Bittium

SafeMove

Security Target: Android VPN

www.bittium.com

Document number [5800613A01]
Version 1.0.10

Document information

Approved by:
Owner: Eskelin, Juha
Delivery: customer representatives, evaluation lab

Version history

Version	Date	Notes	Author	Status
0.0.2	2019.08.02	First draft	Timo Glad	Draft
1.0.2	2019.08.13	Version number changed	Martti Savo-lainen	Draft
1.0.3	2019.11.20	Update app version numbers, clarify Req. 6, add ch7.2	Timo Glad	Draft
1.0.4	2019.11.29	Update app version numbers, add sections 6.3 and 7.3	Timo Glad	Draft
1.0.5	2019.12.05	Update Toughmobile app version number	Timo Glad	Draft
1.0.6	2019.12.12	Update Preparative document version	Timo Glad	Draft
1.0.7	2019.12.15	Update Preparative document version	Timo Glad	Draft
1.0.8	2019.12.23	Update req. 6 and its SFR	Timo Glad	Proposal
1.0.9	2020.04.27	Update version numbers	Timo Glad	Approved
1.0.10	2020.11.24	Update version numbers	Timo Glad	Approved

Table of Contents

1 TERMINOLOGY

Term	Explanation
CentOS	CentOS 7
TOE	Target of Evaluation
VPN tunnel	Encrypted IPSec VPN in tunnel mode
Android	Android M Android N Android O Android P
BTM-R	Bittium Tough Mobile R
BTM-R OS	Bittium Tough Mobile non-GMS (Android M)

2 INTRODUCTION

2.1 Evaluation, TOE and Sponsor Information

Sponsor (Name and Address)	Centro Criptológico Nacional (CCN)
Developer (Name and Address)	Bittium SafeMove Oy Stella Business Park Lars Sonckin Kaari 16 02600 Espoo Finland
Developer PoC (Name and email)	Juha Eskelin <juha.eskelin@bittium.com>
TOE name	Bittium SafeMove VPN
TOE version(s)	Android (generic): 1.2.159 Android (BTM-R): 2020-04-27 @ granite @ c5e05cb
Evaluation type	LINCE + MEC
TOE Guidance	Secure Suite Administrators Guide, v11.1
Product Taxonomy (according to CCN-STIC 140)	Redes privadas virtuales/IPSec

2.2 Evaluation Methodology

[CCN-LINCE-001]	Definición de la Certificación Nacional Esencial de Seguridad (LINCE), Versión 0.1
[CCN-LINCE-002]	Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad (LINCE), Versión 0.1
[CCN-LINCE-003]	Plantilla para la Declaración de Seguridad de la Certificación Nacional Esencial de Seguridad (LINCE), Versión 0.1
[CCN-LINCE-004]	Plantilla del Informe Técnico de Evaluación de la Certificación Nacional Esencial de Seguridad (LINCE), Versión 0.1

3 TOE DESCRIPTION

3.1 TOE Functionality Description

Target of Evaluation (TOE) is Virtual Private Network (VPN) client software. It is responsible for establishing a trusted channel for TCP/IP communication between the TOE and another device or server part of the Operational Environment. The established channel is encrypted and mutually authenticated, ensuring that TOE is communicating with the intended VPN Gateway and that the gateway is communicating with a trusted TOE. The underlying operating system supported by TOE is Android or BTM-R OS depending on the used hardware platform.

TOE supports relevant cryptographic algorithms and is compatible for example with NSA Suite B. Supported cryptographic algorithms are AES-CBC with cryptographic key sizes of 256-bits meeting the NIST SP 800-38A and AES-GCM with cryptographic key sizes 256-bits meeting the NIST SP 800-38D. TOE performs deterministic random bit generation services in accordance of NIST SP 800-90A using CTR_DRBG (AES). IKEv2 with NAT traversal support is implemented as defined in RFC5996 and IPSec architecture as specified in RFC4301. TOE implements the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms AES-GCM-256 as specified in RFC4106 and AES-CBC-256 as specified in RFC3602. For Diffie-Hellman groups TOE supports group 15 as specified in RFC3526, group 16 as specified in RFC3226, group 19, 20, 21 as specified in RFC5903 and group 28, 29, 30 as specified in RFC6954.

3.2 TOE Guidance Identification, Installation and TOE Secure Configurations

Document Name	Document Version	Release Date
Secure Suite Administrators Guide	11.1	2019-05-06
Release Notes for Secure Suite	11.1.100	2019-05-06
SafeMove 11.1.100 Installation and Administration	11.1.100	2019-05-06
SafeMove Management Server 11.1.100 Administrator's Guide	11.1.100	2019-05-06
SafeMove Crypto IP gateway 4.11.582 Administrator's Guide	4.11.582	2019-05-06
SafeMove Android and Windows VPN client Preparative Procedures	1.0.4	2019-12-15
SafeMove CryptoIP Configuration Parameter Guide	1.0.1	2019-11-28

4 OPERATIONAL ENVIRONMENT

TOE Operational Environment consists of client and server hardware and software components.

