TRUSTED SECURITY FILTER

SECURITY TARGET

Edition: **2.2**

28 Oct 09

Previous editions:

Ed. 1 11 May 2006
Ed. 2 16 Aug 2006
Ed. 3 28 June 2007
Ed. 4 29 Oct 2007
Ed. 2.1 9 Oct 2009

Author: **KKK**

Appr.: **PÅT**

All pages in this document shall have the same edition number

TABLE OF CONTENTS

1. SECURITY TARGET INTRODUCTION

1.1 Security Target identification

Title	Security Target for Trusted Security Filter (TSF 101)
Target of evaluation (TOE) Identification	Trusted Security Filter (TSF 101); comprising • OTA hardware: 3AQ 21564 AAAA ICS5, ICS5A, ICS6, ICS6A, ICS6B, ICS7, ICS7A and ICS7B • TSF101 software: 3AQ 21850 CAAA Version 2.1.4 The list of document editions associated with these versions is given in ref. [4].
Assurance level	EAL5 augmented with ALC_FLR.3 (Systematic flaw remediation)

1.2 Security Target overview

The TSF 101 is a product for filtering a fixed and limited set of packet data between two networks of different security classification. Its design shall be trusted to perform red/black separation of data between a Secure and a Non-secure network in a highly specialized IT environment.

1.3 Common Criteria conformance

The TSF 101 has been developed to include components as defined in the Common Criteria (CC) version 2.3 part 2 [2]. The TSF 101 has been developed to conform to the EAL5 assurance level augmented with ALC_FLR.3, as identified in the Common Criteria version 2.3 part 3 [3].

1.4 Related documents

[1]	3AQ 21840 CAAA DEZZA	TSF 101 Security Design
[2]	CCMB-05-08-002	Common Criteria version 2.3 part 2
[3]	CCMB-05-08-003	Common Criteria version 2.3 part 3
[4]	3AQ 21840 XAAA DSL	Document Status List for TSF Security Evaluation

1.5 Abbreviations and acronyms

CC	Common Criteria
CCI	Crypto/Comsec Controlled Item
EAL	Evaluation Assurance Level
FW	Firewall
HW	Hardware
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
NSM	Nasjonal sikkerhetsmyndighet
SF	Security Function
SFP	Security Function Policy

SFR	Security Functional Requirement(s)
SOF	Strength of Function
ST	Security Target
SW	Software
TOE	Target of evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSF 101	Trusted Security Filter (product name)
TSP	TOE Security Policy

1.6 Definitions

Classified information	Classified information is information regarded as sensitive by the security authorities for the owners of the system that comprises the TOE. Sensitive information is information that these security authorities determine must be protected because its unauthorised disclosure will cause perceivable damage.
Secure domain (red)	The domain that handles classified information in clear.
Non-secure domain (black)	The domain that does not handle classified information in clear.

2. TOE DESCRIPTION

This section presents an overview of the TSF 101 to assist potential users to determine whether it meets their needs. Further in this document the TSF 101 will be referred to as the TOE.

Figure 1 shows the TOE in its position as a data filter between two LAN networks.

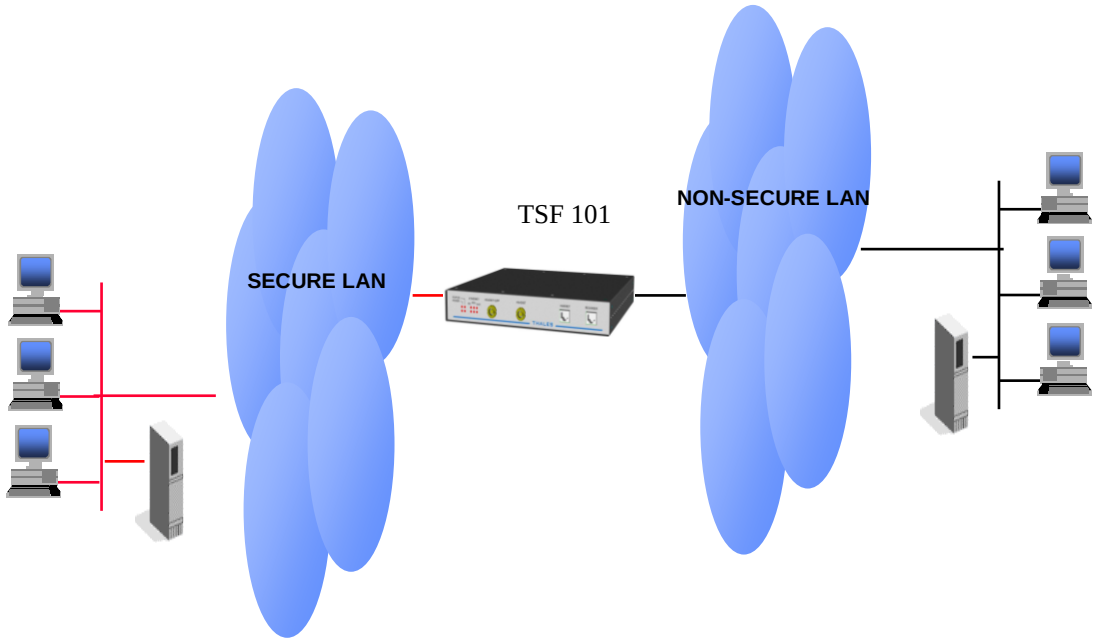

Figure 1 TOE environment

2.1 The TOE HW

The TOE HW provides connection for audio devices, loudspeaker and lamps, and the Ethernet interfaces, as shown in Figure 2 below.

Note that in the scope of this Security Target the TOE HW is used purely as a data filter between two IP based networks, and in this configuration only the Ethernet interfaces and the alarm lamps and indicator lamps are used. All other interfaces are disabled.

