SECODE
Securing Your Business

SECURITY TARGET

FOR

THE SPI FILTER

VERSION 1.0

TABLE OF CONTENTS

DOCUMENT INFORMATION

Document responsible			
Role	**Name**	**Telephone**	**E-mail**
Project Manager	Jorunn Terjesen	+47 99 28 29 35	Jorunn.terjesen@secode.com
Quality Assurance	Ove Nysæter	+47 99 28 29 14	Ove.nysæter@secode.com

Point of Contact - FLO			
Role	**Person**	**Telephone**	**E-mail**
Project Officer	Espen Brendsdal	63 80 85 22	ebrensdal@mil.no

Point of Contact - Developer			
Role	**Name**	**Telephone**	**E-mail**
Project Manager	Trond Inge Olsen	92 20 86 12	Trond.inge.olsen@kongsberg.com
Technical Assurance	Oddvar Gauteplass	92 06 01 05	Oddvar.gateplass@kongsberg.com
Quality Assurance	Anja Heggem	93 05 74 89	Anja.heggem@kongsberg.com

Document history			
Version	**Date**	**Description**	**Author**
1.0	2011-09-08	Public version of the ST	Jorunn Terjesen, Oddvar Gauteplass, Anja Heggem

ABBREVIATIONS

Abbreviation	Description
CC	Common Criteria
CM	Configuration Management
CRC	Control and Reporting Centre
EAL	Evaluation Assurance Level
FBLV	Forsvarets Bakkebaserte Luftvern
IAW	In Accordance With
INFOSEC	Information Security
IT	Information Technology
JRE	Joint Range Extension
KDA	Kongsberg Defense and Aerospace
L11B	Link 11B
L16	Link 16
MIDS	Multifunctional Information Distribution System
MIL-STD	Military Standard
PP	Protection Profile
RT	Real Time
SF	Security Function
SFP	Security Function Policy
SPI	Special Processing Indicator
ST	Security Target
STANAG	Standardization Agreement
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
VMF	Variable Message Format

1. INTRODUCTION (ASE_INT)

The Special Processing Indicator (SPI) filter is a software based filter, designed and implemented to filter messages transferred between networks of different security domains.

The SPI filter software component is the target of evaluation (TOE).

1.1. IDENTIFICATION

ST Title: Security Target for the SPI filter

CC Version: 3.1, revision 3

Assurance level: EAL4

PP Identification: None

TOE name: SPI filter

TOE version:
SPI filter:

- Version 1.2

Non-TOE hardware, software, or firmware required by the TOE:
The SPI filter is installed on the Real Time (RT) Computer, operating system: VxWorks 5.5.1.

The security audit trial is stored on the harddrive of one of the MMI workstations, operating system: Solaris/Linux.

1.2. SECURITY TARGET OVERVIEW

This ST describes the IT security requirements for the SPI filter.

1.3. CC CONFORMANCE CLAIM (ASE_CCL)

The SPI filter Security Target is Part 2 conformant and Part 3 conformant.

1.4. NOTATIONS AND FORMATTING

The notations and formatting used in this ST are consistent with version 3.1 revision 3 of the Common Criteria (CC).

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Deleted words are denoted by ~~strike-through text~~. If a refinement is added as a separate paragraph to an SFR instead of modifying its wording, this paragraph starts with the word "**Refinement:**" in bold text.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *italicized* text.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [Assignment_value].

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration_number).

Assets: Assets to be protected by the TOE are given names beginning with "AS." – e.g. AS.CLASSIFIED_INFO.

Assumptions: TOE security environment assumptions are given names beginning with "A."- e.g., A.Security_Procedures.

Threats: Threat agents are given names beginning with "TA." – e.g., TA.Admin. Threats to the TOE are given names beginning with "TT." – e.g., TT.Filter_Fails. TOE security environment threats are given names beginning with "TE."-- e.g., TE.SPI_Manipulation.

Policies: TOE security environment policies are given names beginning with "P."—e.g., P.Information_AC.

Objectives: Security objectives for the TOE and the TOE environment are given names beginning with "O." and "OE.", respectively, - e.g., O.Filter_msg and OE.Clearance.

2. TOE DESCRIPTION

2.1. SPI FILTER

One of the purposes of the systems, where the SPI filter is installed, is to forward information/messages between systems operating in different security domains.

The SPI filter filters messages sent from NATO SECRET Link 16 networks to NATO CONFIDENTIAL Link 11B networks.

Further denotation in this ST:
The originator of the SPI protected information is named "**originating security domain**".

The link the information is forwarded to is named "**receiving security domain**".

2.2. FILTER POLICY

Tracks with SPI bit set shall only be shared between the originating network and receiving network.

