

NetCrypt Family Series
S20/R100/U1000/U2000
Security Target
2.0

1	Chapter 1 –Introduction	7
1.1	ST Reference	7
1.2	TOE Reference.....	7
1.3	TOE Overview	8
1.3.1	TOE Type	8
1.3.2	TOE Usage	9
1.3.3	TOE Major Security Features.....	11
1.3.4	Non-TOE hardware/software/firmware.	11
1.4	TOE Description	12
1.4.1	Physical Scope of the TOE	12
1.4.2	Logical Scope of the TOE.....	12
1.5	Terms and Acronyms	13
2	Chapter 2 – Conformance Claims	14
2.1	CC Conformance.....	14
2.2	Protection Profile Conformance.....	14
2.3	Package Conformance.....	14
3	Chapter 3 – Security Problem Definition	15
3.1	Assets	15
3.1.1	AST.DATA	15
3.1.2	AST.TSF_DATA	15
3.2	Threats.....	15
3.2.1	T.UNAUTHORISED_PEER.....	15
3.2.2	T.EAVESDROP	15
3.2.3	T.MALFUNCTION.....	15
3.3	Assumptions.....	16
3.3.1	A.TRUSTED_ADMIN.....	16
3.3.2	A.PHYSICAL_ENV	16
3.3.3	A.KEYCRYPT	16
3.3.4	A.TIME_STAMP	16
3.3.5	A.IT_ENVIRONMENT	16
4	Chapter 4 Security Objectives	17
4.1	Security Objectives for the TOE.....	17
	<u>4.1.1 O.AUTHORISED_PEER.....</u>	<u>17</u>

	4.1.2 O.AUDIT	17
	4.1.3 O.CORRECT_OPS	17
	4.1.4 O.PROTECTED_COMMS	17
4.2	Security Objectives for the Operational Environment	17
	4.2.1 OE.TRUSTED_ADMIN	17
	4.2.2 OE.PHYSICAL_ENV	17
	4.2.3 OE.KEYCRYPT	17
	4.2.4 OE.TIME_STAMP	17
	4.2.5 OE.IT_ENVIRONMENT	17
4.3	Security Objectives Rationale	18
	4.3.1 T.UNAUTHORISED_PEER	18
	4.3.2 T.EAVESDROP	18
	4.3.3 T.MALFUNCTION	18
	4.3.4 A.TRUSTED_ADMIN	20
	4.3.5 A.PHYSICAL_ENV	20
	4.3.6 A.KEYCRYPT	20
	4.3.7 A.TIME_STAMP	20
	4.3.8 A.IT_EMVIRONMENT	20
5	Chapter 5 - Security Requirements	21
5.1	Conventions	21
5.2	Security Functional Requirements (SFRs)	22
	5.2.1 Security Audit	22
	5.2.2 Cryptographic Support	22
	5.2.3 Protection of TSF	23
	5.2.4 Trusted Channels	24
5.3	Security Functional Requirement Rationale	25
	5.3.1 O.AUTHORISED_PEER	25
	5.3.2 O.AUDIT	25
	5.3.3 O.CORRECT_OPS	25
	5.3.4 O.PROTECTED_COMMS	26
5.4	Security Functional Requirement Dependency Rationale	27
5.5	Security Assurance Requirements	28
5.6	Security Assurance Requirement Rationale	28
6	Chapter 6 TOE Summary Specification	29
6.1	Security Audit	29
6.2	Cryptographic Support	29
	6.2.1 Cryptographic Operations	29

	6.2.2 Cryptographic Keys Generation.....	30
	6.2.3 Cryptographic Key Destruction	30
	6.3 Protection of the TSF	30
	6.4 Trusted Channels.....	30
7	APPENDIX A.....	32

This page is left blank

1 Chapter 1 –Introduction

1.1 ST Reference

Title	NetCrypt Family Series S20/R100/U1000/U2000 Security Target
Version	2.0
Publication date	8 Sep 2026

Table 1: ST reference

1.2 TOE Reference

TOE Reference: NetCrypt Family Series S20/R100/U1000/U2000

Model name	NetCrypt S20	NetCrypt R100	NetCrypt U1000	NetCrypt U2000
Part number	9910-8000-0723	9910-8000-1190	9910-8000-0733	9910-8000-1281
Firmware version	2.7.2	2.7.2	2.7.2	2.7.2
PCBA version	S20-110-A30	R100-320-B10	U1000-570-A30	U2000-570-A30

Table 2: TOE reference

1.3 TOE Overview

The TOE consists of the following models.