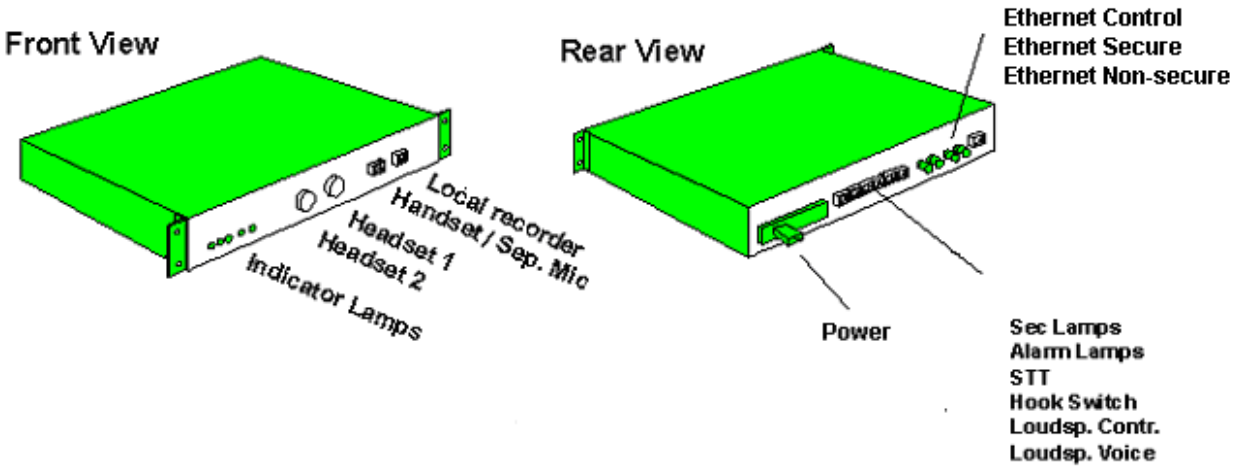

Figure 2 TOE mechanical characteristics

The main function of the TOE HW is to perform red/black separation. The TOE uses an external AC/DC converter. All connectors intended to be handled by installation and maintenance are located at the rear end. The front end has indicator lamps providing information of the status of the TOE, the power and each of the Ethernet interfaces.

The TOE is connected to secure and non-secure LAN by use of 100 Mb/s Ethernet interface on fibre and has also an 10/100 Mb/s electrical Ethernet interface (called Ethernet Control in Figure 2). This interface gives access to the secure Ethernet, but is not in use for the TOE Except for initial setting of the IP addresses of the TOE.

2.2 The TOE SW

The TOE SW performs the following main functions:

- Routing
  The TOE will during normal operation have 2 different LAN connected; one secure LAN, and one non-secure LAN respectively, see Figure 1. This implies that TOE must be able to route IP packets.

- Firewall
  The firewall checks all messages from secure to non-secure domain. The firewall filter is not configurable, except that two different filter sets can be selected. Thus, the TOE can operate in two different locations in the specific IT environment and will accept messages depending on the filter set selected.

- Red/black separation
  The secure (red) and non-secure (black) functions are separated using a combination of privilege levels and isolation of software tasks in different segments. Violation of segment boundaries is protected by the CPU and dedicated hardware..

2.3 Scope of evaluation

- The TOE is the TSF 101 comprising of hardware and software as identified in section 1.1 “Security Target identification”

- The scope of evaluation is evaluation of security functions in the TOE. These security functions are identified in section 6.1”TOE security functions”.

The TEMPEST certification is not within this scope of evaluation.

3. TOE SECURITY ENVIRONMENT

This section provides the statement of the TOE security environment, which identifies and explains all:

1. Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects.

2. Known and presumed threats countered by either the TOE or by the security environment.

3. Organisational security policies the TOE must comply with.

3.1 Assumptions

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

A.PHYSICAL	The system comprising the TOE and the connected networks is installed in a physical protected area, minimum approved for the highest security level of information handled in the system.
A.TRAINING	All TOE managers are trained in the correct use of the TOE.
A.CLEARANCE	All TOE managers have a minimum clearance for the highest security level of information handled in the system, and is authorised for all information handled by the system.
A.MAN.AUTHORISED	Only managers with special authorisation are allowed to do configuration and management of the system including TOE.
A.USAGE	The TOE is used between two LANs in a protected environment and is installed according to the installation guidelines for the TOE.

3.2 Threats

This section identifies the assets, threat agents and threats.

3.2.1 Identification of Assets

The assets within the TOE that needs protection are all classified information transmitted through the TOE.

3.2.2 Identification of Threat Agents

TA.INTERNAL	Personnel which have authorised access to the operations site and which has intent to perform unauthorised actions. These persons may be trained specially to perform their unauthorised actions. They may bring unauthorised software into the site and may be able to load it. They may be supported by entities with unlimited resources.
TA.EXTERNAL	Personnel which do not have access to the operations site and which has the intent to divulge classified information. These persons may have unlimited resources.
TA.USER	Users with no intent to perform unauthorised actions. They may unintentionally perform unauthorised actions.

TA.TECHNICIAN	Technicians with no intent to perform unauthorised actions. They may unintentionally perform unauthorised actions.
TA.MALFUNCTIONS	System malfunctions. System malfunctions to be considered are limited to single point of failure.

3.2.3 Threats

T.CONN.SEC.NON-SEC Classified information on a secure channel may be transferred to non-secure channels.

Threat agents	TA.TECHNICIAN, and/or TA.MALFUNCTIONS. In addition the following must be present: TA.EXTERNAL
Asset	Classified information
Unwanted outcome	Unauthorised personnel get access to classified information.
Attack methods	1. A technician (TA.TECHNICIAN) unintentionally configures or installs the TOE in a way that transfers information on secure channels (i.e. classified information) to non-secure channels. The classified information is picked up from the non-secure channels by persons (TA.EXTERNAL) outside the physically protected area. 2. A malfunction in the TOE implies that information on secure channels (i.e. classified information) is transferred to non-secure channels. The classified information is picked up from the non-secure channels by persons (TA.EXTERNAL) outside the physically protected area.