Non-SPI track can be disseminated freely between networks IAW defined application filters.

Each message received to the filter is inspected. If the SPI-bit is set, the message is not forwarded.

The above approach has one exception:
IAW MIL-STD 6016 and 6011/STANAG 5511, a track received with EMERGENCY or FORCE TELL indication, will pass all filters. In this case the tracks will be transmitted on all links, and the security audit trail shall reflect the transmittal. The SPI indication is retained on the transmitted track where applicable.

2.3. PHYSICAL OVERVIEW

The system where the SPI Filter is integrated consists of several computers dedicated to different functions. The Sealed Area where the computers are located contains equipment and cabling that gives direct access to classified information. All personnel with access shall be authorised for this information and equipment.

Dedicated data links are used for communication with the environment outside the Sealed Area, via Crypto, Firewall or MIDS/L16 Terminal. No other external connection exists (e.g. IP via servers). No wireless devices exist.

The different computers involved are:

MMI Workstations
The Workstation Software acts as a front-end processor for the RT software, presenting results of RT processing to the operator, and provides inputs from the operator to the RT software components. The Workstation software provides all necessary operator interaction capabilities for the operators.

RT (Real Time) CPU
The RT computer hosting the real time software and the SPI Filter component is not accessible for the operators. All operator interactions and information are performed through the MMI workstation computers.

COMM (Communication) CPU #n
The COMM computers are hosting the communication suite. The purpose of the COMM computers is to handle the external interfaces, mainly using serial interfaces. These computers are not accessible for the operator.

Firewall for the JRE IP Interface
The firewall for JRE IP interface shall ensure JRE IP interface message to flow between the internal ethernet and an external interface unit using a dedicated IP address.

Link16/MIDS Terminal
The Multifunctional Information Distribution System (MIDS) is a tactical information radio system, providing Link 16 capabilities to the defence system.

2.4. SPI-FILTER LOGICAL DESIGN

Below the filtering process is described in a flowchart. Input to the filter is a message headed for the receiving security domain. The message is first inspected for SPI bit set to "on" or "off". If the SPI bit is "off" the send function is called, and the message is send. Else if the SPI bit is set to "on", i.e. this message is by the main rule not to leave the system, an event is registered in the security audit trail, and the message is further inspected for any EMERGENCY or FORCE TELL indicator. If there is no such indicator present, the message is stopped. Else if an indicator is present the send function is called and the message is send.

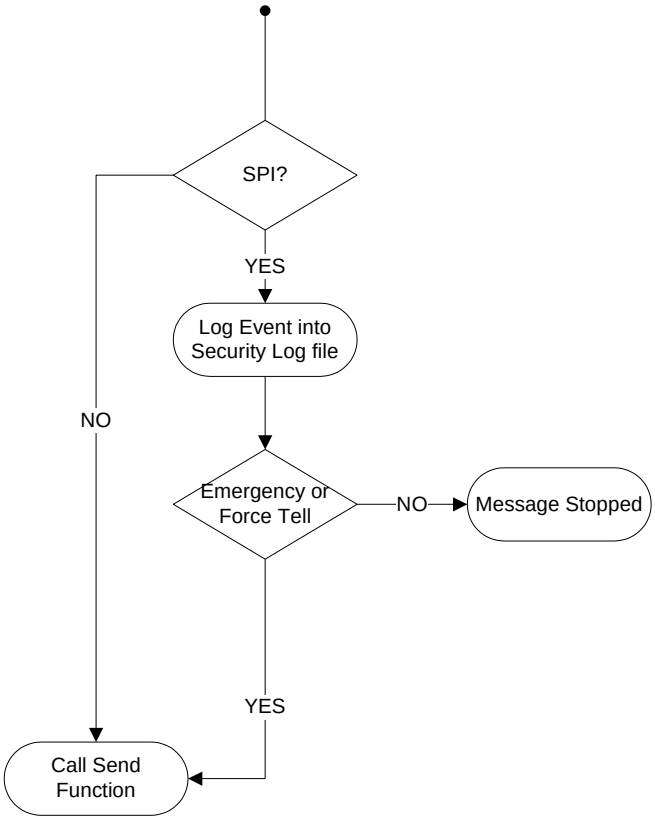

Figure 1; Flowchart of SPI filtering process

2.5. VxWorks Operating System

The structure of the components in VxWorks makes it possible to reuse the same filter for multiple applications.

