Direction centrale de la sécurité des systèmes d'information

Client VPN Application Protection Profile

Creation date	:	June 2008
Reference	:	PP-VPNC-CCv3.1
Version	:	1.3

Courtesy Translation

Courtesy translation of the protection profile registered and certified by the French Certification Body under the reference DCSSI-PP-2008/03.

Table of contents

1 INTRODUCTION 7

1.1 PROTECTION PROFILE IDENTIFICATION 7
1.2 CONTEXT 7
1.3 TARGET OF EVALUATION OVERVIEW 7
1.3.1 TOE type 7
1.3.2 TOE usage 8
1.3.3 TOE logical boundaries 8
1.3.4 Integration of the TOE in its environment 9
1.3.5 Protection Profile use 10

2 CONFORMANCE CLAIMS 11

2.1 CC CONFORMANCE CLAIM 11
2.2 PACKAGE CONFORMANCE CLAIM 11
2.3 PP CONFORMANCE CLAIM 11
2.4 CONFORMANCE CLAIM TO THE PP 11

3 SECURITY PROBLEM DEFINITION 12

3.1 ASSETS 12
3.1.1 Assets protected by the TOE (user data) 12
3.1.2 TOE sensitive assets (TSF data) 12
3.2 ROLES 13
3.3 THREATS 14
3.3.1 Threats concerning the communications 14
3.3.2 Threats concerning the cryptographic keys management 14
3.3.3 Threats concerning VPN security policies and their context 15
3.4 ORGANISATIONAL SECURITY POLICIES (OSP) 15
3.4.1 Provided services 15
3.4.2 Other services 15
3.5 ASSUMPTIONS 16
3.5.1 Interactions with the TOE 16
3.5.2 Host machine 16
3.5.3 Reset 17
3.5.4 Cryptography 18

4 SECURITY OBJECTIVES 19

4.1 SECURITY OBJECTIVES FOR THE TOE 19
4.1.1 Security objectives for services provided by the TOE 19
4.1.2 Security objectives to protect TOE sensitive assets 19
4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT 21
4.2.1 Interactions with the TOE 21
4.2.2 Host machine 22
4.2.3 Reset 22
4.2.4 Cryptography 23

5 SECURITY REQUIREMENTS 24

5.1 SECURITY FUNCTIONAL REQUIREMENTS 24
5.1.1 Definition of underlying security model elements 24
5.1.2 Provided services 27
5.1.3 Authentication 30
5.1.4 Security attributes management 33
5.1.5 Cryptographic key management 33
5.1.6 VPN security policies management 36
5.1.7 Cryptography 38
5.2 SECURITY ASSURANCE REQUIREMENTS 38

6 RATIONALES 39
6.1 SECURITY OBJECTIVES / SECURITY PROBLEM 39
6.1.1 Threats 39
6.1.2 Organisational security policies (OSP) 42
6.1.3 Assumptions 42
6.1.4 Coverage between problem definition and security objectives 45
6.2 SECURITY REQUIREMENTS / SECURITY OBJECTIVES 50
6.2.1 Objectives 50
6.2.2 Coverage between objectives and security requirements 55
6.3 DEPENDENCIES 59
6.3.1 Security functional requirements dependencies 59
6.3.2 Security assurance requirements dependencies 62
6.4 RATIONALE FOR THE EAL 63
6.5 RATIONALE FOR THE EAL AUGMENTATIONS 63
6.5.1 AVA_VAN.3 Focused vulnerability analysis 63
6.5.2 ALC_FLR.3 Systematic flaw remediation 63
ANNEX A ADDITIONAL DESCRIPTION OF THE TOE AND ITS ENVIRONMENT 64
A.1 INTRODUCTION TO VPN TECHNOLOGIES 64
A.2 PHYSICAL LOCATION OF THE TOE WITHIN ITS ENVIRONMENT 64
A.3 TOE FEATURES 68
A.4 POSSIBLE ADDITIONAL FUNCTIONALITIES FOR THE CLIENT VPN APPLICATION 72
ANNEX B DEFINITIONS AND ACRONYMS 73
B.1 DEFINITIONS 73
B.2 ACRONYMS 74
ANNEX C REFERENCES 75

List of figures

Figure 1. Operation without centralized remote administration equipment 65
Figure 2. Operation with specific centralized remote administration equipment 66
Figure 3. Operation with centralized remote administration equipment on an IP encryptor 67
Figure 4. Operation with shared host machine 68

List of tables

Table 1 Mapping threats to security objectives 45
Table 2 Mapping security objectives to threats 47
Table 3 Mapping organisational security policies to security objectives 47
Table 4 Mapping security objectives to organisational security policies 48
Table 5 Mapping assumptions to security objectives for the operational environment 49
Table 6 Mapping security objectives for the operational environment to assumptions 49
Table 7 Mapping security objectives for the TOE to functional requirements 56
Table 8 Mapping functional requirements to security objectives for the TOE 58
Table 9 Functional requirements dependencies 60
Table 10 Assurance requirements dependencies 63

1 Introduction

1.1 Protection Profile identification

Title:	Protection Profile, Client VPN application
Authors:	Trusted Labs S.A.S.
Version:	1.3, June 2008
Sponsor:	DCSSI
CC version:	3.1 revision 2

Remark:

The evaluation assurance level of this protection profile is EAL3 augmented by ALC_FLR.3 and AVA_VAN.3 in accordance with the standard level qualification process defined in [QUA-STD].

1.2 Context

This document is realized on behalf of the French governmental information security authority (Direction Centrale de la Sécurité des Systèmes d'Information, DCSSI). The objective is to supply an administrative scope to the certification of client VPN applications for public and private sectors for their qualification.

1.3 Target of evaluation overview

1.3.1 TOE type

The objective of this protection profile is to define security requirements associated to a VPN application hosted on a client workstation. It so completes the profile « IP encryptor »[1] ([PPnc0502]) which specifies security requirements of a VPN gateway.

« VPN » technologies (Virtual Private Networks) provide the capability to protect dataflows exchanged between two networks equipments interconnected through the use of a non secure public network (as Internet), or provide the capability to protect flows exchanged between a mobile terminal equipment and a remote network equipment through the use of a non secure network (as in nomad VPN case). They offer a security level for network exchanges equivalent to a point-to-point linking, physically and logically dedicated.

The considered TOE type is a client such as IPsec, but products developers implementing an SSL VPN client are allowed to draw one's inspiration from the current PP for the security target writing of their product.

[1] This PP is available in CC3.1 revision 2 under the reference PP-CIP-CCv3.1

1.3.2 TOE usage

The client VPN application provides the capability to establish a communication link between a mobile equipment item not necessarily linked to a predictible address (such as a laptop connected via an access provider or via a companies network) and a VPN gateway located at the edge of a corporate private network. This communication link can potentially use a non secure public network, such as the Internet, and extremely various means of access (such as Wi-Fi), exposing so the communication link to many threats which impose its securisation.

In addition, the TOE can be used in two ways. A user can either interact directly with the client VPN application to establish a VPN link, or interact via an application which is an intermediary between the user and the TOE (in particular it is then the intermediate application which activates the TOE). In this latter case, no distinction will be made between the user and the intermediate application which acts his behalf.

1.3.3 TOE logical boundaries

The main function of the client VPN application is to ensure security of data flowing between mobile equipment and private network gateway (also indicated under the term of IP encryptor) by establishing VPN links. For that purpose, VPN security policies are defined. They include all parameters for a secure connection (encryption and authentication algorithms, keys sizes...)[2], as well as security services which can be enforced (confidentiality and/or authenticity).

Different cryptographic keys are required for security services enforcement ensuring the confidentiality and the authenticity of transmitted applicative data. Moreover, keys are also requiered to ensure the confidentiality and/or the authenticity of remote administration flows. Two approaches can be followed for the management of these keys by the TOE:

- Import of cryptographic keys generated from outside of the TOE,
- Generation of cryptographic keys within the TOE.

In this profile, cryptographic keys are generated from outside of the TOE and imported into the TOE, the security target author can add the keys generation in the TOE, while staying in conformance with this profile.

The user or administrator authentication is performed by a component belonging to the same encryption system as the TOE (as specified in the paragraph 1.3.4.2). This one can be of the following types:

- a module of the client VPN application (included within the security target scope of the TOE in conformance with this PP),
- the remote IP encryptor which will establish a VPN tunnel with the machine hosting the TOE,
- a centralized remote administration equipment,
- the user cryptographic module (USB key or smart card).

The TOE does not manage audit events on the host machine because:

- of the difficulty of exploitation of audit within the mobile machines management, and
- of the TOE administration considered as mainly performed by means of a centralized remote administration equipment.

[2] Keys themselves are managed independently from security policies.

1.3.4 Integration of the TOE in its environment

The TOE is operated within the framework of an encryption system composed of host machine hosting the client VPN application, IP encryptors and administration equipments (or remote processing) being able to host update services of VPN security policies.

In order to integrate itself and communicate with different entities of the system, the TOE shall have VPN security policies and different cryptographic keys types, in particular:

- those allowing secure communication with an IP encryptor (keys used by security services and session keys),
- those allowing remote secure communication with an administrator (this role can be played by a centralized remote administration equipment), in order to renew VPN security policies and import new keys.

Two phases can be distinguished for the integration of the TOE in its environment. On one hand an initialization phase which consists in injecting required information for its correct operation and on the other hand an operational phase where the TOE is really used.

1.3.4.1 Initialization phase

When VPN security policies definition is realized in centralized way on a remote administration equipment so as to be able to distribute automatically these policies in all machines hosting the client VPN application, the VPN application installation shall contain a pre-configuration phase. This phase, performed by an administrator, is required for the policies later load through the use of a secure administration channel.

Nevertheless, the definition (*i.e.* the load) of VPN security policies enabling the client VPN application to be operational can also be performed:

- within the client VPN application during its installation (for example, thanks to the use of a « master »),
- manually by the administrator once the application is installed.

1.3.4.2 Operational phase

During operational phase, the TOE permits an authenticated administrator to locally or remotely import, via a remote processing equipment, new VPN policies and cryptographic keys, used by security services and used for VPN security policies enforcement.

The use of the client VPN application shall be controlled in order to avoid any illicit connection. To this purpose, an authentication shall be ensured by a trusted third party, forming a part of the encryption system[3], and verified by the TOE. It will permit a user to establish a VPN link by enforcing the security policy bound to this user. For an administrator, it will permit to perform administration operations on the TOE.

The administration of client VPN application during operational phase can, in addition, be remotly performed on a centralized[4] (via a server which includes VPN policies) and automatic way, in order to be able to update machines workset in a flexible and fast way without having to upload all of them towards a security administrator. However, in this case, keys providing the capability to protect security administration flows during updates shall be injected during the initialization phase or distributed on an organizational way; these updates concern first of all VPN security policies to be applied to every communication link (policies associated to user, machine and VPN link) and their security context.

[3] The TOE forming a part of the encryption system, the author of a ST which is in conformance with this profile is allowed to make no distinction between the TOE and this trusted third party.
[4] The centralized remote administration equipment plays then the administrator role.

1.3.5 Protection Profile use

Within the scope of this PP, data sent and received via a VPN communication link are supposed to be sensitive information but not to be defence-classified information within the context of French laws and regulations (for example, covering “diffusion restreinte” needs).

Some security properties about assets are qualified as « optional » in the current protection profile. This mention indicates that mechanisms ensuring these properties shall be implemented in the TOE but their application or their use shall not be considered as systematics.

Requirements introduced in this protection profile define minimal rules to which a security target for a client VPN application shall conform; they are not restrictive at all. So, it is possible to add other functionalities (such as, for example, some formulated as assumptions in the current PP) or to also refer to another protection profile. However, any modification of the profile is restricted by the rules associated to the compliance specified under paragraph 2.4. This latter stipulates in particular that for a target which is in conformance with this PP, technical objectives on operational environment can be transferred as objectives on the TOE (and, in the same way, assumptions transferred as threats or organisational security policies). Such a method aims to decrease security dependency of the TOE to its environment. In this context, indications are provided in this PP in the form of application notes to indicate to the security targets writer the objectives on the operational environment which could be transferred as objectives on the TOE.

