# Security Target Lite

**for**

# Voice Stream Interceptor (VSI) Product

## Record of Changes

| Revision | Date | Changed By | Change Description |
|---|---|---|---|
| 0.1 | 08.12.2016 | ASPE | VSI ST Lite based on VSI ST document id SV000008 version 12. |
| 1 | 08.12.2016 | ASPE | Updated according to review sheet SV000073-0.1-RR. |
| 1.1 | 09.03.2021 | LBA | VSI ST Lite based on VSI ST document id SV000008 version 14. |
| 2 | 23.03.2021 | LBA | Updated according to review sheet SV000073-1.1-RR. |

**Table of Contents** **Page**

# 1 Introduction

## 1.1 Purpose

This document is the Security Target (ST) Lite for the Voice Stream Interceptor (VSI) product named in this document as Target of Evaluation (TOE). The Lite version is made for the public release of the Security Target (ST) for the Voice Stream Interceptor (VSI) product.

This Security Target aims at an Evaluation Assurance Level (EAL) 5.

The certification is made by SERTIT and has the project number SERTIT-072.

## 1.2 ST Reference

The security target is identified as:

| | |
|---|---|
| Title: | Security Target – VSI product |
| Version: | 14 |
| Authors: | PSTE and ASPE |
| Publication Date: | 23.03.2021 |
| Doc. Number: | SV000008. |

## 1.3 TOE Reference

The TOE is identified as:

| | |
|---|---|
| Name: | Voice Stream Interceptor |
| Stock Number: | SV000071 |
| Version: | 2 |

## 1.4 TOE Overview

### Two security domains

TOE is normally used in a system solution with two security domains as shown in Figure 1, but can also be used for multiple (more than 2) number of security domains as shown in Figure 3.

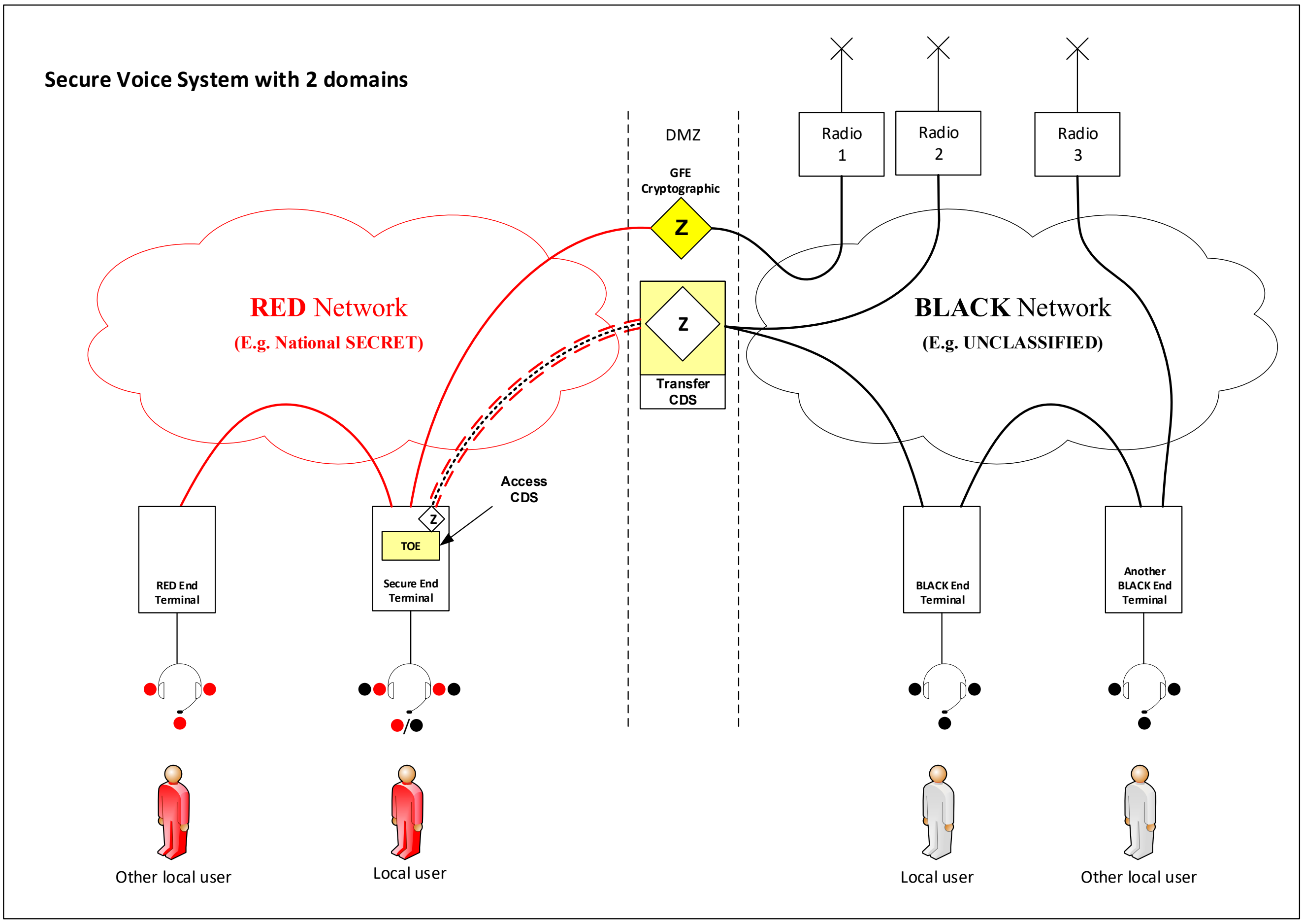

Figure 1 Voice System deployment with two security domains. The shown communication lines are bi-directional.

TOE makes sure that the Secure End Terminal can release voice streams, which only contains BLACK information (shown as dotted black line) and can be transported without loss of integrity (shown as dashed red line between Zs) over the classified network. The integrity check makes sure that no classified information in the classified network can be mixed with the BLACK (unclassified) voice stream. The user can make the selection between sending BLACK or RED information and gets an acknowledgement of the selection by a repeating non-secure warning tone while BLACK selection is made and the user is talking.

TOE is providing a security mechanism, which together with a DMZ is providing a secure release mechanism. In this way the Secure Voice System can interact with unclassified voice BLACK End Terminals or Radio (shown as example for Radio 2) outside the secure area. The unclassified network is not connected to the Internet.

For completeness the encryption of RED information has also been shown, where the Government Furnished Equipment (GFE) encryption is performed before it is transmitted via the radio (shown as example for Radio 1) and decrypted when receiving from the Radio into the RED Network.

The system solution is based on a “defence in depth” security strategy, where a number of security layers are applied. Each of the security layers are shown in Figure 2 both for incoming and outgoing data traffic.

TOE is controlling the suppression of RED incoming voice stream, such that while sending non-classified voice the possible pickup and cross talk of classified voice via the speaker to the microphone can be eliminated. The RED talking user (shown as ‘Other local user’ in Figure 1) will not be aware of the suppression.

### Deployment

The following example deployment illustrates how the TOE can be used (see Figure 2), where the defence in depth approach also has been included.

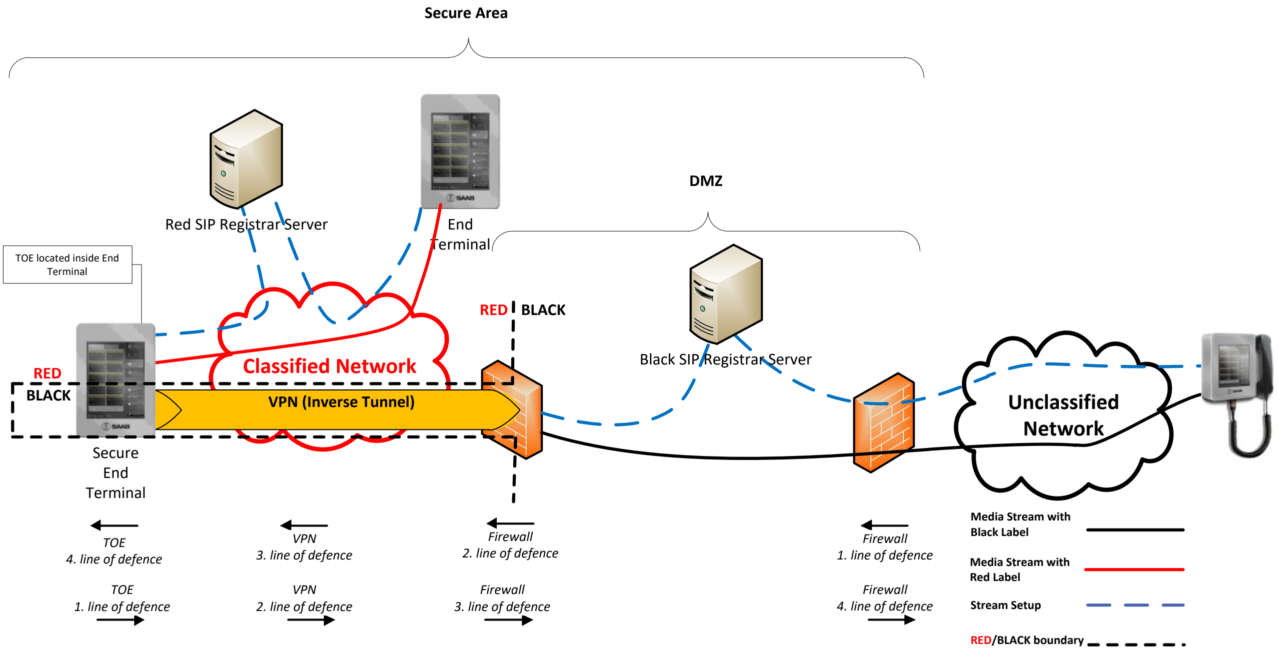

Figure 2 Example deployment of TOE in a secure voice system. Defence in depth has been shown as arrow lines of defence. TOE is located in the Secure End Terminal.

