MLS Voice Guard (MVG)
1.1.1
Security Target

Classification	Document Title	Radical – Business Id	Revision	DTC	Language	Entity Cage Code	Thales Cage Code	PAGE
UNCLASSIFIED	**MLS Voice Guard (MVG)** **Security Target**	**3AQ 32626 AAAB**	**006-lite**	**938**	**EN**	**N4244**	**0026**	**1 of 45**

DOCUMENT CHANGE HISTORY

Revision	Date	Description
006	15.12.2023	Official document version for CC evaluation.
006-lite	2.02.2024	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
Written by	SE Team	CHTE	CHTE	CHTE/HS	HS	HS	HS
Checked by	QA Manager	-	TTA	TTA	TTA	TTA	TTA
Approved by	PDA	ES	ES	ES	ES	ES	ES

Table of Contents

List of Figures

List of Tables

Foreword

This document is the Security Target for the Thales MLS Voice Guard (MVG). The document describes the operating environment and IT product requirements, as well as security functionality implemented in the IT product.

Contact information:

THALES Norway AS
Postboks 744 Sentrum
0106 Oslo
Norway

Telephone:	*(+47) 22 63 83 00*
E-Mail:	*info@thales.no*
Internet:	*http://www.thales.no*

Copyright notice:

All rights are reserved. No part of this document may be photocopied, reproduced, transmitted, translated to another language or stored in any retrieval form without the express written permission of THALES Norway AS.

THALES Norway AS has made every attempt to ensure that the information in this document is correct and complete. However, THALES Norway AS assumes no liability for errors, or for any damage that may result from the use of this document or any product that it accompanies.

1. SECURITY TARGET INTRODUCTION (ASE_INT)

1.1 SECURITY TARGET REFERENCE

Title:	Security Target for the Thales MLS Voice Guard
Version:	See front page
Date:	See front page
Document id:	See page footer

1.2 TOE REFERENCE

TOE Name	MLS Voice Guard
TOE Version	1.1.15
TOE Assurance Level	EAL4 augmented with ALC_FLR.3 and AVA_VAN.4
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 32626	<A-Z . A-Z . A-Z>	<A-Z>	x.x.x

Example: 3AQ 32626 AAAB 1.1.15

1.3 REFERENCED DOCUMENTS

[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).
[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).
[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).
[FIPS-180]	FIPS PUB 180-4 Secure Hash Standard, NIST, August 2015
[MVT-ST]	Thales MLS Voice Terminal Security Target, Thales Norway AS, 2022
[SIP]	SIP: Session Initiation Protocol, IETF, June 2002
[SRTP]	RFC 3711 Secure Real-time Transport Protocol, IETF, July 2003

1.4 TOE OVERVIEW

The Thales MLS Voice Guard (MVG) is part of the Thales MLS Voice Platform for use in military and mission critical environments. The Thales MVG provides voice connectivity, including signalling traffic, between two connected networks with different security levels. The high security level network contains all operator positions within the MVP, and one or more MVGs provide connectivity towards lower security level networks. The MLS Voice Guard provides a trusted information flow control mechanism for VoIP audio streams (RTP/SRTP), as well as signalling for call management (SIP), radio control, and SNMP.

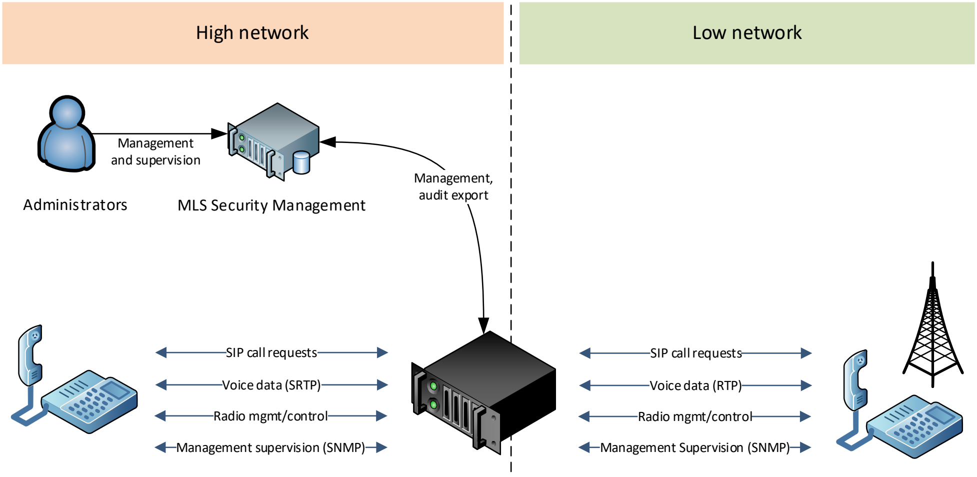

Figure 1-1: TOE high level view

1.4.1 MAJOR SECURITY FEATURES OF THE TOE

The primary purpose of the MVG is to enforce an information flow policy between two security domains. The MVG enforces the defined information flow policy on signalling traffic and voice data streamed between the connected networks.

The MVG provides the following main security features:

Security features	Relevant security functions
Controlled data flow	SF.FILTER SF.STREAM_AUTHENTICATION
Tamper proof and non-bypassable security functions	SF.INTERNAL_PARTITIONING, SF.SELF_TEST
Domain isolation with covert channel mitigation	SF.DOMAIN_ISOLATION, SF.FILTER SF.TRAFFIC_ANALYSIS
Audit logs	SF.AUDIT
Secure configuration, management and supervision	SF.SECURE_STATE, SF.CONFIGURATION
Call setup and packet flow management	SF.FILTER
Stream packet filtering	SF.SRTP_AUTHENTICATION

Table 1-1: TOE security features

The security checks are supported by non-bypassable and self-protecting security functions that ensure the security checks are performed in a controlled and predictable way. This platform separates different parts of the TOE from each other to minimize the chance of interference between processed signalling traffic, and between functions of different criticality. A dedicated information flow control mechanism further restricts internal communication between the different parts of the TOE.

Auditing is performed to allow administrators of the MVG to observe its security performance and to track security relevant events.

The MVG is furthermore designed to maintain a secure state, including controlled start-up and transition between operating states. Self-testing allows verification of the system's operational state and integrity of its configuration.

1.4.2 REQUIRED NON-TOE HARDWARE, SOFTWARE AND FIRMWARE

1.4.2.1 Third party services

The TOE requires the following non-TOE services:

- NTP Server

1.4.2.2 MLS Security Management (non-TOE)

The TOE is configured via the High LAN through the MLS Security Management (MSM) application, used for the management of all MLS Voice Guards (TOE) and MLS Voice Terminals (MVTs) within an MLS Voice Platform.

1.4.2.3 Operator Controller Position (non-TOE)

The Operator Controller Position (OCP) provides the user interface to end users of the MLS Voice System. The MVG relies on the MVT to correctly tag SRTP packets as specified in the MVT Security Target [MVT-ST].

1.4.2.4 Hardware

The TOE is qualified to run on hardware with a specific configuration.

1.4.2.5 Firmware

The MLS Voice Guard relies on Secure Boot to ensure software integrity protection. The Secure Boot mechanism must be configured according to requirements in the MVG installation instructions.

1.5 TOE DESCRIPTION

The MLS Voice Guard (TOE) is an integral part of the MLS Voice Platform. The MLS Voice Platform is integrated with a voice application service providing a MLS Voice System consisting of operator positions, communication servers for telephone and radio communication, audio recording and management terminals. The MLS Voice Guard provides a trusted information flow control mechanism for VoIP connections (SIP/SRTP) with radio management and signalling support.

The MLS Voice System contains one or more MVGs. Each MVG provides connectivity from the highest security level network with lower level networks. This allows the users of the MLS Voice System to communicate towards radios and VoIP phones in a range of different security levels and networks.

1.5.1 THE BUILDING BLOCKS

The TOE is comprised by software running on two distinct hardware instances.

The TOE is the MVG application software, which runs within virtualized environments (partitions). The separation kernel and hardware are not part of the TOE.