Functional requirements ensuring objectives related to import and export of sensitive assets within and outside of the TOE, not distinguish between local administration and remote administration; since security requirements are identical. However, the author of a security target which is in conformance with this profile can plan to distinguish between the two cases to increase security requirements of one of the two administration modes.

In particular, within the scope of a remote administration, the security target shall show that the TOE shall provide the capability to authenticate the remote machine from which the administrator runs its administration operations, and to ensure a secure channel, in integrity and confidentiality, with this machine. Related mechanisms will be included within the TOE.

Application note:

Merging of local and remote administration modes, does not impose a unique mechanism for their implementation within the product.

2 Conformance claims

This chapter contains the following sections:

CC conformance claim (2.1)

Package conformance claim (2.2)

PP conformance claim (2.3)

Conformance claim to the PP (2.4)

2.1 CC conformance claim

This protection profile is conformant with Common Criteria version 3.1.

This PP was written according to CC version 3.1:

- CC Part 1 [CC1]
- CC Part 2 [CC2]
- CC Part 3 [CC3]
- CC evaluation methodology [CEM]

2.2 Package conformance claim

This PP is conformant with the assurance requirements package for the standard level qualification defined in [QUA-STD].

2.3 PP conformance claim

This PP declares no conformance with other PP.

2.4 Conformance claim to the PP

The compliance retained in this PP for Security Targets and Protection Profiles which claim conformance to it is the **demonstrable** compliance according to the definition of CC Part 1 [CC1].

3 Security problem definition

3.1 Assets

The description of every asset provides protection types required for each of them (part *Protection*).

The mention "(opt.)" for "optional", stipulates that the product will have to support mechanisms enabling to ensure this protection, but its application must not be considered as systematics.

3.1.1 Assets protected by the TOE (user data)

D.APPLICATIVE_DATA

Applicative data are data provided from and towards information system applications of mobile equipment and which are transported by the network. They flow between equipment which hosts the TOE and IP encryptor. These data are contained in the payload of the IP packets exchanged between the TOE and the IP encryptor and these data can be temporarily stored within the TOE to be able to process them (*i.e.* enforce security services) before sending them upon untrusted network.

Protection: confidentiality (opt.) and authenticity (opt.).

D.TOPOLOGIC_DATA

Private network topology information (source and destination IP adresses) is contained in IP packets headers.

Protection: confidentiality (opt.) and authenticity (opt.).

3.1.2 TOE sensitive assets (TSF data)

D.VPN_POLICIES

VPN security policies define processings (implicit filtering and security services) to perform on data exchanged between the TOE and an IP encryptor.

This asset also contains security contexts which are linked with security policies. Every security context contains all security parameters required for the application of its associated VPN security policy.

Protection: authenticity and confidentiality.

D.CRYPTO_KEYS

This asset corresponds to all cryptographic keys (symmetric or asymmetric) required for TOE operation such as:

- session keys,
- keys used by security services enforced by VPN security policies,
- keys to protect VPN security policies during their storage,
- keys to protect import of cryptographic keys and VPN security policies within the TOE,
- keys to protect export of VPN security policies outside of the TOE.

Protection: confidentiality (for secret and private keys) and authenticity (for all keys).

D.SOFTWARE

TOE software which permits enforcement of all TOE services.

Protection: integrity.

3.2 Roles

The operation of the TOE in its operational environment handles directly or indirectly the roles described below:

User

User of the machine accessing to coorporate private network through the use of an IP encryptor. This user can send/receive information towards/from this private network through the use of a VPN link established between the client VPN application and the IP encryptor.

Application note

The user can eventualy be an application or a process runned on the host machine in question.

System and network administrator

Administrator who is responsible for the machine. He configures machine parameters (user accounts for example), but does not define VPN security policies.

He configures network parameters of client VPN application, and system parameters which are bound to operational network contexts.

Security administrator

He generates and distributes keys in client VPN application, and he imports VPN security policies and their security contexts that are going to enforce the client VPN application.

He can define and update VPN security policies at the level of a centralized remote administration equipment existing on the coorporate private network so that these policies can be « remote distributed » by every machine hosting the client VPN application during operational phase.

Furthermore, he manages (generation, distribution…) keys and authentication means to access client VPN application.

Hereafter in the document, the administrator role includes the following roles: security administrator and system and network administrator.

3.3 Threats

Standard level qualification policy, within the context of French IT security regulations ("*politique de qualification au niveau standard*"), applies to consumer market products ensuring the protection of sensitive not defence-classified information.

Threatening agents are:

external attackers: any person which plans to connect to a private network and perform operations for which he is not authorized, or any person trying to retrieve information which are not for him.

Administrators (assumption A.ADMIN) and users (assumption A.USER) of the TOE are not viewed as attackers.

3.3.1 Threats concerning the communications

T.REPLAY

An attacker captures a packet sequence flowing through remote flows, corresponding to a complete sequence to perform an administration operation, and replays it in order to gain some benefit.

Threatened assets: D.VPN_POLICIES, D.CRYPTO_KEYS

Application note

An attack path corresponding to this threat could be:

An administrator imports within the TOE, via an administration command « C », a security policy allowing applicative data communication in plain text (no confidentiality) towards the machine « M ». An attacker captures « C ». Shortly after, the machine « M » has to receive confidential data. Thus, the administrator replaces the security policy so as to ensure confidentiality of applicative data. The attacker replays the command « C ». The communication towards the machine « M » will thus be made in plain format but the attacker is alone to know it. The user sends his confidential data in plain text on the VPN link. The attacker intercepts them.

T.ADMIN_USURPATION

An attacker usurps administrator identity and uses it to perform administration operations on client VPN application.

Threatened assets: D.VPN_POLICIES, D.CRYPTO_KEYS

T.USER_USURPATION

An attacker usurps user identity and uses it to access illicitly services provided by VPN client, or to perform operations on the TOE for which the user is allowed.

Threatened assets: D.TOPOLOGIC_DATA, D.APPLICATIVE_DATA, D.CRYPTO_KEYS

3.3.2 Threats concerning the cryptographic keys management

T.KEYS_MODIFICATION

An attacker illicitly modifies cryptographic keys, for example by using the keys import service.

Threatened assets: D.CRYPTO_KEYS

T.KEYS_DISCLOSURE

An attacker illicitly retrieves cryptographic keys.

Threatened assets: D.CRYPTO_KEYS

3.3.3 Threats concerning VPN security policies and their context

T.POL_MODIFICATION

An attacker illicitly modifies VPN security policies and their security contexts. This modification can result for example from modification of import commands sent by the administrator.

Threatened assets: D.VPN_POLICIES

T.POL_DISCLOSURE

An attacker illicitly retrieves VPN security policies and their security contexts.

Threatened assets: D.VPN_POLICIES

3.4 Organisational security policies (OSP)

3.4.1 Provided services

OSP.PROVIDED_SERVICES

The TOE shall enforce VPN security policies defined for users and logical VPN links (established physically between the TOE and an IP encryptor), on data flowing through these links.

It shall also provide all required security services to apply protections specified in these policies:

- confidentiality protection of applicative data,
- authenticity protection of applicative data,
- confidentiality protection of topologic data,
- authenticity protection of topologic data.

Protected assets: D.APPLICATIVE_DATA, D.TOPOLOGIC_DATA

3.4.2 Other services

OSP.CRYPTO

DCSSI cryptographic referentials ([CRYPTO] and [CRYPTO_GESTION]) defined for standard resistance level shall be followed-up for keys management (renewal) and cryptographic functions used within the TOE.

Protected assets: any sensitive asset using cryptography for its protection

Application note

The author of a ST which claim conformance with this PP can consider the addition of the cryptographic keys generation in the TOE.

OSP.POL_EXPORT

The TOE shall provide the capability to export VPN security policies and their security context, stored in the TOE, towards an administrator for reviewing.

Protected assets: D.VPN_POLICIES

3.5 Assumptions

3.5.1 Interactions with the TOE

A.ADMIN

Administrators are not hostile and competent persons with necessary resources for the implementation of their tasks. They are trained to perform the operations for which they are responsible and they follow manuals and administration procedures.

A.USER

The client VPN application user is non hostile person and he is trained to the TOE usage. In particular, he does not have to reveal data allowing him to authenticate himself with the encryption system.

A.REMOTE_ADMIN_EQUIPMENT

It is assumed that the centralized remote administration equipment allowing distributing VPN security policies is hosted on a secure machine which shall be placed in secure premises where access is restricted only to administrators. Its availability is ensured in addition and its correct operation is regularly controlled.

A.IP_ENCRYPTOR

The IP encryptor with which the client VPN application communicates is assumed to record activities which took place on VPN link. Besides, it is meant to activate security alarms allowing to forwards to security administrator any VPN security policies violation on the link in question.

A.AUTHENTICATING_COMPONENT

It is assumed that the encryption system component performing user and administrator authentication is evaluated according to the standard level qualification process defined by the DCSSI in [QUA-STD].

Application note

This component can eventually be integrated on the scope of the TOE during the writing of a security target in conformance with this PP. In this case, the evaluation according to the standard level qualification process will be required.

3.5.2 Host machine

A.MACHINE

It is assumed that the machine on which is installed and run the client VPN application is safely and correctly administered. In particular, it has an antivirus which database is regularly updated and it is protected by a firewall.

In addition, it is assumed that the host machine hosting the client VPN application continues to ensure protection of data retrieved through VPN links.

Finally, it is assumed that the host machine ensures integrity of software allowing enforcement of all TOE services.

A.USER_RIGHTS

It is assumed that the user of the machine hosting the client VPN application does not possess rights for installation, configuration, updating and uninstallation of the client VPN application.

A.CONFIGURATION

It is assumed that the configuration of the machine hosting the client VPN application ensures the protection against impacts of cleartext communications of the machine via different physical or logical interfaces (browsing of Internet sites for example) on communications on VPN links.

Application note

Physical and logical interfaces mentioned in this assumption are those of the machine.

A.COMM

It is assumed that the TOE environment provides the capability to control communications towards and from outside of the machine which does not flow through the TOE.

A.KEYS_EXPORT

It is assumed that the export, by the user, of secret or private cryptographic keys imported or generated within the TOE outside of the machine on which the TOE is installed, is made impossible thanks to the machine configuration.

A.MULTI-USERS

It is assumed that identifications/authentications management of different users from multi-users machine is taken into account by the TOE environment.

3.5.3 Reset

A.RESET

It is assumed that the environment provides the capability to reset the TOE in a secure state.

Application note

This reset in a secure state can be made by organizational or technical ways. For example, it can include the import of reference security policies within the TOE, when these are compromised or supposed compromised, and the integrity check of TOE sensitive assets.

3.5.4 Cryptography

A.ACCESS

It is assumed that the access to different components of the encryption system is restricted thanks to a cryptographic keys management (shared secret, public key infrastructure...) associated to a VPN security policy.

Application note

So an assumption is that secret or private keys, we would like to integrate into the encryption system, shall be distributed and imported within the TOE. These keys shall then be able to be used to prove the TOE membership to the encryption system.

4 Security objectives

4.1 Security objectives for the TOE

4.1.1 Security objectives for services provided by the TOE

O.POL_ENFORCEMENT

The TOE shall enforce VPN security policies included in client VPN application and associated to the authenticated user, to data flowing through VPN links.

Application note

These security policies can include, in particular, confidentiality and authenticity of exchanged data.

O.APPLI_CONFIDENTIALITY

The TOE shall provide mechanisms to protect confidentiality of applicative data which flow between the equipment hosting the client VPN application and an IP encryptor.

O.APPLI_AUTHENTICITY

The TOE shall provide mechanisms to protect authenticity of applicative data which flow between the equipment hosting the client VPN application and an IP encryptor.

O.TOPO_CONFIDENTIALITY

The TOE shall provide mechanisms to protect confidentiality of topologic data which flow between the equipment hosting the client VPN application and an IP encryptor.

O.TOPO_AUTHENTICITY

The TOE shall provide mechanisms to protect authenticity of topologic data which flow between the equipment hosting the client VPN application and an IP encryptor.