The following layers apply for incoming flow:

1. Only allowed protocol type can be sent from Unclassified Network to DMZ.
2. Only allowed protocol type can be sent from DMZ to VPN.
3. Integrity of BLACK information is intact, because RED network equipment cannot modify data inside the VPN tunnel.
4. Sanitation of incoming voice stream and setup is performed, such that defined protocol information is received.

The following layers apply for outgoing flow:

1. TOE performs separation between RED and BLACK information, such that only BLACK information is released to the VPN.

2. VPN is preventing RED information from the Classified Network to mix with the Inverse Tunnel.

3. The Firewall is only allowing information from the VPN to be transmitted, such that no information from the classified network can be transmitted into the DMZ.

4. Only allowed protocol type can be sent from DMZ to Unclassified Network.

IMPORTANT: According to NATO Security Policy an External System must NOT have remote access to the secure system. The Stream Setup in Figure 2 is performed in such a way that the DMZ is acting as a Trusted End Point. This means that the shown Stream Setup is terminated at the DMZ, e.g. no direct setup is performed between the External End Terminal and Secure End Terminal.

Figure 2 shows also that the communication line in Figure 1 actually is defined by the following:

- Voice Stream – the stream of IP packages containing voice information. The Real-time Transport Protocol (RTP) is used for the transportation of Voice Stream.

- Stream Setup – the communication required to setup the Voice Stream communication. The Session Initiation Protocol (SIP), Internet Group Management Protocol (IGMP) and Real-Time Transport Control Protocol (RTCP) are used for the Stream Setup.

The reason for dividing the communication is based on the required real time communication of Voice Stream.

The Stream Setup may require a so called SIP Registrar such that end points can send Voice Stream according to the setup. Sanitization of Stream Setup is performed before send to DMZ, which prevent it from being misused.

TOE stores audits in the underlying IT environment, where self-test, failures and success are stored for later retrieval.

## Multiple security domains

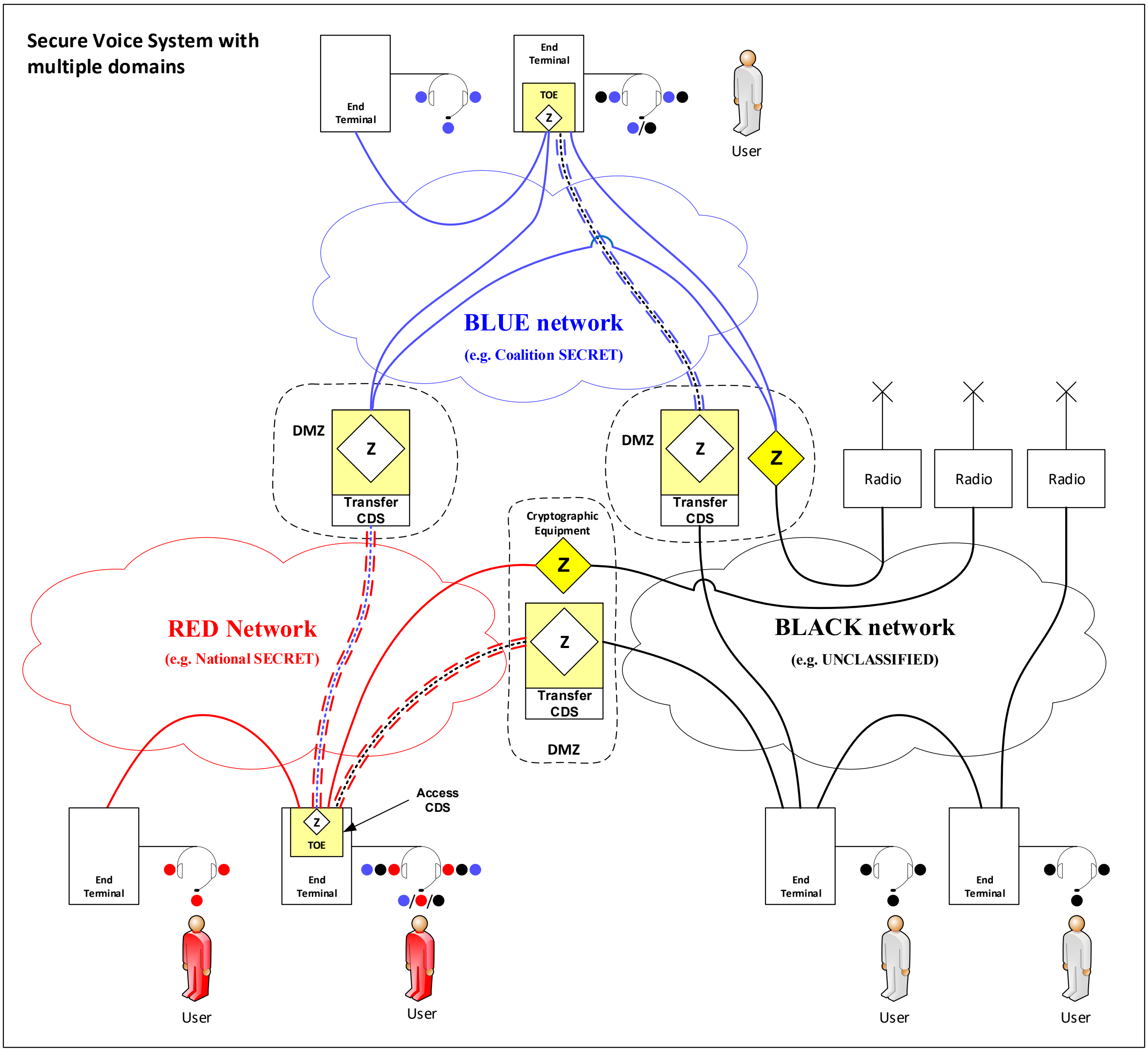

Figure 3 Voice System deployment with more than two security domains.

Support for additional classification levels (as example NATO classified information) is shown in Figure 3. This is performed in a similar way as BLACK information release. In the example, the additional domain is shown as BLUE information, which is transported without loss of integrity (shown as dashed red line between Zs) over the national classified network. The integrity check makes sure that no RED information in the national classified network can be mixed with the BLUE voice stream.

The user can make the selection between sending BLACK, BLUE or RED information. The user gets an acknowledgement of the selection by repeating non-secure warning tone respectively for BLUE or BLACK while BLUE or BLACK selection is made and the user is talking.

TOE is controlling the suppression of BLUE or RED incoming voice stream, such that while sending non-classified BLACK voice the possible pickup and cross talk of classified BLUE or RED voice via the speaker to the microphone can be eliminated. TOE does also support the suppression of RED voice stream, such that while sending BLUE voice the possible pickup and cross talk of classified RED voice to BLUE voice release can be eliminated.

### 1.4.1 Usage and major security features of the TOE

TOE has been designed in such a way that it can be integrated into an overall system solution, where existing standard trusted products are used.

TOE makes it possible to provide the following important capabilities:

1. Secure Conferencing – multiple users can share a conference at the same classification level.
2. Release of classified and unclassified voice to another enclave with the correct classification level.

TOE located in RED domain provides the following security feature, to support the above capabilities:

- TOE is a secure separation mechanism for voice streams, such that:
    - Transmission of BLACK streams to a DMZ does not contain any RED or BLUE stream information.
    - Transmission of BLUE streams to a DMZ does not contain any RED stream information.
    - The user can listen to BLACK, BLUE and RED streams at the same time.
- TOE can minimise Cross talk of classified voice by suppression of incoming RED voice stream to the speaker while sending BLUE voice.
- TOE can minimise Cross talk of classified voice by suppression of incoming RED and BLUE voice stream to the speaker while sending BLACK voice.

Cross talk minimization is a feature, which can be enabled or disabled by a TOE configuration.

TOE located in BLUE domain provides the same security capabilities without the use of RED streams.

**Domain generalisation**

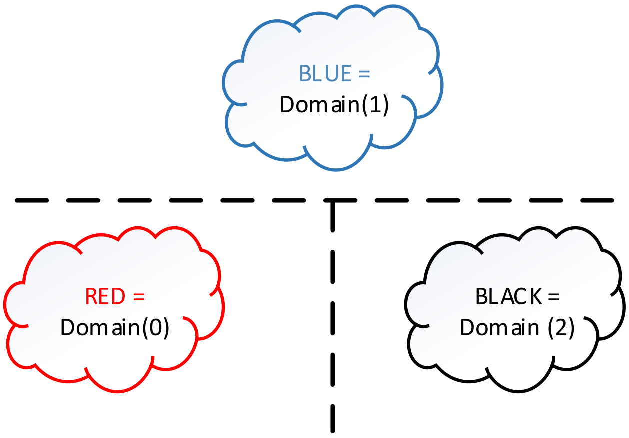

Figure 4 - Classification domains and their relation to the used colour examples.

The description of different classifications has used colours RED, BLUE and BLACK, because RED and BLACK are well known colour schemes used for voice systems. The BLUE colour represents other domains than RED and shall be seen as representing a number of individual domains including both classified and non-classified domains. In this way, TOE supports 3 or more domains.