The MLS Voice Guard is managed through the MLS Security Management software, not part of the TOE.

1.5.1.1 Separation kernel

The TOE runs on top of a separation kernel which provides strict compartmentalization between different TOE subsystems and modules.

1.5.2 NETWORK INTERFACES

The following logical network interfaces are used by the TOE:

Logical interface	**Proc. unit**	**Requirements for TOE Environment**
Traffic interfaces	High, Low	Receiving and sending signalling traffic and audio streams. NTP
MSM interface	High	Management operations initiated by the MSM. Supervision and alarms to the MSM.
SW update interface	High	The Guard provides an interface that allows administrators to perform low level management tasks, such as software updates. The interface is only opened upon request from the MSM.

Table 1-2 Network Interfaces

1.5.3 PERSISTENT STORAGE INTERFACE

The MVG makes use of storage media for executable code, on the high side also for configuration data and log data.

1.5.4 MANAGEMENT OF THE MVG

The TOE provides a protocol for use by the MLS Security Management Centre (MSM). The MVG provides management interfaces for initial configuration and runtime management and supervision. The TOE provides a management interface which is accessed from the MLS Secure Management (MSM).

1.5.5 PARTITIONS AND OPERATING SYSTEMS

The separation kernel offers a trusted mechanism for strict compartmentalization (partitions). The isolation provided by the separation kernel allows security critical modules to be protected from interference by other critical modules or by less critical or security irrelevant modules running on shared hardware. The TOE is composed of a number of partitions, each containing a set of processes. The communication between processes, within or between partitions, is handled through well-defined communication channels controlled by the TSF.

1.5.6 TOE USAGE

The MVG connects VoIP networks from two separate networks at different security levels. The MVG controls information flow between the networks.

The MLS Voice Guard mediates the flow of audio streams by inspecting the SRTP authentication tags of each audio packet. The MLS Voice Terminal (MVT) (part of the OCPs) tags the audio streams based on their classification as selected by operators.

The TOE provides domain isolation and mitigates covert channels by terminating and rebuilding protocol elements. Signalling is processed by a filter that ensures only allowed attributes are allowed through. A traffic analysis function monitors possible illicit information flows through the TOE.

1.5.7 AUDIO STREAM INTEGRITY PROTECTION

Before releasing audio packets from the High security network to the Lower security network, the MVG validates the integrity of the information, and that the authentication tag is valid according to the current release policy.

1.5.8 COVERT CHANNEL MITIGATION

Signalling data may contain information not intended for release, as well as be used for covert information flows. The MVG mitigates covert channels by terminating signalling protocols.

1.5.9 SELF-TESTS

The self-tests ensure verification of the system's operational state and integrity of its configuration.

1.5.10 TOE ENVIRONMENT

1.5.10.1 Physical protection

The TOE environment is required to provide physical protection of the TOE, ensuring that only authorized personnel are allowed physical access to the TOE.

1.5.10.2 Network protection

The TOE environment is required to protect the network, reducing or eliminating the effect of low level network attacks and DoS attacks, complementing the protection mechanisms offered by the MVG.

The TOE provides the following logical network interfaces, which must be protected by the TOE environment as specified:

Logical interface	Proc. unit	Requirements for TOE Environment
Traffic interfaces	High, Low	The TOE Environment restricts access to the intended network nodes. Border protection devices may be necessary to monitor and prevent low level network attacks, including DoS. The internal firewall in MVG ensures that only intended hosts may communicate with the TOE.
MSM interface	High	The TOE Environment ensures access to the interface is limited to the MLS Security Management (MSM) only.
SW update interface	High	The TOE Environment ensures access to the interface is limited to authorized administrators only for software upgrades. The interface is disabled by default, and can be temporarily enabled from the MSM.
NTP Interface	High, Low	Time updates

Table 1-3 Logical interfaces and usage

1.5.10.3 Hardware

The TOE runs on a hardware configuration based on a COTS Intel x64 iU server.

The hardware must be configured according to the MVG guidance manuals.

An UEFI BIOS is installed on the hardware, and is required to provide security functionality such as secure boot, password protection of the BIOS interface and fixed boot order.

1.5.10.4 Separation Kernel

The separation kernel platform provides:

- Secure partitioning mechanism
- Well-defined communication paths between partitions
- Controlled access to hardware resources, including memory
- Low level management API for use by the TSF
- Virtual Ethernet and proprietary drivers for high-volume internal communication.

The TOE is delivered prebuilt and integrated with the separation kernel, which is configured with a specific set of partitions, communication paths, and hardware resource access controls that support the TOE Security Architecture.

2. CONFORMANCE CLAIMS (ASE_CCL)

2.1 CC CONFORMANCE CLAIM

Conformance	Common Criteria for Information Technology Security Evaluation Part 2 conformant: Security Functional Components [CCPART2]. Part 3 conformant: Security Assurance Components [CCPART3]
Assurance level	EAL4 augmented with: • ALC_FLR.3 (Systematic flaw remediation) • AVA_VAN.4 (Methodical vulnerability analysis)
Extended SFRs	FAU_GEN_EXT.1

2.2 PP CONFORMANCE CLAIMS

The Security Target has no Protection Profile claims.

3. SECURITY PROBLEM DEFINITION (ASE_SPD)

3.1 ASSUMPTIONS

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

A.CORRECT_CONFIGURATION	It is assumed that a properly trained and trusted individual will create configuration vectors that correctly represents the information flow policy intended for the TOE.
A.NETWORK_PROTECTED	The TOE environment ensures the networks or computers connected to the TOE is provided with appropriate security measures commensurate with the value of the IT assets protected by the TOE. The TOE environment ensures the TOE prevents attackers from directly accessing the service and management interfaces of the TOE.
A.PHYSICAL_ACCESS_MANAGED	The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE. The non-IT environment provides the TOE with appropriate physical security commensurate with the value of the IT assets protected by the TOE.
A.TRUSTED_AND_TRAINED_ADMIN	The TOE is administered by System Administrators who are authorized for access to the information to be handled by the MVG and the network where the MVG is placed. System Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer’s guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures. System Administrators do not access the TOE directly, but perform management operations through the MLS Security Management (MSM)
A.TRUSTED_MARKING	A user or automated mechanism that assigns a SRTP authentication tag is trusted to set use the SRTP master key designated for the applicable security classification.

3.2 THREATS

3.2.1 GENERAL

This section identifies the assets, threat agents and threats.

3.2.2 IDENTIFICATION OF ASSETS

The following assets are to be protected:

AS.COMMUN_OBJ_CONT

IPC object content is the content of an Inter-Process Communication object and is exchanged (received/read and sent/written) between TOE components.

This is a subset of AS.NON_EXPORTED_RESOURCE.

AS.SIGNALLING

The signalling events, i.e. SIP (e.g. call setup), Radio Control and SNMP, passing through the MVG, and subject to its active information flow policy.

Different types of signalling events are specifically handled by the MVG and decomposed into a set of parameters to be evaluated.

AS.AUDIO_STREAM

An audio stream to be considered for release through the TOE. An authentication tag is required for release from the High security domain, and ensures the integrity of the object's payload and indicates whether the information contained can be released through the TOE.

AS.RELEASABLE_INFORMATION

Information within one of the connected domains that is permissible to release through the TOE.

The TOE operates on the information in the form of signalling traffic (AS.SIGNALLING) or audio stream packets (AS.AUDIO_STREAM).

AS.NON_RELEASABLE_INFORMATION

Information within the domain connected to the high side that is not allowed to be released through the TOE.

AS.EXPORTED_RESOURCE

Information (containing AS.RELEASABLE_INFORMATION) or a service in the High security domain that, according to the MVG security policy, can be accessed by or transferred to a subject in the low security domain.

AS.NON_EXPORTED_RESOURCE

Information in the High security domain that is not allowed to be accessed by or transferred to a subject in the Low security domain. This also includes information within the TOE, such as configuration data, internal communication and executable code.

AS.SECURITY_EVENTS

Security Events recorded by the TOE due to detected security issues while processing information for release.