4.1.2 Security objectives to protect TOE sensitive assets

4.1.2.1 Authentication

O.ADMIN_AUTHENTICATION

The TOE shall check that the administrator was authenticated by an encryption system component before being able to perform administration operations on the TOE. The authentication mechanism used shall be conformant with recommendations of the DCSSI referential [AUTH] for the standard robustness level.

O.USER_AUTHENTICATION

The TOE shall check that the user was authenticated by an encryption system component before being able to access services provided by the TOE and operations allowed to the users. The authentication mechanism used shall be conformant with recommendations of the DCSSI referential [AUTH] for the standard robustness level.

Application note:

The user or administrator authentication can be checked in practice by one of the following encryption system components:

- the client VPN application itself,
- the remote IP encryptor which will establish a VPN link with the machine hosting the TOE,
- the centralized remote administration equipment,
- the user cryptographic module (USB key or smart card).

4.1.2.2 Cryptographic keys management

O.KEYS_IMPORT

The TOE shall provide the capability only to the user and the administrator to import cryptographic keys within the TOE.

O.KEYS_PROTECTION

The TOE shall protect confidentiality of secret and private keys and the integrity of all keys during their import within client VPN application. The integrity protection will have to consist of integrity loss detection and import operation cancellation.

The keys integrity shall be also ensured during their storage; in case of integrity loss detection of the key, the TOE shall cancel the establishment of any VPN link.

Application note

This objective is not relative to remote administration (c.f. O.ADMIN_FLOWS_PROTECTION).

In addition, this objective is completed by O.KEYS_IMPORT which restricts the possibility of cryptographic keys import within the TOE to user and administrator.

4.1.2.3 VPN security policies management

O.POL_IMPORT

The TOE shall provide only to administrators the capability to import VPN security policies and their security contexts.

O.POL_PROTECTION

The TOE shall provide mechanisms to protect integrity and confidentiality of VPN security policies during their import and during their export. During the import, the integrity protection shall consist of integrity loss detection and operation cancellation. During the export, it shall consist in enabling the detection of any integrity loss.

The VPN security policies integrity shall also be ensured during their storage; in case of integrity loss detection of VPN security policy, the TOE shall cancel the establishment of any VPN link.

In addition, the TOE shall provide the capability to export VPN security policies towards an administrator.

Application note

This objective does not concern the remote administration (c.f. O.ADMIN_FLOWS_PROTECTION).

4.1.2.4 Remote administration

O.REPLAY_PROTECTION

The TOE shall detect the replay of sending sequences of the remote administration data. If the attack is detected, the TOE shall answer by cancelling the operation.

O.ADMIN_FLOWS_PROTECTION

The TOE shall ensure integrity and confidentiality of administration flows. Confidentiality protection is not systematically enforced if data flowing through the flow are not confidential. For an incoming flow, integrity protection shall consist of integrity loss detection and operation cancellation. For an outgoing flow, it shall consist in enabling the detection of any integrity loss.

4.1.2.5 Cryptography management

O.CRYPTO

The TOE shall implement cryptographic functions and manage (renew) cryptographic keys in accordance with cryptographic referentials defined by the DCSSI ([CRYPTO] and [CRYPTO_GESTION]) for the standard resistance level.

Application note

The author of a security target which claim conformance with this PP can consider the addition of the cryptographic keys generation in the TOE.

4.2 Security objectives for the operational environment

4.2.1 Interactions with the TOE

OE.ADMIN

Administrators shall be reliable and trained to the tasks which they have to perform on the TOE.

OE.USER

User is trained to the TOE usage and he is made aware of security, in particular with the risks bound to the disclosure of information which he holds and which allow him to authenticate himself to the encryption system.

OE.REMOTE_ADMIN_EQUIPMENT

The centralized remote administration equipment shall be placed in secure premises where access is controlled and restricted to administrators. In addition, its availability shall be ensured and its correct operation regularly controlled.

OE.IP_ENCRYPTOR

The IP encryptor with which client VPN application communicates shall provide the capability to log activities which took place on VPN link. In addition, it shall activate security alarms providing the capability to forward any violation of the VPN security policies on the considered link to a security administrator.

OE.AUTHENTICATING_COMPONENT

The encryption system component performing user and security administrator authentication shall be qualified (at least) to the standard level such as defined by the DCSSI in [QUA-STD].

Application note

This objective on operational environment can be turned into TOE objective in a security target, so that the TOE alone ensures authentication functions; in this case, the authenticating component will be included within the scope of the TOE.

4.2.2 Host machine

OE.MACHINE

The host machine on which client VPN application runs shall be safely, protected and configured so as to ensure its security and security of data that it hosts. In particular, it ensures the integrity of client VPN application which it hosts.

OE.USER_RIGHTS

Only administrators can perform administration tasks relative to client VPN application (installation, configuration, updating and uninstallation).

OE.CONFIGURATION

The configuration of the machine hosting client VPN application shall protect the communications on VPN links against impacts of plaintext communications from the machine via different physical or logical channels.

OE.COMM

The TOE environment shall provide the capability to control communications, towards and from outside of the host machine, which does not flow through the TOE.

OE.KEYS_EXPORT

The configuration of the host machine hosting the client VPN application shall prevent any export outside of the machine by the person who use secret or private cryptographic keys imported or generated within the TOE.

OE.MULTI-USERS

The identifications/authentications management of different users from multi-users machine shall be taken into account by the TOE environment.

4.2.3 Reset

OE.RESET

The environment shall provide the capability to reset the TOE in a secure state.

4.2.4 Cryptography

OE.CRYPTO

Cryptographic keys, generated outside of the TOE, which are injected within the TOE shall be generated in accordance with the recommendations specified in DCSSI cryptographic referentials [CRYPTO] and [CRYPTO_GESTION] for the standard resistance level.

OE.ACCESS

The access to different components of the encryption system shall be restricted thanks to a cryptographic keys management (shared secret, public key infrastructure…) associated to a VPN security policy.

5 Security requirements

5.1 Security functional requirements

5.1.1 Definition of underlying security model elements

The instantiation of security functional requirements is based on subjects, objects, operations, attributes and users defined below.

5.1.1.1 Subjects

S.user_manager

This subject is responsible for the communication with TOE users (U.user) and administrators (U.administrator). It manages, in particular, authentication as well as import and export of TOE sensitive assets.

S.communication_manager

This subject is responsible for the communication with the IP encryptor (U.IP_encryptor), so it enforces VPN security policy associated to a given logical VPN link.

5.1.1.2 Objects

Remark: objects are stored within the TOE in order to be processed or to participate to its operation. They are encapsulated in informations during their communication with the outside of the TOE.

OB.keys

This object corresponds to the sensitive asset D.CRYPTO_KEYS, it is cryptographic keys generated outside of the TOE and used by the TOE.

Application note:

The author of a ST which is in conformance with this profile can introduce cryptographic keys generation into the TOE.

OB.vpn_policies

This object corresponds to the sensitive asset D.VPN_POLICIES, it is VPN security policies and their security contexts used by the TOE.

OB.data

This object corresponds to sensitive assets D.APPLICATIVE_DATA and D.TOPOLOGIC_DATA, it is applicative and topologic informations contained in IP packets exchanged between the TOE and the IP encryptor, via the VPN channel.

5.1.1.3 Operations

import

This operation provides the capability to import a data within the TOE. It is used in the PP for cryptographic keys import and VPN security policies stored within the TOE as well as import of applicative and topologic data.

export

This operation provides the capability to export a data outside of the TOE. It is enforced in the PP to the VPN security policies stored in the TOE as well as to the export of applicative and topologic data.

use

This operation provides the capability to use a data by another operation. It is applied to cryptographic keys to perform cryptographic operations required.

application

This operation provides the capability to enforce a data protection. It is applied to data (applicative and topologic), in order to apply them confidentiality and/or authenticity protections (i.e., the associated security policy), for the transfer towards the IP encryptor, via the VPN channel.

5.1.1.4 Attributes

AT.user_type

This attribute specifies the type of user bound to the subject S.user_manager; this type must be chosen across *"null"*, *"user"*, *"administrator"*. It is an attribute of the subject S.user_manager.

AT.user_id

This attribute is associated to the subject S.user_manager and provides an identifier of the user bound to the subject S.user_manager. It can be chosen as *"null"* (to clarify that no user is authenticated) or *"user identifier"* (any other different value as *"null"* associated to the authenticated user; the values set is not thus finite). It is an attribute of the subject S.user_manager.

AT.user_name

This attribute is associated to the object OB.vpn_policies and specifies to which user this object (therefore this VPN security policy) is associated. The value of this attribute is the user identifier (c.f. description of the attribute AT.user_id). It is an attribute of the object OB.vpn_policies.

AT.VPN_link_id

This attribute corresponds to the identifier of a logical VPN link established between the TOE and a subnetwork of a private network, via an IP encryptor. The value of this attribute is the logical link identifier (thus, the values'set is not finite). It is an attribute of the subject OB.vpn_policies.

AT.data_confidentiality

This attribute is associated to an object OB.vpn_policies and specifies if this object (therefore this VPN security policy) imposes the confidentiality property enforcement on data transmitted to the IP encryptor. This attribute can be chosen across *"true"* or *"false"*. It is an attribute of the object OB.vpn_policies.

AT.data_authenticity

This attribute is associated to an object OB.vpn_policies and specifies if this object (therefore this VPN security policy) imposes the authenticity property enforcement (integrity and authentication of origin) on the data transmitted to the IP encryptor. This attribute can be chosen across *"true"* or *"false"*. It is an attribute of the object OB.vpn_policies.

5.1.1.5 Users

U.administrator

This user is the administrator of the client VPN application such as specified in the paragraph 3.2. It shall be bound to the subject S.user_manager.

U.user

This user is the client VPN application user such as specified in the paragraph 3.2. It shall be bound to the subject S.user_manager.

U.IP_encryptor

This user is the IP encryptor with which the client VPN application communicates via a VPN link. It shall be bound to the subject S.communication_manager.

U.encryptor_system_component

This user is an encryption system component into which fits the client VPN application. It is in charge of the authentication of users and administrators communicating with the TOE.

Application note: this component can be for example:

- the client VPN application itself,
- the remote IP encryptor which will establish a VPN tunnel with the machine hosting the TOE,
- the centralized remote administration equipment,
- the user cryptographic module (USB key or smart card).

General application note to this paragraph:

Applications which send and receive the data OB.data (to which are applied VPN policies) are not considered as "users" in conformance with Common Criteria terminology. Indeed, import and export of informations towards these applications do not require, in this PP, particular protections, thus the processing of these functions is not in the security scope.

However, the writer of a target which is in conformance with this PP can insert this user into the requirements if particular threats are taken into account during information exchange between the TOE and applications.

5.1.2 Provided services

5.1.2.1 VPN communication link management

FDP_ETC.1/EXPORT Export of user data without security attributes

FDP_ETC.1.1/EXPORT The TSF shall enforce the **data access policy** when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2/EXPORT The TSF shall export the user data without the user data's associated security attributes

Non-editorial refinement:

User data are applicative and topologic data contained in IP packets and exchanged between the TOE and an IP encryptor.

FDP_ITC.1/IMPORT Import of user data without security attributes

FDP_ITC.1.1/IMPORT The TSF shall enforce the **data access policy** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/IMPORT The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3/IMPORT The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **[assignment: additional importation control rules]**.

Non-editorial refinement:

User data are applicative and topologic data contained in IP packets and exchanged between the TOE and an IP encryptor.

5.1.2.2 Data access protection

FDP_IFC.1/DATA Subset information flow control

FDP_IFC.1.1/DATA The TSF shall enforce the **data access policy** on **subjects, objects and operations identified by this table:**

Subjects	S.user_manager, S.communication_manager
Objects	OB.data, OB.vpn_policies
Operations	application, import, export

FDP_IFF.1/DATA Simple security attributes

FDP_IFF.1.1/DATA The TSF shall enforce the **data access policy** based on the following types of subject and information security attributes:

Type	element	relevant security attributes(s)
Subjects	S.user_manager, S.communication_manager	AT.user_type, AT.VPN_link_id
Objects	OB.data, OB.vpn_policies	AT.data_authenticity, AT.data_confidentiality

FDP_IFF.1.2/DATA The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

Rule 1: the subject S.communication_manager is allowed to perform application of OB.vpn_policies on OB.data

Rule 2: the subject S.communication_manager is allowed to import OB.data provided the S.user_manager is a "user" (i.e. the value of the attribute S.user_manager.user_type is equal to "user")

Rule 3: the subject S.communication_manager is allowed to export OB.data provided the S.user_manager is a "user" (i.e. the value of the attribute S.user_manager.user_type is equal to "user") and the keys and the VPN security policy are integer.