Generalisation of the RED, BLUE and BLACK voice streams is performed by the following definition:

> *Domain* is an ordered list of voice streams, where *Domain(q)* is the q'th voice stream with domain(q) classification, where $q$=0, 1, 2, 3, …, $n$-1 and $n$ is the total number of domain classifications. *Domain(n-*1*)* is the domain with BLACK (non-classified) or lowest classification and *Domain(*0*)* is the domain with RED or highest classification in the ordered list of voice streams.
>
> TOE can be located in a given *Domain(h)* where $h$ is the highest classification of the domain. TOE is capable of being used for *Domain(k)* classifications, where $k$ belongs to $h$, $h$+1, …, $n$-1. TOE is capable of releasing information to other *Domain(r)*, where $r$ belongs to $h$+1, $h$+2, …, $n$-1.

In the rest of the document will *Domain(h)*, *Domain(k)* and *Domain(r)* be used in accordance with the above definitions.

Examples in relation to Figure 4:

- TOE located in RED domain can be used for *Domain(*0*)*, *Domain(*1*)* and *Domain(*2*)* classification and can release to *Domain(*1*)* and *Domain(*2*)*.
- TOE located in the BLUE domain can be used for *Domain(*1*)* and *Domain (*2*)* classification and can release to *Domain(*2*)*.

- There will not be any TOE in BLACK domain, because no release to a lower classification is possible.

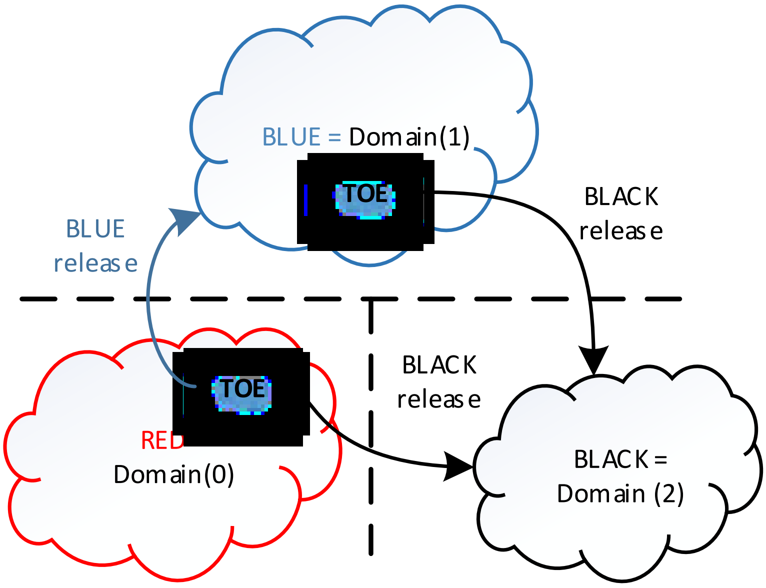

Figure 5 - TOE location in different domains and the possible release of information.

### 1.4.2 TOE type

The Voice Stream Interceptor Product (the TOE) is categorized as an Access Cross Domain Solution (CDS), where voice information with different classification levels can be handled.

### 1.4.3 Required non-TOE hardware/software/firmware

TOE requires the following non-TOE software:

- Common Criteria approved Linux Operating System (reflects the assumption A.SECURE_OS).

- IPsec tunnel (reflects the assumption A.TRUSTED_VPN).

TOE requires the following non-TOE hardware:

- Trusted Platform Module (TPM).

However, the Common Criteria approved Linux Operating System might have indirect requirements.

## 1.5 TOE Description

TOE must control all the communication to the Inverse Tunnels, because TOE makes sure that no *Domain(h)* Voice is sent to the Inverse Tunnel and the correct Voice Stream is sent to a given Inverse Tunnel. The following type of communication has been identified:

1. Voice Stream is composed of the following information:
    a. Voice contents.
    b. Header information.
2. Stream Setup is a set of control protocols and is not intended to carry voice contents.

TOE can be seen as an interceptor between the user application and the Inverse Tunnel, where the interceptor performs the following to prevent *Domain(h)* voice being sent to the Inverse Tunnel:

- The voice contents of the Voice Stream from the application might contain *Domain(h)* voice and is therefore substituted with voice from the microphone attached to TOE.
- Voice Stream is sent to the Inverse Tunnel if and only if the selector is *Domain(r)*, which means that the user is talking *Domain(r)*. To make sure that the user is aware of the *Domain(r)* TALK selection TOE is providing a non-secure warning tone for *Domain(r)*.
- The header information of the Voice Stream could be misused to contain *Domain(h)* voice and is therefore sanitized before it is sent to the Inverse Tunnel.
- The Stream Setup could be misused to contain *Domain(h)* voice and is therefore sanitized before sent to the Inverse Tunnel.
- Voice Stream and Stream Setup received from the Inverse Tunnel could corrupt the integrity of TOE and therefor sanitization is performed of the incoming information from the Inverse Tunnel.
- The user can listen to all *Domain(k)* voice streams. Received voice could cross talk to the microphone, such that higher classified voice would be released on a lower *Domain(m)* classified stream during a *Domain(m)* talk operation. To prevent this unintended release all higher classified received stream can be suppressed. E.g. all higher classified *Domain(p)* streams are suppressed where $p$ is $h$, $h$+1, …, $m$-1.

### 1.5.1 Physical scope

TOE is purely software and can be installed on several physical devices as long as the non-TOE software requirements in section 1.4.3 are valid.

### 1.5.2 Logical scope

The logical scope of TOE is defined by the logical interface in Figure 6. The user can perform *Domain(k)* voice conversations.

The user wants to perform a *Domain(r)* conversation with another Terminal or Radio on the *Domain(r)* network. The following steps are performed:

1. The user makes a *Domain(r)* TALK selection to let TOE know that a *Domain(r)* conversation shall take place.

2. The Non-Trusted Application will initiate the setup of the communication with the Terminal or Radio located on the *Domain(r)* network. The setup is performed with the Requested *Domain(r)* Stream Setup and Sanitized *Domain(r)* Stream Setup interface to/from TOE.

3. The User can listen to the *Domain(r)* voice received on Sanitized *Domain(r)* Voice Stream interface from TOE.

4. The User can talk to the Terminal or Radio on *Domain(r)* network by letting the Non-Trusted Application send voice stream to Requested *Domain(r)* Voice Stream TOE interface and the user is talking into the Microphone TOE interface. The voice stream contents of Requested *Domain(r)* Voice Stream will be substituted with voice from the Microphone interface, such that no higher classified voice stream is contained in the outgoing voice stream. Sanity check of Requested *Domain(r)* Voice Stream is performed.

5. The user will get a non-secure warning tone on the Indicator (speaker) TOE interface as acknowledge from TOE.

6. The user will repeatedly get a non-secure warning tone for the given domain from TOE during the conversation to make him aware that he still is talking *Domain(r)*.

7. The user is also able to listen to *Domain(h)* conversation from the *Domain(h)* Voice Stream TOE interface, when he is not talking.

8. The user can make a *Domain(h)* TALK selection on the Selection TOE interface and continue with a *Domain(h)* conversation as described below.

9. The user can terminate the conversation by letting the Non-Trusted Application initiate a termination via Requested *Domain(r)* Stream Setup and Sanitized *Domain(r)* Stream Setup TOE Interface.

The user wants to perform a *Domain(h)* conversation with another Terminal located on the *Domain(h)* network. The following steps are performed:

1. The user makes a *Domain(h)* TALK selection on the Selection TOE Interface to let TOE know that a *Domain(h)* conversation shall take place.

2. The Non-Trusted Application will initiate the setup of the communication with the Terminal located on the *Domain(h)* network. The setup is performed directly with the other Terminal and TOE is not involved.

3. The User can listen to the *Domain(h)* voice received on *Domain(h)* Voice Stream TOE Interface.

4. The User can talk to the Terminal on *Domain(h)* network by sending voice stream directly to the other terminal. TOE is not involved.

5. The user can terminate the conversation by letting the Non-Trusted Application initiate a termination.  The termination is performed directly with the other Terminal and TOE is not involved.

Self-test is performed during the start-up of TOE. During operation events generated by TOE are stored in the underlying Operating System, which is part of the IT Environment of TOE. In cases where TOE is detecting Audio Failure and Network Failure the secure state is preserved by blocking the Outgoing *Domain(r)* Stream Setup and Outgoing *Domain(r)* Voice Stream.