4.1 Identification

TOE Component	Component Type	Component Version	Required Software	Required Hardware
Bittium SafeMove VPN client for Android	Client	1.2.159	Android M or Android N or Android O or Android P	General Purpose Android Device
Bittium Safemove VPN client for BTM-R	Client	2020-04-27 @ granite @ c5e05cb	BTM-R OS (starting from version SDP3_6.81.0_MR10.1_granite release-keys)	Bittium Tough Mobile R

Operational Environment Component	Component Type	Component Version	Required Software	Required Hardware
Bittium SafeMove CryptoIP Gateway	Server	4.11.582	SafeMove Base Platform based on CentOS 7	General Purpose Computing Platform
Bittium SafeMove Manager	Server	11.1.100	SafeMove Base Platform based on CentOS 7	General Purpose Computing Platform

4.1.1 Server components

Bittium Secure Suite (Bittium SafeMove Crypto IP Gateway and Bittium SafeMove Manager) is a critical part in ensuring the security of the TOE operational environment. It is responsible for providing a trusted channel between the TOE and components in its operational environment. Additionally, it provides a range of remote management capabilities that can be used to enforce policies and configurations related to TOE and its operational environment. These capabilities are different based on the underlying general purpose operating system.

Android / BTM-R OS:

- Management of VPN configuration policies, rules and settings. Mobile Device Management capabilities including:
  - Wipe device
  - Lock device screen
  - Force device status report
  - Collect audit logs

Bittium Secure Suite provides a centralized means of managing a fleet of TOE devices deployed in an organization with the supported platforms.

5 SECURITY PROBLEM DEFINITION

TOE can be described as a software component that provides an encrypted IPSec VPN channel between the device running the TOE and the trusted operational environment where the VPN Gateway resides. TOE supports devices running on supported Android or BTM-R operating system. While the user of the device running TOE can utilize and operate the TOE when accessing the network, configuration and policies of the TOE are managed remotely by a trusted administrator.

It is assumed that there are two different types of threat agents: authorized and unauthorized. The former describes users who are trusted and who have received non-public knowledge and/or training related to the TOE and its proper usage, handling and management. It is assumed that they have access and skills required to make changes to the functionality of the TOE or its operational environment. Authorized threat agents can have physical access to the device running TOE. The latter describes users who are unauthorized and have only public knowledge of the TOE and its operations. Unauthorized threat agents are assumed not to have physical access to the device running TOE.

The threat agents are assumed to be able to access and monitor the encrypted network traffic between the TOE and the operational environment without the ability to decrypt and access clear-text network traffic.

5.1 Threats

5.1.1 Assets

Assets to be protected by the TOE are the following:

Asset	Asset Description	Dimensions to be protected
AS.CONFIDENTIAL_COMMUNICATIONS	Communications which are expected to be encrypted. Within this asset is also included the integrity of the mechanisms that enable the TOE to differentiate between those applications whose communications must be encrypted through the VPN and those which are not confidential.	Confidentiality Integrity

5.1.2 Agents

The threat agents in this SPD may be anyone who has interest in compromising the TOE. The assumed level of expertise for all the threat agents identified below is unsophisticated.

Agent	Agent Description
AG.EXTERNAL	Any agent who is not authorized to handle or operate the TOE.
AG.ADMIN_USER	Any agent who is authorized to configure, handle and operate the TOE and TOE Operational Environment and therefore constitutes a legitimate TOE user if he/she follows

	the established security policy.

5.1.3 Threats

The following table lists the threats addressed by the VPN Client and the operational environment. The assumed level of expertise of the attacker for all the threats identified below is unsophisticated.

Threat	Description of Threat
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromised TSF.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources.
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the TOE security features.
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender because it is not rendered inaccessible after it is no longer used.

5.1.4 Threat descriptions

Threats specified below are addressed by the TOE and the TOE operational environment:

T.TSF_FAILURE

TOE security mechanisms may fail, leading to a compromised TSF.

Assets: AS.CONFIDENTIAL_COMMUNICATIONS

Threat agents: AG.EXTERNAL, AG.ADMIN_USER

T.UNAUTHORIZED_ACCESS

A user may gain unauthorized access to the TOE data. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.

Assets: AS.CONFIDENTIAL_COMMUNICATIONS

Threat agents: AG.EXTERNAL

T.UNAUTHORIZED_UPDATE

A malicious party attempts to supply the end user with an update to the product that may compromise the TOE security features.

Assets: AS.CONFIDENTIAL_COMMUNICATIONS

Threat agents: AG.EXTERNAL

T.USER_DATA_REUSE

User data may be inadvertently sent to a destination not intended by the original sender because it is not rendered inaccessible after it is no longer used.

Assets: AS.CONFIDENTIAL_COMMUNICATIONS

Threat agents: AG.EXTERNAL

5.2 Assumptions

This section specifies the assumptions that must be satisfied by the TOE environment in order for the TOE to provide the security functionality. If the TOE is placed in an operational environment that does not meet these assumptions, the TOE may no longer be able to provide all of its security functionality.