AS.SYSTEM_RESOURCES

Resources that can be consumed by subjects in one of the interconnected security domains through use of the TOE external interfaces, e.g. system memory, persistent storage, processing time.

AS.TSF_INTERNALS — Comprises TSF data (data for the operation of the TOE upon which the enforcement of the SFR relies) and executable code.

3.2.3 IDENTIFICATION OF THREAT AGENTS

The threats and threat agents met by the TOE are diverse and depend on the scenario where it is deployed. The TOE is designed to mediate traffic between two networks of different security levels, while protecting itself and the higher classified network from attackers. Management traffic is separated from other traffic using TLS encryption, effectively reducing available attack vectors.

TA.INTERNAL — An attacker connected to the management interfaces, directly or through the MSM.

TA.USER — An attacker with the ability to interact with one of the traffic interfaces, i.e an authorized user in the High security domain. These attackers may be further classified into the following groups:

- Authenticated users on a controlled network, who are authorized to use the Operator Position, and thus are permitted to release information through the TOE. These users are trusted to assign the correct classification level to audio streams to be released, but may still attempt other attacks towards the TOE or attempt to disclose information through covert channels.
- Authenticated users on a controlled network, who are not authorized access any part of the MLS Voice System. These users are not permitted to provide signalling traffic or audio streams for release by the TOE, and may attempt attacks on the TOE itself or try to have information released.

TA.EXTERNAL — Attackers attempting to reach the TOE through the low traffic interface. These attackers have the intent to divulge classified information, from the TOE itself or its connected networks, or prevent operation of the TOE. The attacker may be an authorized user in one of the connected security domains. These attackers may have unlimited resources.

TA.ATTACKER — An attacker that may interact with any of the TOE interfaces. (TA.INTERNAL, TA.USER or TA.EXTERNAL)

TA.SYSTEM_ERROR — Hardware or software errors may cause faults during operation. Administrators may accidentally introduce errors when installing or updating the TOE improperly.

3.2.4 THREATS

The specific threats to the MVG are:

T.ADMIN_MASQUERADE	TA.ATTACKER may masquerade as an administrator on the MSM or SW update interfaces in order to gain unauthorized access to AS.NON_EXPORTED_RESOURCE or AS.EXPORTED_RESOURCE via the traffic interfaces.

T.AUDIT_COMPROMISE	TA.INTERNAL may view, delete or modify AS.SECURITY_EVENTS, or prevent future AS.SECURITY_EVENTS from being recorded, thus masking an authorized subject's action, disclosing sensitive information or masking an attacker's activities.
T.OBJECT_TAMPERING	TA.USER may modify AS.SIGNALLING or AS.AUDIO_STREAM to make the TOE release AS.NON_RELEASABLE_INFORMATION. Example: A TA.USER that is not allowed to release information through the TOE may send information camouflaged as audio in an SRTP audio stream to circumvent the TOE release policy.
T.COVERT_CHANNEL	TA.USER may initiate an illicit flow of AS.NON_RELEASABLE_INFORMATION from the internal security domain to the external security domain as a result of exploiting a covert channel in the TOE.
T.DOS	TA.USER and TA.EXTERNAL may block others from AS.SYSTEM_RESOURCES via a resource exhaustion attack.
T.INSECURE_STATE	The TOE may be placed in an insecure state as a result of an administrative error during installation or configuration, a fault during installation, (re-)configuration, initialization or during change of mode of operation or as a result of an unsuccessful recovery from a system failure or discontinuity (TA.SYSTEM_ERROR affecting AS.TSF_INTERNALS).
T.MALWARE_INJECTION	A malicious agent in one of the connected security domains (TA.USER, TA.EXTERNAL) may attempt to introduce active content to a network through the TOE, whereby the active content can carry out or trigger actions automatically without an authorized subject in the internal domain directly or knowingly invoking the actions thereby compromising AS.RELEASABLE_INFORMATION or AS.NON_RELEASABLE_INFORMATION.
T.METADATA_LEAK	TA.EXTERNAL may carry out a network-based attack against a TOE interface or released signalling traffic or audio streams in order to obtain AS.NON_RELEASABLE_INFORMATION as metadata attached to the released information. The metadata may disclose potentially compromising information regarding a security domain, such as network and organizational structure, security policies, addresses and directory structure, and which IT systems are in use.

T.NETWORK_ATTACK	TA.EXTERNAL may carry out a network-based attack against AS.EXPORTED_RESOURCE (e.g., by sending malicious signalling traffic to circumvent the TOEs security policy or by introducing viruses or active content into a security domain through the TOE) thereby compromising or affecting the availability of AS.RELEASABLE_INFORMATION or AS.NON_RELEASABLE_INFORMATION.
T.RECONNAISSANCE	TA.EXTERNAL may obtain AS.NON_RELEASABLE_INFORMATION about resources (e.g. IP addresses, port numbers, system names, system date/time, products, versions) from a security domain e.g. by using network scanning techniques, network traffic monitoring, etc.
T. TSF_COMPROMISE	TA.ATTACKER may cause AS.TSF_INTERNALS to be inappropriately accessed (viewed, modified, executed or deleted). The attack may be performed before the TOE is made operational (during delivery), during configuration, normal operation or maintenance (patches).
T.UNAUTHORIZED_ACCESS	A TA.EXTERNAL may gain access to AS.NON_EXPORTED_RESOURCE or AS.EXPORTED_RESOURCE.
T.UNNOTICED_ATTACK	Due to an insufficient audit configuration, the administrator may not have ability to notice potential security violations by TA.ATTACKER that could compromise any asset, thus limiting the administrator’s ability to identify and take action against a possible security breach.

3.3 ORGANISATIONAL SECURITY POLICIES

Organisational security policies (OSPs) are security rules, procedures, or guidelines imposed on the operational environment by the organisation running the TOE.

P.CRYPTOGRAPHY	The TOE shall use approved and validated methods for cryptographic operations, (i.e. hashing).
P.MINIMAL_POSTURE	The Administrator shall ensure that only strictly required services and applications are running on hardware shared with the TOE and in the external services connected to the TOE (e.g. MSM and MVT).

4. SECURITY OBJECTIVES (ASE_OBJ)

4.1 TOE IT SECURITY OBJECTIVES

O.AUDIT

The TOE will provide the capability to generate, and export an audit trail (AS.SECURITY_EVENTS) for security events. The TOE provides secure storage for the audit trail.

O.CONFIGURATION_CHANGE

The TOE will support the capability to perform a dynamic configuration change. Reconfiguration is performed while the TOE is operational, and takes effect immediately.

O.CORRECT_TSF_OPERATION

The TOE will provide a capability to test the TSF to ensure the correct operation of the TSF in its operational environment.

The TOE will provide a runtime self-test capability.

The TOE will take action in response to any failure of a runtime self-test capability.

O.COVERT_CHANNEL_MITIGATION

The TOE calculates the covert channel bandwidth and creates an alarm or prevents signalling when specific thresholds are reached.

O.INTERNAL_LEAST_PRIVILEGE

The TSF will be structured to achieve the principle of least privilege among TSF modules.

O.CONTROLLED_INFORMATION_FLOW

The TOE shall control the flow of information between the security domains by only relaying signalling traffic and audio streams that are allowed according to the information flow policy.

O.MINIMAL_PROXY

The TOE shall provide mechanisms that can be used to limit the amount of information which is transmitted between the security domains. Signalling traffic is decomposed and rebuilt by the MVG. Protocol elements not explicitly allowed are rejected and those not needed are removed.

O.SECURE_STATE

The TOE will preserve secure state during an execution session.

The TOE will provide startup mechanisms to transition the TSF from offline state to an initial secure state without protection compromise.

The TOE will provide procedures and/or mechanisms, which can be used in the event of failure, faults, or discontinuity, to preserve secure state and to transition the TSF back to a secure state without protection compromise.

O.SUBJECT_ISOLATION

The TOE will provide mechanisms to protect each component within the TOE from unauthorized interference by other components.

O.SRTP_INTEGRITY

The TOE will validate the integrity of SRTP audio streams sent from the High domain to the Low domain.