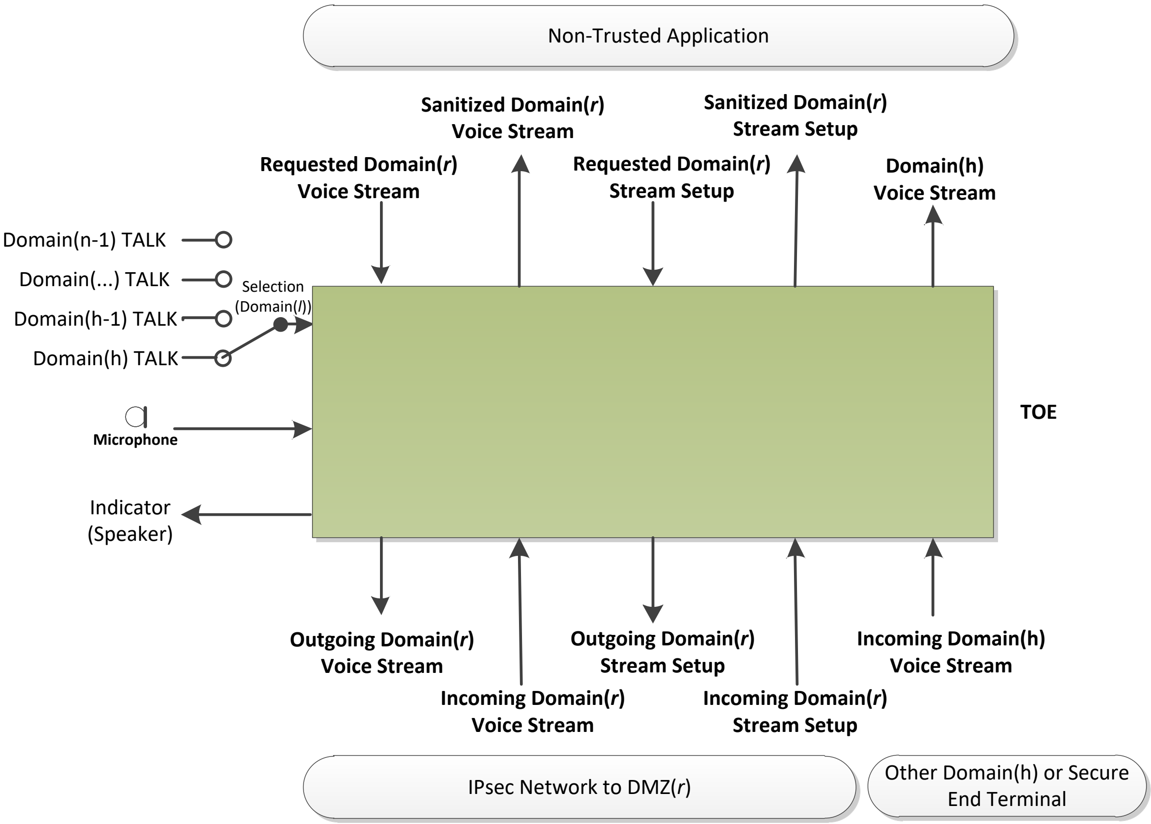
Non-Trusted Application
Sanitized Domain(r) Voice Stream
Sanitized Domain(r) Stream Setup
Requested Domain(r) Voice Stream
Requested Domain(r) Stream Setup
Domain(h) Voice Stream
Domain(n-1) TALK
Domain(...) TALK
Domain(h-1) TALK
Domain(h) TALK
Selection (Domain(l))
Microphone
Indicator (Speaker)
TOE
Outgoing Domain(r) Voice Stream
Outgoing Domain(r) Stream Setup
Incoming Domain(h) Voice Stream
Incoming Domain(r) Voice Stream
Incoming Domain(r) Stream Setup
IPsec Network to DMZ(r)
Other Domain(h) or Secure End Terminal

Figure 6: Overview of TOE with logical interfaces.

Each interface is described in the following table:

| Interface | Description |
|---|---|
| Requested *Domain(r)* Voice Stream | The requested voice stream to be sent on Outgoing *Domain(r)* Voice Stream, which will be sanitized before it is sent. |
| Sanitized *Domain(r)* Voice Stream | The sanitized *Domain(r)* voice stream of the Incoming *Domain(r)* Voice Stream. |
| Requested *Domain(r)* Stream Setup | The *Domain(r)* Stream Setup to be sent on the Outgoing *Domain(r)* Stream Setup, which will be sanitized before it is sent. |
| Sanitized *Domain(r)* Stream Setup | The sanitized *Domain(r)* stream setup of the Incoming *Domain(r)* Stream Setup. |
| *Domain(h)* Voice Stream | The possibly silenced voice stream of the Incoming *Domain(h)* Voice Stream. |
| Incoming *Domain(h)* Voice Stream | The *Domain(h)* Voice Stream to be sent on *Domain(h)* Voice Stream interface to the Non-Trusted Application. |
| Incoming *Domain(r)* Stream Setup | The *Domain(r)* Stream Setup to be sanitized and sent on the Sanitized *Domain(r)* Stream Setup to the Non-Trusted Application. |
| Outgoing *Domain(r)* Stream Setup | The Sanitized *Domain(r)* stream setup of the Requested *Domain(r)* Stream Setup. |
| Incoming *Domain(r)* Voice Stream | The Incoming *Domain(r)* Voice Stream, which will be sanitized and sent on the Sanitized *Domain(r)* Voice Stream interface. |
| Outgoing *Domain(r)* Voice Stream | The substituted *Domain(r)* Voice Stream of the Requested *Domain(r)* Voice Stream. |
| Selection | Selection by the user to talk *Domain(k)*. |
| Microphone | Voice samples from the microphone. |
| Indicator (Speaker) | Speaker for indication of the non-secure warning tone. |

Note: No Outgoing *Domain(h)* Voice Stream has been shown on Figure 6. Outgoing *Domain(h)* Voice Stream can be sent to other TSS on the *Domain(h)* Network without restriction and does therefore not require to be intercepted by TOE.

‘IPsec Network to DMZ’ indicates that the communication of ‘Outgoing *Domain(r)* Voice Stream’, ‘Incoming *Domain(r)* Voice Stream’, ‘Outgoing *Domain(r)* Stream Setup’ and ‘Incoming *Domain(r)* Stream Setup’ are communicated in the Inverse Tunnel, such that communication with *DMZ(r)* can utilise the *Domain(h)* network as a transport medium.

‘Other *Domain(h)* or Secure End Terminal’ shows that ‘Incoming *Domain(h)* Voice Stream’ is transported directly on the *Domain(h)* network and is not using an Inverse Tunnel.

‘Non-Trusted Application’ can be any application utilising the TOE functionality. The application is non-trusted, because TOE is making sure that no higher classified information is released via the Inverse Tunnel.

## 1.6 Approval & Maintenance of this document

This document is part of the VSI Common Criteria Evaluation and will be approved and maintained accordingly.

## 1.7 References

| Ref. No | Title | Identification |
|---|---|---|
| 1. | Common Criteria<br>Part 1: Introduction and general model<br>Part 2: Security functional components<br>Part 3: Security assurance components<br>September 2012, Version 3.1 R4 | CC |

## 1.8 Terms & definitions

| Word/abbreviation/acronym | Explanation |
|---|---|
| Access CDS | General category of IT products e.g. keyboard, video and mouse (KVM) switch etc. |
| CC | Common Criteria. |
| CDS | Cross Domain Solution |
| CIS | Communications and Information Systems. |
| DMZ | De-Militarized Zone. |
| EAL | Evaluation Assurance Level. |
| Inverse tunnel | Mechanism protecting lower classified information in a network at a higher accreditation level (e.g. UNCLASSIFIED information in a SECRET network). |
| LSE | Local Security Environment – A controlled access facility. |
| IGMP | Internet Group Management Protocol |
| IP | Internet Protocol. |
| OSP | Organizational Security Policies. |
| PP | Protection Profile. |
| RTCP | Real-Time Transport Control Protocol |
| RTP | Real-time Transport Protocol |
| Secure End Terminal | End Terminal located in the RED domain including a TOE |
| Secure Voice over IP (SVoIP) | End-to-end secure voice communications over IP-based networks. |
| SERTIT | Norwegian Certification Authority for IT Security |
| SF | Security Function |
| SIP | Session Initiation Protocol |
| ST | Security Target. |
| TOE | Target of Evaluation |
| Transfer CDS | General category of IT products e.g. firewall, content filter, crypto etc. |
| TSF | TOE Security Function |
| TSS | Tactical Subscriber Station is the SAAB product name for the End Terminal |

| Word/abbreviation/acronym | Explanation |
|---|---|
| Voice over Secure IP (VoSIP) | Voice communications that use an encrypted IP network for transmission; however the voice communications are not encrypted end-to end (handset-to-handset).<br>Note that this differs from SVoIP in that VoSIP usually has an unencrypted local VoIP network using standard commercial off-the-shelf (COTS) VoIP phones, which interconnects with a secure IP network for wider communications. |
| VPN | Virtual Private Network |
| Voice Stream Interceptor (VSI) | SAAB product name for the TOE categorized as an Access CDS |

# 2 CONFORMANCE CLAIMS

## 2.1 CC Conformance Claim

The ST is Common Criteria Version 3.1 R4 Part 2 conformant and Part 3 conformant; no extended components have been defined.

## 2.2 PP Claim

The ST does not claim conformance to any registered Protection Profile.

## 2.3 Package Claim

The ST claims conformance to the EAL5 assurance package defined in Part 3 of the Common Criteria Version 3.1 R4.

## 2.4 Conformance Rationale

No conformance rationale is necessary for this evaluation since this ST does not claim conformance to a Protection Profile.

# 3 SECURITY PROBLEM DEFINITION

The purpose of the security problem definition is to define the scope and nature of the security problem the TOE is intended to address.

The environment to which the TOE shall cope with is defined as a number of assets, threat agents, threats, assumptions and policies.

The security problem definition consists of identified assumptions about the environment, threats to assets and organizational security policies.

To facilitate easy definition of threats, organisational security policies, assumptions, security objectives and security requirements, the subjects, objects and operations to be used in the ST are defined first.

