Thales SIX GTS France
4, Avenue des Louvresses
92622 Gennevilliers Cedex
France
Tel.: +33 (0)1 41 30 30 00
Fax: +33 (0)1 41 30 33 57
www.thalesgroup.com

CSPN SECURITY TARGET

NEXIUM SAFECORE 3

Identifiant entité	Identifiant business	CTD	Révision
0026 – F0057	68734409	306	-D

Changes

Changes record			
Revision	**Date**	**Author**	**Modification**
--	01/02/2022	THALES	Creation
-A	15/03/2022	THALES	Update
-B	23/09/2022	THALES	Modifications according to evaluator’s review
-C	26/06/2023	THALES	Updates for SafeCore 1.5.4 version
-D	30/10/2023	THALES	Updates for SafeCore 2.1.1 version

Table of content

Table index

Figure index

1. INTRODUCTION

1.1 DOCUMENT IDENTIFICATION AND SUMMARY

This document describes the security target of the NEXIUM SafeCore Secure Network Function Virtualization Infrastructure developed by Thales within the framework of the CSPN.

1.2 REFERENCE DOCUMENTS

	Title	Reference	version	Classification
[CSPN]	Certification de Sécurité de Premier Niveau	ANSSI-CSPN-CER-P-01/2.1	2.1	NP
[RGS_B]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques	N/A	2.0	NP
[RECOS_NFVI]	Principes de sécurisation applicables aux plateformes virtuelles supportant des fonctions de télécommunications	3659/ANSSI/SDE/DR	1	DR
[ETSI1]	Network Functions Virtualization; Architectural Framework	GS NFV 002 v1.1.1	1.1.1	NP
[ETSI2]	Network Functions Virtualization (NFV) ; Virtual Network Functions Architecture	S NFV-SWA 001 v1.1.1	1.1.1	NP
[CC]	Common Criteria for information technology security evaluation	CCMB-2017-04-002	3.1	NP
[RECOS_x86]	Recommandations de configuration matérielle de postes clients et serveurs x86	DAT-24/ANSSI/SDE/NP	1.0	NP
[CRYPTO]	Guide des mécanismes cryptographiques	ANSSI-PG-083	2.04	NP

Table 1: Reference Documents

1.3 ACRONYMS

Acronym	Signification
BIOS	Basic Input/Output System
CSPN	Certification de Sécurité de Premier Niveau
EMS	Equipment Management System
NFV	Network Function Virtualization
NFVi	Network Function Virtualization infrastructure
RBAC	Role-Based Access Control
TPM	Trusted Platform Module
UEFI	Unified Extensible Firmware Interface
VM	Virtual Machine
VNF	Virtual Network Function

Table 2: Acronyms

2. TOE IDENTIFICATION

The TOE is the **NEXIUM SafeCore platform**. This product associated with the **SafeProd** production environment and the **SafeInstaller** forms a new secure NFV solution.

Editor	*THALES SIX GTS France*
Product	*NEXIUM SafeCore (Thales – Resilient Network – Secured Network Virtualization)*
Evaluated version	*2.1.1*

Table 3: Product identification

3. TOE OVERVIEW

3.1 SYSTEM OVERVIEW

The **NEXIUM SafeCore** solution allows concurrent and secure execution of multiple VMs hosting network functions on a shared x86 hardware. It provides strong logical isolation both between VMs and between VMs and the hardware.