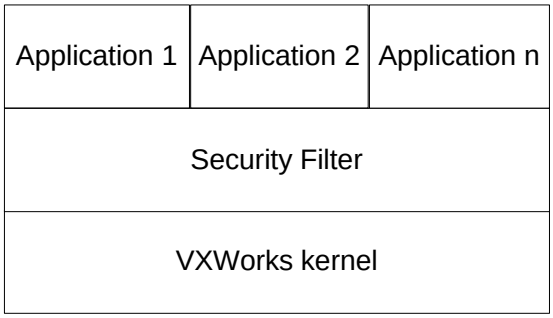

Figure 2; VxWorks OS

3. SECURITY PROBLEM DEFINITION (ASE_SPD)

3.1. THREATS TO SECURITY

3.1.1. ASSETS

AS.Classified_Info: Information classified according to a specific security policy. The information protected by the TOE is classified NATO SECRET.

AS.SPI_Filter: The security mechanisms of the TOE protecting AS.CLASSIFIED_INFO.

3.1.2. THREAT AGENTS

TA.Admin: The KDA administrator preparing the system to be delivered on the CD and the system administrators installing the TOE may unintentionally perform actions jeopardizing the security of the TOE.

TA.Operator: Operators may unintentionally perform unauthorized actions.

TA.Hacker: Personnel with no authorized access to the TOE environment. These threat agents may try to access classified information and may have "unlimited" resources supporting them.

TA.System_Failure: The system may fail due to configuration or system errors.

3.1.3. IDENTIFICATION OF THREATS

3.1.3.1. THREATS TO THE TOE

TT.Information_Leak: By a hacker manipulating of the system, or operator error, information incorrectly crosses security domains.

TT.Filter_Admin: The KDA- or system administrator misconfigures the filter, resulting in information incorrectly crossing security domains.

TT.Filter_Fails: Due to system failure the filter stops functioning and information incorrectly crosses security domains.

TT.Audit_Fails: Due to system failure, or setup configuration error, messages stopped by the system with SPI set to "on", are not audited.

3.1.3.2. THREATS TO THE ENVIRONMENT

TE.SPI_Manipulation: A hacker manipulates the SPI bit of messages and information incorrectly crosses security domains.

TE.Audit_Manipulation: A hacker or an operator manipulates the audit trail to cover illegal actions.

3.2. ORGANIZATIONAL SECURITY POLICIES

P.Information_AC: Information shall be accessed only by authorized individuals and processes.

P.Infosec: The TOE and its environment shall be handled and protected in accordance with The Norwegian Security Act (sikkerhetsloven), and MIL-STD 6016 and 6011/STANAG 5511 when it comes to special processing of messages received with SPI, EMERGENCY and/or FORCE TELL indication.

P.Marking: Incoming NATO SECRET Link 16 messages shall be marked with SPI-bit set to "on", if they require special processing.

P.Audit_Analyze: The security filter audit trail is regularly analyzed.

P.CD_Protection: The CD containing installation and system update files is protected according to Norwegian Security Act (sikkerhetsloven) when transported from the developer to the sites.

3.3. ASSUMPTIONS

A.Security_Procedures: Security procedures for the TOE are established and in use.

A.Usage_of_TOE: The TOE is used in the intended setup described in chapter 2.

A.Surveillance: The SPI-filter is installed in an environment which either is manned, under surveillance, or placed in a protected air defense location

A.Dev_Physical_Protection: The developer has appropriate security measures installed and implemented to protect the TOE against tampering.

A.Competent_Operator_and_Adm: KDA- and system administrators are competent to manage the TOE and the security of the information it contains and all operators know how to use the TOE in a secure manner.

A.No_Misuse_By_Ope_or_Adm: KDA- and system administrators and Operators are trusted not to misuse their authority.

A.Clearance: All personnel with access to the TOE, in the whole life-cycle of the TOE, hold the appropriate security clearance.

A.Connection: The TOE and TOE environment shall not have any connections, directly or indirectly, to unclassified and/or public networks.

4. SECURITY OBJECTIVES (ASE_OBJ)

4.1. TOE SECURITY OBJECTIVES

O.Filter_msg: The TOE shall filter messages based on the SPI-bit when crossing the security domains:
- from the originating domain to the receiving domains

O.Security_audit: The TOE shall have the ability to audit all messages with:
- SPI-bit set (and rejected to forward)
- EMERGENCY or FORCE TELL and SPI-bit set

O.Audit_alarm: The TOE shall give the operator an alarm if the audit trail is not writeable, or runs full.

4.2. OPERATIONAL ENVIRONMENT SECURITY OBJECTIVES

OE.FW: The system shall have a firewall installed filtering the IP based message traffic.

OE.Watchdog: There is a watchdog installed in the system. The operator gets an indication of system including SPI filter status from the watchdog. Green light indicates that the status is OK.

OE.Restart: The system has a restart button for the operator to reestablish normal operation after a system failure.

OE.Non_bypass: System architecture and functionality ensures that it is not possible to bypass the filter. If the filter fails no messages are transmitted to the receiving security domain.