T.TAMPERING Security-critical part of the TOE may be subject to physical attack that may compromise security.

Threat agent	TA.INTERNAL combined with TA.EXTERNAL
Asset	Classified information
Unwanted outcome	Unauthorised personnel get access to classified information.
Attack method	A person (TA.INTERNAL or TA.EXTERNAL) modifies the TOE to transfer information on secure channels (i.e. classified information) to non-secure channels. The classified information is picked up from the non-secure channels by persons (TA.EXTERNAL) outside the physically protected area.

T.MISUSE An attacker may send classified information from the secure to the non-secure network, by the use of data messages.

Threat agent	TA.INTERNAL combined with TA.EXTERNAL
Asset	Classified information
Unwanted outcome	Unauthorised personnel get access to classified information.

Attack method	A person (TA.INTERNAL) introduce/modify software and/or hardware in the secure network to pick up classified information and transfer this information to non-secure channels via the TOE. The classified information is picked up from the non-secure channels by persons (TA.EXTERNAL) outside the physically protected area. This threat increases if this can continue undetected.

T.TEMPEST	Electromagnetic emanations may divulge classified information.
Threat agent	TA.EXTERNAL possibly in combination with TA.INTERNAL
Asset	Classified information
Unwanted outcome	Unauthorised personnel get access to classified information.
Attack method	Information on secure channels (i.e. classified information) is electromagnetically emanated onto non-secure channels. The classified information is picked up from the non-secure channels by persons (TA.EXTERNAL) outside the physically protected area.

T.UNAUTHORISED.USE	Authorised persons may perform unauthorised use of the system's applications and management system inside the operation site.
Threat agent	TA.INTERNAL or TA.USER. In addition the following must be present TA.EXTERNAL.
Asset	Classified information
Unwanted outcome	Unauthorised personnel get access to classified information.
Attack method	Authorised persons may perform intentionally (TA.INTERNAL) or unintentionally (TA.USER) unauthorised use of the operator position applications and management system inside the operation site. The threat is that this may lead to transfer of classified information onto non-secure channels. The classified information is picked up from the non-secure channels by persons (TA.EXTERNAL) outside the physically protected area.

3.3 Organisational security policies

Not applicable.

4. SECURITY OBJECTIVES

4.1 TOE IT Security Objectives

O.ALARM.FAILURE	If a hardware or software failure is detected in the TOE, the TOE shall raise a local alarm.
O.AUDIT	The TOE shall have an audit log that can be viewed by a web browser on the secure network.
O.FW.STATISTICS	The TOE shall perform statistics registration of messages handled by the filter and provide facilities to present them for the TOE manager.
O.FILTER	Classified information shall be prevented from being transmitted on non-secure channels.
O.SELF.TEST	Security critical functions shall be tested by a combination of power-up tests, periodic tests and/or continuous tests.
O.NO.CONFIG	The firewall filter shall not be configurable. The TOE manager shall be able to select sets of predefined filter criteria.

4.2 TOE Non-IT Security Objectives

NO.SEALING	The TOE shall be sealed in such a way that it is easy to see that it has been opened/tampered with.
NO.TEMPEST	TEMPEST evaluation and certification of the TOE is performed by NoNSA. This certification ensures that NO.TEMPEST is achieved. This aspect is not treated further in this document.

4.3 Environment IT Security Objectives

OE.AUDIT	The IT environment shall be able to display the web page with the firewall statistics. The web server resides in the TOE.
OE.MAN.ACCESS	Special authorisation is required to grant access to handle TOE firewall statistics.

4.4 Environment Non-IT Security Objectives

NOE.ACCESS.CTRL	Only authorised persons shall be given physical access to the system comprising the TOE and the connected networks.
NOE.AUDIT	Authorised managers of the TOE must ensure that the TOE firewall statistics and audit log are used and managed effectively. On particular, TOE firewall statistics and audit log should be inspected on a regular basis, appropriate and timely action should be taken on the detection of breaches of security, or events that are likely to lead to a breach in the

	future.
NOE.CCI	The TOE shall be treated as a CCI material.
NOE.CLEARANCE	All users shall have a minimum clearance for the maximum-security level of information handled in the system.
NOE.INSTALL	The responsible for the TOE must ensure that the TOE is installed according to the installation guidelines for the TOE.
NOE.MAN.TRAIN	The TOE managers are fully trained to use and interpret the TOE firewall statistics and audit log.
NOE.PHYS. PROT	The site where the TOE is installed shall have physical protection, which is minimum approved for the highest level of information handled in the system.

5. SECURITY REQUIREMENTS

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

5.1 TOE Security Functional Requirements

The Table 1 list the functional components included in this ST.

Component	Name
FAU_ARP.1	Security alarms
FAU_GEN.1	Audit data generation
FAU_SAR.1	Security audit review
FAU_STG.1	Protected audit trail storage
FDP_IFC.2	Complete information flow control
FDP_IFF.1	Simple security attributes
FDP_IFF.6	Illicit information flow monitoring
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_SMF.1	Specification of Management Functions
FPT_AMT.1	Abstract machine testing
FPT_FLS.1	Failure with preservation of secure state
FPT_PHP.1	Passive detection of physical attack
FPT_SEP.1	TSF domain separation
FPT_STM.1	Reliable Time Stamps

Table 1 TOE Security Functional Requirements

5.1.1 Security Audit

This section involves recognising, recording and storing information related to security relevant activities.

FAU_ARP.1 Security alarms

FAU_ARP.1.1 The TSF shall take [*an action to raise a local alarm*] upon detection of a potential security violation.