FDP_IFF.1.3/DATA The TSF shall enforce the **VPN security policy of the VPN link on the applicative and topologic data (OB.data) contained in IP packets before exporting/importing the IP packets to/from the user:**

Rule 4: the authenticity security protection (i.e. integrity and authentication of origin) must be applied to OB.data if the following conditions hold:

OB.vpn_policies requires authenticity (i.e. OB.vpn_policies.data_authenticity is equal to "True"),

the user linked to S.user_manager is allowed to use the OB.vpn_policies (ie. OB.vpn_policies.user_name is equal to S.user_manager.user_id) and

OB.vpn_policies is associated to the VPN link established with U.IP_encryptor (i.e. OB.vpn_policies.VPN_link_id corresponds to the identifier of the VPN link established with U.IP_encryptor).

Rule 5: the confidentiality security protection must be applied to OB.data if the following conditions hold:

OB.vpn_policies requires confidentiality (i.e. OB.vpn_policies.data_confidentiality is equal to "True"),

the user linked to S.user_manager is allowed to use the OB.vpn_policies (ie. OB.vpn_policies.user_name is equal to S.user_manager.user_id) and

OB.vpn_policies is associated to the VPN link established with U.IP_encryptor (i.e. OB.vpn_policies.VPN_link_id corresponds to the identifier of the VPN link established with U.IP_encryptor).

FDP_IFF.1.4/DATA The TSF shall explicitly authorise an information flow based on the following rules: **[assignment: rules, based on security attributes, that explicitly authorise information flows]**.

FDP_IFF.1.5/DATA The TSF shall explicitly deny an information flow based on the following rules: **[assignment: rules, based on security attributes, that explicitly deny information flows]**.

5.1.2.3 Data authenticity

FDP_UIT.1/DATA Data exchange integrity

FDP_UIT.1.1/DATA The TSF shall enforce the **data access policy** to be able to **transmit and receive** user data in a manner protected from **replay, deletion and modification** errors.

FDP_UIT.1.2/DATA The TSF shall be able to determine on receipt of user data, whether **deletion, modification and replay** has occurred.

Non-editorial refinement:

User data are applicative data and topologic data (OB.data) contained in IP packets provided to the subject that manages VPN communications (S.communication_manager).

In this requirement the TSF communicates with the user U.IP_encryptor.

Application note

The effective or not enforcement of this property is specified in the functional requirement FDP_IFF.1/DATA.

FCO_NRO.1/DATA Selective proof of origin

FCO_NRO.1.1/DATA The TSF shall be able to generate evidence of origin for transmitted **applicative and topologic data (OB.data)** at the request of the **[assignment: list of third parties]**.

FCO_NRO.1.2/DATA The TSF shall be able to relate the **[assignment: list of attributes]** of the originator of the information, and the **[assignment: list of information fields]** of the information to which the evidence applies.

FCO_NRO.1.3/DATA The TSF shall provide a capability to verify the evidence of origin of information to **[assignment: list of third parties]** given **[assignment: limitations on the evidence of origin]**.

Application note

The effective or not enforcement of this property is specified in the functional requirement FDP_IFF.1/DATA.

Applicative and topologic data mentioned in the requirement flow between the TOE and an IP encryptor.

5.1.2.4 Data confidentiality

FDP_UCT.1/DATA Basic data exchange confidentiality

FDP_UCT.1.1/DATA The TSF shall enforce the **data access policy** to be able to **transmit and receive** user data in a manner protected from unauthorised disclosure.

Non-editorial refinement:

User data are applicative data and topologic data (OB.data) contained in IP packets provided by the subject that manages VPN communications (S.communication_manager).

In this requirement the TSF communicates with the user U.IP_encryptor.

Application note

The effective or not enforcement of this property is specified in the functional requirement FDP_IFF.1/DATA.

5.1.3 Authentication

The authentication, performed by a third party, can be checked by one of components of the following system:

- the client VPN application itself,
- the remote IP encryptor which will establish a VPN tunnel with the machine hosting the TOE,
- the centralized remote administration equipment,
- the user cryptographic module (USB key or smart card).

5.1.3.1 User authentication

FIA_UID.2/USER User identification before any action

FIA_UID.2.1/USER The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Non-editorial refinement:

The user considered in this requirement is U.user.

The identification must be performed by a component of the encryption system (U.encryptor_system_component).

FIA_UAU.2/USER User authentication before any action

FIA_UAU.2.1/USER The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Non-editorial refinement:

The user considered in this requirement is U.user.

The authentication must be performed by a component of the encryption system (U.encryptor_system_component).

The authentication mechanism must meet [AUTH] requirements.

FIA_USB.1/USER User-subject binding

FIA_USB.1.1/USER The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:

AT.user_id,

AT.user_type.

FIA_USB.1.2/USER The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:

the security attribute AT.user_id corresponding to the identifier of the user shall be set to the user identifier,

the security attribute AT.user_type shall be set to " user ".

FIA_USB.1.3/USER The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **[assignment: rules for the changing of attributes]**.

Non-editorial refinement:

The user considered in this requirement is U.user.

The subject considered in this requirement is S.user_manager.

5.1.3.2 Administrator authentication

FIA_UID.2/ADMIN User identification before any action

FIA_UID.2.1/ADMIN The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Non-editorial refinement:

The user considered in this requirement is U.administrator.

FIA_UAU.2/ADMIN User authentication before any action

FIA_UAU.2.1/ADMIN The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Non-editorial refinement:

The user considered in this requirement is U.administrator.

The authentication must be performed by a component of the encryption system (U.encryptor_system_component).

The authentication mechanism must meet [AUTH] requirements.

FIA_USB.1/ADMIN User-subject binding

FIA_USB.1.1/ADMIN The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:

AT.user_type.

FIA_USB.1.2/ADMIN The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:

the security attribute AT.user_type shall be set to " administrator ".

FIA_USB.1.3/ADMIN The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **[assignment: rules for the changing of attributes]**.

Non-editorial refinement:

The user considered in this requirement is U.administator.

The subject considered in this requirement is S.user_manager.

5.1.4 Security attributes management

FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the **data access policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 [Editorial refined] The TSF shall allow **nobody** to specify alternative initial values to override the default values when an object or information is created.

Non-editorial refinement:

The TSF shall assign the value "null" to the security attributes AT.user_type and AT.user_id whenever a subject S.user_manager is created.

FMT_MSA.1/MODIFY Management of security attributes

FMT_MSA.1.1/MODIFY The TSF shall enforce the **data access policy** to restrict the ability to **modify** the security attributes **AT.user_type and AT.user_id values** to **the user bound to S.user_manager**.

FMT_MSA.1/QUERY Management of security attributes

FMT_MSA.1.1/QUERY The TSF shall enforce the **data access policy** to restrict the ability to **query** the security attributes **AT.user_type and AT.user_id of S.user_manager, and AT.user_name and AT.vpn_link_id of OB.vpn_policies,** to **S.communication_manager, which is bound to the IP encryptor and manages transmission**.

5.1.5 Cryptographic key management

5.1.5.1 Key policy

FDP_IFC.1/KEY_IMPORT Subset information flow control

FDP_IFC.1.1/KEY_IMPORT The TSF shall enforce the **key management policy** on **subjects, objects and operations identified by this table:**

Subjects	S.user_manager, S.communication_manager
Objects	OB.keys
Operations	import, use

FDP_IFF.1/KEY_IMPORT Simple security attributes

FDP_IFF.1.1/KEY_IMPORT The TSF shall enforce the **key management policy** based on the following types of subject and information security attributes:

Type	element	relevant security attributes(s)
Subjects	S.user_manager, S.communication_manager	AT.user_type
Objects	OB.keys	

FDP_IFF.1.2/KEY_IMPORT The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

Rule 1: the subject S.user_manager is allowed to import keys in OB.keys provided it has been authenticated either as "user" or as "administrator" (i.e. S.user_manager.user_type is equal to "user " or to "administrator ").

Rule 2: the subject S.communication_manager is allowed to use OB.keys.

FDP_IFF.1.3/KEY_IMPORT The TSF shall enforce the **[assignment: additional information flow control SFP rules]**.

FDP_IFF.1.4/KEY_IMPORT The TSF shall explicitly authorise an information flow based on the following rules: **[assignment: rules, based on security attributes, that explicitly authorise information flows]**.

FDP_IFF.1.5/KEY_IMPORT The TSF shall explicitly deny an information flow based on the following rules: **[assignment: rules, based on security attributes, that explicitly deny information flows]**.

Application note

Users U.user and U.adminstrator have to be authenticated with the TOE.

5.1.5.2 Cryptographic key import

FDP_ITC.1/KEY_IMPORT Import of user data without security attributes

FDP_ITC.1.1/KEY_IMPORT The TSF shall enforce the **key management policy** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/KEY_IMPORT The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3/KEY_IMPORT The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

On detection of an anomaly, in particular an integrity problem, the TSF shall discard the data and/or security attributes.

FDP_UCT.1/KEY_IMPORT Basic data exchange confidentiality

FDP_UCT.1.1/KEY_IMPORT The TSF shall enforce the **key management policy** to be able to **receive** user data in a manner protected from unauthorised disclosure.

Non-editorial refinement:

User data are the values of secret and private cryptographic keys provided to the subject that manages the communication with the users (S.user_manager).

FDP_UIT.1/KEY_IMPORT Data exchange integrity

FDP_UIT.1.1/KEY_IMPORT The TSF shall enforce the **key management policy** to be able to **receive** user data in a manner protected from **replay, deletion and modification** errors.

FDP_UIT.1.2/KEY_IMPORT The TSF shall be able to determine on receipt of user data, whether **replay, deletion and modification** has occurred.

Non-editorial refinement:

User data are the values of secret and private cryptographic keys provided to the subject that manages the communication with the users (S.user_manager).

5.1.6 VPN security policies management

5.1.6.1 VPN security policies import/export

FDP_ETC.1/VPN_POL Export of user data without security attributes

FDP_ETC.1.1/VPN_POL The TSF shall enforce the **VPN protection policy** when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2/VPN_POL The TSF shall export the user data without the user data's associated security attributes

FDP_ITC.2/VPN_POL Import of user data with security attributes

FDP_ITC.2.1/VPN_POL The TSF shall enforce the **VPN protection policy** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2/VPN_POL The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3/VPN_POL The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4/VPN_POL The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5/VPN_POL The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

The data shall be imported with the security attribute AT.user_name which corresponds to the identifier of the user who will use this VPN security policy and AT.VPN_link_id which corresponds to the identifier of a link,

On detection of an anomaly, in particular an integrity problem, the TSF shall discard the data and/or security attributes.

5.1.6.2 VPN security policies properties

FDP_UCT.1/VPN_POL Basic data exchange confidentiality

FDP_UCT.1.1/VPN_POL The TSF shall enforce the **VPN protection policy** to be able to **transmit and receive** user data in a manner protected from unauthorised disclosure.

FDP_UIT.1/VPN_POL Data exchange integrity

FDP_UIT.1.1/VPN_POL The TSF shall enforce the **VPN protection policy** to be able to **receive and transmit** user data in a manner protected from **replay, modification and deletion** errors.

FDP_UIT.1.2/VPN_POL The TSF shall be able to determine on receipt of user data, whether **[selection: modification, deletion, insertion, replay]** has occurred.