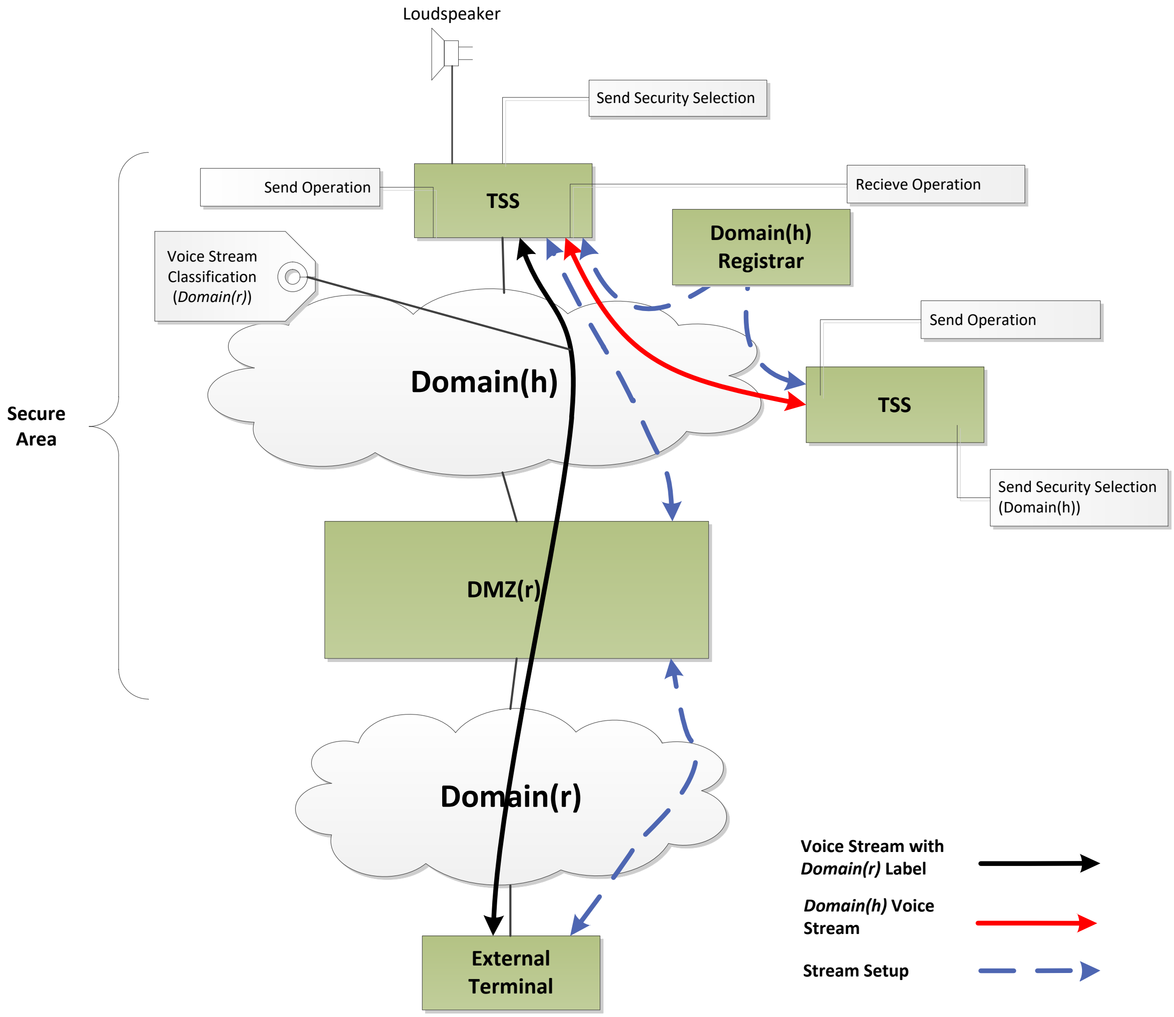

Figure 7: Overview of subjects, objects, security attributes and operations. Users and administrators have not been shown in the figure.

Figure 7 gives an overview of the identified subjects, objects, security attributes and operations, which are defined and described in the following tables. The information flow for *Domain(h)*, *Domain(r)* Voice Stream and Stream setup is also shown, such that information flow end points can be seen. Please note that Stream Setup is terminated by the *Domain(h)* Registrar (for *Domain(h)* voice setup) and *DMZ(r)* (for *Domain(r)* voice setup). VPN tunnel is not shown, because it is not import for the identification of subject and objects.

The personnel that interact with the TOE are:

| Subjects | |
|---|---|
| **Short name** | **Description** |
| S.ADMIN | Authenticated authorized administrator of the TOE. |
| S.USER | Authorized users of the TOE. |

The systems (equipment) that interact with the TOE are:

| Subjects | |
|---|---|
| **Short name** | **Description** |
| S.TSS | Voice End Terminal located inside the secure area (Secure End Terminal). |
| S.DMZ(*r*) | *DMZ(r)* between the *Domain(r)* and *Domain(h)* network with trusted firewall, voice registrar and other means for a secure connection between the two networks. |
| S.EXTERNAL_TERMINAL | Non trusted End Terminal located outside the secure area. |

The (data) objects for the TOE that the TOE will operate upon are:

| Objects | |
|---|---|
| **Short name** | **Description** |
| O. VOICE_STREAM(*r*) | The *Domain(r)* voice stream flowing both in and out from/to the *domain(r)* classified network. |
| O. VOICE_STREAM(*h*) | The *Domain(h)* voice stream flowing from the domain(h) classified network. |
| O.STREAM_SETUP | The setup information for setting up the standard voice stream between Secure End Terminal and External End Terminal.<br>Note: Setup Information is not used for the setup/management of secure voice, only for stream setup. |

| Security Attributes | |
|---|---|
| **Short name** | **Description** |
| SA.VOICE_STREAM_CLASSIFICATION | *Domain(k)* Voice Stream has domain(k) classification. |

| Operations | |
|---|---|
| **Short name** | **Description** |
| Receive | The Authorized user (S.USER) is receiving a Voice Stream. |
| Send | The Authorized user (S.USER) is sending a Voice Stream. Depending on the TALK Selection the send voice will only be able to send *Domain(r)* voice or block the stream.<br>Note: Receive and Send operation can be conducted at the same time; they do not exclude each other. |

## 3.1 Threats

### 3.1.1 Assets

| Assets | |
|---|---|
| **Short name** | **Description** |
| AS.VOICE | *Domain(k)* Classified Voice Stream. |

### 3.1.2 Threat Agents

The following subjects are capable to effectuate threats for the TOE (i.e. Threat Agents):

| Threat Agents | |
|---|---|
| **Short name** | **Description** |
| TA.EXTERNAL | Personnel with no authorized access to the Secure System. These threat agents may try to access the Classified Voice Stream (AS. VOICE) information and may have "unlimited" resources supporting them. |
| TA.INTERNAL | Authenticated authorized users or resource of the Secure System, which are not authorised TOE users. These threat agents may try to manipulate the Classified Voice Stream (AS.VOICE) such that they can be released outside the Secure System. |
| TA.USER | Authenticated authorized users of the TOE. These threat agents may intentionally or unintentionally perform unauthorized actions. |
| TA.TSS_APPLICATION | The Secure End Terminal application utilising the TOE. |

### 3.1.3 Identification of Threats

| Threats | |
|---|---|
| **Short name** | **Description** |
| T.TERMINAL_INTEGRITY | The Secure End Terminal (TA.TSS_APPLICATION) may mix Non-Classified and Classified Voice Stream (AS.VOICE), which could violate the security rules. |
| T.NETWORK_INTEGRITY | An internal user or resource (TA.INTERNAL) may corrupt the Voice Stream, such that Classified Voice Stream (AS.VOICE) could be released to unclassified network. |
| T.WRONG_LABEL | The user (TA.USER) may select a wrong classification of a Voice Stream, which could lead to a violation of the security rules for Classified Voice Stream (AS.VOICE). |
| T.CORRUPT_STREAM | An external user (TA.EXTERNAL) could send a corrupt incoming voice stream, so that a Secure End Terminal integrity failure could lead to a violation of the security rules for Classified Voice Stream (AS.VOICE). |
| T.SETUP | Resources in the DMZ might be used by an external user (TA.EXTERNAL) to perform a tampering setup such that a violation of the security rules for Classified Voice Stream (AS.VOICE) may occur. |
| T.CORRUPT_FORMAT | An external user (TA.EXTERNAL) might corrupt the stream setup, so that a Secure End Terminal integrity failure could lead to a violation of the security rules for Classified Voice Stream (AS.VOICE). |

The security rules used in the above threat is referring to the security policy P.LABELLING_POLICY in next section.

## 3.2 Organizational Security Policies (OSPs)

The operational environment of the TOE is Communications and Information Systems (CIS). CIS are an essential part of military operations and provide commanders at all levels with the means to exercise Command and Control (C2) and disseminate classified information. CIS must be accredited specifically to handle classified information by a National Security Authority (NSA). Operating authority who is handling accredited CIS classified information system must issue instructions for processing, handling and accounting for classified information.

CIS handling classified information shall use a trusted release mechanism for release of *Domain(r)* Voice Stream information. The trusted release mechanism provided by the TOE shall prevent unintended release of *higher* classified stream information.

