable (system parameter) threshold *is not sent to loudspeaker/handset*].
FDP_IFF.1.3	The TSF shall enforce [assignment: *the following rule: Audio is only transmitted when explicitly activated by the operator (PTT)*].
FDP_IFF.1.4	The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *stated in the information flow control SFP*].
FDP_IFF.1.5	The TSF shall explicitly deny an information flow based on the following rules: [assignment: *none*].
	Dependencies: FDP_IFC.1, FMT_MSA.3

6.2.7 Security management

FMT_MOF.1	**Management of security functions behaviour**
FMT_MOF.1.1	The TSF shall restrict the ability to [selection: *determine the behaviour of*] the function [assignment: *security alarms*] to [assignment: *the MSM*].
	Dependencies: FMT_SMR.1, FMT_SMF.1

FMT_MSA.1	**Management of security attributes**
FMT_MSA.1.1	The TSF shall enforce the [assignment: *none*] to restrict the ability to [selection: *modify*] the security attributes [assignment: *shown in Table 6-2*] to [assignment: *the roles shown in the table*].
	Dependencies: [FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1
FMT_MSA.2	**Secure security attributes**
FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for [assignment: *security attributes*].
	Dependencies: [FDP_ACC.1 or FDP_IFC.1], FMT_MSA.1, FMT_SMR.1
FMT_MSA.3	**Static attribute initialization**
FMT_MSA.3.1	The TSF shall enforce the [assignment: *information flow control SFP*] to provide [selection: *restrictive*] default values for security attributes that are used to enforce the *SFP*.
FMT_MSA.3.2	The TSF shall allow the [assignment: *none*] to specify alternative initial values to override the default values when an object or information is created.
	Dependencies: FMT_MSA.1, FMT_SMR.1

Security attribute	Role	Access
Transmission security status The status shall specify whether the microphone is connected to a non-secure channel.	OCP user	Read, write
Available security levels The allowed security classifications to be used in the OCP	MSM (*)	Read, write
SRTP Master Key	MSM (*)	Read, write
Loudspeaker max security level	MSM (*)	Read, write
Handset RX/TX max security level	MSM (*)	Read, write

Table 6-2 Management of user security attributes

(* Configuration is managed centrally by the MLS Security Management)

6.2.8 Protection of the TOE Security Functions

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: [assignment: *single point failures*].
	Dependencies: (none)
FPT_TST.1	**TSF self test**
FPT_TST.1.1	The TSF shall run a suite of self tests [selection: *during initial start-up, periodically during normal operation,* at the conditions [assignment: at regular intervals]] to demonstrate the correct operation of [selection: *the TSF*].
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of [assignment: *none*].
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of [selection: *TSF*].
	Dependencies: (none)

6.2.9 Trusted path

(1) This section specifies the trusted path/channels of the TOE.

FTP_TRP.1(1)	**Trusted Path**
FTP_TRP.1.1(1)	The TSF shall provide a communication path between itself and [selection: *local*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [assignment: *modification, disclosure*]. (Note: OCP users are local users.)
FTP_TRP.1.2(1)	The TSF shall permit [selection: *the TSF, local users*] to initiate communication via the trusted path. (Note: OCP users are local users.)
FTP_TRP.1.3(1)	The TSF shall require the use of the trusted path for [selection: [assignment: *security indications]*].
	Dependencies: (none)
FTP_TRP.1(2)	**Trusted Path**
FTP_TRP.1.1(2)	The TSF shall provide a communication path between itself and [selection: *remote*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [selection: *modification*, [assignment: *none*]].

FTP_TRP.1.2(2)	The TSF shall permit [selection: *the TSF*, *remote users*] to initiate communication via the trusted path.
FTP_TRP.1.3(2)	The TSF shall require the use of the trusted path for [selection: [assignment: *protection of SRTP audio streams*]].
	Dependencies: (none)

6.3 TOE security assurance requirements

(1) The assurance level of the TOE is EAL4 augmented with ALC_FLR.3 (*) Systematic flaw remediation. The assurance components are summarised in Table 6-3.