5.1.6.3 Miscellaneous

FDP_IFC.1/VPN_POL Subset information flow control

FDP_IFC.1.1/VPN_POL The TSF shall enforce the **VPN protection policy** on **subjects, objects and operations identified by this table:**

Subjects	S.user_manager, S.communication_manager
Objects	OB.vpn_policies
Operations	application, import, export

FDP_IFF.1/VPN_POL Simple security attributes

FDP_IFF.1.1/VPN_POL The TSF shall enforce the **VPN protection policy** based on the following types of subject and information security attributes:

Type	element	relevant security attributes(s)
Subjects	S.user_manager, S.communication_manager	AT.user_type, AT.VPN_link_id
Objects	OB.vpn_policies	

FDP_IFF.1.2/VPN_POL The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

Rule 1: the subject S.user_manager is allowed to import a VPN security policy in OB.vpn_policies provided it has been authenticated as an administrator (i.e. S.user_manager.user_type is equal to "administrator")

Rule 2: the subject S.user_manager is allowed to export a VPN security policy from OB.vpn_policies provided it has been authenticated as an administrator (i.e. S.user_manager.user_type is equal to "administrator")

Rule 3: the subject S.communication_manager is allowed to perform application of OB.vpn_policies.

FDP_IFF.1.3/VPN_POL The TSF shall enforce the

any user can trigger the export of a VPN security policy,

[assignment: additional information flow control SFP rules].

FDP_IFF.1.4/VPN_POL The TSF shall explicitly authorise an information flow based on the following rules: **[assignment: rules, based on security attributes, that explicitly authorise information flows]**.

FDP_IFF.1.5/VPN_POL The TSF shall explicitly deny an information flow based on the following rules: **[assignment: rules, based on security attributes, that explicitly deny information flows]**.

5.1.7 Cryptography

Cryptographic keys generation is not a part of security problem definition of this PP but can be considered in a ST which claim conformance to this one. The target writer can use the requirement FCS_CKM.1 with [CRYPTO] as cryptographic standard and introduce functional requirements required to cover FCS_CKM.1 dependencies, namely: (FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4).

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform **[assignment: list of cryptographic operations]** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **DCSSI cryptographic referentials ([CRYPTO] and [CRYPTO_GESTION])**.

FCS_CKM.3 Cryptographic key access

FCS_CKM.3.1 The TSF shall perform **[assignment: type of cryptographic key access]** in accordance with a specified cryptographic key access method **[assignment: cryptographic key access method]** that meets the following: **[assignment: list of standards]**.

Non-editorial refinement:

When the lifetime of a key is over, another key must be used for communication on VPN links. The list of standards shall meet [CRYPTO] and [CRYPTO_GESTION] requirements.

5.2 Security assurance requirements

The evaluation assurance level of this protection profile is EAL3 augmented by ALC_FLR.3 and AVA_VAN.3 in conformance with the standard level qualification process defined in [QUA-STD].

6 Rationales

6.1 Security objectives / security problem

6.1.1 Threats

6.1.1.1 Threats concerning the communications

T.REPLAY

To prevent the threat:

no action.

To detect the occurence of the threat, the TOE shall:

detect administration operations replay (O.REPLAY_PROTECTION).

To react to the threat, the TOE shall:

cancel the administration operation which is victim of replay attack (O.REPLAY_PROTECTION).

T.ADMIN_USURPATION

To prevent the threat:

the TOE shall enforce administrator authentication to the encryption system and check this authentication, before performing any administration operation (O.ADMIN_AUTHENTICATION),

the access to different components of the encryption system shall be restricted thanks to a cryptographic keys management associated to a VPN security policy (OE.ACCESS),

the authenticating component shall be certified to the standard level (OE.AUTHENTICATING_COMPONENT).

To detect the occurence of the threat, the TOE shall:

no action.

To react to the threat, the TOE shall:

no action.

T.USER_USURPATION

To prevent the threat:

the TOE shall enforce user authentication to the encryption system and check this authentication before accessing services provided by the TOE or performing any administration operation authorized to the users (O.USER_AUTHENTICATION),

the access to different components of the encryption system shall be restricted thanks to a cryptographic keys management associated to a VPN security policy (OE.ACCESS),

the authenticating component shall be certified to the standard level (OE.AUTHENTICATING_COMPONENT).

To detect the occurence of the threat, the TOE shall:

no action.

To react to the threat, the TOE shall:

no action.

6.1.1.2 Threats concerning the cryptographic keys management

T.KEYS_MODIFICATION

To prevent the threat:

- the TOE shall ensure integrity protection of cryptographic keys during their storage (O.KEYS_PROTECTION),
- the TOE shall authenticate users and administrators, in order to be able to determine their access rights (O.USER_AUTHENTICATION and O.ADMIN_AUTHENTICATION).
- the TOE authorizes only authenticated users and administrators to import cryptographic keys within the TOE (O.KEYS_IMPORT),
- the authenticating component shall be certifed to the standard level (OE.AUTHENTICATING_COMPONENT),

To detect the occurence of the threat, the TOE shall:

- detect the integrity loss of cryptographic keys during their local import (O.KEYS_PROTECTION),
- detect the integrity loss of cryptographic keys during their remote import (O.ADMIN_FLOWS_PROTECTION),

To react to the threat, the TOE shall:

- cancel any local import operation of cryptographic keys where integrity loss would be detected (O.KEYS_PROTECTION),
- cancel any remote import operation of cryptographic keys where integrity loss would be detected (O.ADMIN_FLOWS_PROTECTION).

T.KEYS_DISCLOSURE

To prevent the threat:

- the TOE shall ensure confidentiality protection of keys during their local import (O.KEYS_PROTECTION),
- the TOE shall ensure confidentiality protection of keys during their remote import (O.ADMIN_FLOWS_PROTECTION),
- the TOE shall authenticate users and administrators, in order to be able to determine their access rights (O.USER_AUTHENTICATION and O.ADMIN_AUTHENTICATION).
- the TOE shall only authorize authenticated users and administrators to import cryptographic keys within the TOE (O.KEYS_IMPORT),
- the authenticating component shall be certified to the standard level (OE.AUTHENTICATING_COMPONENT),
- the TOE shall protect itself against keys export outside of the TOE (OE.KEYS_EXPORT),
- the TOE shall provide the capability to regularly renew cryptographic keys in order to increase the difficulty of the reuse of the revealed keys (O.CRYPTO).

To detect the occurence of the threat, the TOE shall:

no action

To react to the threat, the TOE shall:

allow resetting in a secure state (OE.RESET).

6.1.1.3 Threats concerning VPN security policies and their context

T.POL_MODIFICATION

To prevent the threat:

- the TOE shall ensure integrity protection of VPN policies during their storage (O.POL_PROTECTION),
- the TOE shall authenticate administrators, in order to be able to determine their access rights (O.ADMIN_AUTHENTICATION).
- the TOE shall only authorize authenticated administrators to import security policies within the TOE (O.POL_IMPORT),
- the authenticating component shall be certified to the standard level (OE.AUTHENTICATING_COMPONENT).

To detect the occurence of the threat, the TOE shall:

- detect the integrity loss of VPN policies during their local import (O.POL_PROTECTION),
- allow detection of any integrity loss of VPN policies during their local export (O.POL_PROTECTION),
- detect the integrity loss of VPN policies during their remote import (O.ADMIN_FLOWS_PROTECTION),
- allow detection of any integrity loss of VPN policies during their remote export (O.ADMIN_FLOWS_PROTECTION).

To react to the threat, the TOE shall:

- cancel any local import operation of VPN policies where integrity loss would be detected (O.POL_PROTECTION),
- cancel any remote import operation of VPN policies where integrity loss would be detected (O.ADMIN_FLOWS_PROTECTION),
- allow resetting in a secure state (OE.RESET).

T.POL_DISCLOSURE

To prevent the threat:

- the TOE shall ensure confidentiality protection of VPN policies during their local import and local export (O.POL_PROTECTION),
- the TOE shall ensure confidentiality protection of VPN policies during their remote import and remote export (O.ADMIN_FLOWS_PROTECTION),
- the TOE shall authenticate administrators, in order to be able to determine their access rights (O.ADMIN_AUTHENTICATION).
- the TOE shall only authorize authenticated administrators to import security policies within the TOE (O.POL_IMPORT),
- the authenticating component shall be certified to the standard level (OE.AUTHENTICATING_COMPONENT).

To detect the occurence of the threat, the TOE shall:

- no action

To react to the threat, the TOE shall:

- no action

6.1.2 Organisational security policies (OSP)

6.1.2.1 Provided services

OSP.PROVIDED_SERVICES

This OSP is enforced by O.APPLI_CONFIDENTIALITY, O.APPLI_AUTHENTICITY, O.TOPO_CONFIDENTIALITY and O.TOPO_AUTHENTICITY which impose that the TOE provides corresponding security services. It is also covered by O.POL_ENFORCEMENT which imposes that these security services are enforced on data flowing through VPN links.

Furthermore, OE.ACCESS ensures that cryptographic keys were distributed (thanks to a keys management) to perform the origin authentication, required if the security policy stipulates the authenticity protection of data transmitted on the VPN link.

In addition, O.USER_AUTHENTICATION ensures that a policy associated to the user (that we shall therefore have authenticated) will be used on the established VPN link. The knowledge of the logical VPN link identifier is ensured by the machine configuration which can be accessed and modified only by an administrator (OE.USER_RIGHTS).

Finally, OE.IP_ENCRYPTOR takes part in this OSP, because it ensures that operations relative to the VPN link are logged and that security alarms are generated to indicate operational failures. It so provides the capability to detect and process errors or attacks after an analysis of audit events and security alarms.

6.1.2.2 Other services

OSP.CRYPTO

This OSP is enforced by the objectives O.CRYPTO (for cryptography used by the TOE) and OE.CRYPTO (for cryptography used by TOE environment).

OSP.POL_EXPORT

This OSP is enforced by O.POL_PROTECTION which ensures that VPN security policies can be exported towards an administrator.

6.1.3 Assumptions

6.1.3.1 Interactions with the TOE

A.ADMIN

This assumption is upheld by OE.ADMIN which imposes the training of administrators to the tasks they will have to perform.

A.USER

This assumption is upheld by OE.USER which imposes the training to the TOE usage and the awareness of users to security problems bound to the use of a VPN.

A.REMOTE_ADMIN_EQUIPMENT

This assumption is completely upheld by OE.REMOTE_ADMIN_EQUIPMENT which ensures the availability of the centralized remote administration equipment as well as the restricted and secured access to this one.

A.IP_ENCRYPTOR

This assumption is completely upheld by OE.IP_ENCRYPTOR which imposes that the IP encryptor traces the activity of VPN links on which it communicates and forward all violations of VPN security policies to a security administrator so that this one can analyze and process errors or attacks if necessary.

A.AUTHENTICATING_COMPONENT

This assumption is completely upheld by OE.AUTHENTICATING_COMPONENT which ensures the qualification of the encryption system equipment permitting the authentication to the standard level defined by the DCSSI in [QUA-STD].

6.1.3.2 Host machine

A.MACHINE

This assumption is completely upheld by OE.MACHINE which ensures that the host machine is safely, protected and configured so as to ensure its own security and the security for data that it hosts.

Moreover this objective on the environment ensures the software integrity.

A.USER_RIGHTS

This assumption is completely upheld by OE.USER_RIGHTS which ensures that only administrators can perform system administration tasks.

A.CONFIGURATION

This assumption is upheld by OE.CONFIGURATION which protects from impacts of communication channel not managed by the TOE on VPN links communications and this assumption is also upheld by OE.COMM which ensures that the environment can control communications, towards and from the host machine, which not flow through the TOE.

A.COMM

This assumption is upheld by OE.COMM which ensures that any communication not flowing through the TOE can be controlled by TOE environment.

A.KEYS_EXPORT

This assumption is upheld by OE.KEYS_EXPORT which ensures that the user cannot export cryptographic keys (secret and private) which are imported or generated within the TOE.

A.MULTI-USERS

This assumption is completely upheld by the objective OE.MULTI-USERS which ensures that the identifications/authentications management of different users from multi-users machine is taken into account by TOE environment.

6.1.3.3 Reset

A.RESET

This assumption is completely upheld by OE.RESET which ensures that the TOE can be reset in a secure state.

6.1.3.4 Cryptography

A.ACCESS

This assumption is completely upheld by OE.ACCESS which restricts access to different components of the encryption system thanks to a cryptographic keys management associated to a VPN security policy.