OE.TOE_Env_Protect: The environment of the TOE shall be secured according to defense requirements, and prevent hackers to get access to TOE connected systems and communication lines.

OE.TOE_Dev_Env_Protect: The developer environment shall be secure in a way that prevents hacker access of any kind.

OE.Training_Ope_Adm: The operators, KDA- and system administrators of the systems shall be trained to securely operate and manage the systems.

OE.Authentication: The KDA- and system administrators of the system shall be properly authenticated.

OE.Audit_Trail_Protect: The audit trail is protected by access control mechanisms in MMI workstation operating system (Solaris /Linux).

OE.Audit_Analysis: The system administrator of the systems shall regularly, according to the security procedures, analyze the audit records.

OE.Clearance: The operators, KDA- and system administrators of the systems shall hold a appropriate security clearance of at least "HEMMELIG".

4.3. SECURITY OBJECTIVES RATIONALE

The table below shows that all threats, assumptions, and security policies of the TOE are met by one or more TOE or environment security objective. In the next sections a rationale is given for each of these tracings.

Objectives	Threats, Assumptions, Policies	TT.Information_Leak	TT.Filter_Admin	TT.Filter_Fails	TT.Audit_Fails	TE.SPI_Manipulation	TE.Audit_Manipulation	P.Information_AC	P.Infosec	P.Marking	P.Audit_Analyze	P.CD_Protection	A.Security_Procedures	A.Usage_of_TOE	A.Surveillance	A.Dev_Physical_Protection	A.Competent_Ope_and_Adm	A.No_Misuse_By_Ope_or_Adm	A.Clearance	A.Connection
O.Filter_msg		X							X											
O.Security_audit											X									
O.Audit_alarm					X															
OE.FW		X				X														X
OE.Watchdog				X																
OE.Restart				X																
OE.Non_bypass		X		X																
OE.TOE_Env_Protect		X				X		X					X		X					X
OE.TOE_Dev_Env_Protect						X						X				X				
OE.Training_Ope_Adm		X	X		X					X		X	X	X			X	X		
OE.Authentication							X	X												
OE.Audit_Trail_Protect							X													
OE.Audit_Analysis					X						X									
OE.Clearance																			X	

Table 1; Tracing of objectives to threats, assumptions, and policies.

4.4. THREATS

4.4.1. TT.INFORMATION_LEAK

The threat **TT.Information_Leak** is met by the TOE objective **O.Filter_msg**: The TOE shall filter messages based on the SPI-bit . The objective states that information from the originating domain protected by the special indicator shall be prevented from being transferred to the receiving domains.

Further the objectives to the environment **OE.FW**, **OE_Non_bypass**, **OE.TOE_Env_Protect,** and **OE.Training_Ope_Adm** supports the main objective by:

- restricting incoming IP traffic through the firewall
- ensuring that the filter cannot be bypassed
- physically securing the premises where the filter is installed
- and states that proper training is required.

4.4.2. TT.FILTER.ADMIN

The threat **TT.Filter.Admin** is met by the objective **OE.Training_Ope_Adm** which ensures that the KDA- and system administrators are properly trained.

4.4.3. TT.FILTER.FAILS

The threat **TT.Filter.Fails** is met by the objective **OE.Non_Bypass** which ensures that the system is designed not to let any messages through if the filter fails. In addition the objectives **OE.Watchdog** and **OE.Restart** ensures that a failure is detected and that the system is restarted in a secure state.

4.4.4. TT.AUDIT.FAILS

The threat **TT.Audit.Fails** is met by the objective **O.Audit_alarm** which gives an alarm in case the audit trail is not writeable or the audit storage is running full. In addition the objectives **OE.Audit_Analysis** will detect if the audit trail is corrupt, and the objective **OE.Training_Ope_Adm** which will ensure proper training of KDA- and system administrator.

4.4.5. TE.SPI_MANIPULATION

The threat **TE.SPI.Manipulation** is met by the objective **OE.FW** which protects the TOE from outside attacks and by the objectives **OE.TOE_Env_Protect** and **OE.TOE_Dev_Env_Protect** which ensures that the TOE is physically secured both in the defense and the developer premises.

4.4.6. TE.AUDIT_MANIPULATION

The threat **TE.Audit_Manipulation** is met by the objective **OE.Authentication** that ensures that the KDA- and system administrators are properly authenticated and by **OE.Audit_Trail_Protect** that ensures that file containing the audit trail is protected by the access control mechanisms of the operating system.

4.5. POLICIES

4.5.1. P.INFORMATION_AC

The policy **P.Information_AC** is met by the environment objective **OE.Authentication** which requires the KDA- and system administrators to be properly authenticated before getting access to the TOE. In addition the objective **OE.TOE_Env_Protect** restricts the physical access to the TOE equipment.