Dependencies: FAU_SAA.1 Potential violation analysis is included.

FAU_GEN.1 **Audit data generation**

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

a) Start-up and shutdown of the audit functions

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

c) [*Firewall statistics*].

Dependencies: FPT_STM.1 Reliable time stamps is included.

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, 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*].

FAU_SAR.1 **Security audit review**

FAU_SAR.1.1 The TSF shall provide [*TOE Manager*] with the capability to read [*all*] from the audit records.

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

Dependencies: FAU_GEN.1 Audit data generation is included.

FAU_STG.1 **Protected audit trail storage**

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

FAU_ STG.1.2 The TSF shall be able to [*prevent*] unauthorised modifications to the stored audit records in audit trail.

Dependencies: FAU_GEN.1 Audit data generation is included.

5.1.2 User Data Protection

This section specifies the User Data Protection security requirements for the TOE.

FDP_IFC.2 Complete information flow control

FDP_IFC.2.1 The TSF shall enforce the [*information flow control SFP*] on [*the following subjects:*

- *TOE secure domain functions and*
- *TOE non-secure domain functions*

for the following information:

- *potentially classified information (secure information) and*
- *unclassified information (non-secure information)*]

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

Note: The TOE information flow control SFP includes the policy statement to reject unacceptable messages attempted transmitted from the secure domain to the non-secure domain.

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

Dependencies: FDP_IFF.1 Simple security attributes is included.

FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the [*information flow control SFP*] based on the following types of subject and information security attributes: [*The subjects are identified as blocks in the information flow block diagram, which is a part of the Information flow control SFP. The Information flow shall be controlled by the Information flow control SFP*].

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: [*The rules are specified in the information flow control SFP*].

FDP_IFF.1.3 The TSF shall enforce [*no additional information flow control SFP rules*].

FDP_IFF.1.4 The TSF shall provide [*no list of additional SFP capabilities*].

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: [stated in the information flow control SFP].

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [none].

Dependencies: FDP_IFC.1 is covered as FDP_IFC.2 is included.
FMT_MSA.3 is included.

FDP_IFF.6 Illicit information flow monitoring

FDP_IFF.6.1 The TSF shall enforce the [information flow control SFP] to monitor the [*illicit information flows through the firewall*] when it exceeds the [*none*].

Dependencies: AVA_CCA.1 Covert channel analysis is included.
FDP_IFC.1 Subset information flow control is covered as

FDP_IFC.2 is included.

5.1.3 Security Management

This section specifies the Security Management of the TOE.

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [*information flow control SFP*] to restrict the ability to [*modify*] the security attributes [*none*] to [*none*].

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control. FDP_IFC.1 Subset information flow control is covered as FDP_IFC.2 is included.]
FMT_SMR.1 Security roles is included
FMT_SMF.1 Specification of Management Functions is included

.

FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the [*information flow control SFP*] to provide [*restrictive*] default values for security attributes that are used to enforce the *SFP*.

FMT_MSA.3.2 The TSF shall allow the [none] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes is included.
FMT_SMR.1 Security roles is included.

FMT_SMF.1 Specification of management functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [Reset firewall filter statistics, selecting sets of predefined filter criteria].

Dependencies: No dependencies.

.

5.1.4 Protection of the TOE Security Functions

This section specifies the Protection of the TSF of the TOE.

FPT_AMT.1 Abstract machine testing

FPT_AMT.1.1 The TSF shall run a suite of tests [*during initial start-up, periodically during normal operation*] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

Dependencies: No dependencies.

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [*violation of memory boundaries, uncontrolled access to trusted code, and inconsistency between code stored in Flash memory and code stored in DRAM*].

Dependencies: ADV_SPM.1 Informal TOE security policy model is included.

FPT_PHP.1 Passive detection of physical attack

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

Dependencies: No dependencies.

FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies.

FPT_STM.1 **Reliable time stamps**

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

Dependencies: No dependencies.

5.2 Security requirements for the IT environment

This section details the IT security requirements to be met by the IT environment of the TOE. Table 2 lists the IT security requirements to be provided by the IT environment.

Component	Name
FAU_SAA.1	Potential violation analysis
FAU_SAR.1.Env	Audit Review
FIA_UID.1	Timing of identification
FMT_SMR.1	Security roles

Table 2 Security requirements for the IT environment

5.2.1 Security audit

This section involves recognising, recording and storing information related to security relevant activities.

FAU_SAA.1 Potential violation analysis

FAU_SAA.1.1 The IT environment shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation in the TSP.

FAU_SAA.1.2 The IT environment shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [*none*] known to indicate a potential security violation.

b) [*None*]

Dependencies: FAU_GEN.1 Audit data generation is included.

FAU_SAR.1.Env Audit review

FAU_SAR.1.1 The IT environment shall provide [*authorised users*] with the capability to read [*firewall statistics*] from the audit records.

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

Dependencies: FAU_GEN.1 Audit data generation is included. The TOE provides this functionality.

5.2.2 User identification

FIA_UID.1 Timing of identification

FIA_UID.1.1 The IT environment shall allow [*none*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The IT environment shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of the user.

Dependencies: No dependencies.

5.2.3 Security Management

FMT_SMR.1 Security roles

FMT_SMR.1.1 The IT environment shall maintain the roles [*TOE manager*].

FMT_SMR.1.2 The IT environment shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification is included.

5.3 TOE security assurance requirements

The assurance requirements for this Security Target, taken from Part 3 of the CC, comprise the EAL5 level of assurance, augmented with ALC_FLR.3. The assurance components are summarised in Table 3 below.