6.1.4 Coverage between problem definition and security objectives

Threats	Security objectives	Rationale
T.REPLAY	O.REPLAY_PROTECTION	Section 6.1.1
T.ADMIN_USURPATION	O.ADMIN_AUTHENTICATION, OE.AUTHENTICATING_COMPONENT, OE.ACCESS	Section 6.1.1
T.USER_USURPATION	O.USER_AUTHENTICATION, OE.AUTHENTICATING_COMPONENT, OE.ACCESS	Section 6.1.1
T.KEYS_MODIFICATION	O.KEYS_PROTECTION, O.USER_AUTHENTICATION, OE.AUTHENTICATING_COMPONENT, O.ADMIN_AUTHENTICATION, O.KEYS_IMPORT, O.ADMIN_FLOWS_PROTECTION	Section 6.1.1
T.KEYS_DISCLOSURE	O.KEYS_PROTECTION, OE.AUTHENTICATING_COMPONENT, O.USER_AUTHENTICATION, O.ADMIN_AUTHENTICATION, O.ADMIN_FLOWS_PROTECTION, O.CRYPTO, O.KEYS_IMPORT, OE.KEYS_EXPORT, OE.RESET	Section 6.1.1
T.POL_MODIFICATION	O.POL_IMPORT, OE.AUTHENTICATING_COMPONENT, O.POL_PROTECTION, O.ADMIN_AUTHENTICATION, O.ADMIN_FLOWS_PROTECTION, OE.RESET	Section 6.1.1
T.POL_DISCLOSURE	OE.AUTHENTICATING_COMPONENT, O.POL_PROTECTION, O.ADMIN_AUTHENTICATION, O.ADMIN_FLOWS_PROTECTION, O.POL_IMPORT	Section 6.1.1

Table 1 Mapping threats to security objectives

Security objectives	Threats
O.POL_ENFORCEMENT	
O.APPLI_CONFIDENTIALITY	
O.APPLI_AUTHENTICITY	
O.TOPO_CONFIDENTIALITY	
O.TOPO_AUTHENTICITY	
O.ADMIN_AUTHENTICATION	T.ADMIN_USURPATION, T.KEYS_MODIFICATION, T.KEYS_DISCLOSURE, T.POL_MODIFICATION, T.POL_DISCLOSURE
O.USER_AUTHENTICATION	T.USER_USURPATION, T.KEYS_MODIFICATION, T.KEYS_DISCLOSURE
O.KEYS_IMPORT	T.KEYS_MODIFICATION, T.KEYS_DISCLOSURE
O.KEYS_PROTECTION	T.KEYS_MODIFICATION, T.KEYS_DISCLOSURE
O.POL_IMPORT	T.POL_MODIFICATION, T.POL_DISCLOSURE
O.POL_PROTECTION	T.POL_MODIFICATION, T.POL_DISCLOSURE
O.REPLAY_PROTECTION	T.REPLAY
O.ADMIN_FLOWS_PROTECTION	T.KEYS_MODIFICATION, T.KEYS_DISCLOSURE, T.POL_MODIFICATION, T.POL_DISCLOSURE
O.CRYPTO	T.KEYS_DISCLOSURE
OE.ADMIN	
OE.USER	
OE.REMOTE_ADMIN_EQUIPMENT	
OE.IP_ENCRYPTOR	
OE.AUTHENTICATING_COMPONENT	T.ADMIN_USURPATION, T.USER_USURPATION, T.KEYS_MODIFICATION, T.KEYS_DISCLOSURE, T.POL_MODIFICATION, T.POL_DISCLOSURE
OE.MACHINE	
OE.USER_RIGHTS	
OE.CONFIGURATION	

Security objectives	Threats
OE.COMM	
OE.KEYS_EXPORT	T.KEYS_DISCLOSURE
OE.MULTI-USERS	
OE.RESET	T.KEYS_DISCLOSURE, T.POL_MODIFICATION
OE.CRYPTO	
OE.ACCESS	T.ADMIN_USURPATION, T.USER_USURPATION

Table 2 Mapping security objectives to threats

Organisational security policies (OSP)	Security objectives	Rationale
OSP.PROVIDED_SERVICES	O.APPLI_AUTHENTICITY, O.TOPO_CONFIDENTIALITY, O.TOPO_AUTHENTICITY, OE.IP_ENCRYPTOR, O.APPLI_CONFIDENTIALITY, O.POL_ENFORCEMENT, O.USER_AUTHENTICATION, OE.USER_RIGHTS, OE.ACCESS	Section 6.1.2
OSP.CRYPTO	O.CRYPTO, OE.CRYPTO	Section 6.1.2
OSP.POL_EXPORT	O.POL_PROTECTION	Section 6.1.2

Table 3 Mapping organisational security policies to security objectives

Security objectives	Organisational security policies (OSP)
O.POL_ENFORCEMENT	OSP.PROVIDED_SERVICES
O.APPLI_CONFIDENTIALITY	OSP.PROVIDED_SERVICES
O.APPLI_AUTHENTICITY	OSP.PROVIDED_SERVICES
O.TOPO_CONFIDENTIALITY	OSP.PROVIDED_SERVICES
O.TOPO_AUTHENTICITY	OSP.PROVIDED_SERVICES
O.ADMIN_AUTHENTICATION	
O.USER_AUTHENTICATION	OSP.PROVIDED_SERVICES
O.KEYS_IMPORT	
O.KEYS_PROTECTION	
O.POL_IMPORT	
O.POL_PROTECTION	OSP.POL_EXPORT
O.REPLAY_PROTECTION	
O.ADMIN_FLOWS_PROTECTION	
O.CRYPTO	OSP.CRYPTO
OE.ADMIN	
OE.USER	
OE.REMOTE_ADMIN_EQUIPMENT	
OE.IP_ENCRYPTOR	OSP.PROVIDED_SERVICES
OE.AUTHENTICATING_COMPONENT	
OE.MACHINE	
OE.USER_RIGHTS	OSP.PROVIDED_SERVICES
OE.CONFIGURATION	
OE.COMM	
OE.KEYS_EXPORT	
OE.MULTI-USERS	
OE.RESET	
OE.CRYPTO	OSP.CRYPTO
OE.ACCESS	OSP.PROVIDED_SERVICES

Table 4 Mapping security objectives to organisational security policies

Assumptions	Security objectives for the operational environment	Rationale
A.ADMIN	OE.ADMIN	Section 6.1.3
A.USER	OE.USER	Section 6.1.3
A.REMOTE_ADMIN_EQUIPMENT	OE.REMOTE_ADMIN_EQUIPMENT	Section 6.1.3
A.IP_ENCRYPTOR	OE.IP_ENCRYPTOR	Section 6.1.3
A.AUTHENTICATING_COMPONENT	OE.AUTHENTICATING_COMPONENT	Section 6.1.3
A.MACHINE	OE.MACHINE	Section 6.1.3
A.USER_RIGHTS	OE.USER_RIGHTS	Section 6.1.3
A.CONFIGURATION	OE.CONFIGURATION, OE.COMM	Section 6.1.3
A.COMM	OE.COMM	Section 6.1.3
A.KEYS_EXPORT	OE.KEYS_EXPORT	Section 6.1.3
A.MULTI-USERS	OE.MULTI-USERS	Section 6.1.3
A.RESET	OE.RESET	Section 6.1.3
A.ACCESS	OE.ACCESS	Section 6.1.3

Table 5 Mapping assumptions to security objectives for the operational environment

Security objectives for the operational environment	Assumptions
OE.ADMIN	A.ADMIN
OE.USER	A.USER
OE.REMOTE_ADMIN_EQUIPMENT	A.REMOTE_ADMIN_EQUIPMENT
OE.IP_ENCRYPTOR	A.IP_ENCRYPTOR
OE.AUTHENTICATING_COMPONENT	A.AUTHENTICATING_COMPONENT
OE.MACHINE	A.MACHINE
OE.USER_RIGHTS	A.USER_RIGHTS
OE.CONFIGURATION	A.CONFIGURATION
OE.COMM	A.CONFIGURATION, A.COMM
OE.KEYS_EXPORT	A.KEYS_EXPORT
OE.MULTI-USERS	A.MULTI-USERS
OE.RESET	A.RESET
OE.CRYPTO	
OE.ACCESS	A.ACCESS

Table 6 Mapping security objectives for the operational environment to assumptions

6.2 Security requirements / security objectives

6.2.1 Objectives

6.2.1.1 Security objectives for the TOE

Security objectives for services provided by the TOE

O.POL_ENFORCEMENT

This objective is covered by:

FDP_ETC.1/EXPORT which ensures that VPN policies must be enforced on applicative and topologic data exported outside of the TOE,

FDP_ITC.1/IMPORT which ensures that VPN policies must be enforced on applicative and topologic data imported within the TOE,

FDP_IFC.1/DATA which defines the flows control policy of frames exchanged between a user, the TOE and an IP encryptor,

FDP_IFF.1/DATA which

specifies the VPN security policy to be enforced and authorizes the application of confidentiality protection,

specifies the VPN security policy to be enforced and authorizes the application of authenticity protection (i.e. integrity and authentication of origin),

authorizes the data (topologic and applicative) access for enforcement of protections specified in VPN security policies used and the send on the VPN link,

FDP_IFC.1/KEY_IMPORT which defines the flow control policy of keys,

FDP_IFF.1/KEY_IMPORT which ensures the access to keys in order to ensure protections specified in VPN security policies,

FMT_MSA.1/QUERY, FMT_MSA.1/MODIFY, FDP_IFC.1/VPN_POL and FDP_IFF.1/VPN_POL which ensure the access to VPN policies and to their attributes so that they are enforced,

FDP_ITC.2/VPN_POL which ensures that VPN security policies stored within the TOE are associated to a user name and to a VPN link,

FIA_USB.1/USER which provides the capability to determine if a user is authenticated as such with the TSF and if the identifier of this authenticated user is known

FMT_MSA.1/QUERY which authorizes access to the user identifier,

FMT_MSA.3 which ensures that the attributes AT.user_type and AT.user_id are initialized by default to a restrictive value to protect itself against any attempt to breach the TOE security mechanisms.

O.APPLI_CONFIDENTIALITY

This objective is covered by:

FDP_UCT.1/DATA which ensures the confidentiality of applicative data flowing between the TOE and the IP encryptor.

O.APPLI_AUTHENTICITY

This objective is covered by:

FDP_UIT.1/DATA which ensures the integrity of applicative data flowing between the IP encryptor and the TOE.

FCO_NRO.1/DATA which ensures the origin authentication of applicative data flowing between the TOE and the IP encryptor.

O.TOPO_CONFIDENTIALITY

This objective is covered by:

FDP_UCT.1/DATA which ensures the confidentiality of topologic data flowing between the TOE and the IP encryptor.

O.TOPO_AUTHENTICITY

This objective is covered by:

FDP_UIT.1/DATA which ensures the integrity of topologic data flowing between the IP encryptor and the TOE.

FCO_NRO.1/DATA which ensures the origin authentication of topologic data flowing between the TOE and the IP encryptor.

Security objectives to protect TOE sensitive assets

Authentication

O.ADMIN_AUTHENTICATION

The objective is covered by:

FIA_UAU.2/ADMIN to ensure administrator authentication by an encryption system component and to ensure the check of this authentication before permiting the connection to the subject S.user_manager which performs (in particular) administration commands (i.e. import and export of TOE sensitive assets) (FDP_IFC.1/KEY_IMPORT, FDP_IFF.1/KEY_IMPORT, FDP_IFC.1/VPN_POL and FDP_IFF.1/VPN_POL). To be known as authenticated with the TOE, the administrator will have to be bound on the subject S.user_manager to put the attribute AT.user_type as *"administrator"* (FIA_USB.1/ADMIN). This attribute is initialized by default to a restrictive value to protect itself against any attempt to breach the TOE security mechanisms (FMT_MSA.3), it is modifiable (FMT_MSA.1/MODIFY) and available for consultation (FMT_MSA.1/QUERY).

Its dependency FIA_UID.2/ADMIN to ensure the identification of the administrator who tries to be bound on the above-cited subject.