Model	Diagram
NetCrypt S20	
NetCrypt R100	
NetCrypt U1000	
NetCrypt U2000	

Table 3: TOEs in the family series

The table below highlights the differences across the different models, otherwise the major security features of each model are the same.

Model	Ethernet	Console	Emergency Erasure	Battery	Power supply
NetCrypt S20	4 x 10/100/1000 BaseT	RS-232	No	Yes	12 VDC
NetCrypt R100	4 x 10/100/1000 BaseT	RS-232	Yes	Yes	18-32V VDC
NetCrypt U1000	4 x 100/1000 BaseT	RS-232	Yes	Yes	110/240 VAC
NetCrypt U2000	4 x 100/1000 BaseT	RS-232	Yes	Yes	110/240 VAC

Table 4: Hardware differences across different TOE models.

1.3.1 TOE Type

The TOE is a hardware Internet Protocol (IP) encryptor.

1.3.2 TOE Usage

The TOE comes with the following interfaces:

- 2 x Trusted Ports
- 1 x External Port
- 1 x Management Port
- 1 x Console Port

The following provides further details of each interface.

Interface	Purpose	Labels	Ethernet Specification
Trusted port, also known as RED ports	Connected to the internal network. User traffic is transmitted in clear over these ports.	T1, T2	Gigabit NIC 10/100/1000Mbps Auto-sensing
External port	Connected to the public or untrusted network. User traffic is transmitted encrypted over this port.	Ext	Gigabit NIC 10/100/1000Mbps Auto-sensing
Management port	A TOE user manages the TOE over TCP/IP protocol. The port requires that the TOE user to authenticate to a KeyCrypt token before he/she can access the security management functions.	Mgmt	Gigabit NIC 10/100/1000Mbps Auto-sensing
Console port	A TOE user manages the TOE over RS-232. This is meant as a backup to manage the TOE in case a TOE user fails to access the security management functions via Management port. This port also allows a TOE user to handle TOE security-relevant events such as emergency erasure, lockdown, etc.	RS-232	Not applicable

Table 5: TOE interfaces

The TOE operates with a peer TOE to establish an IPsec tunnel. In turn, a trusted channel is established between the TOE and peer TOE. The diagram below illustrates the TOE usage.

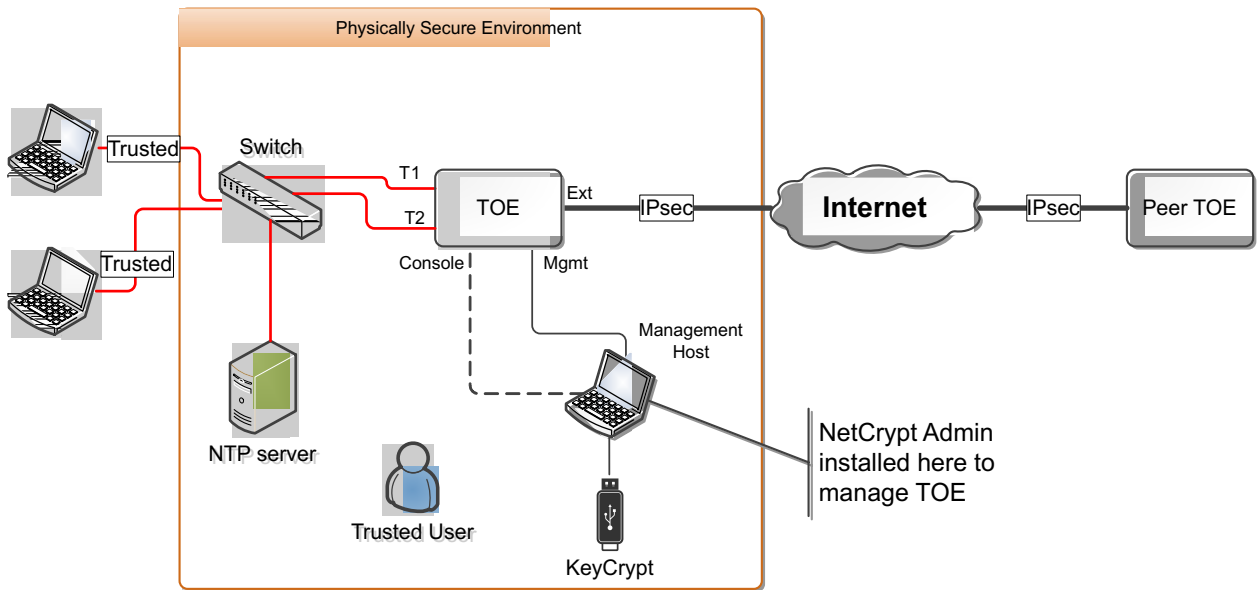


Figure 1: TOE usage

1.3.3 TOE Major Security Features

The TOE primarily establishes a trusted channel with a peer TOE. The following summarises the TOE's major security features.