The main functionality of the TOE is to implement the policy for labelling in an automated way. The TOE documentation supports operating authorities with CIS handling classified information to be accredited, where *Domain(r)* Voice Stream information flows by tunnelling. The tunnelling provides a means to interconnect the TOE and the unclassified network using the classified network as communication bearer service.

| OSP | |
|---|---|
| **Policy** | **Description** |
| P.CIS_DEFINITION_POLICY | The TOE, classified and unclassified network are according to AC/322-D/0030 defined as one CIS and under the control of one and the same CIS operating authority. |
| P.CIS_PERSONNEL_POLICY | CIS operators are military personnel with authorised access to the CIS based on their security clearance. |
| P.CIS_INTERCONNECTION_POLICY | Interconnection from both CIS classified and unclassified network to other CIS are known and controlled according to AC/322-D/0030 by the CIS operating authority. |
| P.VOICE_PROCEDURES_POLICY | The TOE shall, by an appropriate release mechanism, pass speech traffic as securely as possible consistent with accuracy, speed and the needs of command and control (C2) according to the Combined Communications Electronics Board (CCEB) in the Allied Communications Publication (ACP) 125 “Radiotelephone Procedures”. |
| P.LABELLING_POLICY | The TOE shall implement and comply with the labelling policy appropriate for handling classified information. This policy defines the<br>• *Labelling*: the trusted indication of the classification level of the voice stream.<br>• *Security rules:* the set of rules for the circumstances under which information will be allowed for declassification. In [SFP. STREAM(*r*)] this policy is fully defined, see section 6.1.2.1 and 6.1.3.1. |

## 3.3 Assumptions

The following are threats handled as assumptions, since it is not the TOE’s responsibility to counter these threats.

| Assumptions | |
|---|---|
| **Assumption** | **Description** |
| A.SECURE_IP | Secure End Terminal containing TOE is connected to a Secure IP network, which means that measures for the secure transmission is fulfilled. |
| A.SECURE_LOCATION | TOE is located in a secure area. |
| A.SECURE_OS | TOE is executing on a Common Criteria evaluated OS with Assurance Level 3 or higher, or relevant PP, and has been configured with a hardening setup. |
| A.TRUSTED_VPN | TOE has a VPN connection to the *DMZ(r)*, to prevent access to classified voice stream (AS.VOICE). |

| | |
|---|---|
| | Note: A threat could be stated instead of the assumption. However, the trusted VPN is very generic security functionality and will be available in the IT Environment. Therefore the threat has not been stated and instead an assumption has been made. |

# 4 SECURITY OBJECTIVES

The high-level solution is divided into a two part solution, one part is the TOE, and the second part is the operational environment of TOE. Each part of the high-level solution has its own set of objectives to address the security problem.

## 4.1 TOE Security Objectives

| TOE Security Objectives | |
|---|---|
| **Objective** | **Description** |
| OT.SANITY_CHECK | The TOE shall perform sanity check of Requested *Domain(r)* Voice Stream Header, Requested *Domain(r)* Stream Setup, Incoming *Domain(r)* Voice Stream Header and Incoming *Domain(r)* Stream Setup. |
| OT.SELECTOR | The TOE shall support the user in the reliable *Domain(k)* TALK operation.<br>The TOE shall issue a non-secure warning tone when receiving the Requested *Domain(r)* Voice Stream and the selector is in position *Domain(r)* TALK.<br>The non-secure warning tone is repeated periodically, while receiving Requested *Domain(r)* Voice Stream and the selector is in position *Domain(r)* TALK. |
| OT.SUBSTITUTION | The TOE shall provide Outgoing *Domain(r)* Voice Stream, where the Voice content of Requested *Domain(r)* Voice Stream is substituted with the incoming microphone stream.<br>Substitution with incoming microphone stream is only made, when selector is *Domain(r)* TALK. Otherwise, the outgoing Voice Stream is blocked. |
| OT.SEND | The TOE shall send Domain(r) Voice Stream and Setup through the trusted release (OE.TRUSTED_RELEASE). |
| OT.LOG | The TOE shall store the failure of the substitution, integrity check and sanity check in a log. |
| OT.ROBUST | The TOE shall be robust, such that internal TOE errors are handled appropriately. |
| OT.SUPPRESS | The TOE can prevent cross talk from the local speaker of the incoming *Domain(p)* Voice Stream, where $p$ is $h$, $h$+1, …, $m$-1 and selector is *Domain(m)* TALK and receiving Requested Voice Stream. |

## 4.2 Operational Environment Security Objectives

This section defines the Security Objectives of the TOE and its environment. The Security Objectives reflect the stated intent to counter all identified threats. They comply with all organizational security policies identified and uphold all assumptions.

| Operational Environment Security Objectives | |
|---|---|
| **Objective** | **Description** |
| OE.SECURE_IP | The communication infrastructure used by the TOE shall be a Secure IP. |
| OE.SECURE_LOCATION | The TOE shall be installed within controlled access facilities (LSE). |
| OE.ENVIRONMENTAL | The TOE shall operate within the manufacturer's environmental specification. |
| OE.ACOUSTIC_FEEDBACK | The risk of acoustic feedback in the environment shall be addressed by operational procedures. |
| OE.INSTRUCTED_USERS | Trusted direct users are assigned, instructed and shall act as such in using equipment where the TOE is located. |
| OE.INSTRUCTED_ADMIN | Trusted direct users are assigned, instructed and shall act as such to manage the TOE. |
| OE.EVALUATED_OS | The operating system the TOE makes use of shall be evaluated OS. SFR FPT_STM.1, FMT_MSA.1 and FMT_SMR.1 shall be part of the OS due to dependencies between TOE SFRs. |
| OE.LOG_ACCESS | The IT Environment shall allow only the administrator (S.ADMIN) read access to the Log. |
| OE.READ_LOG | The S.ADMIN shall be able to read the TOE Log. |
| OE.TRUSTED_RELEASE | A trusted release security mechanism between the classified network within the LSE and the external system shall be used for the release of Unclassified Voice Streams. The trusted Voice Stream Labelling of the TOE is utilised by the trusted release security mechanism. |
| OE.TRUSTED_REGISTRAR | A trusted release security mechanism between the classified network within the LSE and the external system shall provide a trusted SIP Registrar. |
| OE.PREVENT_ACCESS | A Trusted VPN between the TOE and *DMZ(r)* shall be used. The trusted VPN act as an inverse tunnel, such that uncontrolled access to the classified network is prevented. In this way, the Classified Network is only used as a pure transport of voice. |

## 4.3 Security Objectives Rationale

### 4.3.1 Security Objective Coverage

This section provides tracings between objectives for the TOE and what threats are being countered by the objective(s) and what OSPs being enforced by the security objectives.

Also the tracing between each security objective for the operational environment and the threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective is shown.

| Threats & Assumptions<br>Objectives | T.TERMINAL_INTEGRITY | T.NETWORK_INTEGRITY | T.WRONG_LABEL | T.CORRUPT_STREAM | T.SETUP | T.CORRUPT_FORMAT | A.SECURE_IP | A.SECURE_LOCATION | A.SECURE_OS | A.TRUSTED_VPN | P.CIS_DEFINITION_POLICY | P.CIS_PERSONNEL_POLICY | P.CIS_INTERCONNECTION_POLICY | P.VOICE_PROCEDURES_POLICY | P.LABELLING_POLICY |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| OT.SELECTOR | X | | X | | | | | | | | | | | X | X |
| OT.SANITY_CHECK | X | | | X | X | X | | | | | | | | X | X |
| OT.SUBSTITUTION | X | | | | | | | | | | | | | X | X |
| OT.SEND | | | X | | | | | | | | | | | X | X |
| OT.LOG | X | | | | | | | | | | | | | | |
| OT.ROBUST | X | | | | | | | | | | | | | | |
| OT.SUPPRESS | X | | | | | | | | | | | | | | |
| OE.SECURE_IP | | X | | | | | X | | | | | | | | |
| OE.SECURE_LOCATION | | X | | | | | | X | | | X | X | | | |
| OE.ENVIRONMENTAL | X | | X | | | | | | | | | | | | |
| OE.ACOUSTIC_FEEDBACK | X | | | | | | | | | | | | | | |
| OE.INSTRUCTED_USERS | | | X | | | | X | X | X | | | X | | | |
| OE.INSTRUCTED_ADMIN | X | | | | | | X | X | X | X | | X | | | |
| OE.EVALUATED_OS | X | | X | | | | | | X | | | | | | |
| OE.LOG_ACCESS | X | | | X | | | | | | | | | | | |
| OE.READ_LOG | X | | | X | | | | | | | | | | | |
| OE.TRUSTED_RELEASE | X | X | | | | | | | | | | | X | | |
| OE.TRUSTED_REGISTRAR | | | | | X | | | | | | | | | | |
| OE.PREVENT_ACCESS | | X | | X | | | | | | X | | | | | |

## 4.4 Security Objectives Sufficiency

### 4.4.1 Threats

#### 4.4.1.1 T.TERMINAL_INTEGRITY

The End Terminal has an underlying execution environment, which must guarantee no tampering and therefore requires a secure execution platform provided by the OE.EVALUATED_OS and OE.ENVIRONMENTAL. The robustness of TOE due to internal errors is handled by OT.ROBUST.

The main function of the TOE is to perform a secure substitution (OT.SUBSTITUTION) of microphone signal according to security rules. Furthermore, the substitution relies on that the microphone stream is reflecting the TA.USER classification selection OT.SELECTOR. The substitution relies on correct Requested *Domain(r)* Voice Stream, which is checked by OT.SANITY_CHECK.

The microphone might pick up unintended classified voice in the environment, which is handled by operational procedure OE.ACOUSTIC_FEEDBACK and OT.SUPPRESS.

The resulting substituted output from the TOE can be used by a trusted release mechanism OE.TRUSTED_RELEASE.

Outgoing *Domain(r)* Voice Stream will be blocked when attempting to send while OT.SELECTOR is *Domain(h)* TALK.

Audits will be stored for later read by the environment OE.READ_LOG in OT.LOG. To prevent other than OE.INSTRUCTED_ADMIN to read the log the log is protected by OE.LOG_ACCESS.