O.USER_AUTHENTICATION

The objective is covered by:

FIA_UAU.2/USER to ensure the user authentication by an encryption system component and to ensure the check of this authentication

before the user can be bound to S.user_manager which performs (in particular) the import and export orders of TOE sensitive assets (FDP_IFC.1/KEY_IMPORT, FDP_IFF.1/KEY_IMPORT, FDP_IFC.1/DATA, FDP_IFF.1/DATA),

before the TOE authorizes the VPN links establishment (FMT_MSA.1/QUERY permits to access to the user type). Indeed, the user will have to be bound on the subject S.user_manager to set up the attribute AT.user_type as *"User"* (FIA_USB.1/USER) and the user identifier AT.user_id, both modifiable

(FMT_MSA.1/MODIFY). In addition, FMT_MSA.3 ensures that AT.user_type and AT.user_id are initialized by default to a restrictive value to protect itself against any attempt to breach the TOE security mechanisms. The establishment of VPN link will be then authorized (FDP_ETC.1/EXPORT and FDP_ITC.1/IMPORT),

its dependency FIA_UID.2/USER to ensure the identification of the user which tries to be bound on the above-cited subject.

Cryptographic keys management

O.KEYS_IMPORT

This objective is covered by:

FDP_ITC.1/KEY_IMPORT which ensures that the security policy of keys import is correctly enforced during their import within the TOE,

FDP_IFC.1/KEY_IMPORT which defines the flow control policy for the keys import within the TOE,

FDP_IFF.1/KEY_IMPORT to

ensure that keys import within the TOE can only be performed by an administrator or a user authenticated as such with the TSF (FMT_MSA.1/QUERY and FMT_MSA.1/MODIFY specify the management of the attribute AT.user_type which provides the capability to determine whether it is an administrator or not),

state that only the subject S.user_manager can import keys,

FIA_USB.1/ADMIN which provides the capability to determine if an administrator is authenticated as such with the TSF,

FIA_USB.1/USER which provides the capability to determine if a user is authenticated as such with the TSF,

FMT_MSA.3 which ensures that the attribute AT.user_type is initialized by default to a restrictive value to protect itself against any attempt to breach the TOE security mechanisms.

O.KEYS_PROTECTION

This objective is covered by:

FDP_UCT.1/KEY_IMPORT which ensures the confidentiality of cryptographic keys imported within the TOE (so in particular, when they are imported locally),

FDP_ITC.1/KEY_IMPORT which ensures the detection of any integrity loss of cryptographic keys imported within the TOE (so in particular, when they are imported locally). It also ensures the cancellation of the import in case of anomaly,

FDP_IFC.1/DATA and FDP_IFF.1/DATA which ensures that the keys integrity is checked during their use (i.e. their use for the application of security properties to data sent on the VPN link); this so ensures that the storage protected their integrity.

In addition, this objective is completed by O.KEYS_IMPORT which limits the possibility of cryptographic keys import within the TOE to user and administrator.

VPN security policies management

O.POL_IMPORT

This objective is covered by:

FDP_ITC.2/VPN_POL which ensures that the import security policy of VPN policies is correctly enforced during their import within the TOE,

FDP_IFC.1/VPN_POL which defines the flows control policy of frames exchanged between the TOE and an administrator or a user in order to define the parameters of security policies used by the TOE,

FDP_IFF.1/VPN_POL to

ensure that the import of VPN security policies within the TOE is only performed by an administrator authenticated as such with the TSF (FMT_MSA.1/QUERY provides the capability to determine whether it is an administrator),

state that only the subject S.user_manager can import VPN security policies,

FIA_USB.1/ADMIN which provides the capability to determine that an administrator is authenticated as such with the TSF,

FMT_MSA.3 which ensures that the attribute AT.user_type is initialized by default to a restrictive value to protect itself against any attempt to breach the TOE security mechanisms.

O.POL_PROTECTION

This objective is covered by:

FDP_UCT.1/VPN_POL which ensures the confidentiality of VPN security policies imported within and exported from the TOE (so in particular, when they are imported locally),

FDP_UIT.1/VPN_POL which ensures the detection of any integrity loss of the VPN security policies imported within and exported from the TOE (so in particular, when they are imported locally),

FDP_IFF.1/DATA which ensures that the VPN security policies integrity is checked during their use (i.e. their application to data, for the send on the VPN link); this so ensures that the storage protected their integrity. For the answer, if an integrity loss is detected, the VPN link cannot become established.

FIA_USB.1/ADMIN which provides the capability to determine if an administrator is authenticated as such with the TSF,

FMT_MSA.3 which ensures that the attribute AT.user_type is initialized by default to a restrictive value to protect itself against any attempt to breach the TOE security mechanisms,

FDP_ETC.1/VPN_POL which ensures that the export is authorized only towards an administrator authenticated as such with the TSF (FMT_MSA.1/QUERY provides the capability to determine if the user is an administrator),

FDP_IFF.1/VPN_POL to

state that only the subject S.user_manager can export VPN security policies,

state that the import of VPN security policies is subjected to an access control; so participating to the integrity protection of VPN security policies during their storage.

Remote administration

O.REPLAY_PROTECTION

This objective is covered by the following requirements, which ensure that the administration operation replay is detected and the operation is canceled:

during the import and during the export of VPN security policies within the TOE (FDP_UIT.1/VPN_POL),

during the import of cryptographic keys within the TOE (FDP_UIT.1/KEY_IMPORT).

O.ADMIN_FLOWS_PROTECTION

This objective is covered by:

FDP_UCT.1/VPN_POL which ensures the confidentiality of VPN security policies imported within and exported from the TOE (so in particular, contained in administration flows transmitted towards the TOE),

FDP_UIT.1/VPN_POL which ensures the detection of any integrity loss of VPN security policies imported within the TOE (so in particular, contained in administration flows transmitted towards the TOE). It also ensures the cancellation of the import in case of anomaly,

FDP_UCT.1/KEY_IMPORT which ensures the confidentiality of cryptographic keys imported within the TOE (so in particular, contained in administration flows transmitted towards the TOE),

FDP_UIT.1/KEY_IMPORT which ensures the detection of any integrity loss of cryptographic keys imported within the TOE (so in particular, contained in administration flows transmitted towards the TOE).

Cryptography management

O.CRYPTO

This objective is covered by:

FCS_COP.1 which ensures the use of cryptographic functions compliant with the DCSSI cryptographic referential,

FCS_CKM.3 which ensures that the TOE implements mechanisms imposing cryptographic keys renewal.

6.2.2 Coverage between objectives and security requirements

Security objectives	Functional requirements for the TOE	Rationale
O.POL_ENFORCEMENT	FDP_IFF.1/DATA, FMT_MSA.3, FIA_USB.1/USER, FDP_ITC.2/VPN_POL, FMT_MSA.1/QUERY, FDP_IFF.1/KEY_IMPORT, FDP_IFF.1/VPN_POL, FDP_ETC.1/EXPORT, FDP_ITC.1/IMPORT, FDP_IFC.1/DATA, FDP_IFC.1/VPN_POL, FMT_MSA.1/MODIFY, FDP_IFC.1/KEY_IMPORT	Section 6.2.1
O.APPLI_CONFIDENTIALITY	FDP_UCT.1/DATA	Section 6.2.1
O.APPLI_AUTHENTICITY	FDP_UIT.1/DATA, FCO_NRO.1/DATA	Section 6.2.1
O.TOPO_CONFIDENTIALITY	FDP_UCT.1/DATA	Section 6.2.1
O.TOPO_AUTHENTICITY	FDP_UIT.1/DATA, FCO_NRO.1/DATA	Section 6.2.1
O.ADMIN_AUTHENTICATION	FIA_UID.2/ADMIN, FIA_UAU.2/ADMIN, FDP_IFC.1/KEY_IMPORT, FDP_IFC.1/VPN_POL, FIA_USB.1/ADMIN, FMT_MSA.1/MODIFY, FMT_MSA.3, FDP_IFF.1/KEY_IMPORT, FMT_MSA.1/QUERY, FDP_IFF.1/VPN_POL	Section 6.2.1
O.USER_AUTHENTICATION	FIA_UID.2/USER, FIA_UAU.2/USER, FMT_MSA.3, FIA_USB.1/USER, FDP_ETC.1/EXPORT, FDP_ITC.1/IMPORT, FMT_MSA.1/MODIFY, FMT_MSA.1/QUERY, FDP_IFC.1/DATA, FDP_IFF.1/DATA, FDP_IFC.1/KEY_IMPORT, FDP_IFF.1/KEY_IMPORT	Section 6.2.1
O.KEYS_IMPORT	FDP_IFF.1/KEY_IMPORT, FIA_USB.1/USER, FIA_USB.1/ADMIN, FMT_MSA.3, FDP_ITC.1/KEY_IMPORT, FDP_IFC.1/KEY_IMPORT, FMT_MSA.1/QUERY, FMT_MSA.1/MODIFY	Section 6.2.1
O.KEYS_PROTECTION	FDP_UCT.1/KEY_IMPORT, FDP_UIT.1/KEY_IMPORT, FDP_IFF.1/DATA, FDP_IFC.1/DATA, FDP_ITC.1/KEY_IMPORT	Section 6.2.1

Security objectives	Functional requirements for the TOE	Rationale
O.POL_IMPORT	FMT_MSA.3, FIA_USB.1/ADMIN, FDP_IFF.1/VPN_POL, FDP_ITC.2/VPN_POL, FDP_IFC.1/VPN_POL, FMT_MSA.1/QUERY	Section 6.2.1
O.POL_PROTECTION	FDP_UCT.1/VPN_POL, FDP_UIT.1/VPN_POL, FIA_USB.1/ADMIN, FMT_MSA.3, FDP_IFF.1/DATA, FDP_IFF.1/VPN_POL, FDP_ETC.1/VPN_POL, FMT_MSA.1/QUERY	Section 6.2.1
O.REPLAY_PROTECTION	FDP_UIT.1/KEY_IMPORT, FDP_UIT.1/VPN_POL	Section 6.2.1
O.ADMIN_FLOWS_PROTECTION	FDP_UCT.1/KEY_IMPORT, FDP_UIT.1/KEY_IMPORT, FDP_UCT.1/VPN_POL, FDP_UIT.1/VPN_POL	Section 6.2.1
O.CRYPTO	FCS_COP.1, FCS_CKM.3	Section 6.2.1

Table 7 Mapping security objectives for the TOE to functional requirements

Functional requirements for the TOE	Security objectives
FDP_ETC.1/EXPORT	O.POL_ENFORCEMENT, O.USER_AUTHENTICATION
FDP_ITC.1/IMPORT	O.POL_ENFORCEMENT, O.USER_AUTHENTICATION
FDP_IFC.1/DATA	O.POL_ENFORCEMENT, O.KEYS_PROTECTION, O.USER_AUTHENTICATION
FDP_IFF.1/DATA	O.POL_ENFORCEMENT, O.KEYS_PROTECTION, O.POL_PROTECTION, O.USER_AUTHENTICATION
FDP_UIT.1/DATA	O.APPLI_AUTHENTICITY, O.TOPO_AUTHENTICITY
FCO_NRO.1/DATA	O.APPLI_AUTHENTICITY, O.TOPO_AUTHENTICITY
FDP_UCT.1/DATA	O.APPLI_CONFIDENTIALITY, O.TOPO_CONFIDENTIALITY
FIA_UID.2/USER	O.USER_AUTHENTICATION
FIA_UAU.2/USER	O.USER_AUTHENTICATION
FIA_USB.1/USER	O.POL_ENFORCEMENT, O.USER_AUTHENTICATION, O.KEYS_IMPORT
FIA_UID.2/ADMIN	O.ADMIN_AUTHENTICATION
FIA_UAU.2/ADMIN	O.ADMIN_AUTHENTICATION
FIA_USB.1/ADMIN	O.ADMIN_AUTHENTICATION, O.KEYS_IMPORT, O.POL_IMPORT, O.POL_PROTECTION
FMT_MSA.3	O.POL_ENFORCEMENT, O.ADMIN_AUTHENTICATION, O.USER_AUTHENTICATION, O.KEYS_IMPORT, O.POL_IMPORT, O.POL_PROTECTION
FMT_MSA.1/MODIFY	O.POL_ENFORCEMENT, O.ADMIN_AUTHENTICATION, O.USER_AUTHENTICATION, O.KEYS_IMPORT
FMT_MSA.1/QUERY	O.POL_ENFORCEMENT, O.ADMIN_AUTHENTICATION, O.USER_AUTHENTICATION, O.KEYS_IMPORT, O.POL_IMPORT, O.POL_PROTECTION