Table 4-1: TOE Security Objectives

4.2 TOE ENVIRONMENT SECURITY OBJECTIVES

OE.MINIMAL_POSTURE

The TOE environment ensures the High network interface of the MVG is connected to a network segment limited to MLS Voice System components.

OE.NETWORK

The TOE Environment will ensure the network used for the security domains are protected according to the sensitivity and integrity protection required for the information contained within the domains.

The TOE Environment ensures access to the MVG from the High security level network is limited to other MLS Voice System components.

OE.PHYSICAL_ACCESS_MANAGED

The TOE is deployed in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.

Physical security will be provided for the TOE by the non-IT environment commensurate with the value of the IT assets protected by the TOE.

OE.CONFIGURATION

A properly trained and trusted individual will configure the TOE in a way that correctly reflects the environment's requirements for controlling the flow of information between the connected security requirements.

OE.TRUSTED_AND_TRAINED_ADMIN

Sites using the TOE will ensure that administrators are trusted and aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.

OE.TRUSTED_MARKING	A Operator Position (OCP) is trusted to correctly assign authentication tags to audio streams (AS.RELEASABLE_INFORMATION, AS.NON_RELEASABLE_INFORMATION), in accordance with applicable security policies and their respective guidelines. The assurance of the process for assigning authentication tags must be commensurate with the value of the information that the labels are created for. The trust extends to the equipment and software used to perform the tagging, such as the MLS Voice Terminal (MVT).
OE.PLATFORM	The OE provides the required separation kernel and hardware platform, consisting of two instances, running on individual processing units, connected internally. The processing units provide the fundamental tools for isolating internal components using the Intel processor’s hardware virtualization support.
OE.TIME_SOURCE	The OE provides a NTP time service.

Table 4-2: Security objectives for the TOE Environment

5. EXTENDED COMPONENTS DEFINITION (ASE_ECD)

5.1 EXTENDED COMPONENTS DEFINITION (SFRS)

The following extended component has been included in this Security Target because the FAU_GEN.1 Common Criteria component was found to be unsuitable as stated.

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 SECURITY FUNCTIONAL REQUIREMENTS (SFRS)

6.1.1 CLASS FAU: SECURITY AUDIT

6.1.1.1 Security audit data generation (FAU_GEN)

6.1.1.1.1 FAU_GEN_EXT.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps (not satisfied, see 8.2.2).

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 *not specified* level of audit;

(c) All auditable events listed in Table 6-1;

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, *information specified in column three of* Table 6-1.

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN_EXT.1	None.	None.
FAU_STG.1	None.	None.
FAU_STG.3	Actions taken due to exceeding of a threshold.	None.
FCS_COP.1	None.	None.
FDP_ETC.2	~~Successful export of information.~~ Note: FDP_ETC.2 covers audio streams (rtp), which are not relevant to audit packet by packet. SIP calls are audited by the TOE environment.	None.
FDP_IFC.2	None.	None.
FDP_IFF.1	~~decisions on requests for information flow.~~	None.

Requirement	Auditable Events	Additional Audit Record Contents
	Rejected requests for information flow.	
FDP_UIT.1	The identity of any user or subject attempting to use the user data exchange mechanisms, but who is unauthorised to do so.	None.
FMT_MSA.1	All modifications of the values of security attributes.	None.
FMT_MSA.3	Modifications of the default setting of permissive or restrictive rules. All modifications of the initial values of security attributes.	None.
FMT_MTD.1	All modifications to the values of TSF data.	None
FMT_MTD.3	All rejected values of TSF data.	None.
FPT_FLS.1	Failures detected by the FPT_TST.1 tests.	None.
FPT_RCV.4	The inability to return to a secure state after a failure of the TSF. The detection of a failure of a security function.	None.
FPT_TST.1	Execution of the TSF self-tests and the results of the tests.	None.
FTP_TRP.1	~~All attempted uses of the trusted path functions.~~ ~~Identification of the user associated with all trusted path invocations, if available.~~ Note: FDP_ETC.2 covers audio streams (rtp), which are not relevant to audit packet by packet. SIP calls are audited by the TOE environment.	~~Object attributes: Originator, recipient, security label.~~
FDP_ITC.2	None.	None.
FPT_TDC.1	None.	None.

Table 6-1: Auditable Events

6.1.1.2 Security audit event storage (FAU_STG)

6.1.1.2.1 FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN_EXT.1 Audit data generation.

FAU_STG.1.1: The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2: The TSF shall be able to *prevent* unauthorised modifications to the stored audit records in the audit trail.

6.1.1.2.2 FAU_STG.3 Action in case of possible audit data loss

Hierarchical to: No other components.

Dependencies: FAU_STG.1 Protected audit trail storage.

FAU_STG.3.1: The TSF shall *delete entries older than a configurable number of days* if the audit trail ~~exceeds~~ **reaches** *the available storage capacity*.

6.1.2 CLASS FCS: CRYPTOGRAPHIC SUPPORT

6.1.2.1 Cryptographic operation (FCS_COP)

6.1.2.1.1 FCS_COP.1 Cryptographic operation (cryptographic hashing)

Hierarchical to: No other components.

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

FCS_COP.1.1: The TSF shall perform *cryptographic hashing and message authentication services* in accordance with a specified cryptographic algorithm *HMAC-SHA-2* and cryptographic key size *128 bits* that meet the following: *FIPS PUB 180-4 [FIPS-180]*.

6.1.3 CLASS FDP: USER DATA PROTECTION

6.1.3.1 Export from the TOE (FDP_ETC)

6.1.3.1.1 FDP_ETC.2 Export of user data with security attributes

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control,
or FDP_IFC.1 Subset information flow control]

FDP_ETC.2.1: The TSF shall enforce the *Information Release SFP* when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2: The TSF shall export the user data with the user data’s associated security attributes.

FDP_ETC.2.3: The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4: The TSF shall enforce the following rules when user data is exported from the TOE:

a) Audio streams in the direction Low to High: SRTP Authentication Tag is added.

b) Audio streams in the direction High to Low: SRTP Authentication Tag is validated and removed.

6.1.3.2 Information flow control policy (FDP_IFC)

6.1.3.2.1 FDP_IFC.2/r Complete information flow control (Information Release SFP)

Hierarchical to: FDP_IFC.1 Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.2.1/r: The TSF shall enforce the *Information Release SFP based on content-based protection requirements and release conditions* on *all signalling traffic and audio streams mediated by the TOE between the two connected domains* and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2/r: 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.

6.1.3.2.2 FDP_IFC.2/i Complete information flow control (Internal Flow Control SFP)

Hierarchical to: FDP_IFC.1 Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.2.1/i: The TSF shall enforce the *Internal Flow Control SFP* on *all inter-process communication* and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2/i: 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.

6.1.3.3 Information flow control functions (FDP_IFF)

6.1.3.3.1 FDP_IFF.1/r Simple security attributes (Information Release SFP)

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1/r: The TSF shall enforce the *Information Release SFP* based on the following types of subject and information security attributes:

All information:

- *object release direction,*
- *object type,*

SRTP packets:

- authentication tag
- stream authorization (associated call)

Signalling traffic (SIP call handling, radio control and management, and SNMP management and supervision):

- *protocol parameters*

FDP_IFF.1.2/r: The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

- Signalling traffic: The operation is allowed by the policy defined by the active configuration vector.
- Audio Stream: The SRTP authorization tag is valid, and the packet is associated with an active call.

FDP_IFF.1.3/r: The TSF shall enforce the additional information flow rules:

- A security event shall be audited if the specific flow has been determined by traffic analysis to exceed the reporting threshold.

FDP_IFF.1.4/r: The TSF shall explicitly authorise an information flow based on the following rules: *none*

FDP_IFF.1.5/r: The TSF shall explicitly deny an information flow based on the following rules:

- The specific flow has been determined by traffic analysis to exceed the covert channel threshold.