- **Security Audit**
The TOE generates audit logs of security relevant events associated with the trusted channel.
- **Cryptographic Support**
The TOE implements cryptographic operations that supports the establishment of trusted channel.
- **Protection of TSF**
The TOE implements self-tests mechanism that preserves the TOE's secure state when a malfunction is detected.
- **Trusted Channel**
The TOE establishes trusted channel with a peer TOE to protect user data that is transported over the channel.

1.3.4 Non-TOE hardware/software/firmware.

The required non-TOE hardware/software/firmware are as follows:

Item	Purpose
NetCrypt Administrative Management software (NetCrypt Admin)	This is a software application that runs on a host machine. The host machine connects to the TOE via the TOE's Management Port. A TOE user uses this software application to access the TOE security management functions. For a TOE user to access the TOE security management functions, the TOE user must insert his/her KeyCrypt into the host machine. KeyCrypt shall then identify and authenticate the TOE user. Upon successful identification and authentication, the TOE user shall gain access to the TOE's security management functions This is part of the TOE deliverables.
KeyCrypt	This is a USB token that a TOE user uses as part of a 2-Factor Authentication (2FA) process to access the TOE's security management functions. This is to be purchased separately by the user. This is part of the TOE deliverables.
Cryptographic Token Personalization tool	Software application to personalize KeyCrypt. This is part of KeyCrypt deliverables.
Peer TOE	The TOE communicates with a peer TOE to establish an IPsec tunnel, in turn, establishing a trusted channel.
NTP server	The NTP server provides reliable timestamp to the TOE for audit generation purpose.

Table 6: Non-TOE

1.4 TOE Description

1.4.1 Physical Scope of the TOE

The physical scope of the TOE consists of the following components.

- Mechanical enclosure
- PCB assembly
- Firmware

The parts of the TOE are delivered using the following methods.

Item	Description	Format	Delivery method
TOE	hardware Internet Protocol (IP) encryptor.	hardware	Local delivery: ST Engineering delivery team Overseas delivery: Trusted courier
Netcrypt Series (S20/U1000/U2000/R100) Administrator's Guide, version 2.0.3	TOE user guidance	pdf file stored in a CD	
NetCrypt Administrative Management installer v2.7.6	A user uses the application for the following purposes: • Access NetCrypt's security management functions. • Create Master token and Administrator's token.	exe file stored in a CD	

Table 7: TOE deliverables

1.4.2 Logical Scope of the TOE

The TOE comprises of several security features. The following sections further elaborate each of the security feature.

1.4.2.1 Security Audit

The TOE can generate audit records of security-relevant events occurring on the TOE. The generated audit records include the attributes, date, time and event message. The TOE provides TOE users with the ability to retrieve and view audit records stored within the TOE. The TOE can only store up to a maximum of 10,000 audit records, where the oldest audit records are overwritten by new audit records.

1.4.2.2 Cryptographic Support

The TOE implements cryptographic operations that supports establishment of trusted channel. These cryptographic operations supports IKEv2 for keys derivations and device authentications, and IPsec (ESP only) for confidentiality and integrity protections of user data in transit.

The TOE also implements a Group Transport Key (GTK) which provides an additional layer of confidentiality and data integrity protection during IKEv2.

1.4.2.3 Protection of TSF

The TOE implements cryptographic self-test during initial startup to ensure that its cryptographic functions are operating correctly. The self-test may also be initiated manually by a TOE user.

1.4.2.4 Trusted Channels

The TOE provides secure IPsec communication channel between TOE and another peer TOE after successful device-to-device authentication through IKEv2 protocol.

1.5 Terms and Acronyms

The following table describes the acronyms used in this document:

TERM	DEFINITION
2FA	Two-Factor Authentication
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CSP	Critical Security Parameters
CC	Common Criteria version 3.1
EAL	Evaluation Assurance Level
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
IPSEC	Internet Protocol Security
SA	Security Association
SP	Security Policy
SPI	Security Parameter Index
UDP	User Datagram Protocol
ESP	Encapsulating Security Payload
DH	Diffie-Hellman
ECP	Elliptic Curve Groups modulo a Prime (ECP Groups)
RSA	Rivest–Shamir–Adleman public-key cryptosystems

2 Chapter 2 – Conformance Claims

2.1 CC Conformance

The Security Target and its TOE conforms with Common Criteria Information Technology Security Evaluation Version 3.1, Revision 5

- Part 2 extended
- Part 3 conformant

2.2 Protection Profile Conformance

The ST does not claim conformance to any Protection Profile.