#### 4.4.1.2 T.NETWORK_INTEGRITY

The transportation of the voice stream is performed by an OE.PREVENT_ACCESS on OE.SECURE_IP network in an OE.SECURE_LOCATION, such that the AS.VOICE voice streams is handled securely.

Furthermore, an unintended alternation might be performed in the secure network of the Outgoing *Domain(r)* Voice Stream. The alternation is protected by the OE.TRUSTED_RELEASE.

#### 4.4.1.3 T.WRONG_LABEL

The labeling of the voice stream is based on a trusted OT.SEND. The read back (OT.SELECTOR) of the label by OT.SEND must be observed by OE.INSTRUCTED_USERS. The internal handling of the label cannot be manipulated due to the underlying OE.EVALUATED_OS working at the correct OE.ENVIRONMENTAL conditions.

#### 4.4.1.4 T.CORRUPT_STREAM

Unauthorised access to stream is prevented by OE.PREVENT_ACCESS and Sanity check (OT.SANITY_CHECK) will detect corrupt incoming *Domain(r)* Voice Stream or Requested *Domain(r)* Voice Stream, so that they are according to the expected package format.

Audits will be stored for later read by the environment OE.READ_LOG in OT.LOG. To prevent other than OE.INSTRUCTED_ADMIN to read the log the log is protected by OE.LOG_ACCESS.

#### 4.4.1.5 T.SETUP

Illegal format of Stream Setup is prevented by OT.SANITY_CHECK and OE.TRUSTED_REGISTRAR and will detect corrupt incoming setup, so that they are according to the expected subset of SIP.

#### 4.4.1.6 T.CORRUPT_FORMAT

Sanity check (OT.SANITY_CHECK) will detect corrupt Incoming *Domain(r)* Stream Setup, so that they are according to the expected package format.

### 4.4.2 Organizational Security Policies

P.CIS_DEFINITION_POLICY is directly covered by OE.SECURE_LOCATION.

The P.CIS_PERSONNEL_POLICY is covered by OE.INSTRUCTED_USERS and OE.INSTRUCTED_ADMIN and physical protected by OE.SECURE_LOCATION.

P.CIS_INTERCONNECTION_POLICY is directly covered by OE.TRUSTED_RELEASE.

P.VOICE_PROCEDURES_POLICY and P.LABELLING_POLICY are directly covered by OT.SUBSTITUTION and OT.SEND and supported by OT.SELECTOR and OT.SANITY_CHECK for the secure transmission to the trusted interconnection.

### 4.4.3 Assumptions

#### 4.4.3.1 A.SECURE_IP

A.SECURE_IP is directly covered by OE.SECURE_IP, securely administrated by OE.INSTRUCTED_ADMIN and securely used by OE.INSTRUCTED_USERS.

#### 4.4.3.2 A.SECURE_LOCATION

A.SECURE_LOCATION is directly covered by OE.SECURE_LOCATION, securely administrated by OE.INSTRUCTED_ADMIN and securely used by OE.INSTRUCTED_USERS.

#### 4.4.3.3 A.SECURE_OS

A.SECURE_OS is directly covered by OE.EVALUATED_OS, securely administrated by OE.INSTRUCTED_ADMIN and securely used by OE.INSTRUCTED_USERS.

#### 4.4.3.4 A.TRUSTED_VPN

A.TRUSTED_VPN is directly covered by OE.PREVENT_ACCESS, securely administrated by OE.INSTRUCTED_ADMIN.

# 5 EXTENDED COMPONENTS DEFINITION

No additional extended components are needed and therefore none are defined.

# 6 SECURITY REQUIREMENTS

## 6.1 Security Functional Requirements (SFRs)

### 6.1.1 FAU Security Audit

### 6.1.1.1 FAU_GEN.1 Audit data generation

Hierarchical to:

- No other components.

Dependencies:

- FPT_STM.1 Reliable time stamps.

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

a) Start-up and shutdown of the audit functions;
b) All auditable events for the [~~selection, choose one of: minimum, basic, detailed,~~ not specified] level of audit; and
c) [~~assignment: other specifically defined auditable events~~ None].

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [~~assignment: other audit relevant information~~ None].

### 6.1.2 Information flow control policy (FDP_IFC)

### 6.1.2.1 FDP_IFC.1(1) Subset information flow control

Hierarchical to:

- No other components.

Dependencies:

- FDP_IFF.1(1) Simple security attributes

FDP_IFC.1.1(1) The TSF shall enforce the [SFP. STREAM(*r*)] on [the subjects S.TSS and S.DMZ(*r*) via OE.PREVENT_ACCESS, Send operation, on the information O. VOICE_STREAM(*r*)].

### 6.1.2.2 FDP_IFC.1(2) Subset information flow control

Hierarchical to:

- No other components.

Dependencies:

- FDP_IFF.1(2) Simple security attributes

FDP_IFC.1.1(2) The TSF shall enforce the [SFP. SETUP(*r*)] on [the subjects S.TSS and S.DMZ(*r*) via OE.PREVENT_ACCESS, Send operation, on the information O.STREAM_SETUP].

### 6.1.2.3 FDP_IFC.1(3) Subset information flow control

Hierarchical to:

- No other components.

Dependencies:

- FDP_IFF.1(3) Simple security attributes

FDP_IFC.1.1(3) The TSF shall enforce the [SFP.STREAM(*h*)] on [the subjects S.TSS, Receive operation, on the information O.VOICE_STREAM(*h*)].

## 6.1.3 Information flow control functions (FDP_IFF)

### 6.1.3.1 FDP_IFF.1(1) Simple security attributes

Hierarchical to:

- No other components.

Dependencies:

- FDP_IFC.1(1) Subset information flow control
- FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1(1) The TSF shall enforce the [SFP. STREAM(*r*)] based on the following types of subject and information security attributes: [the subjects S.TSS and S.DMZ(*r*), on the information O. VOICE_STREAM(*r*), using security attributes SA.VOICE_STREAM_CLASSIFICATION].

FDP_IFF.1.2(1) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [Domain(*r*) Send operation shall permit O. VOICE_STREAM(*r*) to flow from S.TSS to S.DMZ(*r*) via OE.TRUSTED_RELEASE].

FDP_IFF.1.3(1) The TSF shall enforce the [following sequence of steps:

A) Perform sanity check of Header Information in Requested Voice Stream (O. VOICE_STREAM(*r*)) from S.TSS and
B) Substitution of Voice contents in Requested Voice Stream with Microphone Signal for O. VOICE_STREAM(*r*) flowing from S.TSS to S.DMZ(*r*) and
C) Add non-secure warning tone and periodically repeat the addition of the warning tone to the Indicator (Speaker)].

FDP_IFF.1.4(1) The TSF shall explicitly authorise an information flow based on the following rules: [

A) Sanity check of Incoming *Domain(r)* Voice Stream O. VOICE_STREAM(*r*) with classification label SA.VOICE_STREAM_CLASSIFICATION=*Domain(r)* from S.DMZ(*r*) and
B) Send the sanitized O. VOICE_STREAM(*r*) to S.TSS].

FDP_IFF.1.5(1) The TSF shall explicitly deny an information flow based on the following rules: [ SA.VOICE_STREAM_CLASSIFICATION =*Domain(h)* shall deny O.VOICE_STREAM(*r*) to flow from S.TSS].

The following actions should be auditable:

a) ~~Minimal: Decisions to permit requested information flows.~~
b) Basic: All decisions on requests for information flow.
c) ~~Detailed: The specific security attributes used in making an information flow enforcement decision.~~
d) ~~Detailed: Some specific subsets of the information that has flowed based upon policy goals (e.g. auditing of downgraded material).~~

### 6.1.3.2 FDP_IFF.1(2) Simple security attributes

Hierarchical to:

- No other components.

Dependencies:

- FDP_IFC.1(2) Subset information flow control
- FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1(2) The TSF shall enforce the [SFP. SETUP(*r*)] based on the following types of subject and information security attributes: [the subjects S.TSS and S.DMZ(*r*), on the information O. STREAM_SETUP, using no security attribute].

FDP_IFF.1.2(2) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [None].

FDP_IFF.1.3(2) The TSF shall enforce the [following sequence of steps:

A) Perform sanity check of Requested Stream Setup (O.STREAM_SETUP) from S.TSS and
B) Send the sanitized O.STREAM_SETUP to S.DMZ(*r*) via OE.TRUSTED_RELEASE].

FDP_IFF.1.4(2) The TSF shall explicitly authorise an information flow based on the following rules: [

A) Perform sanity check of Incoming Stream Setup (O.STREAM_SETUP) from S.DMZ(*r*) and
B) Send the sanitized O.STREAM_SETUP to S.TSS].

FDP_IFF.1.5(2) The TSF shall explicitly deny an information flow based on the following rules: [None].

The following actions should be auditable:

a) ~~Minimal: Decisions to permit requested information flows.~~
b) Basic: All decisions on requests for information flow.
c) ~~Detailed: The specific security attributes used in making an information flow enforcement decision.~~
d) ~~Detailed: Some specific subsets of the information that has flowed based upon policy goals (e.g. auditing of downgraded material).~~

#### 6.1.3.3 FDP_IFF.1(3) Simple security attributes

Hierarchical to:

- No other components.

Dependencies:

- FDP_IFC.1(3) Subset information flow control
- FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1(3) The TSF shall enforce the [SFP. STREAM(*h*)] based on the following types of subject and information security attributes: [the subjects S.TSS, on the information O. VOICE_STREAM(*h*), using security attributes SA.VOICE_STREAM_CLASSIFICATION].