6.1.3.3.2 FDP_IFF.1/i Simple security attributes (Internal Flow Control Policy)

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1/i: The TSF shall enforce the *Internal Flow Control SFP* based on the following types of subject and information security attributes:

- Subject security attributes ‘subject identity’ (process id, partition id)

- Information security attributes: destination process, destination partition, priority level

FDP_IFF.1.2/i: The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

- *The operation is allowed by the communication flows defined between TOE processes.*

FDP_IFF.1.3/i: The TSF shall enforce the additional information flow rules: *None*.

FDP_IFF.1.4/i: The TSF shall explicitly authorise an information flow based on the following rules: *none*

FDP_IFF.1.5/i: The TSF shall explicitly deny an information flow based on the following rules: *none*

6.1.3.4 Inter-TSF user data integrity transfer protection (FDP_UIT)

6.1.3.4.1 FDP_UIT.1 Data exchange integrity

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

[FTP_ITC.1 Inter-TSF trusted channel, or

FTP_TRP.1 Trusted path]

FDP_UIT.1.1: The TSF shall enforce the *Information Release SFP* to *transmit and receive* user data in a manner protected from *modification and insertion* errors.

FDP_UIT.1.2: The TSF shall be able to determine on receipt of user data, whether *modification or insertion* has occurred.

Note: This requirement applies to SRTP audio streams.

6.1.3.5 Import from outside of the TOE (FDP_ITC)

6.1.3.5.1 FDP_ITC.2 Import of user data with security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]
FPT_TDC.1 Inter-TSF basic TSF data consistency

FDP_ITC.2.1: The TSF shall enforce the *information flow control SFP(s)* when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2: The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3: The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4: The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5: The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

a) Audio streams in the direction High to Low: SRTP Authentication Tag is validated*.*

b) Audio streams in the direction Low to High: None.

6.1.4 CLASS FMT: SECURITY MANAGEMENT

6.1.4.1 Management of security attributes (FMT_MSA)

6.1.4.1.1 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions.

FMT_MSA.1.1: The TSF shall enforce the *Information Release SFP* to restrict the ability to *query, modify, or delete* the security attributes *TOE configuration vectors*, and SRTP Authentication Keys to *the MLS Security Management (MSM) and* SW update interface.

6.1.4.1.2 FMT_MSA.3 Static attribute initialisation (restrictive rule set values)

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes,

FMT_SMR.1 Security roles.

FMT_MSA.3.1: The TSF shall enforce the *Information Release SFP* to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2: The TSF shall allow *MLS Security Management* to specify alternative initial values to override the default values when an object or information is created.

6.1.4.2 Management of TSF data (FMT_MTD)

6.1.4.2.1 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1: The TSF shall restrict the ability to *query, modify* the *configuration data* to *the MSM and* SW update interface.

6.1.4.2.2 FMT_MTD.3 Secure TSF data

Hierarchical to: No other components.

Dependencies: FMT_MTD.1 Management of TSF data.

FMT_MTD.3.1: The TSF shall ensure that only secure values are accepted for TSF data.
Application Note: Secure implies that the values are consistent (e.g. all required parameters are set), and are valid within the defined range for the TSF data (e.g., an audit enable/disable indicator must be within range of a Boolean type).

6.1.5 CLASS FPT: PROTECTION OF THE TSF

6.1.5.1 Fail secure (FPT_FLS)

The requirements of this family ensure that the TOE will always enforce its SFRs in the event of identified categories of failures in the TSF.

6.1.5.1.1 FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

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

a) failures from self-tests covered by FPT_TST.1;

Application Note: TSF failure modes vary and may include “hard” failures such as those associated with hardware failure or unrecoverable software errors, and “soft” failures such as intermittent hardware errors and recoverable software errors.

Application Note: The TSF is not expected to protect itself against all types of hardware errors. For example, a radiation induced change of a single bit in a memory access control register could result in an incorrect (but valid) memory location being accessed. This would not always be detected by the hardware.

6.1.5.2 Trusted Recovery (FPT_RCV)

The requirements of this family ensure that the TSF can determine that the TOE is started up without protection compromise and can recover without protection compromise after discontinuity of operations. This family is important because the start-up state of the TSF determines the protection of subsequent states.

6.1.5.2.1 FPT_RCV.4 Function recovery

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_RCV.4.1: The TSF shall ensure that *TOE self-test, state transitions (e.g. disabled mode),* and *object release (success and failure)* have the property that the function either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

6.1.5.3 TSF self-test (FPT_TST)

6.1.5.3.1 FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1: The TSF shall run a suite of self-tests *periodically during normal operation* to demonstrate the correct operation of the TSF.

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 *stored TSF executable code*.

6.1.5.4 Inter-TSF TSF data consistency (FPT_TDC)

6.1.5.4.1 FPT_TDC.1 Inter-TSF basic TSF data consistency

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TDC.1.1: The TSF shall provide the capability to consistently interpret *SRTP Authentication Tags* when shared between the TSF and another trusted IT product.

FPT_TDC.1.2: The TSF shall *validate the integrity of SRTP Authentication Tags for audio streams going in the direction High to Low* when interpreting the TSF data from another trusted IT product.

6.1.6 CLASS FTP: TRUSTED PATH/CHANNELS

6.1.6.1 Trusted path (FTP_TRP)

6.1.6.1.1 FTP_TRP.1 Trusted Path

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_TRP.1.1: The TSF shall provide a communication path between itself and *remote MLS Voice Terminal* users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *modification of SRTP audio streams*.

FTP_TRP.1.2: The TSF shall permit *the TSF or remote users* to initiate communication via the trusted path.

FTP_TRP.1.3: The TSF shall require the use of the trusted path for *protection of audio streams received by or sent from the TOE*.

Note 1: The requirement applies to SRTP audio streams, and is limited to the parts of SRTP packets covered by the SRTP authentication tag.

Note 2: In FTP_TRP.1.2, "*remote users"* is to be understood as users of the MVTs in the system.

6.2 SECURITY ASSURANCE REQUIREMENTS (SARS)

The TOE is evaluated to EAL4 augmented with ALC_FLR.3 and AVA_VAN.4.

The security assurance requirements for the TOE are selected according to EAL4 augmented with ALC_FLR.3 (systematic flaw remediation) and AVA_VAN.4 (Methodical vulnerability analysis).

From CC Part 3:

> **EAL4** provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and **complete** interface specification, guidance documentation, **a** description of the **basic modular** design of the TOE, **and a subset of the implementation,** to understand the security behaviour.
>
> The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification and TOE design, selective independent confirmation of the developer

test results, and a vulnerability analysis (based upon the functional specification, TOE design, **implementation representation, security architecture description** and guidance evidence provided) demonstrating resistance to penetration attackers with **an Enhanced-Basic** attack potential.

EAL4 also provides assurance through the use of development environment controls **and additional** TOE configuration management **including automation,** and evidence of secure delivery procedures.

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.

The AVA_VAN.4 component ensures that a methodical vulnerability analysis has been performed.

7. TOE SUMMARY SPECIFICATION (ASE_TSS)

7.1 TOE SECURITY FUNCTIONS

7.1.1 SF.AUDIT

The TOE is able to generate audit records for the following events:

- Configuration data changed
- Covert Channel thresholds reached
- Changes to operational state
- Results from TOE Self-Tests
- Changes to system time
- Invalid signalling parameter
- Invalid SRTP authentication

The TOE allows the Audit log to be exported to the MLS Security Management centre.

This implements FAU_GEN_EXT.1, FAU_STG.1, FAU_STG.3.

7.1.2 SF.CONFIGURATION

The TOE provides a MSM interface for remote access from the MLS Security Management (MSM).

The SF restricts the ability to perform configuration changes to authorized MLS Security Management (MSM) instances and SW update interface only (FMT_MSA.1, FMT_MTD.1). The SF ensures secure and restrictive values for configuration vector attributes and SRTP authentication keys (FMT_MSA.3, FMT_MTD.3).

7.1.3 SF.DOMAIN_ISOLATION

The TOE mitigates the risk of unintended disclosure of information between the domains by disassembling and reconstructing protocol elements being relayed by the MVG.