3.2 TOE DESCRIPTION

3.2.1 TOE Boundary

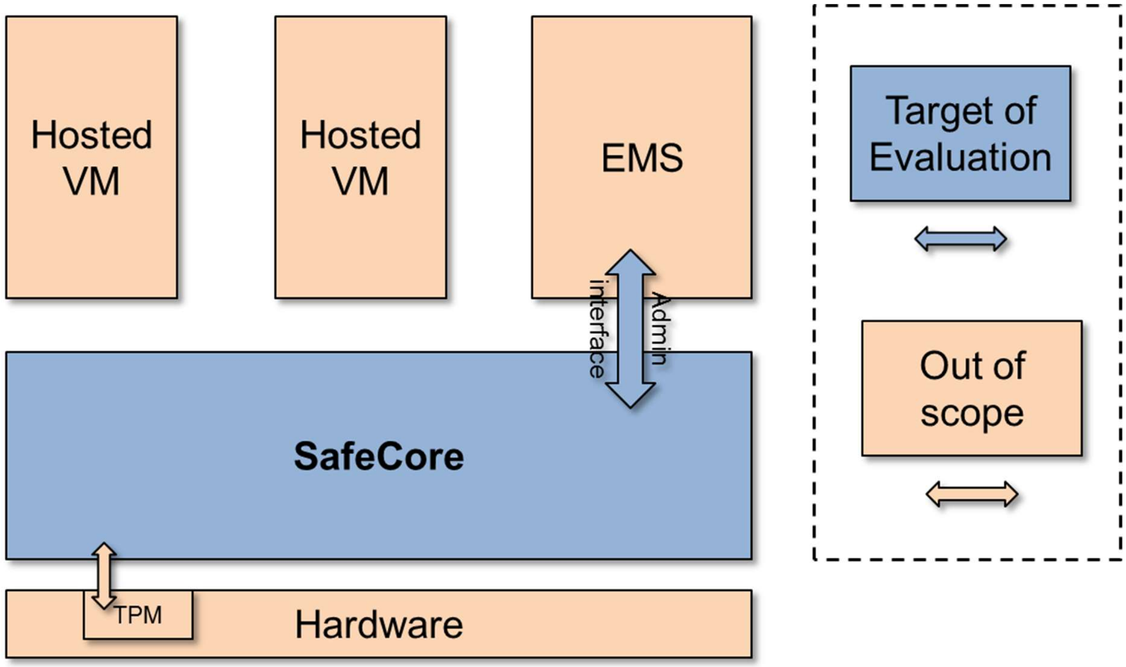

Figure 1: TOE Boundary

The TOE is the **NEXIUM SafeCore** virtualization software version 2.1.1. Other components of the **NEXIUM SafeCore** system as well as the hosted VMs are considered part of the operational environment. The hardware equipment hosting the TOE and other enabling elements, EMS included, are outside of the scope of the TOE described in this document.

NEXIUM SafeCore is designed to be integrated inside a client's information system, similarly to the virtualized equipment it hosts.

3.2.2 Installation

The TOE is delivered on a host computer, ready to operate, without requiring any installation procedure.

The delivery is compound of:

- The applicative software (TOE),
- The TOE's user manual
- A dedicated hardware, hosting the TOE

3.2.3 Available functions

The TOE provides the following functionalities:

- Dedicated access for local hypervisor management inside dedicated VM (EMS)
- Internal data flow isolation and protection
- Secure data storage for both the TOE and hosted VMs
- Certificates and keys management
- Audit data generation and storage
- Logical isolation between hosted VM and hardware resources
- Secure boot

3.2.4 Users

The TOE administration and supervision functions access is based on fixed local, non-Linux-administrative accounts, controlled by a SELinux RBAC authentication. Existing roles in the TOE are described in *Table 4*.

Network (net) roles are associated with internal commutation and VM management. *Security* (sec) roles are associated with the TOE's secret information handling. Finally, *local* (loc) roles are associated with the TOE's management.
Operator-type roles only provide supervision/reading commands while administrator-type roles provide access to read/write commands. Each user account is protected by a password.

Role	Linux users	SELinux users	SELinux roles
Local administrator	**adminloc**	sfc_adminloc_u	sfc_adminloc_r
Network administrator	**adminnet**	sfc_adminnet_u	sfc_adminnet_r
Security administrator	**adminsec**	sfc_adminsec_u	sfc_adminsec_r
Local operator	**operloc**	sfc_operloc_u	sfc_operloc_r
Network operator	**opernet**	sfc_opernet_u	sfc_opernet_r
Security operator	**opersec**	sfc_opersec_u	sfc_opersec_r

Table 4: User profiles and roles

3.3 OPERATIONAL CONTEXT

The TOE is integrated inside the client's network infrastructure. It hosts Virtualized Network Functions (VNFs) and is located in a private environment, with restricted access.

3.4 ASSUMPTIONS

3.4.1 Physical environment

A1 - A.HOST_HARDWARE

The TOE is installed, using its genuine installer on a dedicated X86_64 computer meeting at least the following requirements:

- At least 1 Ethernet port
- At least 50GB of non-volatile memory
- A RAM of at least 4GB size
- At least 2 cores
- The hardware host has to be configured following the recommendations described in ANSSI's technical note RECOS_x86. Additionally, it must support Intel VT-x and VT-d (Intel Virtualization Technology for Directed I/O) as well as UEFI secure boot.
- The host provides the TOE with a cryptographic resource respecting the TPM 2.0 standard certified EAL3 or above.