Assurance class		Assurance components
Configuration Management	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.3	Development tools CM coverage
Class ADO: Delivery and operation	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, generation and start-up procedures
Class ADV: Development	ADV_FSP.3	Semiformal functional specification
	ADV_HLD.3	Semiformal high-level design
	ADV_IMP.2	Implementation of the TSF
	ADV_INT.1	Modularity
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.2	Semiformal correspondence demonstration
	ADV_SPM.3	Formal TOE security policy model
Class AGD: Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Class ALC: Life Cycle support	ALC_DVS.1	Identification of security measures
	ALC_FLR.3	Systematic Flaw Remediation
	ALC_LCD.2	Standardised life-cycle model
	ALC_TAT.2	Compliance with implementation standards
Class ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.2	Testing: low level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Class AVA: Vulnerability assessment	AVA_CCA.1	Covert channel analysis
	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.3	Moderately resistant

Table 3 Assurance Requirements: EAL5

5.4 Strength of Function Claim

A Strength of Function (SOF) claim is not applicable for the TOE. There are no TOE security functions that are probabilistic or permutational.

6. TOE SUMMARY SPECIFICATION

6.1 TOE security functions

This describes the security functions provided by the TOE to meet the security functional requirements specified for the TOE in chapter 5.1.

6.1.1 SF.Security.Alarm

The TOE will raise a local alarm indication in the following situations:

- A firewall test failure is detected in the TOE.
- A hardware or software failure is detected in the TOE.

6.1.2 SF.Information.Flow.Control

The information flow control provides flow control between the user interfaces and the secure and non-secure network and information flow control between the secure and non-secure network. The flow control rules are based on:

- All messages from the secure network to the non-secure network are filtered in a firewall.
- The TOE manager can select sets of predefined filter criteria.

6.1.3 SF.Self.Test

The testing of TOE will detect errors in the security critical functions on the TOE. If a firewall failure, or a hardware or software failure is detected in the TOE, an alarm is generated.

6.1.4 SF.Fail.Secure

The most serious violation of the TSF is that classified data on the secure network is sent on the non-secure network. The following measure shall prevent this to happen as a result of TOE-failures:

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

6.1.5 SF.Passive.Protection

The TOE has a physical sealing.

6.1.6 SF.Domain.Separation

The TOE has the following domains:

- Non-secure domain
- Secure domain

The firewall checks all messages from secure to non-secure domain.

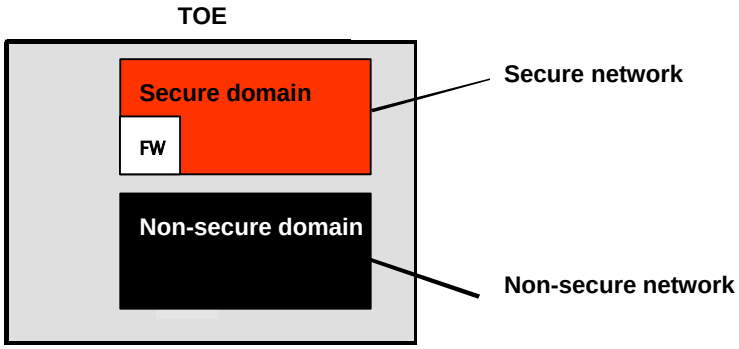

Figure 3 TOE Domains

6.1.7 SF.Firewall.Statistics

The TOE can display TOE Firewall Statistics by means of a web browser. The statistics displays the number of messages accepted and rejected for each recognized message type in current and previous measuring period, and the maximum number of accepted message within a measuring period.

The TOE manager can reset the firewall statistics.

6.1.8 SF.Audit.Log

The TOE can display the TOE audit log by means of a web browser.

6.2 Assurance measures

Table 4 lists the assurance components defined by the EAL5 augmented with ALC_FLR.3 and the documentation submitted as assurance measures.

Assurance component	Component name	Assurance measure
ACM_AUT.1	Partial CM automation	3aq 21850 aaaa TSF CM plan PRO1026 Styre Konfigurasjon.
ACM_CAP.4	Generation support and acceptance procedures	3aq 21850 aaaa TSF CM plan
ACM_SCP.3	Development tools CM coverage	3aq 21850 aaaa TSF CM plan
ADO_DEL.2	Detection of modification	PRO 2024 Deliver Products
ADO_IGS.1	Installation, generation and start-up procedures	3aq 41202 abaa eo TSF Technical Manual. 3aq 21850 xaaa bgzza TSF SW Installation guide
ADV_FSP.3	Semiformal functional specification	TSF Security Design [1].
ADV_HLD.3	Semiformal high-level design	TSF Security Design [1].
ADV_IMP.2	Implementation of the TSF	Various source code modules for the TSF, VHDL code for HW.
ADV_INT.1	Modularity	TSF Security Design [1].
ADV_LLD.1	Descriptive low-level design	TSF Security Design [1].
ADV_RCR.2	Semiformal correspondence demonstration	TSF Security Design [1].
ADV_SPM.3	Formal TOE security policy model	TSF Security Design [1].
AGD_ADM.1	Administrator guidance	3aq 41202 abaa eo TSF Technical Manual.
AGD_USR.1	User guidance	3aq 41202 abaa eo TSF Technical Manual.

Assurance component	Component name	Assurance measure
ALC_DVS.1	Identification of security measures	POL 0046 Utg. 14 Grunnlagsdokument for sikkerhet for Thales Norway AS (Thales Norway security regulations)
ALC_FLR.3	Systematic flaw remediation	3aq 41202 abaa eo TSF Technical Manual. PRC 1411 Manage support
ALC_LCD.2	Standardised life-cycle model	3aq 21850 aaaa TSF CM plan
ALC_TAT.2	Compliance with implementation standards	3aq 21850 aaaa TSF CM plan
ATE_COV.2	Analysis of coverage	TSF Security Design [1].
ATE_DPT.2	Testing: low level design	3AQ 21850 QPZZA.
ATE_FUN.1	Functional testing	3AQ 21850 QPZZA.
ATE_IND.2	Independent testing – sample	Performed at the Thales Norway lab by an independent evaluation agency
AVA_CCA.1	Covert channel analysis	TSF Security Design [1].
AVA_MSU.2	Validation of analysis	TSF Security Design [1].
AVA_SOF.1	Strength of TOE security function evaluation	TSF Security Target.
AVA_VLA.3	Moderately resistant	TSF Security Design [1].