FDP_IFF.1.2(3) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [None].

FDP_IFF.1.3(3) The TSF shall enforce the [None].

FDP_IFF.1.4(3) The TSF shall explicitly authorise an information flow based on the following rules: [

A) Incoming Voice Stream O.VOICE_STREAM(h) with classification SA.VOICE_STREAM_CLASSIFICATION=Domain(h) from S.TSS and
B) Silence payload of all O. VOICE_STREAM(*p*) for *p*=*h*, *h*+1, …, *m*-1 when SA.VOICE_STREAM_CLASSIFICATION=*Domain(m)* and Requested Voice Stream is active and
C) Forward O. VOICE_STREAM(*p*) from step B) to S.TSS application].

FDP_IFF.1.5(3) The TSF shall explicitly deny an information flow based on the following rules: [ None].

The following actions should be auditable:

a) ~~Minimal: Decisions to permit requested information flows.~~
b) Basic: All decisions on requests for information flow.
c) ~~Detailed: The specific security attributes used in making an information flow enforcement decision.~~
d) ~~Detailed: Some specific subsets of the information that has flowed based upon policy goals (e.g. auditing of downgraded material).~~

### 6.1.4 Management of security attributes (FMT_MSA)

#### 6.1.4.1 FMT_MSA.3 Static attribute initialisation

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 [SFP. STREAM(*r*), SFP. SETUP(*r*) and SFP. STREAM(*h*)] to provide [~~selection, choose one of:~~ restrictive~~, permissive, [assignment: other property]~~] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [S.ADMIN] to specify alternative initial values to override the default values when an object or information is created.

The following actions should be auditable:

a) Basic: Modifications of the default setting of permissive or restrictive rules.
b) Basic: All modifications of the initial values of security attributes.

### 6.1.5 Fail secure (FPT_FLS)

#### 6.1.5.1 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: [Audio Failure and Network Failure].

The following actions should be auditable:

a) Basic: Failure of the TSF.

### 6.1.6 TSF self test (FPT_TST)

#### 6.1.6.1 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 [~~selection:~~ during initial start-up~~, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self-test should occur]~~] to demonstrate the correct operation of [~~selection: [assignment: parts of TSF],~~ the TSF].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of [~~selection: [assignment: parts of TSF data], TSF data~~ No TSF Data].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of [~~selection: [assignment: parts of TSF],~~ TSF].

The following actions should be auditable:

a) Basic: Execution of the TSF self-tests and the results of the tests.

### 6.1.7 Trusted path (FTP_TRP)

#### 6.1.7.1 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 [~~selection: remote,~~ 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 [~~selection: modification, disclosure, [assignment: other types of integrity or confidentiality violation]~~*Domain(r)* selector modification].

FTP_TRP.1.2 The TSF shall permit [~~selection: the TSF,~~ local users~~, remote users~~] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [~~selection: initial user authentication, [assignment: other services for which trusted path is required]~~The user shall verify that non-secure warning tone is issued on the speaker and repeated when *Domain(r)* selector is selected and sending Requested *Domain(r)* Voice Stream].

The following actions should be auditable:

a) ~~Minimal: Failures of the trusted path functions.~~
b) ~~Minimal: Identification of the user associated with all trusted path failures, if available.~~
c) Basic: All attempted uses of the trusted path functions.
d) ~~Basic: Identification of the user associated with all trusted path invocations, if available.~~

### 6.2 Security Assurance Requirements (SARs)

The assurance level required for the TOE is EAL 5 and augmented with ALC_FLR.3.

## 6.3 Security Requirements Rationale

| Security Objective<br>Security Functional Requirement (SFR) | OT.SELECTOR | OT.SANITY_CHECK | OT.SUBSTITUTION | OT.SEND | OT.LOG | OT.ROBUST | OT.SUPPRESS |
|---|---|---|---|---|---|---|---|
| FAU_GEN.1 | | | | | X | | |
| FDP_IFC.1(1) | | X | X | | | | |
| FDP_IFC.1(2) | | X | | | | | |
| FDP_IFC.1(3) | | | | | | | X |
| FDP_IFF.1(1) | | X | X | X | | | |
| FDP_IFF.1(2) | | X | | X | | | |
| FDP_IFF.1(3) | | | | | | | X |
| FMT_MSA.3 | | X | X | | | | X |
| FPT_FLS.1 | | | | | | X | |
| FPT_TST.1 | | | | | | X | |
| FTP_TRP.1 | X | | | | | | |

### 6.3.1 OT.SELECTOR

The objective OT.SELECTOR is implemented by FTP_TRP.1, where selected operation is written back to the user.

### 6.3.2 OT.SANITY_CHECK

The objective OT.SANITY_CHECK is directly implemented FDP_IFC.1(1), FDP_IFC.1(2), FDP_IFF.1(1), FDP_IFF.1(2) and FMT_MSA.3, where voice stream and setup is checked for correct protocol format.

### 6.3.3 OT.SUBSTITUTION

The objective OT.SUBSTITUTION is implemented FDP_IFC.1(1), FDP_IFF.1(1) and FMT_MSA.3 is defining the correct substitution by the SFP, which also defines the security rules in OT.SUBSTITUTION.

### 6.3.4 OT.SEND

The objective OT.SEND to send *Domain(r)* Voice Stream and Setup via the trusted release is covered by FDP_IFF.1(1) and FDP_IFF.1(2) respectively.

### 6.3.5 OT.LOG

The objective OT.LOG is directly implemented by FAU_GEN.1 for the generation of audit information specified by each of the audit generating SFRs (FDP_IFC.1(1,2,3), FDP_IFF.1(1,2,3), FDP_ITC.1(1,2,3), FMT_MSA.3, FPT_FLS.1, FPT_TST.1 and FTP_TRP.1).

FAU_GEN.1 has a dependency to FPT_STM.1, which is realised by OE.EVALUATED_OS. Therefore FPT_STM.1 has not been included as TOE SFR.

FMT_MSA.3 has dependencies to FMT_MSA.1 and FMT_SMR.1, which is realised by OE.EVALUATED_OS. Therefore FMT_MSA.1 and FMT_SMR.1 have not been included as TOE SFR.

### 6.3.6 OT.ROBUST

The objective OT.ROBUST is directly implemented by FPT_FLS.1 and FPT_TST.1 for detection of internal TOE failures.

### 6.3.7 OT.SUPPRESS

The objective OT.SUPPRESS is directly implemented by FDP_IFC.1(3), FDP_IFF.1(3) and FMT_MSA.3.

# 7 TOE SUMMARY SPECIFICATION

The TOE Summary specification defines the instantiation of the security requirements for the TOE.

The first subsection describes the TOE Security Functions (TSF) and their correspondence to the stated security requirements. The next subsection states the assurance measures for the TOE to ensure the correct implementation of TSF.

## 7.1 TOE Security Functions

An overview of all TOE Security Functions and which Security Requirements they fulfill is given in the following table. Further descriptions of TSFs are given in subsections below.

In general TOE is:

- Generating security events for later investigation. The stored events can be collected by the IT Environment.

| Security Functional Requirement (SFR)<br>TOE Security Function (TSF) | FAU_GEN.1 | FDP_IFC.1(1) | FDP_IFC.1(2) | FDP_IFC.1(3) | FDP_IFF.1(1) | FDP_IFF.1(2) | FDP_IFF.1(3) | FMT_MSA.3 | FPT_FLS.1 | FPT_TST.1 | FTP_TRP.1 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| SF-1 BLACK Setup | X | | X | | | X | | | | | |
| SF-2 BLACK Voice | X | X | | | X | | | | | | X |
| SF-3 Cross Talk | X | | | X | | | X | | | | |
| SF-4 Self-test and preserve secure state | X | | | | | | | X | X | X | |

### 7.1.1 SF-1 *Domain(r)* Setup

*Domain(r)* Setup is sanitized both from the untrusted TSS application and the *DMZ(r)* and controlled by information control flow according to the security policy.

The configuration file for TOE is empty by default, which will prevent any communication on the *Domain(r)* Setup until the Administrator has made a proper configuration setup.

### 7.1.2 SF-2 *Domain(r)* Voice

The SF makes sure that the voice stream is *Domain(r)* only and is transmitted via the trusted release communication path and controlled by information control flow according to the security policy. To make sure that no *Domain(h)* information is contained in the *Domain(r)* voice stream the following is performed:

- Sanitization of header information.

- For *Domain(r)* TALK selection: Substitution of voice contents with microphone voice, which is known not to contain *Domain(h)* voice, before sending *Domain(r)* Voice Stream.

- For *Domain(h)* TALK selection: Block of voice contents before sending *Domain(r)* Voice Stream.

Misuse is prevented by providing the user a non-secure warning tone, such that the probability of a wrong selection is minimized.

The configuration file for TOE is empty as default, which will prevent any communication on the *Domain(r)* Voice Stream until the Administrator has made a proper configuration setup.

### 7.1.3 SF-3 Cross Talk

Cross talk of classified voice is minimised by suppression of incoming *Domain(h)* voice stream to the speaker while sending *Domain(r)* voice.

SF-3 can be disabled or enabled by TOE configuration. As restrictive default is SF-3 enabled and can be disabled by the Administrator of TOE.

### 7.1.4 SF-4 Self-test and preserve secure state

During start-up of TOE a self-test is performed and during operation, failure monitoring is performed such that a secure state can be preserved.