Assumption	Description of Assumption
A.NO_TOE_BYPASS	Information that's not related to establishing a VPN tunnel cannot flow into the network or from the network to the underlying operating system without passing through the TOE.
A.PHYSICAL	It is assumed that authorized administrators take measures to ensure that unauthorized users don't get physical access to the VPN gateway. It is assumed that authorized users of the TOE take measures to ensure that unauthorized users don't get physical access to the TOE.
A.TRUSTED_CONFIG	Personnel configuring the TOE and its operational environment will follow the applicable security configuration guidance.
A.NOEVIL	It is assumed that those administrators or users belonging to the authority, who are authorized to securely manage the TOE and its operational environment, are trustworthy and they have been trained sufficiently to carry out these security management tasks in a proficient manner.
A.SINGLEUSER	It is assumed that the TOE is used and under the control of a single user only.
A.KEYS	It is assumed that the crypto-materials (for example keys used for the encryption of TOE data storage or the key provided to the user) entered into the TOE are of good quality, not disclosed and only distributed to the appropriate devices and users.
A.MINIMUM_PLATFORM	The Platform, including the hardware and operating system will be chosen from the list provided by the TOE provider and the configuration will be compliant with the guidelines provided by TOE provider in its Preparative Procedures documents.

6 SECURITY OBJECTIVES

6.1 Security Objectives of the Target of Evaluation (TOE)

This section identifies and describes the security objectives that are to be addressed by the TOE.

Objective	Objective Description
O.VPN_TUNNEL	The TOE will provide a network communication channel protected by encryption that ensures that the VPN client communicates with an authenticated VPN gateway.
O.RESIDUAL_INFORMATION_CLEARING	The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
O.TOE_ADMINISTRATION	The TOE will provide mechanisms to allow administrators configure the TOE.

6.2 Security Objectives for the Operational Environment

The following are the security objectives for the operational environment of the TOE that are necessary for the TOE to meet its security objectives.

Objective	Objective Description
OE.NO_TOE_BYPASS	Information cannot flow onto the network to which the TOE host device is connected to without passing through the TOE. Information cannot flow from the network to which the TOE host device is connected to without passing through the TOE.
OE.PHYSICAL	TOE consuming organization shall be responsible for ensuring that physical access to TOE and VPN Gateway is restricted to authorized users.
OE.TRUSTED_CONFIG	TOE operational environment administrator shall provide TOE configurations that follow the applicable security configuration guidance and the security requirements defined by the consuming organization to ensure that the TOE can be operated only in a secure manner by the TOE user.
OE.NOEVIL	TOE consuming organization shall be responsible for ensuring that the TOE users and TOE operational environment administrators shall be trustworthy and that they have received sufficient training and knowledge for carrying out TOE management tasks in a proficient manner.
OE.SINGLEUSER	TOE is used and under the control of a single user only.
OE.KEYS	Cryptographic key material (e.g. keys used for authenticating TOE to the VPN gateway) are of good quality, not disclosed and distributed only to the appropriate devices. TOE users should not have access to the cryptographic keys used in the VPN.
OE.MINIMUM_PLATFORM	Consuming organization shall select the hardware and software for the TOE and its operational environment from the list provided by the TOE provider and ensure that the configuration follows of the said hardware and software follows the documented guidelines provided by the TOE provider.

6.3 Security Objectives Rationale

6.3.1 Security Objectives Coverage

	T.TSF_FAILURE	T.UNAUTHORIZED_ACCESS	T.UNAUTHORIZED_UPDATE	T.USER_DATA_REUSE
O.VPN_TUNNEL		X		X
O.RESIDUAL_INFORMATION_CLEARING		X		X
O.TOE_ADMINISTRATION		X	X	
OE.NO_TOE_BYPASS		X		
OE.PHYSICAL		X		
OE.TRUSTED_CONFIG		X	X	
OE.NOEVIL		X		
OE.SINGLEUSER		X		
OE.KEYS		X		X
OE.MINIMUM_PLATFORM	X			X

Table 1: Threats to security objectives

6.3.2 Security Objectives Sufficiency

6.3.2.1 Rationale for Threats

The following rationale provides justification that the security objectives are suitable to counter each individual threat and that each security objective tracing back to a threat actually contributes to the mitigation of that threat.

T.TSF_FAILURE

This threat is addressed by requiring the TOE to be used in specified platforms **(OE.MINIMUM_PLATFORM)** that provides necessary functionality to protect the data sent through the trusted channel in case the establishment of the vpn tunnel fails.