2.3 Package Conformance

The ST is conformant to Common Criteria Evaluation Assurance Level 2 (CC EAL2).

3 Chapter 3 – Security Problem Definition

This chapter identifies the following:

- Assumptions about the TOE's operational environment.
- IT related threats to the organization countered by the TOE.
- Environmental threats requiring controls to provide sufficient protection.

3.1 Assets

3.1.1 AST.DATA

The primary asset is the user data transported between the TOE and peer TOE.

3.1.2 AST.TSF_DATA

Secondary asset is TSF data that supports the establishment of trusted channel between the TOE and peer TOE.

3.2 Threats

The following lists the threats addressed by the TOE and the operational environment.

The TOE protects user data as primary asset by means of cryptographic functions. Thus, the cryptographic functions, their keys and CSP itself are also objects of attacks. These threats are defined here.

3.2.1 T.UNAUTHORISED_PEER

An attacker may impersonate as an authorised TOE peer to establish a secure channel with the TOE which leads to disclosure of AST.DATA.

3.2.2 T.EAVESDROP

An attacker eavesdrops and tampers on communication channel between a TOE and a peer TOE which leads to disclosure and integrity of AST.DATA or AST.TSF_DATA.

3.2.3 T.MALFUNCTION

An attacker may use a malfunction of the TOE to deactivate, modify, or circumvent the TSF to compromise the integrity or confidentiality of AST.DATA or AST.TSF_DATA.

3.3 Assumptions

This section describes the assumptions.

3.3.1 A.TRUSTED_ADMIN

The TOE users are trusted and well-trained; this includes adhering to guidance documentations.

3.3.2 A.PHYSICAL_ENV

The TOE shall be deployed in a physically secure environment

3.3.3 A.KEYCRYPT

KeyCrypt token provides appropriate protection for the 2-Factor Authentication keys.

3.3.4 A.TIME_STAMP

The operational environment shall provide a reliable time stamp to the TOE.

3.3.5 A.IT_ENVIRONMENT

The management host and other networking devices (e.g. switch) shall operate in a secure environment and keep up to date with latest security patches.

4 Chapter 4 Security Objectives

This chapter identifies the security objectives of the TOE and the operational environment. The security objectives identify the responsibilities of the TOE and the operational environment in meeting the security needs.

4.1 Security Objectives for the TOE

The following subsections describe security objectives for the TOE:

4.1.1 O.AUTHORISED_PEER

The TOE shall identify and authenticate the peer TOE before a trusted channel is established.

4.1.2 O.AUDIT

The TOE shall generate audits of security-relevant events.

4.1.3 O.CORRECT_OPS

The TOE shall enter a secure state upon negative results of self-tests.

4.1.4 O.PROTECTED_COMMS

The TOE shall establish a secure channel with a peer TOE. The secure channel shall protect the integrity and confidentiality of AST.DATA and AST.TSF_DATA in transit.

4.2 Security Objectives for the Operational Environment

This section defines the security objectives for the operational environment.

4.2.1 OE.TRUSTED_ADMIN

The TOE users are trusted and well-trained; this includes adhering to guidance documentations.

4.2.2 OE.PHYSICAL_ENV

The TOE user shall deploy the TOE in a physically secure environment.

4.2.3 OE.KEYCRYPT

The administrator shall ensure a cryptographic token will be used to store 2FA authentication keys.

4.2.4 OE.TIME_STAMP

The TOE user shall ensure that the operational environment provides a reliable time stamp to the TOE.

4.2.5 OE.IT_ENVIRONMENT

The TOE user shall ensure that the IT equipments supporting the operational of the TOE are always set up and used in a secure environment and kept up to date.

4.3 Security Objectives Rationale

	T.UNAUTHORISED_PEER	T.EAVESDROP	T.MALFUNCTION	A.TRUSTED_ADMIN	A.PHYSICAL_ENV	A.TIME_STAMP	A.KEYCRYPT	A.IT_ENVIRONMENT
O.AUTHORISED_PEER	✓							
O.AUDIT			✓					
O.CORRECT_OPS			✓					
O.PROTECTED_COMMS		✓						
OE.TRUSTED_ADMIN			✓	✓				
OE.PHYSICAL_ENV					✓			
OE.TIME_STAMP						✓		
OE.KEYCRYPT							✓	
OE.IT_ENVIRONMENT								✓

Table 8 Mapping of Security Problem Definition to Security Objectives

4.3.1 T.UNAUTHORISED_PEER

O.AUTHORISED_PEER addresses this threat by requiring all peer TOE to be identified and authenticated before TOE established a secure channel with the peer TOE. This verifies the identity and authenticity of the peer TOE. Hence, reducing the risk of attacker compromising the confidentiality of the AST.DATA.