Table 4: Assurance measures

Ref. [4] is the document status list that includes the assurance measures listed in Table 4.

7. PROTECTION PROFILES CLAIMS

There are no protection profile claims.

8. RATIONALE

8.1 Introduction

This section demonstrates that the TOE provides an effective set of IT security countermeasures within the security environment and that the TOE summary specification addresses the requirements.

8.2 Security Objectives for the TOE Rationale

Threats/ Assumptions Objectives	T.CONN.SEC.NON-SEC	T.TAMPERING	T.MISUSE	T.TEMPEST	T.UNAUTHORISED.USE	A.PHYSICAL	A.TRAINING	A.CLEARANCE	A.MAN.AUTHORISED	A.USAGE
O.ALARM.FAILURE	x									
O.AUDIT			x							
O.FW.STATISTICS			x							
O.FILTER	x		x							
O.SELF.TEST	x									
O.NO.CONFIG	x									
NO.SEALING		x								
NO.TEMPEST	x			x						
OE.AUDIT			x							
OE.MAN.ACCES					x				x	
NOE.ACCESS.CTRL						x		x		
NOE.AUDIT			x							
NOE.CCI		x					x			
NOE.CLEARANCE								x		
NOE.INSTALL	x			x		x	x			x
NOE.MAN.TRAIN	x		x				x			
NOE.PHYS.PROT		x				x				

Table 5 Mapping of Objectives to Threats and Assumptions

As can be seen from Table 5, at least one objective, either TOE or environment, as applicable meets all threats and assumptions. The coverage of the threats and assumptions countered by the TOE is discussed in the subsections below.

T.CONN.SEC.NON-SEC

The TOE controls the separation of non-secure and secure information and the information flowing from the secure to the non-secure network (O.FILTER) which is not configurable (O.NO.CONFIG). A failing in domain separation will be detected during power-up and/or normal operation (O.SELF.TEST). A local alarm indication is given by detection of hardware or software failure (O.ALARM.FAILURE). The TOE managers are fully trained to handle and interpret the TOE equipment (NOE.MAN.TRAIN). The TOE is installed (NOE.INSTALL) and given TEMPEST protection (NO.TEMPEST) according to established guidelines.

T.TAMPERING

To prevent tampering the TOE is installed in physical protected area that is provided with access control system (NOE.PHYS.PROT). The TOE is also sealed, so it is easy to see that the seal has been broken (NO.SEALING). Periodical manual inspection will detect possible tampering (NOE.CCI).

T.MISUSE

All messages from the secure network to the non-secure network are checked in the TOE firewall (O.FILTER). The TOE will count all messages that is allowed to pass the firewall and all messages that is rejected by the firewall and update the firewall statistics page with this information (O.FW.STATISTICS). The TOE will store event on rejected messages in the audit log (O.AUDIT). The TOE manager is trained (NOE.MAN.TRAIN) to inspect the firewall statistics and audit log (NOE.AUDIT) by means of a web browser (OE.AUDIT) to stop any attempt to misuse the covert channels.

T.TEMPEST

The TOE shall be installed according to installation guidelines (NOE.INSTALL), which complies with the TEMPEST installation guidelines (NO.TEMPEST).

T.UNAUTHORISED.USE

Users need special authorisation to handle the configuration and management part of the TOE (OE.MAN.ACCES).

A.PHYSICAL

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

A.TRAINING

The TOE managers are fully trained to handle and interpret the TOE (NOE.CCI and NOE.MAN.TRAIN). The technicians should be trained to install the TOE according to the installation guidelines (NOE.INSTALL).

A.CLEARANCE

Only authorised persons shall be given physical access to the system comprising the TOE and the connected networks (NOE.ACCESS.CTRL and NOE.CLEARANCE).

A.MAN.AUTHORISED

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

A.USAGE

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

8.3 Security Requirements Rationale

8.3.1 Requirements are appropriate

Table 6 identifies which SFRs satisfy the Objectives in chapter 4.

Component / Objectives	FAU_ARP.1	FAU_GEN.1	FAU_SAR.1	FAU_STG.1	FDP_IFC.2	FDP_IFF.1	FDP_IFF.6	FMT_MSA.1	FMT_MSA.3	FMT_SMF.1	FPT_AMT.1	FPT_FLS.1	FPT_PHP.1	FPT_SEP.1	FPT_STM.1
O.ALARM.FAILURE	x														
O.AUDIT		x	x	x											x
O.FW.STATISTICS		x	x				x			x					
O.FILTER					x	x						x		x	
O.SELF.TEST											x	x			
O.NO.CONFIG						x		x	x	x					
NO.SEALING													x		

Table 6: Mapping of Objectives to SFRs

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

8.3.1.1 Security Functional Requirements vs. Objectives

FAU_ARP.1 Security alarms

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

FAU_GEN.1 Audit data generation

The TOE registers auditable events indicating type of event and outcome of the event from the TOE (O.AUDIT) and firewall statistics (O.FW.STATISTICS).

FAU_SAR.1 Audit review

The TOE provides the capability to read the information from the audit records (O.AUDIT) and firewall statistics (O.FW.STATISTICS).

FAU_STG.1 Protected audit trail storage

The TOE protects the audit log (O.AUDIT) from deletion and modification of stored events.

FDP_IFC.2 Complete information flow control

The TOE enforces the firewall filter on all messages sent from the secure network to the non-secure network (O.FILTER).