4.5.2. P.INFOSEC

The policy **P.Infosec** is met by the objective **O.Filter.msg** which ensures that only personnel authorized for the information protected by the SPI get access to it.

4.5.3. P.MARKING

The policy **P.Marking** is met by the environment objectives **OE.Training_Ope_Adm** which ensures that the personnel are trained in the procedures of how to use SPI on messages.

4.5.4. P.AUDIT_ANALYZE

The policy **P.Audit_Analyze** is met by the environment objective **OE.Audit_Analysis** which requires the system administrators to regularly analyze the security filter audit trail. This objective is supported by the objective **O.Security_audit** that requires security events to be recorded.

4.5.5. P.CD_PROTECTION

The policy **P.CD_Protection** is met by the environment objectives **OE.TOE_Dev_Env_Protect** and **OE.Training_Ope_Adm,** which ensures that the CD is protected by the developer's personnel when created and by the system administrator when installed.

4.6. ASSUMPTIONS

4.6.1. A.SECURITY_PROCEDURES

The assumption **A.Security_Procedures** is met by the environment objective **OE.TOE.Env_Protect** which requires security procedures to be in place to physically protect the TOE and the objective **OE.Training_Ope_Adm** which ensures that the personnel operating the TOE are properly trained.

4.6.2. A.USAGE_OF_TOE

The assumption **A.Usage_of_TOE** is met by the objective **OE.Training_Ope_Adm** which ensures that the personnel operating the TOE are properly trained.

4.6.3. A.SURVEILLANCE

The assumption **A.Surveillance** is met by the environment objective **OE.TOE.Env_Protect** which requires security measures to be in place to physically protect the TOE.

4.6.4. A.DEV_PHYSICAL_PROTECTION

The assumption **A.Dev_Physical_Protection** is met by the environment objective **OE.TOE_Dev_Env_Protect** that ensures that the development environment shall implement security measures protecting the TOE in the development phase.

4.6.5. A.COMPETENT_OPE_AND_ADM

The assumption **A.Competent_Ope_and_Adm** is met by the environment objective **OE.Training_Ope_Adm**. The objective states that the operators, KDA- and system administrators shall be properly trained to operate and manage the TOE in a secure manner.

4.6.6. A.NO_MISUSE_BY_OPE_OR_ADM

The assumption **A.No_Misuse_By_Ope_or_Adm** is met by the environment objective **OE.Training_Ope_Adm**. The objective states that training of operators, KDA- and system administrator shall prevent them from misuse of the TOE.

4.6.7. A.CLEARANCE

The assumption **A.Clearance** is met by the environment objective **OE.Clearance** which states that all personnel developing or operating the TOE shall hold a security clearance of "HEMMELIG"

4.6.8. A.CONNECTION

The assumption **A.Connection** is met by the environment objective **OE.FW** which ensures that connections to other systems are filtered and monitored, and by the objective **OE.TOE_Env_Protect** which ensures that communication equipment is physically protected.

5. EXTENDED COMPONENTS DEFINITION (ASE_ECD)

Not applicable.

6. SECURITY REQUIREMENTS (ASE_REQ)

6.1. SECURITY FUNCTIONAL REQUIREMENTS (SFRS)

Functional Class	Functional Components
FAU	FAU_GEN.1, FAU_STG.4
FDP	FDP_IFC.2, FDP_IFF.1,

Table 2; Functional requirements for the TOE.

6.1.1. FDP_IFC.2

FDP_IFC.2.1 The TSF shall enforce the [**SPI filter SFP**] on:
[List of subjects:
- **Originating domains**
- **Receiving domains**

Information:
- **Link 16 messages**
- **Link 11B messages]**

and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

6.1.2. FDP_IFF.1

FDP_IFF.1.1 The TSF shall enforce the [**SPI filter SFP]** based on the following types of subject and information security attributes:
[**List of subjects:**
- **Originating domain**
- **Receiving domains**

Information:
- **Link16 messages**
- **Link 11B messages**

Security attributes:
- **SPI-bit**]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:
[**Forwarding of Link 16 messages and Link 11B messages from the originating domains to the receiving domains when the SPI-bit of the message is set to off**].

FDP_IFF.1.3 The TSF shall enforce the [**SPI filter SFP**].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [**The message has EMERGENCY or FORCE TELL indicators**].

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

[**Forwarding of Link 16 messages and Link 11B messages from the originating domains to the receiving domains when the SPI-bit of the message is set to on**].

6.1.3. FAU_GEN.1

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

a) Start-up and shut-down of the audit functions;

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

c) Specially defined auditable events:
[
- **All messages forwarded with EMERGENCY or FORCE TELL and SPI-bit set**
- **All messages with SPI-bit set and rejected to forward**]

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, [**None**].