4.3.2 T.EAVESDROP

O.PROTECTED_COMMS addresses this threat by requiring TOE and identified and authenticated peer TOE to establish a secure channel. The secure channel shall protect the integrity and confidentiality of AST.DATA and AST.TSF_DATA in transit. Hence, reducing the risk of attacker compromising the confidentiality of AST.DATA and AST.TSF_DATA.

4.3.3 T.MALFUNCTION

O.CORRECT_OPS addresses this threat by requiring that TOE performs self-tests. The self-tests shall improve the TOE's opportunity to detect possible malfunctions. In turn, reducing the risk of attacker compromising integrity or confidentiality of AST.DATA or AST.TSF_DATA by exploiting the TOE's malfunction state.

O.AUDIT requires that the TOE generates audit logs for security-relevant events. Together with **OE.TRUSTED_ADMIN**, which would require that TOE users following the user guidance to monitor the audit log periodically, should further improve the opportunity to detect possible malfunction, in turn, mitigating it. As a result, further reducing the risk of attacker compromising integrity or confidentiality of AST.DATA or AST.TSF_DATA by exploiting the TOE's malfunction state. **OE.TIME_STAMP** shall support **O.AUDIT** by providing a reliable timestamp

4.3.4 A.TRUSTED_ADMIN

This assumption is directly upheld by OE.TRUSTED_ADMIN.

4.3.5 A.PHYSICAL_ENV

This assumption is directly upheld by OE.PHYSICAL_ENV.

4.3.6 A.KEYCRYPT

This assumption is directly upheld by OE.KEYCRYPT.

4.3.7 A.TIME_STAMP

This assumption is directly upheld by OE.TIME_STAMP.

4.3.8 A.IT_ENVIRONMENT

This assumption is directly upheld by OE.IT_ENVIRONMENT.

5 Chapter 5 - Security Requirements

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, dated: April 2017 and all international interpretations.

5.1 Conventions

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Assignment: Indicated with ***bold italicized*** text;
- Refinement: Indicated with **bold** text;
- Selection: Indicated with *italicized* text;
- Iteration: Indicated by appending the iteration symbol.

e.g. FCS_COP.1/AES, FCS_COP.1/RSA

Extended SFRs are identified by having a label 'EXT' after the requirement name.

5.2 Security Functional Requirements (SFRs)

5.2.1 Security Audit

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 <i>not specified</i> level of audit; and c) <i>Refer to Appendix A for the list of all auditable events</i>
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, <i>no other audit relevant information.</i>
FAU_SAR.1	Audit Review
FAU_SAR.1.1	The TSF shall provide <i>Administrators</i> with the capability to read <i>Key Exchange Logs and Packet Processing Logs</i> from the audit records.
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.2.2 Cryptographic Support

FCS_CKM.1/RSA	Cryptographic Key Generation
FCS_CKM.1.1/RSA	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm <i>RSA cryptographic key pair generation</i> and specified cryptographic key sizes <i>4096-bits</i> that meet the following: <i>SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms (Version 1.3), Chapter 7.3 Random Number Generator with Specific Distribution.</i>
FCS_CKM.1/SYM	Cryptographic Key Generation
FCS_CKM.1.1/SYM	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm <i>HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512</i> and specified cryptographic key sizes <i>256, 384, 512 bits</i> that meet the following: <i>FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code", and FIPS Pub 180-3, "Secure Hash Standard".</i>
FCS_CKM.4	Cryptographic Key Destruction
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified

cryptographic key destruction method **zeroization** that meets the following:
none.

**FCS_COP.1/Data
Encryption/Decryption**

Cryptographic operation

FCS_COP.1.1/Data
Encryption/Decryption

The TSF shall perform **data encryption and decryption** in accordance with a specified cryptographic algorithm **AES used in CBC mode** and cryptographic key sizes **256 bits** that meet the following: **FIPS PUB 197 "Advanced Encryption Standard (AES)"**.

Application note: Implemented as part of IKEv2 and IPsec.