A2 - A.OPERATION_ENVIRONMENT

The host device is assumed to be deployed in an environment which doesn't allow an attacker to have extended physical access to the TOE in its operating state. However, the host device isn't under constant surveillance and can be subject to acts, malicious or not, compromising its integrity:

- USB peripheral insertion
- Manipulation of network connections

3.4.2 Organizational measures

A3 - A.USER_AWERENESS

The TOE's users are considered trusted and trained to its installation, administration and use. They are aware of restricted data handling procedures. The users have access to the documents required for the TOE correct use.

A4 - A.CONFIGURATION

It is assumed that the TOE's installer has been correctly configured, especially regarding resource allocations, in order to prevent multiple hosted VMs to execute threads on a shared core.

3.5 DEPENDENCIES

All hardware and software resources required by the TOE to fulfill its mission are supplied to the client. No dependency with external elements is considered.

4. DESCRIPTION OF PROTECTED ASSETS

This section lists sensitive assets. For each of them, it associates a “security needs” attribute indicating what protection the asset needs.

4.1 USER DATA

Alias	Description	Security needs
D.VM_DATA	Data contained in hosted VMs virtual disks.	Confidentiality and integrity
D.TRANSFERED_DATA	Data to and from hosted VMs at the time they are transferred through the TOE.	Confidentiality

Table 5: Protected user data

4.2 TOE DATA

Alias	Description	Security needs
D.CONFIG_PARAM	This asset groups all TOE configuration parameters that don’t need any protection against disclosure. (firmware version, certificates …)	Integrity
D.SUPERVISION_DATA	This asset groups all TOE supervision data (TOE state and audit record generated by the TOE), as well as the keys protecting them.	Integrity
D.TIME_BASE	This asset represents the reliable time base kept within the TOE and used by the TOE.	Integrity
D.TOE_SECRETS	This asset represent the keys used by the TOE to protect local persistent data.	Integrity and Confidentiality
D.PASSWORDS	Users’ passwords	Integrity and Confidentiality
D.UPDATE_KEYS	Symmetric and asymmetric cryptographic keys used for software update ciphering and authentication.	Integrity, Confidentiality and Authenticity
D.SOFTWARE	This asset represents the TOE (as the TOE is software).	Integrity, Confidentiality and Authenticity

Table 6: Protected TOE data

4.3 HARDWARE DATA

Alias	Description	Security needs
D.BIOS	Hardware configuration (BIOS)	Integrity

Other hardware elements hosting or connected to the TOE are outside of the scope of this evaluation.

5. THREAT DESCRIPTION

Administrators and operators are not considered attackers. Attackers are entities that can belong to the organization hosting the TOE but don't have authorized access to the TOE.

T1 – T.VM_COMPROMISION

- An attacker tries to use a compromised VM hosted by the TOE in order to access the stored data of another hosted VM or the TOE itself.

T2 – T.ISOLATION_BREACH

- An attacker tries to breach the network isolation mechanisms protecting the transferred data inside the TOE.

T3 – T.SOFTWARE_COMPROMISION

- An attacker tries to compromise the TOE software in order to compromise security functions.

T4 – T.ILLICIT_HW_USE

- An attacker physically accesses the hard drive of the TOE's host hardware in order to extract secrets (keys or passwords) from the TOE.

T5 – T.UNAUTHORIZED_ACCESS

- An attacker tries to masquerade as an administrator of the TOE in order to modify configuration parameters affecting its security.

T6 – T.TIME_BASE_TAMPERING

- An attacker tampers with the TOE's time base in order to falsify log/audit data or to impact certificate validity period.

T7 – T.UPDATE_COMPROMISION

- An attacker attempts to compromise the update process for TOE update in order to undermine the security functionality of the device.

T8 – T.SUPERVISION_COMPROMISION

- An attacker attempts to compromise the supervision data of the TOE in order to camouflage malicious activities.

T9 – T.BIOS_COMPROMISION

- An attacker attempts to modify the BIOS configuration in order to degrade or bypass TOE's security functions.