6.1.4. FAU_STG.4

FAU_STG.4.1 The TSF shall ***overwrite the oldest stored audit records*** **and [give an alarm to the operator]** if the audit trail **is full**.

Refinement: An alarm will also be given to the operator if the VxWorks I/O System Functions detect any error in the writing operation.

6.2. Security Assurance Requirements (SARs)

Assurance Class	Assurance Components
ADV	ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3
AGD	AGD_OPE.1, AGD_PRE.1
ALC	ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.1, ALC_LCD.1, ALC_TAT.1
ATE	ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2
AVA	AVA_VAN.3

Table 3; Assurance requirements EAL4

For the detailed requirements refer to section 8.

6.3. Security Requirements Rationale

This section gives the relation between SFRs and security objectives.

TOE functional requirements	Objectives for the TOE	O.Filter_msg	O.Security_audit	O.Audit_alarm
FDP_IFC.2		X		
FDP_IFF.1		X		
FAU_GEN.1			X	
FAU_STG.4				X

Table 4; Tracing of functional requirements to objectives.

6.3.1. O.FILTER_MSG

The objective **O.Filter_msg**: The TOE shall filter messages based on the SPI-bit , is met by the TOE security requirement **FDP _IFC.2,** which ensures that the SPI filter policy is enforced between the originating domain and the receiving domains.

The requirement **FPD_IFF.1** ensures that only messages with SPI-bit set to "off" is transferred, except for messages with EMERGENCY or FORCE TELL Indicator.

6.3.2. O.SECURITY_AUDIT

The objective **O.Security_audit**, is met by the TOE requirement **FAU_GEN.1** that ensures that an audit record is generated for all messages with SPI bit set to "on" and stopped, and for all messages sent with EMERGENCY or FORCE TELL indicators and SPI set to "on".

6.3.3. O.AUDIT_ALARM

The objective **O.Audit_alarm** is met by the TOE requirement **FAU_STG.4** which ensures that the operator gets an alarm when the audit trail is full.

6.3.4. SFR DEPENDENCIES

The table below shows the dependencies of the security functional requirement of the TOE and gives a rationale for each of them.

Security functional requirement	Dependency	Rationale
FDP.IFC.2 Complete information control	FDP_IFF.1 Simple security attributes	Included.
FDP_IFF.1 Simple security attributes	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	The FDP_IFC.1 and the FMT_MSA.3 is handled by the environment and not included in the ST.
FAU_GEN.1 Audit data generation	FPT_STM.1 Reliable time stamps	Reliable time stamps are provided by the environment (OS), and FPT_STM.1 is as a result not included.

Security functional requirement	Dependency	Rationale
FAU_STG.4 Prevention of audit loss	FAU_STG.1 Protected audit trail storage	The audit trail is protected by access control mechanisms in the environment (OS) and FAU_STG.1 is as a result not included.

Table 5; Security functional requirements dependency rationale.

6.4. SAR RATIONALE

This ST contains the assurance requirements from the CC EAL4 assurance package.

7. TOE SUMMARY SPECIFICATION (ASE_TSS)

7.1. TOE SECURITY FUNCTIONS SPECIFICATION

This section describes the security functions provided by the TOE to meet the security functional requirements specified for the TOE in section 6.1.

7.1.1. SF.FILTER_ON_SPI-BIT

The TOE filters messages coming from the originating security domain headed for the receiving security domains. The SPI-bit of the messages are checked. When the SPI bit is set the message is rejected. An exception is messages with EMERGENCY or FORCE TELL indication, these messages are forwarded.

7.1.2. SF.MSG_AUDIT

The TOE audits all incoming messages with the SPI-bit set, including messages with EMERGENCY or FORCE TELL indicators. The auditing starts when the filter is turned on. The audit record is stored in one of the MMI computers.

7.1.3. SF.AUDIT_ALARM

The system will generate an alarm when the audit trail is not writeable or when the audit record space is full.

7.2. SECURITY FUNCTIONS RATIONALE

The table below shows that all TOE security requirements can be traced to at least one TOE security function.

TOE security functions	TOE functional requirements	FDP_IFC.2	FDP_IFF.1	FAU_GEN.1	FAU_STG.4
SF.Filter_on_SPI-bit		X	X		
SF.MSG.audit				X	
SF.Audit_Alarm					X

Table 6; Tracing of security functions to requirements.

7.2.1. SF.FILTER_ON_SPI-BIT

The TOE security function, **SF.Filter_on_SPI-bit**; "The TOE filters messages coming from the originating security domain headed for the receiving security domains. The SPI-bit of the messages are checked. When the SPI bit is set the message is rejected", meets the TOE security requirement **FDP_IFC.2** which requires the messages to be filtered on SPI-bit and the requirement **FDP_IFF.1** which defines the filtering function.