T.UNAUTHORIZED_ACCESS

This threat is addressed by requiring the TOE to use an encrypted & mutually authenticated VPN tunnel **(O.VPN_TUNNEL)** which enforces protection **(OE.NO_TOE_BYPASS)** to the communications of the TOE along with **(O.TOE_ADMINISTRATION)** and **(OE.TRUSTED_CONFIG)** which ensures that configurations after

initial bootstrap can only be taken into use by the authorized administration. **(OE.PHYSICAL), (OE.SINGLEUSER)** and **(OE.NOEVIL)** ensures that physical access to TOE is restricted to an authorized user. **(OE.MINIMUM_PLATFORM)** and **(OE.KEYS)** ensures that the access to the certificate and private key stored in the non-volatile memory is protected making them available only for the TOE while **(O.RESIDUAL_INFORMATION_CLEARING)** ensures that the negotiated session keys for the VPN are removed from the volatile memory after no longer required and certificate, private key and configurations stored on the non-volatile memory on the TOE can be made unusable by initiating a factory reset on the underlying TOE platform.

T.UNAUTHORIZED_UPDATE

This threat is addressed by requiring the TOE to prevent configuration by any other than authorized users **(O.TOE_ADMINISTRATION)** either remotely utilizing a trusted channel or locally. **(OE.TRUSTED_CONFIG)** contributes in mitigating the threat by cryptographic signature verification of configurations.

T.USER_DATA_REUSE

This threat is addressed by enforcing a mutually authenticated & encrypted VPN tunnel **(O.VPN_TUNNEL)** for connections from the TOE. **(O.RESIDUAL_INFORMATION_CLEARING)** and **(OE.KEYS)** contributes in mitigating the threat by enforcing that negotiated session keys are cleared from memory after no longer required rendering the session data from the connection inaccessible whereas **(OE.MINIMUM_PLATFORM)** ensures that the underlying device and operating system has support for cleaning the data from volatile memory and providing functionality for restoring the non-volatile memory used by the TOE to factory settings.

7 TOE FUNCTIONAL SECURITY

7.1 TOE Functional Security Specification

7.1.1 Fundamental Security Requirements (RFS) for VPN Customers

This section covers the programs (software) used as a VPN client in remote access connections, as well as those that are commonly used to connect mobile devices to the organization's network (for example remote workers).

This section should be used for devices applied in the following use case:

- Remote access VPN:
  - When a software program is used to connect to remote users (for example, employees working from home) through the internet with the organization's network.

Information regarding the requirements for VPN Server devices (also called VPN terminators or VPN Gateway) is not covered by this section.

Below are the requirements that the VPN client software must meet, both general due to common functionalities with other types of products, and specific for the family of products in which it is integrated.

7.1.1.1 Information Flow Control

REQ. 1

TOE will allow establishing validity periods and lifetimes for the IKEv2 and IPsec channels. If validity period expires, the communication channel is renegotiated.

REQ. 2

TOE shall use IPsec to provide a trusted communication channel between itself and a VPN Gateway that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of channel data modification.

REQ. 3

The TSF shall ensure that all IP traffic (other than IP traffic required to establish the VPN connection) flows through the IPsec VPN client.

7.1.1.2 Protection of Products and its Services

REQ. 4

TOE shall ensure that in case of failure of any component, security policies are not violated by allowing unauthorized information flows.

7.1.1.3 Cryptographic Requirements

REQ. 5

In case TOE provides a deterministic random bit generation (RBG) service, the TOE should:

- Utilize CTR_DRBG (AES)
- Use a seed of at least one entropy source that accumulates entropy from several sources or have a studied entropy source, with a minimum of entropy bits at least equal to the greater security strength of the keys and hashes that it will generate.

Application Note

TOE maintains an internal entropy pool that is augmented by collecting entropy from the underlying operating system. Internal entropy pool is used to generate the seed value for TOE.

REQ. 6

TOE shall reset all plaintext secret and private cryptographic keys and CSPs when no longer required.

Application Note

TOE resets all plaintext secrets and private cryptographic keys and CSPs after approximately 3 minutes of IPsec re-keying when connection reset is forced through the UI. Reset procedure may vary slightly depending on the target hardware and execution environment.

TOE resets all plaintext secrets and private cryptographic keys and CSPs after 2 re-keying rounds when SA has expired because of lifetime restrictions.

REQ. 7

Protection of the keys and the cipher material: The TOE should not store keys in non-volatile memory. It can only do so when it is digitally wrapped or encrypted, or when it meets any of the following criteria:

- The unencrypted key is not part of the key chain.
- The unencrypted key does not allow access to the encrypted data after initial use.
- The unencrypted key is written to an external storage device to be used as an authorization factor.

7.1.1.4 IKEv2 Requirements

REQ. 8

TOE shall perform [*encryption and decryption]* when utilizing IKEv2 in accordance with a specified cryptographic algorithm *AES operating* in CBC mode with cryptographic key sizes of 256-bits.

REQ. 9

TOE shall perform cryptographic hashing services in accordance with specified cryptographic algorithms SHA-256, SHA-384, SHA-512 and message digest sizes of 256, 384, 512 bits for IKEv2.

REQ. 10

TOE shall perform digital signature verification services during IKEv2 with one of the following algorithms:

- RSA with key lengths of 3072 or higher.
- Elliptic Curve Digital Signature Algorithm (ECDSA) with key lengths of 256 or higher.