Assurance class	Assurance component name	Assurance family
ADV: Development	Security architecture description	ADV_ARC.1
	Complete functional specification	ADV_FSP.4
	Implementation representation of the TSF	ADV_IMP.1
	Basic modular design	ADV_TDS.3
AGD: Guidance documents	Operational user guidance	AGD_OPE.1
	Preparative procedures	AGD_PRE.1
ALC: Life-cycle support	Production support, acceptance procedures and automation	ALC_CMC.4
	Problem tracking CM coverage	ALC_CMS.4
	Delivery procedures	ALC_DEL.1
	Identification of security measures	ALC_DVS.1
	Systematic flaw remediation	ALC_FLR.3 (*)
	Developer defined life-cycle model	ALC_LCD.1
	Well-defined development tools	ALC_TAT.1
ASE: Security Target evaluation	Conformance claims	ASE_CCL.1
	Extended components definition	ASE_ECD.1
	ST introduction	ASE_INT.1
	Security objectives	ASE_OBJ.2
	Derived security requirements	ASE_REQ.2
	Security problem definition	ASE_SPD.1
	TOE summary specification	ASE_TSS.1
ATE: Tests	Analysis of coverage	ATE_COV.2
	Testing: basic design	ATE_DPT.1

	Functional testing	ATE_FUN.1
	Independent testing - sample	ATE_IND.2
AVA: Vulnerability assessment	Focused vulnerability analysis	AVA_VAN.3

Table 6-3 Security assurance requirement

EAL4 is considered appropriate for the TOE when placed in an operational environment with the properties and policies described by the security problem definition. The security problem definition has been selected to apply to operational environments for classified networked information systems in military organizations.

The ALC_FLR.3 component has been included to provide assurance for the developer's procedures for handling and patching security flaws discovered in the TOE.

6.4 Security requirements rationale

6.4.1 Requirements are appropriate

(1) The table below identifies which SFRs satisfy which Objectives

Requirement / Objectives	FAU_ARP.1(1)	FAU_ARP.1(2)	FAU_GEN_EXT.1	FCS_COP.1	FTP_ITC.1	FPT_TDC.1	FDP_IFC.2	FDP_IFF.1	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FPT_FLS.1	FPT_TST.1	FTP_TRP.1
O.ALARM.FAILURE	x	x													
O.CROSS-TALK							x	x							
O.SEC.ATTRIBUTES								x	x	x	x	x			
O.SEC.NON-SEC	x	x			x	x	x						x	x	
O.SELF.TEST													x	x	
O.TX.STATUS							x	x							x
O.NEIGHBOUR															x
O.AUDIT			x												
O.RECORDING			x												
O.TRAFFIC_DATA_INTEGRITY				x	x	x									

Table 6-4: Mapping of Objectives to SFRs

(2) As it can be seen in Table 6-4 all objectives are satisfied by at least one SFR and all SFRs are required to meet at least one objective.

O.ALARM.FAILURE

The TOE will raise an alarm indication locally (FAU_ARP.1(1) and to the MSM (FAU_ARP.1(2)) if a TOE software failure is detected.

O.CROSS-TALK

The TSF shall enforce flow control (FDP_IFC.2) to avoid information leak from the higher classified channels to lower classified channels, including forwarding of received audio towards loudspeaker/handset according to security level (FDP_IFF.1).

O.SEC.ATTRIBUTES

The transmission security status is interpreted by the TOE (FDP_IFF.1), while configurable TSF data is validated by the TOE (FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3)

O.SEC.NON-SEC

The TOE enforces the flow control policies for information to prevent unintended disclosure of information (FTP_ITC.1, FPT_TDC.1, FDP_IFC.2). The TOE maintains a secure state during

operation (FPT_FLS.1, FPT_TST.1). Potential security issues are audited (FAU_ARP.1(1), FAU_ARP.1(2)).

O.SELF.TEST

The TOE performs self tests (FPT_TST.1) and preserves a secure state should a fault be detected (FPT_FLS.1).

O.TX.STATUS

The TOE presents the correct security status to the OCP user, to prevent users from talking classified to non-secure channels (FDP_IFC.2, FDP_IFF.1). The TOE gives the OCP user an unambiguous indication of whether the microphone is connected to channels with lower security level (FTP_TRP.1).

O.NEIGHBOUR

The TOE gives neighbour security status which is used to inform the operator about possible low security microphone connections on the operator positions defined to be neighbours (FTP_TRP.1).

O.AUDIT

The Objective is directly fulfilled by FAU_GEN_EXT.1.

O.RECORDING

The Objective is directly fulfilled by FAU_GEN_EXT.1.

O.TRAFFIC_DATA_INTEGRITY

The TOE implements a hashing and validation mechanism (FCS_COP.1) to provide and verify SRTP authentication tags in audio streams. The TOE ensures the correct authentication tags are added to outgoing traffic according to the active security level (FTP_ITC.1, FPT_TDC.1).