This SF implements the information flow control requirements FDP_IFC.2/r, and FDP_IFF.1/r.

7.1.4 SF.FILTER

The TOE performs an extensive evaluation of all signalling traffic, based on the active configuration vector. The TOE ensures that only attributes that do not violate the Information Flow Policy are allowed to be part of released signalling traffic. This security function ensures that signalling parameters are rejected if required by the current configuration. The SF support implementation of the filtering requirements from FDP_IFC.2/r and FDP_IFF.1/r.

7.1.5 SF.INTERNAL_PARTITIONING

The TOE is composed of a number of modules, separated according to responsibilities and security implementation. This SF enforces limitations on the TOE internal information flow according to well-defined communication paths. This implements the information flow requirements in FDP_IFC.2/i and FDP_IFF.1/i.

7.1.6 SF.SECURE_STATE

The TOE ensures that it is initialized to a secure state before entering operation.

The TOE maintains a secure state during operation, whenever transitioning between runtime states and on detected failures.

The TOE will transition to disabled mode or halt if required to preserve a secure state. The secure state and recovery SF implements FPT_FLS.1, FPT_RCV.4.

7.1.7 SF.SELF_TEST

The TOE performs periodic self-tests on the signalling filter and SRTP audio filter. If a self-test fails, the TOE will perform a state change to disabled mode.

The SF implements FPT_TST.1.

7.1.8 SF.STREAM_AUTHENTICATION

The TOE supports SRTP authentication tags for integrity protection of audio streams. The Authentication tags are verified when received from the High security domain, and removed prior to release to the Low security domain.

The TOE ensures only SRTP packets with a valid authentication tag and association with an active SIP call are allowed to flow from the High to the Low network.

The authentication tags provides audio integrity protection FDP_ETC.2, FDP_UIT.1 and FTP_TRP.1. The TOE implements hashing algorithms.

7.1.9 SF.TRAFFIC_ANALYSIS

The TOE inspects the traffic processed by the parameter filter and audio stream handler. An analysis is performed to detect likely covert channel issues, and an alarm is raised to alert administrators through the MSM interface (FDP_IFF.1/r). If a discard threshold is reached, the traffic is blocked by the TOE (FDP_IFF.1/r).

8. RATIONALE

The rationale demonstrates that threats, assumptions and policies form a basis for the definition of security objectives. Likewise, it is demonstrated that the chosen security requirements cover all security objectives, and that security functions in the TOE or its environment fully cover the security requirements.

8.1 SECURITY OBJECTIVES RATIONALE

In the following subsections every security objective is correlated with identified threats and assumptions. It is furthermore shown that all identified threats are covered by a security objective.

The following three tables (Table 8-1, Table 8-2 and Table 8-3) demonstrate that all threats, assumption and policies are covered by a security objective. Some threats are fully covered by a single security objective, while others need more than one security objective to be fully covered.

Threats Security objectives	T.ADMIN_MASQUERADE	T.AUDIT_COMPROMISE	T.OBJECT_TAMPERING	T.COVERT_CHANNEL	T.DOS	T.INSECURE_STATE	T.MALWARE_INJECTION	T.METADATA_LEAK	T.NETWORK_ATTACK	T.RECONNAISSANCE	T.TSF_COMPROMISE	T.UNAUTHORIZED_ACCESS	T.UNNOTICED_ATTACK
O.AUDIT	X	X		X					X	X		X	X
O.CONFIGURATION_CHANGE						X							
O.CONTROLLED_INFORMATION_FLOW							X	X					
O.CORRECT_TSF_OPERATION						X							
O.INTERNAL_LEAST_PRIVILEGE	X	X		X					X	X			
O.MINIMAL_PROXY				X			X	X		X			
O.SRTP_INTEGRITY			X					X					
O.SECURE_STATE					X	X			X		X		
O.SUBJECT_ISOLATION	X					X			X	X	X		
O.COVERT_CHANNEL_MITIGATION				X									
OE.MINIMAL_POSTURE	X								X	X	X		
OE.NETWORK			X		X				X	X	X	X	X
OE.PHYSICAL_ACCESS_MANAGED											X	X	X

Threats Security objectives	T.ADMIN_MASQUERADE	T.AUDIT_COMPROMISE	T.OBJECT_TAMPERING	T.COVERT_CHANNEL	T.DOS	T.INSECURE_STATE	T.MALWARE_INJECTION	T.METADATA_LEAK	T.NETWORK_ATTACK	T.RECONNAISSANCE	T.TSF_COMPROMISE	T.UNAUTHORIZED_ACCESS	T.UNNOTICED_ATTACK
OE.CONFIGURATION				X									
OE.TRUSTED_AND_TRAINED_ADMIN		X									X		X
OE.TRUSTED_MARKING													
OE.PLATFORM	X					X			X		X		X
OE.TIME_SOURCE		X											

Table 8-1: TOE threats coverage

Security objectives	A.CORRECT_CONFIGURATION	A.NETWORK_PROTECTED	A.PHYSICAL_ACCESS_MANAGED	A.TRUSTED_AND_TRAINED_ADMIN	A.TRUSTED_MARKING
OE.MINIMAL_POSTURE		X			
OE.NETWORK	X	X			
OE.PHYSICAL_ACCESS_MANAGED			X		
OE.CONFIGURATION	X				
OE.TRUSTED_AND_TRAINED_ADMIN	X			X	
OE.TRUSTED_MARKING					X
OE.PLATFORM					
OE.TIME_SOURCE	X				

Table 8-2: Assumptions coverage

Security objectives	P.CRYPTOGRAPHY	P.MINIMAL_POSTURE
O.AUDIT		
O.CONFIGURATION_CHANGE		
O.CORRECT_TSF_OPERATION		
O.INTERNAL_LEAST_PRIVILEGE		X
O.CONTROLLED_INFORMATION_FLOW		
O.MINIMAL_PROXY		
O.SRTP_INTEGRITY	X	
O.SECURE_STATE		
O.SUBJECT_ISOLATION		
OE.MINIMAL_POSTURE		X
OE.PHYSICAL_ACCESS_MANAGED		
OE.CONFIGURATION		
OE.TRUSTED_AND_TRAINED_ADMIN		
OE.TRUSTED_MARKING		
OE.PLATFORM		X
OE.TIME_SOURCE		
OE.NETWORK		X

Table 8-3: Policies coverage

8.1.1 THREATS MET BY OBJECTIVES RATIONALE

The following rationale describes how each threat is met by the TOE or TOE Environment.

T.ADMIN_MASQUERADE

The TOE Environment ensures that only the associated MLS Security Management centre may access the MSM and SW update interfaces (OE.MINIMAL_POSTURE). The TOE and TOE Environment mitigates attack vectors to management functions from the traffic interfaces (O.INTERNAL_LEAST_PRIVILEGE, O.SUBJECT_ISOLATION, OE.PLATFORM). In addition the TOE records an audit trail for administrative operations (O.AUDIT).

T.AUDIT_COMPROMISE

The TOE ensures the TOE audit trail is available to authorized administrators by exporting auditable events to the controlling MLS Security Management (O.AUDIT). The TOE is compartmentalized to prevent attackers from interfering with audit generation or storage (O.INTERNAL_LEAST_PRIVILEGE). The TOE Environment ensures administrators are trained to correctly configure and monitor the system (OE.TRUSTED_AND_TRAINED_ADMIN), and supply the TOE with a reliable time source (OE.TIME_SOURCE).

T.OBJECT_TAMPERING

The TOE prevents tampering of audio streams going from the High to the Low domain through the use of SRTP authentication tags (O.SRTP_INTEGRITY).

It is the responsibility of the TOE Environment to offer the appropriate protection (OE.NETWORK) in the Low domain, where SRTP is not available.

T.COVERT_CHANNEL

The exploitation of residual covert channels are mitigated by decomposing and rebuilding all signalling traffic and audio streams, and removing or mapping attributes according to the defined security policy (O.INTERNAL_LEAST_PRIVILEGE, O.MINIMAL_PROXY). Possible leaks through «free text» parameters are mitigated in the traffic analyzer by monitoring covert channels. The TOE generates audit logs that may be analysed (O.AUDIT) by the TOE Environment. The TOE Environment is responsible for correct configuration of the TOE to minimize covert channels (OE.CONFIGURATION, O.COVERT_CHANNEL_MITIGATION).