REQ. 11

For IKEv2 message authentication services the TOE may use:

- HMAC-SHA-2 (AES-CBC)

REQ. 12

TOE shall implement IKEv2 protocol with NAT traversal options.

REQ. 13

TOE shall ensure that all IKEv2 protocols perform peer authentication using a RSA, ECDSA that uses X.509v3 certificates.

REQ. 14

TOE shall ensure the encrypted payload in the IKEv2 protocol uses the cryptographic algorithms AES-CBC-256.

REQ. 15

TOE shall ensure that IKEv2 Security Association (SA) lifetime can be configured by an administrator based on elapsed time in seconds.

REQ. 16

TOE shall ensure that all IKEv2 protocols implement at least one Diffie-Hellman group of the following:

- 3072-bit MODP GROUP dh-group 15;
- 4096-bit MODP GROUP dh-group 16;
- 256-bit random ECP GROUP dh-group 19, 384-bit random ECP GROUP dh-group 20 and 512-bit random ECP GROUP dh-group 21;
- Brainpool P256r1 dh-group 28, Brainpool P384r1 dh-group 29 and Brainpool P512r1 dh-group 30.

REQ. 17

TOE shall generate the secret value X used in the exchange of Diffie-Hellman keys ("x" in gx mod p) using the specified RBG and with a bit length of at least twice the security bits associated with the DH group negotiated.

REQ. 18

TOE generates nonces for the IKEv2. The probability of repeating a nonce during the lifetime of an established IPsec SA must be less than or equal to 1/(2128).

7.1.1.5 IPSec Requirements

REQ. 19

TOE shall perform [*encryption and decryption]* in accordance with a specified cryptographic algorithm *AES operating* in CBC or GCM mode with cryptographic key sizes of 256-bits.

REQ. 20

TOE shall perform cryptographic hashing services in accordance with specified cryptographic algorithms SHA-256, SHA-384, SHA-512 and message digest sizes of 256, 384, 512 bits for IPSec when utilizing AES-CBC and 16-octet Integrity Check Value when utilizing AES-GCM.

REQ. 21

For IPSec message authentication services the TOE may use:

- HMAC-SHA-2 (AES-CBC)
- 16-octect Integrity Check Value (AES-GCM)

REQ. 22

TOE shall ensure the encrypted payload in the IPSec protocol uses the cryptographic algorithms AES-CBC-256 and AES-GCM-256.

REQ. 23

TOE shall ensure that IPSec Security Association (SA) lifetime can be configured by an administrator based on elapsed time in seconds.

REQ. 24

TOE shall implement the IPsec architecture. TOE shall implement tunnel mode and/or transport mode.

Application Note

TOE supports only tunnel mode. Transport mode is not supported.

REQ. 25

TOE shall implement the IPsec protocol ESP using the cryptographic algorithms AES-GCM-256 and AES-CBC-256 together with a Secure Hash Algorithm (SHA)-based HMAC.

7.2 Cryptographic Mechanisms of TOE

ID	Cryptographic Mechanism	Comments
Cryptographic Requirements		
CRYPT.1	CTR_DRBG (AES)	Deterministic random bit generation
IKEv2		
CRYPT.2	AES-CBC-256	(key size 256 bits)
CRYPT.3	SHA-2 with message digest size 256-bits	
CRYPT.4	SHA-2 with message digest size 384-bits	
CRYPT.5	SHA-2 with message digest size 512-bits	
CRYPT.6	RSA with key length of 3072-bits or higher	
CRYPT.7	ECDSA with key length of 256-bits or higher	
CRYPT.8	HMAC-SHA-2 256-bits with truncated output of 128 bits	
CRYPT.9	HMAC-SHA-2 384-bits with truncated output of 192 bits	
CRYPT.10	HMAC-SHA-2 512-bits with truncated output of 256 bits	
CRYPT.11	3072-bit MODP GROUP dh-group 15	
CRYPT.12	4096-bit MODP GROUP dh-group 16	
CRYPT.13	256-bit random ECP GROUP dh-group 19	
CRYPT.14	384-bit random ECP GROUP dh-group 20	
CRYPT.15	512-bit random ECP GROUP dh-group 21	
CRYPT.16	Brainpool P256r1 dh-group 28	
CRYPT.17	Brainpool P384r1 dh-group 29	
CRYPT.18	Brainpool P512r1 dh-group 30	
CRYPT.19	ansi-x9.62 (nonce generation)	
CRYPT.20	nist-sp-800-90 (nonce generation)	
IPsec		
CRYPT.21	AES-GCM-256	
CRYPT.22	AES-CBC-256	
CRYPT.23	16-octet Integrity Check Value (ICV)	(in AES-GCM)
CRYPT.24	HMAC-SHA-2 256-bits with truncated output of 128 bits	(in AES-CBC)
CRYPT.25	HMAC-SHA-2 384-bits with truncated output of 192 bits	(in AES-CBC)
CRYPT.26	HMAC-SHA-2 512-bits with truncated output of 256 bits	(in AES-CBC)

7.3 Rationale for Security Functional Requirements

7.3.1 Coverage

The following table provides a mapping of SFRs to the security objectives of the TOE, showing that each security functional requirement addresses at least one security objective and that each security objectives of the TOE is covered, at least, by one SFR.