6.4.1.1 Security Functional Requirements vs. Objectives

FAU_ARP.1(1) Security alarms

(1) The TOE will raise a local alarm indication if a TOE software failure is detected (O.ALARM.FAILURE). A failure that is reported may compromise the secure/non-secure protection (O.SEC.NON-SEC).

FAU_ARP.1(2) Security alarms

(2) The TOE will raise an alarm to the MSM if a TOE software failure is detected (O.ALARM.FAILURE). The TOE will transmit the alarm to the MSM. A failure that is reported may compromise the secure/non-secure protection (O.SEC.NON-SEC).

FAU_GEN_EXT.1 Audit data generation

(3) The TOE will send auditable events (O.AUDIT) to the security management system (MSM). The MSM will receive auditable events from the TOE and provide facilities to securely store the audit data and present them for authorised management operators.

(4) The TOE will record audio channels to a centralised Voice Recorder (O.RECORDING). Such recordings may be used for later investigations into security incidents.

FCS_COP.1 Cryptographic operation (cryptographic hashing)

(5) The TOE implements integrity protection for information objects using hashing of the information objects using approved cryptographic algorithms (O.TRAFFIC_DATA_INTEGRITY).

FTP_ITC.1 Inter-TSF trusted channel

(6) The TOE provides trusted channel to MVG for transfer of voice data according to the classification defined by the security indication presented to the user by the TOE; i.e. audio is not transmitted on channels with lower security level than displayed by the security indication (O.TRAFFIC_DATA_INTEGRITY, O.SEC.NON-SEC).

FPT_TDC.1 Inter-TSF basic TSF data consistency

(7) The TOE marks transmitted audio streams with Authentication Tags according to the displayed security level such that the MVG securely can make decisions on whether data can pass to certain lower security levels (O.TRAFFIC_DATA_INTEGRITY, O.SEC.NON-SEC).

(8) The TOE checks Authentication Tags in received audio streams to ensure proper actions allowed for the authenticated security level (O.TRAFFIC_DATA_INTEGRITY, O.SEC.NON-SEC).

FDP_IFC.2 Complete information flow control

(9) The TOE has complete information flow control that controls all information flow. The information flow control prevents higher classified information to be transferred to lower classified channels (O.SEC.NON-SEC) via and by means of the MVG. Unacceptable acoustic cross-talk is prevented by controlled forwarding of received audio to loudspeaker and handset, and blocking of audio microphones when no active transmission (O.CROSS-TALK). The TOE gives correct security status, which prevents the user to talk classified on non-secure channels (O.TX.STATUS). The Traffic_Data information flow control policy regulates how the TOE shall maintain the network separation security policy. The SFP is defined by FDP_IFC.2 and FDP_IFF.1.

FDP_IFF.1 Simple security attributes (information flow control)

(10) The transmission security status is a security attribute (O.SEC.ATTRIBUTES) that controls the information flow (O.TX.STATUS, O.CROSS-TALK).

FMT_MOF.1 Management of security functions behaviour

(11) The TOE receives security parameters according to Table 6-2 (O.SEC.ATTRIBUTES) from the MSM.

FMT_MSA.1 Management of security attributes

(12) The validity of security attributes received from the MSM, are checked by the TOE (O.SEC.ATTRIBUTES).

FMT_MSA.2 Secure security attributes

(13) The TOE checks that the security attributes are secure (O.SEC.ATTRIBUTES).

FMT_MSA.3 Static attribute initialisation

(14) The default values for security attributes shall be restrictive (O.SEC.ATTRIBUTES).

FPT_FLS.1 Failure with preservation of secure state

(15) The TOE is designed to fail in a safe manner. This includes failure during self test (O.SELF.TEST, O.SEC.NON-SEC).

FPT_TST.1 TSF Self Test

(16) Security critical functions will be tested by a combination of power-up tests, periodic tests, and/or continuous tests (O.SELF.TEST). A failure detected during this test, may compromise the secure/non-secure protection (O.SEC.NON-SEC).

FTP_TRP.1 Trusted path

(17) The TOE gives the OCP user an unambiguous indication of whether the microphone is connected to a non-secure channel (O.TX.STATUS). The TOE gives neighbour security status which is used to inform the operator about possible low security microphone connections on the operator positions defined to be neighbours (O.NEIGHBOUR).

6.4.2 Security dependencies are satisfied

(1) The table below shows a mapping of Functional Components to their dependencies.