FDP_IFF.1 Simple security attributes

The TOE enforces the information flow control SFP based on the attributes of the messages checked by the filter (O.FILTER). The TOE has an information flow control SFP that is non-configurable (O.NO.CONFIG).

FDP_IFF.6 Illicit information flow monitoring

The TOE updates the firewall statistics when a message is accepted or rejected in the firewall (O.FW.STATISTICS).

FMT_MSA.1 Management of security attributes

The security attributes are non-configurable (O.NO.CONFIG).

FMT_MSA.3 Static attribute initialization

The security attributes are non-configurable (O.NO.CONFIG).

FMT_SMF.1 Specification of management functions

The TOE manager is able to reset the firewall statistics (O.FW.STATISTICS) and to select sets of predefined filter criteria (O.NO.CONFIG).

FPT_AMT.1 Abstract machine testing

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

FPT_FLS.1 Failure with preservation of secure state

The TOE is designed to fail in a safe manner. This includes failure during self-test (O.SELF.TEST) and failure that compromises the secure/non-secure protection (O.FILTER).

FPT_PHP.1 Passive detection of physical attack

The TOE has sealing (NO.SEALING) to protect the TOE against tampering.

FPT_SEP.1 TSF domain separation

To handle both secure and non-secure information , the TOE has well defined division between the secure and non-secure domain. All message transferred from the secure network to the non-secure network is filtered in the firewall (O.FILTER).

FPT_STM.1 Reliable time stamps

Auditable events are stored with reliable time stamps (O.AUDIT).

8.3.1.2 Objectives vs. Security Functional Requirements

O.ALARM.FAILURE

The TOE will raise a local alarm indication (FAU_ARP.1) if a potential security violation is detected due to failure in the TOE.

O.AUDIT

The TOE will generate audit records (FAU_GEN.1) with reliable time stamps (FPT_STM.1) and store the record in a protected storage (FAU_STG.1) that is made available for audit (FAU_SAR.1) by the TOE manager.

O.FW.STATISTICS

The TOE shall generate statistics (FAU_GEN.1 and FDP_IFF.6) and make it available for audit (FAU_SAR.1) for the purpose of potential violation analysis by the TOE manager. It shall be possible for the TOE manager to reset the firewall statistics counters (FMT_SMF.1).

O.FILTER

The TOE shall ensure that information transmitted from secure domain to non-secure domain is unclassified by enforcing the information flow control SFP trough the TOE (FDP_IFC.2). This information flow control SFP is non-configurable (FDP_IFF.1).

The TOE ensures preservation of a secure state after a single failure (FPT_FLS.1).

The TOE provides separation of the TOE domains: secure domain and non-secure domain (FPT_SEP.1).

O.SELF.TEST

The TOE ensures that security critical functions are tested by a combination of power-up tests and periodic tests (FPT_AMT.1).

The TOE ensures preservation of a secure state after a single failure (FPT_FLS.1).

O.NO.CONFIG

The TOE filter parameters (FDP_IFF.1) shall be hard coded at compile time and not configurable (FMT_MSA.1 and FMT_MSA.3). The TOE manager can select sets of predefined filter criteria (FMT_SMF.1).

NO.SEALING

The TOE shall have passive protection (FPT_PHP.1).

8.3.2 Environment requirements are appropriate

Table 7 identifies which Security requirements for the IT environment that satisfy the Objectives in chapter 4.

Components / Environment IT Objectives	FAU_SAA.1	FAU_SAR.1.Env	FIA_UID.1	FMT_SMR.1
OE.AUDIT	x	x		x
OE.MAN.ACCES			x	x

Table 7: Mapping of Environment IT Objectives to Components

As seen in Table 7**,** all objectives are satisfied by at least one Security requirement for the IT environment and all Security requirements for the IT environment are required to meet at least one Environment IT Objectives.

8.3.2.1 Environment IT Security Objectives vs. Security Requirements for the IT Environment

OE.AUDIT

Authorised operators (FMT_SMR.1) can display the TOE web page with the firewall statistics from a workstation on the secure network (FAU_SAR.1.Env). This is used for the potential violation analysis (FAU_SAA.1).

OE.MAN.ACCES

Management operators can after a successful login (FIA_UID.1) perform management and configuration and manage audit records as determined by their role (FMT_SMR.1).

8.3.3 Security dependencies are satisfied

Table 8 shows a mapping of Functional Components to their dependencies.

Functional Component	**Dependency**	**Included**
TOE Security Functional Requirements		
FAU_ARP.1	FAU_SAA.1	YES
FAU_GEN.1	FPT_STM.1	YES
FAU_SAR.1	FAU_GEN.1	YES
FAU_STG.1	FAU_GEN.1	YES
FDP_IFC.2	FDP_IFF.1	YES
FDP_IFF.1	FDP_IFC.1	YES
	FMT MSA.3	YES
FDP_IFF.6	AVA.CCA.1	YES
	FDP_IFC.1	YES (Note 1)

Functional Component	Dependency	Included
FMT_MSA.1	FDP_IFC.1	YES (Note 1)
	(FDP_ACC.1)	NO (Note 2)
	FMT.SMR.1	YES
	FMT_SMF.1	YES
FMT_MSA.3	FMT_MSA.1	YES
	FMT_SMR.1	YES
FMT_SMF.1	None	
FPT_AMT.1	None	
FPT_FLS.1	ADV_SPM.1	YES (Note 3)
FPT_PHP.1	None	
FPT_SEP.1	None	
FPT_STM.1	None	
Security requirements for the IT environment		
FAU_SAA.1	FAU_GEN.1	YES
FAU_SAR.1.Env	FAU_GEN.1	YES
FIA_UID.1	None	
FMT_SMR.1	FIA.UID.1	YES

Table 8: Security Requirements dependencies

Note1: FDP_IFF.6 and FMT_MSA.1 have a dependency to FDP_IFC.1, which is covered by FDP_IFC.2.