	O.VPN_TUNNEL	O.RESIDUAL_INFORMATION_CLEARING	O.TOE_ADMINISTRATION
REQ. 1	X		
REQ. 2	X		
REQ. 3	X		
REQ. 4	X		
REQ. 5	X		
REQ. 6	X	X	
REQ. 7	X	X	
REQ. 8	X		
REQ. 9	X		
REQ. 10	X		
REQ. 11	X		
REQ. 12	X		
REQ. 13	X		
REQ. 14	X		
REQ. 15			X
REQ. 16	X		
REQ. 17	X		
REQ. 18	X		
REQ. 19	X		
REQ. 20	X		
REQ. 21	X		
REQ. 22	X		
REQ. 23			X
REQ. 24	X		
REQ. 25	X		

7.3.2 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives.

O.VPN_TUNNEL

TOE implements the following mutually authenticated and encrypted trusted channel: VPN-tunnel for TOE communications and remote management.

The VPN tunnel supports enforcement of lifetimes for expiration for IKEv2 and IPSEC SAs (Req. 1), authenticated and encrypted IPSEC tunnel between the TOE and the VPN gateway (Req. 2), enforcement of traffic flows from TOE to the network are encapsulated inside the VPN tunnel (Req. 3) and that in case of failure of a component the established policy is not violated by allowing unauthorized traffic flows (Req. 4) and utilization of a Deterministic Random Bit Generation (Req. 5),

The VPN tunnel supports for IKEv2 encryption and decryption with AES-CBC with 256-bit key sizes (Req. 8), cryptographic hashing services with algorithms SHA-256, SHA-384 and SHA-512 with message digests 256, 384, 512 bits (Req. 9), digital signature verification with RSA key lengths 3072 or higher and ECDSA with key lengths 256 or higher (Req. 10), message authentication services HMAC-SHA-2 for AES-CBC (Req. 11), NAT traversal options (Req. 12), performing peer authentication with RSA and ECDSA x.509v3 certificates (Req. 13), usage of cryptographic algorithms AES-CBC-256 for encrypted payloads (Req. 14) and the Diffie-Hellman groups 3072-bit MODP GROUP dh-group 15, 4096-bit MODP GROUP dh-group 16, 256-bit random ECP GROUP dh-group 19, 384-bit random ECP GROUP dh-group 20, 512-bit random ECP GROUP dh-group 21, Brainpool P256r1 dh-group 28, Brainpool P384r1 dh-group 29, Brainpool P512r1 dh-group 30 (Req. 16), generation and size of secret value X used in Diffie-Hellman key exchange (Req. 17) and nonce generation probability during a SA lifetime (Req. 18).

The VPN tunnel supports for IPSEC encryption and decryption with AES operating in CBC- or GCM-mode with keysizes of 256-bits (Req. 19), cryptographic hashing services with algorithms SHA-256, SHA-384 and SHA-512 with message digests 256, 384, 512 bits when utilizing AES-CBC and 16-octect Integrity Check Value when utilizing AES-GCM (Req. 20), message authentication services HMAC-SHA-2 for AES-CBC and 16-octet Integrity Check Value for AES-GCM (Req. 21), usage of cryptographic algorithms AES-CBC-256 and AES-GCM-256 for encrypted payloads (Req. 22), implementing IPSEC architecture in tunnel mode (Req. 24) and IPSEC protocol ESP utilizing cryptographic algorithms AES-CBC-256 and AES-GCM-256 together with SHA-based HMAC (Req. 25).

O.RESIDUAL_INFORMATION_CLEARING

TOE ensures that the volatile residual information generated during VPN tunnel establishment, re-keying and teardown is cleared by the TOE after it's no longer required.

- Req. 6 ensures that TOE clears session keys from the volatile memory when no longer required
- Req. 7 ensures that TOE does not store keys to non-volatile memory with the exception of certificate and private key stored in the platform keystore (Android keystore) used to authenticate the TOE to the VPN gateway

O.TOE_ADMINISTRATION

TOE ensures that only the authorized administrator is able to modify the configuration of the TOE by ensuring that configurations imported by the TOE have a valid cryptographic signature.

- Req. 15 ensures that IKE SA lifetime can be configured by an administrator
- Req. 23 ensures that IPSEC SA lifetime can be configured by an administrator

8 TOE SUMMARY SPECIFICATION

8.1 Information Flow Control

Lifetimes of the VPN tunnel IKEv2 and IPSec SAs the TOE negotiates can be enforced by the TOE and/or the VPN Gateway simultaneously by defining validity periods in the client and/or the server configuration. Lifetime of the tunnel can be configured based on a time period, the amount of transferred bytes or the amount of transferred packets. When the lifetime of a VPN tunnel expires either on the TOE or on the VPN Gateway, the existing tunnel is closed preventing any data being sent through the expired tunnel and a new tunnel is negotiated and established between the TOE and the VPN Gateway.