7.2.2. SF.MSG_AUDIT

The TOE security function **SF.MSG.audit**, "The TOE audits all incoming messages with the SPI-bit set, including messages with EMERGENCY or FORCE TELL indicators. The auditing starts when the filter is turned on. The audit record is stored in one of the MMI computers.", meets the audit requirement of **FAU_GEN.1**.

7.2.3. SF.AUDIT_ALARM

The TOE security function **SF.Audit_Alarm**; "The system will generate an alarm when the audit trail is not writeable or when the audit record space is full.", meets the requirements for detection when an audit trail runs full and sending an alarm to the operator (**FAU_STG.4**).

8. ASSURANCE REQUIREMENTS

8.1. DEVELOPMENT (ADV)

8.1.1. SECURITY ARCHITECTURE DESCRIPTION (ADV_ARC.1)

The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.[ADV_ARC.1.1C]

The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs. [ADV_ARC.1.2C]

The security architecture description shall describe how the TSF initialisation process is secure. [ADV_ARC.1.3C]

The security architecture description shall demonstrate that the TSF protects itself from tampering. [ADV_ARC.1.4C]

The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality. [ADV_ARC.1.5C]

8.1.2. COMPLETE FUNCTIONAL SPECIFICATION (ADV_FSP.4)

The functional specification shall completely represent the TSF.[ADV_FSP.4.1C]

The functional specification shall describe the purpose and method of use for all TSFI. [ADV_FSP.4.2C]

The functional specification shall identify and describe all parameters associated with each TSFI.[ADV_FSP.4.3C]

The functional specification shall describe all actions associated with each TSFI.[ADV_FSP.4.4C]

The functional specification shall describe all direct error messages that may result from an invocation of each TSFI.[ADV_FSP.4.5C]

The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification. [ADV_FSP.4.6C]

8.1.3. IMPLEMENTATION REPRESENTATION OF THE TSF (ADV_IMP.1)

The implementation representation shall define the TSF to a level of detail such that the TSF can be generated without further design decisions.[ADV_IMP.1.1C]

The implementation representation shall be in the form used by the development personnel.[ADV_IMP.1.2C]

The mapping between the TOE design description and the sample of the implementation representation shall demonstrate their correspondence.[ADV_IMP.1.3C]

8.1.4. BASIC MODULAR DESIGN (ADV_TDS.3)

The design shall describe the structure of the TOE in terms of subsystems.[ADV_TDS.3.1C]

The design shall describe the TSF in terms of modules.[ADV_TDS.3.2C]

The design shall identify all subsystems of the TSF.[ADV_TDS.3.3C]

The design shall provide a description of each subsystem of the TSF.[ADV_TDS.3.4C]

The design shall provide a description of the interactions among all subsystems of the TSF.[ADV_TDS.3.5C]

The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.[ADV_TDS.3.6C]

The design shall describe each SFR-enforcing module in terms of its purpose and relatonship with other modules.[ADV_TDS.3.7C]

The design shall describe each SFR-enforcing module in terms of its SFR-related interfaces, return values from those interfaces, interaction with other modules and called SFR-related interfaces to other SFR-enforcing modules.[ADV_TDS.3.8C]

The design shall describe each SFR-supporting or SFR-non-interfering module in terms of its purpose and interaction with other modules.[ADV_TDS.3.9C]

The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.[ADV_TDS.3.10C]

8.2. GUIDANCE DOCUMENTS (AGD)

8.2.1. OPERATIONAL USER GUIDANCE (AGD_OPE.1)

The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.[AGD_OPE.1.1C]

The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.[AGD_OPE.1.2C]

The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.[AGD_OPE.1.3C]

The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.[AGD_OPE.1.4C]

The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.[AGD_OPE.1.5C]

The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.[AGD_OPE.1.6]

The operational user guidance shall be clear and reasonable.[AGD_OPE.1.7C]

8.2.2. PREPARATIVE PROCEDURES (AGD_PRE.1)

The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.[AGD_PRE.1.1C]

The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.[AGD_PRE.1.2C]

8.3. LIFE-CYCLE SUPPORT (ALC)

8.3.1. PRODUCTION SUPPORT, ACCEPTANCE PROCEDURES AND AUTOMATION (ALC_CMC.4)

The TOE shall be labelled with its unique reference.[ALC_CMC.4.1C]

The CM documentation shall describe the method used to uniquely identify the configuration items.[ALC_CMC.4.2C]

The CM system shall uniquely identify all configuration items.[ALC_CMC.4.3C]