Note2: The dependency FMT_MSA.1 -> FDP_ACC.1 is not required as FMT_MSA.1 -> FDP_IFC.1 is included (only one of these must be included according to CC).

Note3: FPT_FLS.1 has a dependency to ADV_SPM.1, which is covered by ADV_SPM.3.

8.4 TOE summary specification rationale

Table 9 shows how TOE Security Functions satisfy SFRs.

TOE Security functions	SFRs	Description
SF.Security.Alarm	FAU_ARP.1	The TOE security alarm function will raise a local alarm upon detection of a hardware failure or software failure in the TOE (FAU_ARP.1).
SF.Information.Flow.Control	FDP_IFC.2, FDP_IFF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1	The TOE information flow control controls all information flows (FDP_IFC.2) determined by the hard coded filter settings (FDP_IFF.1, FMT_MSA.1, and FMT_MSA.3). The TOE manager can select sets of predefined filter criteria.
SF.Self.Test	FPT_AMT.1	The TOE self-test function performs an underlying abstract machine testing (FPT_AMT.1).
SF.Fail.Secure	FPT_FLS.1	The fail secure function preserves a secure state after failure (FPT_FLS.1).
SF.Passive.Protection	FPT_PHP.1	The TOE sealing is constructed so that physical tampering is easily discovered (FPT_PHP.1).
SF.Domain.Separation	FPT_SEP.1	The domain separation function separates the TOE domain into non-secure network and secure network (FPT_SEP.1).
SF.Audit.Log	FAU_GEN.1, FAU_STG.1, FAU_SAR.1, FPT_STM.1	The TOE audit log function record auditable events (FAU_GEN.1) in an audit log. The stored events can not be modified or deleted (FAU_STG.1). The audit log can be viewed by authorized users (FAU_SAR.1) on the secure network. The auditable events are stored with a reliable time stamp (FPT_STM.1).
SF.Firewall.Statistics	FAU_GEN.1, FAU_SAR.1, FDP_IFF.6, FMT_SMF.1	The TOE firewall statistics function presents statistics (FDP_IFF.6 and FAU_SAR.1) of messages accepted and rejected by the firewall (FAU_GEN.1). The TOE manager can reset the statistics (FMT_SMF.1).

Table 9: TOE Security Functions satisfy SFRs

Strength of TOE security function analysis shall be performed on probabilistic or permutational functions.

The TOE does not have any probabilistic or permutational functions. Hence, there are no TOE security functions having a TOE security function claim and there is no further strength of TOE security function analysis required.

9. CHANGES

Changes in edition 2.

Action to SERTIT comment 3: Chapter 1.5 – NSM replaces NoNSA

Action to SERTIT comment 5: Chapter 2 – TSF 101 replaces TSF.

Action from Thales review: Chapter 2 – Secure and non-secure added to figure 1.

Action to SERTIT comment 6: Chapter 2.2 – Red/black separation is clarified

Action from Thales review: Chapter 3.2.3 – T.MISUSE: firewall -> TOE

Action from Thales review: Chapter 4.4 – NOE.MAN.TRAIN; "...and audit log" added.

Action to EOR 1-3: Chapter 5.1.3 – Dependencies under FMT_MSA.1 was entered twice in edition 1. The second has been removed.

Action to EOR 1-2: Chapter 5.1.4 – FPT_STM.1 added

Action to EOR 1-1: Chapter 5.2.1 – FAU_SAR.1.2 added

Action to EOR 1-1: Chapter 5.2.3 - FMT_SMR.1.2 added

Action to SERTIT comment 7: Chapter 5.4 – SOF claim is NA.

Action to EOR 1-4: Chapter 6.1.4 – "voice or" is removed.

Action from Thales review: Chapter 6.2 – ATE_IND.2: TCN -> Thales Norway

Action to EOR 1-2: Chapter 8.3. - FPT_STM.1 is included.

Action from Thales review: Chapter 8.3.2 – FMT_SMR.1 shall also satisfy OE.AUDIT. Mismatch between table and text. Cross added to table.

Action to EOR 1-2: Chapter 8.4 – FPT_STM.1 is included.

End of changes in edition 2

Changes in edition 3:

Chapter 1.1: Exhaustive list of OTA HW Item Change Status included in the TSF 101 security evaluation.

Chapter 5.1.4: FPT_FLS.1 is changed from [Single Point of failure] to an explicit list of protection mechanisms.

Table 4: Assurance measure for ALC_DVS.1 is updated.

End of changes in edition 3.

Changes in edition 4:

Table 1: FPT_STM.1 Reliable Time Stamps is added to the table.

End of changes in edition 4.

Changes in edition AAAA 2.1:

The document has changed variant code to AAAA and the edition starts at 2.1 to follow the product line codification with document versions according to the software generation they apply to.

Chapter 1.1 Software version is updated.

Chapter 1.4 Reference 1 is updated.

Chapter 2.2 The firewall bullet is updated to reflect selection of two filter sets.

FMT_SMF.1.1 Selection sets of predefined filter criteria is added to the bracket.

EAL5 is augmented with ALC_FLR.3 throughout the document.

End of changes in edition AAAA 2.1.

Changes in edition AAAA 2.2:

Chapter 4.1 O.NO.CONFIG updated to include sets of predefined filter criteria.

Chapter 6.1.2 SF.Information.Flow.Control updated to include sets of predefined filter criteria.

Chapter 8.3.1 Table 6 updated for O.NO.CONFIG and FMT_SMF.1.

Chapter 8.3.1.1 FMT_SMF.1 updated with O.NO.CONFIG.

Chapter 8.3.1.2 O.NO.CONFIG updated with FMT_SMF.1 and O.FW.STATISTICS corrected for FMT_SMF.1.

Chapter 8.4 SF.Information.Flow.Control updated with FMT_SMF.1.

End of changes in edition AAAA 2.2.