TOE Security Functional Requirements addressed: REQ. 1

TOE can establish an IPsec VPN tunnel to an endpoint defined in the configuration policy. The endpoint authentication is done using X.509 certificates that are required to be transferred to the TOE through another method usually during the initial provisioning. Supported algorithms and modes include:

- Block ciphers: AES-CBC with key lengths up to 256 bits.
- Hash functions: SHA-2 with hash function lengths up to 512 bits.
- Message authentication: HMAC-SHA-256-128, HMAC-SHA-384-192, HMAC-SHA-512-256.
- Authenticated encryption mode of AES-GCM with 16-octet Integrity Check Value (ICV).
- Digital signature algorithms RSA and ECDSA.
- Key exchange algorithms using the DH groups 15, 16, elliptic curve groups 19, 20 and 21 (P-256, P-384 and P-521) and for IKEv2 brainpool elliptic curve groups 28-30 (256bit, 384bit, 512bit).

TOE Security Functional Requirements addressed: REQ. 2

TOE enforcement of the IP traffic depends on the underlying general purpose operating system and its capabilities and restrictions. On Android TOE utilizes Android VPN Framework provided by the platform.

On BTM-R OS TOE can enforce IP data traffic flows. When TOE is initializing and configuration is not yet loaded, TOE will drop all IP traffic until the initialization has finished and TOE has loaded the configuration policy. Once the VPN policy has been loaded TOE will enforce IP traffic based on the defined rules.

On generic Android device TOE can enforce IP data traffic flows only when the VPN tunnel has been successfully negotiated. Once the VPN tunnel has been established TOE will enforce IP traffic based on the defined rules.

TOE Security Functional Requirements addressed: REQ. 3

8.2 Protection of the Products and its Services

TOE enforcement of security policies depend on the underlying operating system and its capabilities and restrictions. On Android TOE utilizes Android VPN Framework provided by the platform.

On BTM-R Android TOE can enforce the IP traffic based on the configuration policy.

On generic Android TOE can enforce the IP traffic based on the configuration policy after the VPN tunnel has been successfully negotiated. Once the VPN tunnel has been negotiated, TOE will enforce the configuration policy for the IP traffic between the TOE platform and the network.

TOE Security Functional Requirements addressed: REQ. 4

8.3 Cryptographic Requirements

TOE performs all deterministic random bit generation services using CTR_DRBG (AES). This can be configured on the TOE or the VPN Gateway configuration policy.

TOE Security Functional Requirements addressed: REQ. 5

When existing VPN tunnel is re-keyed because of an expired lifetime, TOE will erase the cryptographic secrets related to that tunnel after 2 re-keying operations by overwriting them in volatile memory (RAM). Two re-keying operations are necessary to ensure that the established VPN connection does not break uncontrollably causing the established underlying connection to break but that the re-keying operation is handled in a controlled manner without interruptions.

When existing VPN tunnel is re-keyed because either TOE or VPN Gateway has received a delete payload from the other party, TOE will erase the cryptographic secrets related to that tunnel by overwriting them in volatile memory (RAM) after 3 minutes of deletion.

TOE Security Functional Requirements addressed: REQ. 6

TOE stores private keys to the keystore provided by the TOE platform (Android Keystore). When the VPN tunnel is established, the negotiated session keys are stored in the volatile memory and are cleared from the memory once the session is removed.

TOE Security Functional Requirements addressed: REQ. 7

8.4 IKEv2 Requirements

TOE performs encryption and decryption of IKEv2 in accordance with a specified cryptographic algorithm AES operating in CBC mode with cryptographic key sizes of 256-bits.

TOE Security Functional Requirements addressed: REQ. 8

TOE performs cryptographic hashing services for IKEv2 in accordance with the following cryptographic algorithms when utilizing AES-CBC:

- SHA-2 with message digest sizes 256-, 384- or 512-bits

These can be configured on the TOE or the VPN Gateway configuration policy for each VPN tunnel separately.

TOE Security Functional Requirements addressed: REQ. 9

TOE performs digital signature verification services during IKEv2 with the following algorithms:

- RSA with key length of 3072-bits or higher
- ECDSA with key length of 256-bits or higher

TOE Security Functional Requirements addressed: REQ. 10

For IKEv2 message authentication TOE supports HMAC-SHA-2 with truncated output sizes of 128, 192 and 256 bits with AES-CBC.

TOE Security Functional Requirements addressed: REQ. 11

TOE supports IKEv2 protocol with NAT traversal.

TOE Security Functional Requirements addressed: REQ. 12

TOE supports peer authentication between the TOE and the VPN Gateway with RSA and ECDSA X.509v3 certificates for all IKE protocols supported. When TOE attempts to negotiate a VPN tunnel it sends its public certificate to the VPN Gateway which will verify its validity. If the certificate is deemed invalid, the negotia-

tion will fail with an error. If the certificate is valid the authentication succeeds and the negotiation can continue.