Functional Component	Dependency	Included	Comments
TOE Security Functional Requirements			
FAU_ARP.1(1)	FAU_SAA.1	NO	Note 2) below
FAU_ARP.1(2)	FAU_SAA.1	NO	Note 2) below
FAU_GEN:_EXT.1	FPT_STM.1	NO	Note 6) below
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	NO	Note 7) below
	FCS_CKM.4	NO	Note 5) below

FTP_ITC.1	None	YES	
FPT_TDC.1	None	YES	
FDP_IFC.2	FDP_IFF.1	YES	
FDP_IFF.1	FDP_IFC.1	YES	Note 1) below
	FMT MSA.3	YES	
FMT_MOF.1	FMT_SMR.1	NO	Note 3) below
	FMT_SMF.1	NO	Note 4) below
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	YES	Note 1) below
	FMT_SMF.1	NO	Note 4) below
	FMT_SMR.1	NO	Note 3) below
FMT_MSA.2	FDP_IFC.1	YES	Note 1) below
	FMT_MSA.1	YES	
	FMT_SMR.1	NO	Note 3) below
FMT_MSA.3	FMT_MSA.1	YES	
	FMT_SMR.1	NO	Note 3) below
FPT_FLS.1	None		
FPT_TST.1	None		
FTP_TRP.1	None		

Table 6-5: Security Requirements dependencies

Note 1: FDP_IFC.1 is covered by FDP_IFC.2 which is included.

Note 2: Basic threshold detection for security audit analysis purposes is covered in the Voice Application (required non-TOE SW).

Note 3: The TOE does not recognize any security roles, role functionality are handled by the Voice Application (required non-TOE SW).

Note 4: FMT_MOF.1 and FMT_MSA.1 have a dependency to FMT_SMF.1 which is not included as it is part of the Voice Application SW, ref. 1.4.3.

Note 5: Key destruction is not relevant as FCS_COP.1 covers hashing only. Keys and signing operations are handled by the TOE environment.

Note 6: Timestamps are provided by the TOE Environment through OE.TIME_SOURCE.

Note 7: TOE does not generate keys, it uses those received from the environment (MSM) (OE.SRTP_KEYS).

6.4.3 SAR rationale

The baseline SARs specified in this ST are according to EAL4. The ALC_FLR.3 component has been included to provide assurance for the developer's procedures for handling and patching security flaws discovered in the TOE.

7. TOE SUMMARY SPECIFICATION (ASE_TSS)

7.1 TOE security functions

This describes the security functions provided by the TOE to meet the security functional requirements specified for the TOE in chapter 6.2.

7.1.1 Security functions list

This section is left blank intentionally.

7.1.2 SF.Security.Alarm

(1) The TOE will raise a local alarm indication, and raise an alarm to the security management system, MSM (required non-TOE SW) in the following situation:

a) A potential security violation in the TOE

(2) Alarms are time-stamped by the security management system (MSM).

7.1.3 SF.Information.Flow.Control

(1) The information flow control provides flow control between the user interfaces and the secure partitions in the TOE and information flow control between the secure and non-secure network via and by means of the MVG. The flow control rules are based on:

a) When there is a possibility that non-secure microphones may pick up from secure sources, the audio handling on the TOE will block secure audio to the audio devices.

b) The TOE will prevent the microphones to be connected to the non-secure network (via and by means of the MVG) by tagging SRTP audio packets. Only voice data destined for a lower security level shall be tagged according to the Security Indicator.

7.1.4 SF.Security.Management

(1) The TOE can receive the following security management information:

a) Allowed security levels to use on OCP

b) Set SRTP authentication keys

c) Voice rules for loudspeaker and handset (maximum security level to monitor)

7.1.5 SF.Self.Test

(1) The testing of TOE will detect errors in the security critical functions on the TOE and it will detect security indication errors. If a failure is detected in the TOE, an alarm is generated and the TOE is halted if required.

7.1.6 SF.Fail.Secure

(1) The most serious violation of the TSF is that higher classified voice or data on the secure network is sent on a lower classified channel. The following measures shall prevent this to happen as a result of TOE-failures:

a) The TOE is designed to handle single failures without violating the trusted functionality. If the TOE fails, it will fail in a safe manner.

b) The audio part of TOE is designed in such a way that the trusted functionality in TOE do not rely on any other modules in the OCP. TOE informs the OCP user directly of whether the microphone is connected to a lower classified channel.