**FCS_COP.1/Cryptog
raphic Signature**

Cryptographic operation

FCS_COP.1.1/Cryptog
raphic Signature

The TSF shall perform **cryptographic signature services** (generation and verification) in accordance with a specified cryptographic algorithm **RSA (digital signature)** and cryptographic key sizes **4096 bits** that meet the following: **PKCS#1 standard (Version 1.5)**.

Application note: Implemented as part of IKEv2

**FCS_COP.1/Cryptog
raphic Hashing**

Cryptographic operation

FCS_COP.1.1/Cryptog
raphic Hashing

The TSF shall perform **cryptographic hashing** in accordance with a specified cryptographic algorithm **SHA-256 and SHA-512** and cryptographic keys sizes **none** that meet the following: **FIPS PUB 180-4, "Secure Hash Standard"**.

Application note: Implemented as part of IKEv2.

**FCS_COP.1/Keyed-
hash Message
Authentication**

Cryptographic operation

FCS_COP.1.1/Keyed-
hash Message
Authentication

The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm **HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512** and cryptographic key size **256, 384, 512 bits** that meet the following: **FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code", and FIPS Pub 180-3, "Secure Hash Standard"**.

Application note: Implemented as part of IKEv2 and IPsec

5.2.3 Protection of TSF

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: **failure of FPT_TST.1**.

Application note: In the secure state (TOE in non-operational mode), all input and output through the network interface ports are disabled. As an indicator of self-test failure, the alarm LED would be activated.

FPT_TST.1**TSF Testing**

FPT_TST.1.1

The TSF shall run a suite of self-tests *during initial start-up, at the request of the authorised user* to demonstrate the correct operation of:

- ***FCS_COP.1/Data Encryption/Decryption***
- ***FCS_COP.1/Cryptographic Hashing***
- ***FCS_COP.1/Keyed-hash Message Authentication***

FPT_TST.1.2

The TSF shall provide authorised users with the capability to verify the integrity of ***none***.

FPT_TST.1.3

The TSF shall provide the capability to verify the integrity of ***none***.

5.2.4 Trusted Channels**FTP_ITC.1****Inter-TSF trusted channels**

FTP_ITC.1.1

The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2

The TSF shall permit the *TSF, another trusted IT product* to initiate communication via the trusted channel.

FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for ***transportation of AST.DATA***.

5.3 Security Functional Requirement Rationale

	O.AUTHORISED_PEER	O.AUDIT	O.CORRECT_OPS	O.PROTECTED_COMMS
FAU_GEN.1		x		
FAU_SAR.1		x		
FCS_CKM.1/RSA				x
FCS_CKM.1/SYM				
FCS_CKM.4				x
FCS_COP.1/Data Encryption/Decryption				x
FCS_COP.1/Cryptographic Signature				x
FCS_COP.1/Cryptographic Hashing				x
FCS_COP.1/Keyed-hash Message Authentication				x
FPT_FLS.1			x	
FPT_TST.1			x	
FTP_ITC.1	x			x

Table 9: Security requirement rationale mapping

5.3.1 O.AUTHORISED_PEER

The TOE shall identify and authenticate the peer TOE before a secure channel is established.
The following security functional requirements contribute to satisfying this security objective:

FTP_ITC.1	specifies the requirement for a trusted channel to be established with another trusted IT product, which included identification and authentication of the peer trusted IT product.
-----------	---

5.3.2 O.AUDIT

The TOE shall generate audits of security-relevant events. The following security functional requirements contribute to satisfying this security objective:

FAU_GEN.1	specifies generation of audit records for security relevant-events.
FAU_SAR.1	specifies the functions for administrators to review audit records.

5.3.3 O.CORRECT_OPS

The TOE shall enter a secure state upon negative results of self-tests. The following security

functional requirements contribute to satisfying this security objective:

FPT_TST.1	specifies self-tests to verify the correctness of cryptographic functions.
FPT_FLS.1	specifies preservation of secure state upon failure FPT_TST.1

5.3.4 O.PROTECTED_COMMS

The TOE shall establish a secure channel with a peer TOE. The secure channel shall protect the integrity and confidentiality of AST.DATA and AST.TSF_DATA in transit. The following security functional requirements contribute to satisfying this security objective:

FCS_CKM.4	specifies the key destruction method for the transient cryptographic keys that are generated during the establishment of trusted channel.
FCS_CKM.1/RSA FCS_CKM.1/SYM	specifies the key generation method for the establishment of trusted channel.
FCS_COP.1.1/Data Encryption/Decryption FCS_COP.1/Cryptographic Signature FCS_COP.1/Cryptographic Hashing FCS_COP.1/Keyed-hash Message Authentication	specify the cryptographic algorithms and communication protocol to establish a trusted channel with another trusted IT product.
FTP_ITC.1	specifies the requirement for a trusted channel to be established with another trusted IT product.