T.DOS

The TOE monitors health attributes (O.SECURE_STATE) to limit the effects of denial of service attacks or during high traffic scenarios.

The primary protection against denial of service attacks are provided by the TOE Environment through controlled network access (OE.NETWORK).

T.INSECURE_STATE

The TOE provides mechanisms to prevent entering an insecure state, including periodic self-tests (O.SECURE_STATE). The TOE ensures a secure state during and after a configuration update from the MSM (O.CONFIGURATION_CHANGE). TSF integrity is verified during boot (OE.PLATFORM) and during operation (O.CORRECT_TSF_OPERATION).

The TOE prevents interference between different parts through decomposition and controlled information flows (O.SUBJECT_ISOLATION), and separation is further supported by the operating system and hardware (OE.PLATFORM).

T.MALWARE_INJECTION

The TOE prevents malware from being relayed by acting as a minimal proxy, limiting the attributes to be transferred according to configuration (O.MINIMAL_PROXY), relaying allowed attributes and objects only (O.CONTROLLED_INFORMATION_FLOW).

T.METADATA_LEAK

The TOE ensures only permitted protocol elements and values allowed to be released from the High to the Low network. The active configuration vector defines the allowed signalling traffic

(O.CONTROLLED_INFORMATION_FLOW, O.MINIMAL_PROXY) and unintended information cannot be injected into SRTP packets (O.SRTP_INTEGRITY).

T.NETWORK_ATTACK

The TOE Environment mitigates networked attacks (OE.NETWORK, OE.MINIMAL_POSTURE), and provides a high assurance separation kernel platform (OE.PLATFORM). The TOE minimizes feasible attack vectors and the ability for an attacker to exploit residual vulnerabilities (O.INTERNAL_LEAST_PRIVILEGE, O.SUBJECT_ISOLATION, O.SECURE_STATE), and records security related events (O.AUDIT).

T.RECONNAISSANCE

Reconnaissance operations are audited if detected (O.AUDIT). The TOE provides a compartmentalized design that limits the ability to perform reconnaissance (O.INTERNAL_LEAST_PRIVILEGE, O.SUBJECT_ISOLATION), and limits information sent through the MVG (O.MINIMAL_PROXY).

The TOE Environment mitigates reconnaissance attempts through protecting the network environment and the deployed TOE. (OE.NETWORK, OE.MINIMAL_POSTURE)

T.TSF_COMPROMISE

The TOE Environment validates the integrity of AS.TSF_INTERNALS during startup, while the TOE performs regular self-tests of the flow controls for signalling traffic (parameter filter) and audio streams (srtp tagging). The TOE architecture and security policy mitigates an attacker’s ability to exploit residual vulnerabilities to bypass the TOE Security Policy (O.SUBJECT_ISOLATION, OE.MINIMAL_POSTURE, OE.PLATFORM). The TOE provides mechanisms to ensure a secure state (O.SECURE_STATE).

The TOE Environment mitigates physical and network attack vectors (OE.PHYSICAL_ACCESS_MANAGED, OE.NETWORK) and ensures administrators follow guidance documentation (OE.TRUSTED_AND_TRAINED_ADMIN).

T.UNAUTHORIZED_ACCESS

The TOE Environment mitigates the ability for an attacker to gain unauthorized access to the TOE through physical and network protection appropriate for the information in the connected security domains (OE.NETWORK, OE.PHYSICAL_ACCESS_MANAGED). Malicious behaviour is subject to auditing (O.AUDIT).

T.UNNOTICED_ATTACK

The TOE Environment (OE.PLATFORM) verifies the integrity of the TOE executable code.

The TOE Environment mitigates the risk of an undiscovered attack by ensuring proper configuration of the TOE (O.AUDIT, OE.TRUSTED_AND_TRAINED_ADMIN), and protecting networks and physical access (OE.NETWORK, OE.PHYSICAL_ACCESS_MANAGED).

8.1.2 ASSUMPTIONS MET BY OBJECTIVES FOR THE ENVIRONMENT RATIONALE

A.CORRECT_CONFIGURATION

The assumption is upheld by OE.TRUSTED_AND_TRAINED_ADMIN and OE.CONFIGURATION, supported by external services (OE.NETWORK, OE.TIME_SOURCE).

A.NETWORK_PROTECTED

OE.NETWORK and OE.MINIMAL_POSTURE directly upholds the assumption.

A.PHYSICAL_ACCESS_MANAGED

OE.PHYSICAL_ACCESS_MANAGED directly upholds the assumption.

A.TRUSTED_AND_TRAINED_ADMIN

OE.TRUSTED_AND_TRAINED_ADMIN directly upholds the assumption.

A.TRUSTED_MARKING

OE.TRUSTED_MARKING directly upholds the assumption.

8.1.3 POLICIES

P.CRYPTOGRAPHY

The TOE uses approved cryptographic algorithms and implementation (O.SRTP_INTEGRITY).

P.MINIMAL_POSTURE

The TOE and TOE Environment provides the minimum external interfaces required to implement the MVG functionality (O.INTERNAL_LEAST_PRIVILEGE, OE.MINIMAL_POSTURE, OE.NETWORK, OE.PLATFORM)

8.2 SECURITY REQUIREMENTS RATIONALE

8.2.1 RATIONALE FOR SECURITY FUNCTIONAL REQUIREMENTS TO COVER OBJECTIVES

The following table show that requirements are appropriate to cover TOE security objectives.

Objectives **Req.**	O.AUDIT	O.CONFIGURATION_CHANGE	O.CORRECT_TSF_OPERATION	O.INTERNAL_LEAST_PRIVILEGE	O.CONTROLLED_INFORMATION_FLOW	O.MINIMAL_PROXY	O.SRTP_INTEGRITY	O.SECURE_STATE	O.SUBJECT_ISOLATION	O.COVERT_CHANNEL_MITIGATION
FAU_GEN_EXT.1	X									
FAU_STG.1	X									
FAU_STG.3	X									
FCS_COP.1							X			
FDP_ETC.2							X			
FDP_IFC.2/r					X	X				

FDP_IFC.2/i				X	X				X	
FDP_IFF.1/r					X	X				X
FDP_IFF.1/i				X	X				X	
FDP_UIT.1							X			
FMT_MSA.1		X								
FMT_MSA.3		X								
FMT_MTD.1		X								
FMT_MTD.3		X								
FPT_FLS.1			X					X		
FPT_RCV.4			X					X		
FPT_TST.1								X		
FTP_TRP.1							X			
FDP_ITC.2							X			
FPT_TDC.1							X			

Table 8-4: Security objectives satisfaction

O.AUDIT

The objective is implemented by requirements for generating (FAU_GEN_EXT.1), and storing (FAU_STG.1, FAU_STG.3) audit data.

O.CONFIGURATION_CHANGE

The objective is implemented by the FMT class requirements, and TSF management operations (FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_MTD.3).

O.CORRECT_TSF_OPERATION

The TOE provides secure fault and recovery mechanisms (FPT_FLS.1, FPT_RCV.4).

O.INTERNAL_LEAST_PRIVILEGE

The TSF strictly limits the information flow between components (FDP_IFC.2/i, FDP_IFF.1/i).

O.CONTROLLED_INFORMATION_FLOW

The objective is implemented through rigorous information flow control mechanisms internally and externally (FDP_IFC.2/r, FDP_IFF.1/r, FDP_IFF.1/i) on all information flows in and out of the TOE.

O.MINIMAL_PROXY

The objective is implemented by the Information Release SFP, which minimizes covert channels and relayed attributes for all information relayed by the TOE between the connected security domains (FDP_IFC.2/r, FDP_IFF.1/r).