7.1.7 SF.Trusted.Path

(1) The TOE provides a trusted path between itself and the OCP user for security indication.

7.1.8 SF.Audit.Generation

(1) The TOE generates auditable events and security audit logs to the security management system (MSM) as well as sending audio streams to a centralised voice recorder.

7.1.9 SF.Trusted.Voice.Stream

(1) By means of cryptographic methods and non-repudiation services, the TOE will ensure data consistency and integrity by creating trusted channels across the network towards the MVGs to convey voice data on different separated security levels.

7.2 TOE summary specification rationale

The table below shows how TOE Security Functions satisfy SFRs.

TOE Security functions	SFRs	Description
SF.Security.Alarm	FAU_ARP.1(1), FAU_ARP.1(2)	The TOE security alarm function will raise security alarms automatically upon a potential security violation detected (FAU_ARP.1(2), FAU_ARP.1(1)).
SF.Information.Flow.Control	FDP_IFC.2, FDP_IFF.1	The TOE information flow control controls all information flows (FDP_IFC.2) determined by the transmission security status (FDP_IFF.1).
SF.Security.Management	FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3	The TOE security management function has a mode of operation as installation parameter (FMT_MOF.1) and receives security configuration from the management system (FMT_MSA.1). These values are validated (FMT_MSA.2) and the default values are restrictive (FMT_MSA.3).
SF.Fail.Secure	FPT_FLS.1	The fail secure function preserves a secure state after failure.
SF.Self.Test	FPT_TST.1	The TOE self test function performs an underlying testing of the TOE.
SF.Trusted.Path	FTP_TRP.1	The TOE has trusted path/channels to the OCP user to ensure that the OCP user unambiguously is made aware whether the microphone is connected to a non-secure channel. The microphone is directly connected to the TSF. The OCP user is also made aware of ongoing lower classified transmission on the neighbouring OCPs.
SF.Audit.Generation	FAU_GEN_EXT.1	Generation of audit record of auditable events in the TOE as well as sending selected audio-data for central recording outside the TOE.
SF.Trusted.Voice.Stream	FCS_COP.1, FPT_TDC.1, FTP_ITC.1,	By means of cryptographic methods (FCS_COP.1) ensuring data consistency and integrity (FPT_TDC.1), creating trusted channels (FTP_ITC.1) across the network to MVG, for the purpose of interchanging voice data (by means of the MVG) with different separated security levels to and from the TOE.

Table 7-1: TOE Security Functions satisfy SFRs

8. NOTES

8.1 Acronyms and Abbreviations

CC	Common Criteria
EAL	Evaluation Assurance Level
HMI	Human Machine Interface
HW	Hardware
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
MLS	Multi Level Security
MSM	MLS Security Management
MVG	MLS Voice Guard
MVP	MLS Voice Platform
MVS	MLS Voice System
MVT	MLS Voice Terminal
OCP	Operator Controller Position
PTT	Push To Talk
RTP	Real Time Protocol
SAR	Security Assurance Requirements
SFP	Security Function Policies
SFR	Security Functional Requirement(s)
SIP	Session Initiation Protocol
SMA	Site Management Application
SRS	Software Requirements Specification
SRTP	Secure RTP (Real Time Protocol)
ST	Security Target
STT	Step To Talk
SW	Software
TOE	Target of evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TX	Transmission (outgoing audio)
VoIP	Voice over IP

8.2 Definitions

Classified and Unclassified information	Classified information is information regarded as sensitive by the security authorities for the owners of the system that comprises the TOE. Sensitive information is information that these security authorities determine must be protected because its unauthorised disclosure will cause perceivable damage. In describing information, channels, networks, etc., the use of the terms; «classified» / «unclassified», “secure” / “non-secure” and “red” / ”black”, are generic relative representations of two different classification levels where the former is considered a higher classification than the latter.
Operator Controller Position (OCP)	The Operator Controller Position is typically a panel PC hosting the Voice Application, the MVT and is directly connecting to the audio accessories (headset, handset, PTT, STT, speakers) via USB interfaces.
Voice Application	Required SW implementing the application specific part of the OCP that implements the business logic not subject to security certification. It requires the MVT (and MVP) as a platform for secure voice handling. There might be application specific parts of SW also in the MVG
Authentication Tag	The SRTP traffic is tagged with Authentication Tags based on the pre-placed master keys, one for each security level and traffic type. Traffic types: • Radio and Loop RX (multicast) • Radio TX • Telephone RX/TX