5.4 Security Functional Requirement Dependency Rationale

Requirements	Dependencies	Inclusion/Rational for non-inclusion
FAU_GEN.1	FPT_STM.1	FPT_STM.1 is upheld by OE.TIME_STAMP.
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FCS_CKM.1/RSA	[FCS_CKM.2, or FCS_COP.1]	FCS_COP.1/Cryptographic Signature
	FCS_CKM.4	FCS_CKM.4
FCS_CKM.1/SYM	[FCS_CKM.2, or FCS_COP.1]	FCS_COP.1 Data Encryption/Decryption FCS_COP.1 Keyed-hash Message Authentication
	FCS_CKM.4	FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1/RSA FCS_CKM.1/SYM
FCS_COP.1 Data Encryption/Decryption	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1/SYM
	FCS_CKM.4	FCS_CKM.4
FCS_COP.1 Cryptographic Signature	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1/RSA
	FCS_CKM.4	FCS_CKM.4
FCS_COP.1 Cryptographic Hashing	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Not applicable. Cryptographic hashing does not require key.
	FCS_CKM.4	FCS_CKM.4
FCS_COP.1 Keyed-hash Message Authentication	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1/SYM
	FCS_CKM.4	FCS_CKM.4
FPT_FLS.1 Failure with preservation of secure state	No Dependencies	Not applicable
FPT_TST.1 TSF testing	No Dependencies	Not applicable
FPT_ITC.1 Inter-TSF trusted channel	No Dependencies	Not applicable

Table 10: SFRs Dependencies

5.5 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 2 components, as specified in (CC) part 3. No operations are applied to the assurance components.

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

Table 11: SAR for EAL2

5.6 Security Assurance Requirement Rationale

The evaluation assurance package selected for the evaluation of the TOE is Evaluation Assurance Level 2 (EAL2). EAL2 was chosen to provide a low to moderate level of assurance that is consistent with commercial products of this sort. The chosen assurance level is appropriate with the threats defined for the environment (physical protection by the environment, limited interface and access to the TOE).

6 Chapter 6 TOE Summary Specification

6.1 Security Audit

The TOE relies on the operational environment to provide the reliable timestamp for the audit logs stored in the storage area. The logs provide an audit trail of all security-relevant events with corresponding dates and time. Any potential attacks related to malfunction of TOE shall be logged.

The TOE maintains the following audit log classifications:

- Key Exchange store
- Packet Processing store

Each classification has limited audit records storage capacity which can only store up to a maximum of 10,000 audit records. The oldest audit records are then overwritten by new audit records.

This TSF is mapped to the following SFRs: FAU_GEN.1, FAU_SAR.1.

6.2 Cryptographic Support

The TOE provides cryptographic functions such as RSA digital signature and verification, symmetric data encryption/decryption and integrity verification using secure hashing. All defined cryptographic functions use algorithm and key sizes as specified in the security policy of the TOE (during TOE configuration).

The table below summarizes the cryptographic operations and SFRs mapping.

6.2.1 Cryptographic Operations

IPSEC				
	Service	Method	Standard	SFR
ESP	Encryption	AES-256 CBC	FIPS 197	FCS_COP.1/Data Encryption/Decryption,

Table 12: IPSec

IKEv2				
	Service	Method	Standard	SFR
Messages	Encryption	AES-256 CBC	FIPS 197	FCS_COP.1/Data Encryption/Decryption
Messages	Authentication	HMAC- SHA-256, HMAC- SHA-382, HMAC- SHA- 512	FIPS 198-1, FIPS 180-3	FCS_COP.1/Keyed-hash Message Authentication
Peer Authentication	Signature services (RSA)	RSA signing	PKCS#1	FCS_COP.1/Cryptographic Signature
Peer Authentication	Hash for signatures	SHA-256 bits, 512 bits	FIPS 180-4	FCS_COP.1/Cryptographic Hashing

Table 13: IKEv2

6.2.2 Cryptographic Keys Generation

Key	Used For	Key Size (Bit)	Key Generation Standard	SFR
RSA	Device Authentication	4096	PKCS#1	FCS_CKM.1/ RSA
IKEv2 /IPsec	Key expansion	256, 384 or 512	HMAC- SHA-256, HMAC- SHA-382, HMAC- SHA- 512	FCS_CKM.1/ SYM

Table 14: Key generations

6.2.3 Cryptographic Key Destruction

The TOE destroys cryptographic keys in the memory by overwriting the specific memory with zeroes. This happens in the following events:

- Expiration of IPsec sessions keys
- Purging of shared secret
- Derived keys after DH key exchange.