The CM system shall provide automated measures such that only authorised changes are made to the configuration items.[ALC_CMC.4.4C]

The CM system shall support the production of the TOE by automated means.[ALC_CMC.4.5C]

The CM documentation shall include a CM plan.[ALC_CMC.4.6C]

The CM plan shall describe how the CM system is used for the development of the TOE.[ALC_CMC.4.7C]

The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.[ALC_CMC.4.8C]

The evidence shall demonstrate that all configuration items are being maintained under the CM system.[ALC_CMC.4.9C]

The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.[ALC_CMC.4.10C]

8.3.2. PROBLEM TRACKING CM COVERAGE (ALC_CMS.4)

The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; and security flaw reports and resolution status.[ALC_CMS.4.1C]

The configuration list shall uniquely identify the configuration items.[ALC_CMS.4.2C]

For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.[ALC_CMS.4.3C]

8.3.3. DELIVERY PROCEDURES (ALC_DEL.1)

The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.[ALC_DEL.1.1C]

The developer shall use the delivery procedures.[ALC_DEL.1.2D]

8.3.4. IDENTIFICATION OF SECURITY MEASURES (ALC_DVS.1)

The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.[ALC_DVS.1.1C]

8.3.5. DEVELOPER DEFINED LIFE-CYCLE MODEL (ALC_LCD.1)

The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.[ALC_LCD.1.1C]

The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.[ALC_LCD.1.2C]

8.3.6. WELL-DEFINED DEVELOPMENT TOOLS (ALC_TAT.1)

Each development tool used for implementation shall be well-defined.[ALC_TAT.1.1C]

The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.[ALC_TAT.1.2C]

The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.[ALC_TAT.1.3C]

8.4. TESTS (ATE)

8.4.1. ANALYSIS OF COVERAGE (ATE_COV.2)

The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.[ATE_COV.2.1C]

The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.[ATE_COV.2.2C]

8.4.2. TESTING: BASIC DESIGN (ATE_DPT.1)

The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems and SFR-enforcing modules in the TOE design.[ATE_DPT.1.1C]

The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.[ATE_DPT.1.2C]

8.4.3. FUNCTIONAL TESTING (ATE_FUN.1)

The test documentation shall consist of test plans, expected test results and actual test results.[ATE_FUN.1.1C]

The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the

results of other tests.[ATE_FUN.1.2C]

The expected test results shall show the anticipated outputs from a successful execution of the tests.[ATE_FUN.1.3C]

The actual test results shall be consistent with the expected test results.[ATE_FUN.1.4C]

8.4.4. INDEPENDENT TESTING - SAMPLE (ATE_IND.2)

The TOE shall be suitable for testing.[ATE_IND.2.1C]

The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.[ATE_IND.2.2C]

8.5. VULNERABILITY ASSESSMENT (AVA)

8.5.1. FOCUSED VULNERABILITY ANALYSIS (AVA_VAN.3)

The TOE shall be suitable for testing.[AVA_VAN.3.1C]

9. ASSURANCE MEASURES

Table 7 lists the assurance components defined by the EAL4 package and the documentation submitted as assurance measures, (to be filled in as the documents are drawn up).

Assurance component	Component name	Assurance measures
ADV_ARC.1	Security architecture description	*Security Design for the SPI filter*
ADV_FSP.4	Complete functional specification	*Security Design for the SPI filter*
ADV_IMP.1	Implementation representation of the TSF	*Source code for the SPI filter.*
ADV_TDS.3	Basic modular design	*Security Design for the SPI filter*
AGD_OPE.1	Operational user guidance	Operational user guidance *for the SPI filter*
AGD_PRE.1	Preparative procedures	Preparative procedures *for the SPI filter*
ALC_CMC.4	Production support, acceptance procedures and automation	*CM plan for the SPI filter*
ALC_CMS.4	Problem tracking CM coverage	*CM plan for the SPI filter*
ALC_DEL.1	Delivery procedures	*Delivery Procedures for the SPI filter*
ALC_DVS.1	Identification of security measures	*KDA Physical and Procedural security*
ALC_LCD.1	Developer defined life-cycle model	*CM plan for the SPI filter*
ALC_TAT.1	Well-defined development tools	*CM plan for the SPI filter*
ATE_COV.2	Analysis of coverage	*Security Testing of the SPI filter*
ATE_DPT.1	Testing: basic testing	*Security Testing of the SPI filter*
ATE_FUN.1	Functional testing	*Security Testing of the SPI filter*
ATE_IND.2	Independent testing – sample	*EVIT Security Testing of the SPI filter*
AVA_VAN.3	Focused vulnerability analysis	*Vulnerability analysis of the SPI filter*

Table 7; Assurance Measures.