O.SRTP_INTEGRITY

The TOE implements integrity protection for SRTP audio streams (FDP_ETC.2, FDP_UIT.1, FTP_TRP.1, FDP_ITC.2, FPT_TDC.1), using approved cryptographic algorithms (FCS_COP.1).

O.SECURE_STATE

The objective is met by requirements for secure state recovery, secure failure handling (FPT_FLS.1, FPT_RCV.4) and periodic self-tests (FPT_TST.1).

O.SUBJECT_ISOLATION

The objective is met by implementing the Internal Information Flow Control SFP (FDP_IFC.2/i, FDP_IFF.1/i).

O.COVERT_CHANNEL_MITIGATION
This objective is implemented as follows: Upon traffic analysis determining that the covert channel has exceeded the set threshold, a security event will be reported (FDP_IFF.1/r) and further flow can be denied if traffic exceeds a discard threshold (FDP_IFF.1/r).

8.2.2 FUNCTIONAL SECURITY REQUIREMENTS DEPENDENCIES

The table shows each component’s direct dependencies to other components. This demonstrates that the set of security requirements form a mutually supportive and consistent whole.

TOE Requirement	Dependency	Included	Rationale
FAU_GEN_EXT.1	FPT_STM.1	No	Timestamps are provided by the TOE Environment through OE.TIME_SOURCE
FAU_STG.1	FAU_GEN_EXT.1	Yes	
FAU_STG.3	FAU_STG.1	Yes	
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	Yes No	Key destruction is not relevant for the TOE, as FCS_COP.1 covers HMAC only and thus obsolete keys are not sensitive information. .
FDP_ETC.2	FDP_ACC.1 or FDP_IFC.1	Yes	Higher-level SFR: FDP_IFC.2
FDP_IFC.2	FDP_IFF.1	Yes	
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	Yes Yes	Higher-level SFR: FDP_IFC.2
FDP_UIT.1	FDP_ACC.1 or FDP_IFC.1 FTP_ITC.1 or FTP_TRP.1	Yes Yes	Higher-level SFR: FDP_IFC.2
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMF.1 FMT_SMR.1	Yes No No	Higher-level SFR: FDP_IFC.2 Access to management functions is managed by the MSM (TOE Environment). User roles are handled by the MSM (TOE Environment).

TOE Requirement	Dependency	Included	Rationale
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes No	 User roles are handled by the MSM (TOE Environment).
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	No No	Access to management functions is managed by the MSM (TOE Environment). User roles are handled by the MSM (TOE Environment).
FMT_MTD.3	FMT_MTD.1	Yes	
FPT_FLS.1	None		
FPT_RCV.4	None		
FPT_TST.1	None		
FTP_TRP.1	None		
FDP_ITC.2	FDP_ACC.1 or FDP_IFC.1 FTP_ITC.1 or FTP_TRP.1 FPT_TDC.1	Yes Yes Yes	Higher-level SFR: FDP_IFC.2
FPT_TDC.1	None		

Table 8-5: Functional requirements dependency check

8.2.3 TOE SECURITY ASSURANCE REQUIREMENTS RATIONALE

The TOE meets the assurance requirements for EAL4 augmented by ALC_FLR.3 and AVA_VAN.4.

The TOE stresses assurance from best practice development practices. Through review of vendor-supplied evidence and independent testing the Assurance Requirements confirm the implementation of these practices.

The selected assurance level ensures the TOE fulfills national requirements for use in military and governmental networks, handling and separating information as specified in the TOE Overview and TOE Description.

8.3 TOE SUMMARY SPECIFICATION RATIONALE

8.3.1 TOE SECURITY FUNCTIONAL REQUIREMENTS SATISFACTION

This chapter demonstrates that the TOE Security Functions completely implement the TOE Security Functional Requirements.

Table 8-6 shows that each Security Functional Requirement is covered by at least one TOE Security Function and vice versa.

The table is supported by a rationale demonstrating that each SFR is completely implemented by one or more TSFs, described along with each TSF in Ch. 7.1.

SF Req.	SF.AUDIT	SF.CONFIGURATION	SF.DOMAIN_ISOLATION	SF.FILTER	SF.INTERNAL._PARTITIONING	SF.STREAM_AUTHENTIC	SF.SECURE_STATE	SF.SELF_TEST	SF.TRAF
FAU_GEN_EXT.1	X								
FAU_STG.1	X								
FAU_STG.3	X								
FCS_COP.1						X			
FDP_ETC.2						X			
FDP_IFC.2/r			X	X					
FDP_IFC.2/i					X				
FDP_IFF.1/r			X	X					X
FDP_IFF.1/i					X				
FDP_UIT.1						X			
FMT_MSA.1		X							
FMT_MSA.3		X							
FMT_MTD.1		X							
FMT_MTD.3		X							
FPT_FLS.1							X		
FPT_RCV.4							X		
FPT_TST.1								X	
FTP_TRP.1						X			

Table 8-6: Functional requirements satisfaction

8.4 PP RATIONALE

Not applicable

9. NOTES

9.1 NOTATION

The following notation is used for detailing Security Functional Requirements:

- **Bold text** is used for minor changes to the standard requirement text, to improve language or readability.
- *Italic text* is used to show where assignments or selections have been made by the developer.
- ~~Strikethrough~~ is used to show where requirement text or irrelevant assignment text has been removed from requirements.

Iteration of security requirements is done by adding an abbreviation to the requirement. The title of each related chapter will contain a short description or reference. Example:

FMT_MTS.1/ADM Management of TSF Data (System Administrators)

FMT_MTD.1/SYS Management of TSF Data (System partition API)

9.2 ABBREVIATION AND ACRONYMS

Acronym	**Extended**
IPC	Inter-Process Communication See IPC object below.
MLS	Multi-Level Security
MSM	MLS Security Management (Centre)
MVT	MLS Voice Terminal. The part of the Operator Controller Position responsible for handling SRTP audio streams and ensuring correct SRTP tagging.
NTP	Network Time Protocol, RFC 5905
OCP	Operator Controller Position
SIP	Session Initiation Protocol
SRTP	Secure Real-time Transport Protocol [SRTP] Secure profile of the Real-time Transport Protocol for audio and video over IP networks. Provides authentication, integrity and replay attack protection.

Table 9-1: Acronyms

9.3 TERMINOLOGY

Administrator	Personnel responsible for the maintenance of the TOE and connected services.
Advanced Host Controller Interface	A technical standard defined by Intel that specifies the operation of disk controllers using a serial interface.
Border Protection Device	Network nodes protecting the TOE from network based attacks and reconnaissance. A typical configuration involves a content inspecting firewall with intrusion detection, denial of service mitigation, and optionally antivirus and malware detection. The Border Protection Devices are selected by the TOE Environment according to the level of assurance required for the connected networks.
Attribute Based Access Control (ABAC)	The attribute based access control implemented by the TOE, which provides automated release of signalling traffic and audio streams based on the active configuration and their associated parameters/content.
IPC object	An information object used for TOE-internal communication between the TOE partitions, or between the TOE and software processes on the High and Low processing units. IPC objects are subject to control by the reference monitor, ensuring that only approved communication channels between TOE Partitions are allowed. The TSF implements its own mechanisms, in addition to relying on services provided by the separation kernel.
MLS Security Management (MSM)	The MLS Security Management (MSM) application is used for the management of all MLS Voice Guards (TOE) and MLS Voice Terminals (MVTs) within a MLS Voice Platform.
Partition	The TOE is separated into a number of partitions, managed by an embedded separation kernel. Each partition's resources, communication channels and available CPU time is managed completely by the separation kernel, ensuring that individual partitions are protected from interference from other partitions.
Partition ID	Uniquely identifies a separation kernel partition (across all processing units).
Process	Generic term for the runtime representation of TOE executable code being executed inside a TOE partition.
Process ID	Unique identifier for a specific process within the TOE (across all processing units).
Signalling traffic	Signalling traffic includes SIP signalling for establishment of VoIP connections [SIP], SNMP management and supervision, and radio remote control. Signalling events are processed separately from Audio Streams.
System Administrator	Users accessing the TOE management functions through the MSM or SW update interfaces.

Table 9-2: Terminology