	T1 - T.VM_COMPROMISION	T2 - T.ISOLATION_BREACH	T3 - T. SOFTWARE_COMPROMISION	T4 – T. ILLICIT_HW_USE	T5 - T.UNAUTHORIZED_ACCESS	T6 - T.TIME_BASE_TAMPERING	T7 - T.UPDATE_COMPROMISION	T8 – T.SUPERVISION_COMPROMISION	T9 – BIOS_COMPROMISION
D.VM_DATA	X								
D.TRANSFERED_DATA		X							
D.CONFIG_PARAM					X				
D.SUPERVISION_DATA						X		X	
D.TIME_BASE						X			
D.TOE_SECRETS				X					
D.PASSWORDS				X					
D.UPDATE_KEYS				X			X		
D.TOE_SOFTWARE			X						
D.BIOS									X

Table 7 : Assets coverage by threats

6. SECURITY FUNCTIONS DESCRIPTION

This section describes the security functions implemented by the TOE:

SF1: SF.KEY_GENERATION

To generate keys, the TOE obtains its entropy from a physical source which output is undistinguishable from a true random number [RGS_B], [CRYPTO]. This source shall be an EAL3, or above, certified TPM 2.0.

This is applied to keys used for:

- UEFI Secure Boot verification chain (generated during the TOE installation)
- hardware disks encryption (generated during the TOE installation)
- SSH keys generation (generated during boot procedure)

SF2: SF.ACCESS_CONTROL

The TOE can only be accessed, locally or using the EMS' admin interface (see Fig. 1) after authentication. The TOE ensures that created passwords contain:

- At least 16 characters
- At least 1 uppercase letter
- At least 1 lowercase letter
- At least 1 number
- At least 1 special character among: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", "+", ",", "-", ".", "/", ":", ";", "<", "=", ">", "?", "[", "\", "]", "_", "{", "|", "}", " € ", " " ", " ' ", "~", " ` " and " "

Passwords are saved in salted hash form in an encrypted partition, dedicated to secret elements.

Additionally, an administrator or operator's session is closed after a 5 minutes period of user inactivity.

SF3: SF.CRYPTO_ISOLATION

The TOE protects in confidentiality and integrity the keys it uses for data protection by the use of a master key safely stored in the host's hardware TPM. This key is only used to open the partition containing the keys cyphering every other partitions of the system, including hosted VMs virtual disks.

SF4: SF_SECURITY_ERASURE

The TOE shall allow for the erasure of all generated keys, including D.TOE_SECRETS, and saved passwords when given the order.

SF5: SF_LOG

The TOE shall store in a dedicated encrypted partition and protect the integrity of security events. Including (but not limited to):

- User authentication
- Authentication failures

- Key generation

The TOE associates, at least, to each event the following metadata:

- Event severity
- Time of occurrence
- User logged (if any at the time)
- Additional data depending on the event type.

SF6: SF.SECURE_BOOT

On TOE restart, it shall control, using UEFI secure boot:

- Boot chain integrity
- Software integrity and authenticity

SF7: SF.FLOW_ISOLATION

The TOE allows isolation between internal data flow by only allowing the network administrator (“*adminnet”)* to instantiate communication bridges and by preventing any direct access to the hardware from a VM (or vice-versa).

No other mean of communication (ex: pipelines, mailboxes …) can be instantiated between VMs.

7. RATIONALE

	T1 - T.VM_COMPROMISION	T2 - T.ISOLATION_BREACH	T3 - T. SOFTWARE_COMPROMISION	T4 – T. ILLICIT_HW_USE	T5 - T.UNAUTHORIZED_ACCESS	T6 - T.TIME_BASE_TAMPERING	T7 - T.UPDATE_COMPROMISION	T8 – T.SUPERVISION_COMPROMISION	T9 – T.BIOS_COMPROMISION
SF1 - SF.KEY_GENERATION			X	X			X	X	
SF2 - SF_ACCESS_CONTROL					X	X	X		
SF3 - SF.CRYPTO_ISOLATION	X								
SF4 - SF_SECURITY_ERASURE				X					
SF5 - SF_LOG			X		X			X	
SF6 - SF.SECURE_BOOT	X		X			X			X
SF7 - SF.FLOW_ISOLATION		X							
A1 - A.HOST_HARDWARE			X		X	X			
A2 - A.OPERATION_ENVIRONMENT				X		X			X
A3 - A.USER_AWERENESS		X			X				
A4 - A.CONFIGURATION	X	X							

Table 8: Threat cover by Security functions and assumptions