This TSF is mapped to the following SFRs: FCS_CKM.4

6.3 Protection of the TSF

The TOE performs a cryptographic self-test during initial start-up or at request of authorised Administrator to ensure that this critical security function is functional. The self-test performed includes cryptographic algorithms Known Answer Test for AES256, SHA2 and HMAC.

In the event of self-tests failure, the TOE will enter a secure state (TOE in non-operational mode), all input and output through the network interface ports are disabled. As an indicator of self-test failure, the alarm LED would be activated. TOE may recover only after self-test passes.

This TSF is mapped to the following SFR: FPT_TST.1, FPT_FLS.1.

6.4 Trusted Channels

The TOE provides provide secure IPsec (AES 256 CBC together with SHA2 based HMAC cryptographic algorithms) communication between TOE and another peer TOE after successful device-to-device authentication using IKEv2 protocol.

During TOE provisioning, an RSA cryptographic key (4096 bits) is generated within the TOE for signing purposes during TOE-to-TOE authentication. The Key exchange protocol used is IKEv2 as according to RFC7296. During the initial phase of key exchange, Diffie- Hellman key exchange with 4096 bits or ECP P521 bits may be used to generate the shared secret on both TOE. After which, it will be sent through a key expansion function to derive multiple keys for different purposes (encryption, integrity protection, authentication, signing and derivation of further key materials). Using this set of derived keys, the TOE performs data encryption/decryption (AES 256 CBC), data integrity protection (HMAC) of key exchange data. During key exchange, the cryptographic hash (SHA-256 or SHA-512 bits) is used in conjuncture with the RSA key for signing and authentication purposes. Also, the keyed hash message authentication (HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512) is used to protect the integrity of the data (as according the PRF algorithm defined in RFC7296) during key exchange. Upon successful key exchange, an IPsec tunnel between TOEs is created and the generated IPsec session keys shall be used for encryption/decryption (AES-256-CBC) of user data. The maximum IKEv2 SA lifetime is limited

to 24 hours for phase 1 SAs and 8 hours for phase 2 SAs.

This TSF is mapped to the following SFR: FTP_ITC.1, FCS_COP.1/Data Encryption/Decryption, FCS_COP.1/Cryptographic Signature, FCS_COP.1/Cryptographic hashing, FCS_COP.1/Keyed-hash Message Authentication.

7 APPENDIX A

1. List of Audit Logs

Log Types	Status/Errors	Meaning
Key Management	Initiating IKE SA to x.x.x.x	Starting of the key exchange protocol with another trusted IT device
Key Management	SA Init Established (I)	Initiator successfully completed the key exchange protocol with another trusted IT device
Key Management	SA Init Established (R)	Responder successfully completed the key exchange protocol with another trusted IT device
Key Management	Child SA (I) Established	Initiator successfully completed the traffic key exchange protocol with another trusted IT device
Key Management	Child SA (R) Established	Responder successfully completed the traffic key exchange protocol with another trusted IT device
Key Management	Receiving DPD request from x.x.x.x and sending acknowledgement	Device receiving dead peer detection heartbeat from another trusted IT device.
Key Management	Sending DPD request to x.x.x.x	Device sending dead peer detection heartbeat to another trusted IT device.
Key Management	Passed CRL retrieval from Directory server	Device successfully retrieve CRL from Directory server
Key Management	Failed to retrieve CRL from Directory server	Device failed to retrieve CRL from Directory server
Key Management	Peer ID certificate criteria don't match	Certificate credentials of peer device does not match with current device's configuration
Key Management	Unsupported Authentication method 1	This error is mostly related to the above error "Peer ID certificate criteria don't match"
Key Management	Failed to public decrypt Auth data	Likely to be caused by non-matching RSA key pair
Key Management	Packet failed Authentication verification	This error is mostly related to the above error "Packet failed Authentication verification"
Key Management	Failed to allocate/decode payload	Unable to decipher IKE payloads
Key Management	Unsupported exchange type xx in message. Is transport key used?	Unknown or unsupported exchange type Check if is Group Transport Key is used
Key Management	No proposal chosen	Maybe caused by unsupported encryption/integrity algorithm or group key type
Packet Processing	Eth(x) : link up	When port eth(x) is connected
Packet Processing	Eth(x) : link down	When port eth(x) is disconnected

Packet Processing	System start-up	System boot-up
Packet Processing	System shutdown	System is shutting down.