TOE Security Functional Requirements addressed: REQ. 13

TOE supports encrypting payloads in IKEv2 protocol with the following cryptographic algorithms:

- AES-CBC-256

The algorithm to be used for a VPN tunnel can be configured in the TOE or in the VPN Gateway configuration policy.

TOE Security Functional Requirements addressed: REQ. 14

On IKEv2 TOE supports lifetime restrictions for established security association (SA) based on elapsed time in seconds. These settings are defined in the configuration policy of the TOE. After lifetime counter expires, existing SA is deleted and a new one is negotiated. When negotiation succeeds TOE uses the new SA. Lifetimes can be configured separately for each VPN tunnel.

TOE Security Functional Requirements addressed: REQ. 15

TOE supports the following Diffie-Hellman groups for IKEv2 protocol:

- 3072-bit MODP GROUP dh-group 15
- 4096-bit MODP GROUP dh-group 16
- 256-bit random ECP GROUP dh-group 19
- 384-bit random ECP GROUP dh-group 20
- 512-bit random ECP GROUP dh-group 21
- Brainpool P256r1 dh-group 28
- Brainpool P384r1 dh-group 29
- Brainpool P512r1 dh-group 30

The Diffie-Hellman groups supported for a VPN tunnel can be configured on the TOE or on the VPN Gateway configuration policy for each VPN tunnel separately.

TOE Security Functional Requirements addressed: REQ. 16

TOE generates secret value used in the exchange of Diffie-Hellman keys (“x” in gx mod p) with a bit length of twice the security bits associated with the DH group used for negotiation.

TOE Security Functional Requirements addressed: REQ. 17

TOE generates nonces for IKE from the random generator defined in the configuration policy supporting the following generators:

- ansi-x9.62
- nist-sp-800-90

TOE Security Functional Requirements addressed: REQ. 18

8.5 IPsec Requirements

TOE performs encryption and decryption of IPSec traffic flowing through the VPN tunnel in accordance with a specified cryptographic algorithm AES operating in GCM or CBC mode with cryptographic key sizes of 256-bits.

TOE Security Functional Requirements addressed: REQ. 19

TOE performs cryptographic hashing services for IPSec in accordance with the following cryptographic algorithms:

- AES-CBC:
  - SHA-2 with message digest sizes 256-, 384- or 512-bits
- AES-GCM:
  - 16-octet Integrity Check Value

These can be configured on the TOE or the VPN Gateway configuration policy for each VPN tunnel separately.

TOE Security Functional Requirements addressed: REQ. 20

For IPsec message authentication the TOE supports HMAC-SHA-2 with truncated output sizes 128, 192 and 256 bits with AES-CBC, and 16-octect Integrity Check Value (ICV) with AES-GCM.

TOE Security Functional Requirements addressed: REQ. 21

TOE supports encrypting payloads in IPSec protocol with the following cryptographic algorithms:

- AES-CBC-256
- AES-GCM-256

The algorithm to be used for a VPN tunnel can be configured in the TOE or in the VPN Gateway configuration policy.

TOE Security Functional Requirements addressed: REQ. 22

On IPSec TOE supports lifetime restrictions for established security association (SA) based on elapsed time in seconds. These settings are defined in the configuration policy of the TOE. After lifetime counter expires, existing SA is deleted and a new one is negotiated. When negotiation succeeds TOE uses the new SA. Life-times can be configured separately for each VPN tunnel.

TOE Security Functional Requirements addressed: REQ. 23

TOE implements IPsec architecture, supporting only tunnel mode. The supported mode can be configured in the TOE configuration policy and on the VPN Gateway configuration policy.

TOE Security Functional Requirements addressed: REQ. 24

TOE implements the IPsec protocol ESP using the cryptographic algorithms AES-GCM-256 and AES-CBC-256 together with a Secure Hash Algorithm SHA-2 HMAC. The cryptographic algorithms along with the secure hash algorithm can be configured on the TOE or on the VPN Gateway configuration policy for each VPN tunnel separately.

TOE Security Functional Requirements addressed: REQ. 25

9 REFERENCES

[CC31p2]	Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components Version 3.1, Review 5
[CEM31]	Common Criteria for Information Technology Security Evaluation. Evaluation Methodology. Version 3.1 Review 5
[CCN-LINCE-001]	Definición de la Certificación Nacional Esencial de Seguridad (LINCE), Versión 0.1
[CCN-LINCE-002]	Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad (LINCE), Versión 0.1
[CCN-LINCE-003]	Plantilla para la Declaración de Seguridad de la Certificación Nacional Esencial de Seguridad (LINCE), Versión 0.1
[CCN-LINCE-004]	Plantilla del Informe Técnico de Evaluación de la Certificación Nacional Esencial de Seguridad (LINCE), Versión 0.1
[CCN-STIC-140]	Taxonomía de referencia para productos de Seguridad TIC
[CCN-STIC-141]	Taxonomía de referencia para productos de Seguridad TIC para ENS Medio y Bajo