Functional requirements for the TOE	Security objectives
FDP_IFC.1/KEY_IMPORT	O.POL_ENFORCEMENT, O.ADMIN_AUTHENTICATION, O.KEYS_IMPORT, O.USER_AUTHENTICATION
FDP_IFF.1/KEY_IMPORT	O.POL_ENFORCEMENT, O.ADMIN_AUTHENTICATION, O.KEYS_IMPORT, O.USER_AUTHENTICATION
FDP_ITC.1/KEY_IMPORT	O.KEYS_IMPORT, O.KEYS_PROTECTION
FDP_UCT.1/KEY_IMPORT	O.KEYS_PROTECTION, O.ADMIN_FLOWS_PROTECTION
FDP_UIT.1/KEY_IMPORT	O.KEYS_PROTECTION, O.REPLAY_PROTECTION, O.ADMIN_FLOWS_PROTECTION
FDP_ETC.1/VPN_POL	O.POL_PROTECTION
FDP_ITC.2/VPN_POL	O.POL_ENFORCEMENT, O.POL_IMPORT
FDP_UCT.1/VPN_POL	O.POL_PROTECTION, O.ADMIN_FLOWS_PROTECTION
FDP_UIT.1/VPN_POL	O.POL_PROTECTION, O.REPLAY_PROTECTION, O.ADMIN_FLOWS_PROTECTION
FDP_IFC.1/VPN_POL	O.POL_ENFORCEMENT, O.ADMIN_AUTHENTICATION, O.POL_IMPORT
FDP_IFF.1/VPN_POL	O.POL_ENFORCEMENT, O.ADMIN_AUTHENTICATION, O.POL_IMPORT, O.POL_PROTECTION
FCS_COP.1	O.CRYPTO
FCS_CKM.3	O.CRYPTO

Table 8 Mapping functional requirements to security objectives for the TOE

6.3 Dependencies

6.3.1 Security functional requirements dependencies

Requirements	CC dependencies	Satisfied dependencies
FMT_MSA.3	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/MODIFY
FMT_MSA.1/MODIFY	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_IFC.1/DATA
FMT_MSA.1/QUERY	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_IFC.1/DATA
FDP_IFC.1/VPN_POL	(FDP_IFF.1)	FDP_IFF.1/VPN_POL
FDP_IFF.1/VPN_POL	(FDP_IFC.1) and (FMT_MSA.3)	FMT_MSA.3, FDP_IFC.1/VPN_POL
FCS_COP.1	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.1/KEY_IMPORT
FCS_CKM.3	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.1/KEY_IMPORT
FDP_ETC.1/EXPORT	(FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.1/DATA
FDP_ITC.1/IMPORT	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FMT_MSA.3, FDP_IFC.1/DATA
FDP_IFC.1/DATA	(FDP_IFF.1)	FDP_IFF.1/DATA
FDP_IFF.1/DATA	(FDP_IFC.1) and (FMT_MSA.3)	FMT_MSA.3, FDP_IFC.1/DATA
FDP_UIT.1/DATA	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/VPN_POL
FCO_NRO.1/DATA	(FIA_UID.1)	
FDP_UCT.1/DATA	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/VPN_POL
FIA_UID.2/USER	No dependency	
FIA_UAU.2/USER	(FIA_UID.1)	FIA_UID.2/USER
FIA_USB.1/USER	(FIA_ATD.1)	
FIA_UID.2/ADMIN	No dependency	
FIA_UAU.2/ADMIN	(FIA_UID.1)	FIA_UID.2/ADMIN
FIA_USB.1/ADMIN	(FIA_ATD.1)	
FDP_IFC.1/KEY_IMPORT	(FDP_IFF.1)	FDP_IFF.1/KEY_IMPORT
FDP_IFF.1/KEY_IMPORT	(FDP_IFC.1) and (FMT_MSA.3)	FMT_MSA.3, FDP_IFC.1/KEY_IMPORT
FDP_ITC.1/KEY_IMPORT	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/KEY_IMPORT
FDP_UCT.1/KEY_IMPORT	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/KEY_IMPORT

Requirements	CC dependencies	Satisfied dependencies
FDP_UIT.1/KEY_IMPORT	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/KEY_IMPORT
FDP_ETC.1/VPN_POL	(FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.1/VPN_POL
FDP_ITC.2/VPN_POL	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/VPN_POL
FDP_UCT.1/VPN_POL	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/VPN_POL
FDP_UIT.1/VPN_POL	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/VPN_POL

Table 9 Functional requirements dependencies

6.3.1.1 Rationale for unsatisfied dependencies

The dependency FMT_SMR.1 of FMT_MSA.3 is not satisfied. Roles are defined by the value of the attribute AT.user_type of the subject S.user_manager.

The dependency FMT_SMR.1 of FMT_MSA.1/MODIFY is not satisfied. Roles are defined by the value of the attribute AT.user_type of the subject S.user_manager.

The dependency FMT_SMF.1 of FMT_MSA.1/MODIFY is not satisfied. There is no specific attributes management function in the model.

The dependency FMT_SMR.1 of FMT_MSA.1/QUERY is not satisfied. Roles are defined by the value of the attribute AT.user_type of the subject S.user_manager.

The dependency FMT_SMF.1 of FMT_MSA.1/QUERY is not satisfied. There is no specific attributes management function in the model.

The dependency FCS_CKM.4 of FCS_COP.1 is not satisfied. This dependency is not applicable because keys destruction is not include in the scope of the TOE.

The dependency FCS_CKM.4 of FCS_CKM.3 is not satisfied. This dependency is not applicable because keys destruction is not include in the scope of the TOE.

The dependency FTP_ITC.1 or FTP_TRP.1 of FDP_UIT.1/DATA is not satisfied. This dependency is not required because the TOE does not use a secure channel or path but communicates via secure frames.

The dependency FIA_UID.1 of FCO_NRO.1/DATA is not satisfied. This dependency is not required because the origin authentication of frames issued and received by the TOE is independent from users identification ("user" and "administrator"). In addition the TOE usage is not subjected to the identification of the TOE and the cipher unit.

The dependency FTP_ITC.1 or FTP_TRP.1 of FDP_UCT.1/DATA is not satisfied. This dependency is not required because the TOE does not use a secure channel or path but communicates via secure frames.

The dependency FIA_ATD.1 of FIA_USB.1/USER is not satisfied. This dependency is not required because security attributes associated to the users are maintained by the subject S.user_manager.

The dependency FIA_ATD.1 of FIA_USB.1/ADMIN is not satisfied. This dependency is not required because security attributes associated to the users are maintained by the subject S.user_manager.

The dependency FMT_MSA.3 of FDP_ITC.1/KEY_IMPORT is not satisfied. This dependency is not applicable because OB.keys does not use attributes.

The dependency FTP_ITC.1 or FTP_TRP.1 of FDP_UCT.1/KEY_IMPORT is not satisfied. This dependency is not required because the TOE does not use a secure channel or path but communicates via secure frames.

The dependency FTP_ITC.1 or FTP_TRP.1 of FDP_UIT.1/KEY_IMPORT is not satisfied. This dependency is not required because the TOE does not use a secure channel or path but communicates via secure frames.

The dependency FPT_TDC.1 of FDP_ITC.2/VPN_POL is not satisfied. This dependency is not applicable because the administrator who imports security policies is trustworthy and he transforms those policies in order to be correctly interpreted by the TOE.

The dependency FTP_ITC.1 or FTP_TRP.1 of FDP_ITC.2/VPN_POL is not satisfied. This dependency is not required because the TOE does not use a secure channel or path but communicates via secure frames.

The dependency FTP_ITC.1 or FTP_TRP.1 of FDP_UCT.1/VPN_POL is not satisfied. This dependency is not required because the TOE does not use a secure channel or path but communicates via secure frames.

The dependency FTP_ITC.1 or FTP_TRP.1 of FDP_UIT.1/VPN_POL is not satisfied. This dependency is not required because the TOE does not use a secure channel or path but communicates via secure frames.

6.3.2 Security assurance requirements dependencies

Requirements	CC dependencies	Satisfied dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.3, ADV_TDS.2
ADV_FSP.3	(ADV_TDS.1)	ADV_TDS.2
ADV_TDS.2	(ADV_FSP.3)	ADV_FSP.3
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.3
AGD_PRE.1	No dependency	
ALC_CMC.3	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.3, ALC_DVS.1, ALC_LCD.1
ALC_CMS.3	No dependency	
ALC_DEL.1	No dependency	
ALC_FLR.3	No dependency	
ALC_DVS.1	No dependency	
ALC_LCD.1	No dependency	
ASE_CCL.1	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	No dependency	

Requirements	CC dependencies	Satisfied dependencies
ASE_INT.1	No dependency	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) and (ASE_OBJ.2)	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	No dependency	
ASE_TSS.1	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	ADV_FSP.3, ASE_INT.1, ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.3, ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.3, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
ATE_DPT.1	(ADV_ARC.1) and (ADV_TDS.2) and (ATE_FUN.1)	ADV_ARC.1, ADV_TDS.2, ATE_FUN.1
AVA_VAN.3	(ADV_ARC.1) and (ADV_FSP.2) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1)	ADV_ARC.1, ADV_FSP.3, AGD_OPE.1, AGD_PRE.1

Table 10 Assurance requirements dependencies

6.3.2.1 Rationale for unsatisfied dependencies

The dependency ADV_IMP.1 of AVA_VAN.3 is not satisfied. This dependency is not required in accordance with the EAL required for the standard qualification [QUA-STD].

The dependency ADV_TDS.3 of AVA_VAN.3 is not satisfied. This dependency is not required in accordance with the EAL required for the standard qualification [QUA-STD].

6.4 Rationale for the EAL

The evaluation assurance level of this protection profile is EAL3 augmented by ALC_FLR.3 and AVA_VAN.3 in accordance with the standard level qualification process defined in [QUA-STD].

6.5 Rationale for the EAL augmentations

6.5.1 AVA_VAN.3 Focused vulnerability analysis

Augmentation required by the standard qualification process [QUA-STD].

6.5.2 ALC_FLR.3 Systematic flaw remediation

Augmentation required by the standard qualification process [QUA-STD].

Annex A Additional description of the TOE and its environment

A.1 Introduction to VPN technologies

This section introduces various standards used in VPN technologies. This section is only introduced for an informative purpose. Security services described in this profile were partially established on the basis of those offered by these standards, but this profile does not claim conformance with any of these.

A.1.1 IPsec

IPsec (IP security) is a set of standards implementing mechanisms to secure IP (IPv4 and IPv6) by offering authentication, integrity and confidentiality services ([RFC2401]).

IPsec provides these services by using two protocols for data exchange security:

AH (Authentication Header) provides the authentication of the origin and the on-the-fly integrity of IP packets. It can also provide an optional protection against replay attacks ([RFC2402]).

ESP (Encapsulating Security Payload) provides confidentiality, protection against replay attacks and an optional authentication of the origin and the on-the-fly integrity of a part of IP packets, which part does not contain the IP header ([RFC2406]).

These two protocols can be combined and used in one out of the two following data exchange modes:

Transport mode: the IP packet is sent by adding specific parts to AH and/or ESP.

Tunnel mode: the IP packet is encapsulated in a new IP packet containing specific parts of AH and/or ESP.

IPsec uses the concept of security association (SA) covered by AH and ESP. A security association provides the capability to define characteristics of a unidirectional connection: IP destination address, security protocol (AH or ESP), security parameters index (SPI), used cryptographic algorithms, used keys, expiration date and expiration hour, etc. This association is used to enforce a security policy during processing of IP packets flowing through the connection.

IPsec also provides protocols to manage cryptographic keys and security associations:

IKE (Internet Key Exchange): [RFC2409]. The part about management of security associations is covered by ISAKMP ([RFC2408]), whereas keys exchange is covered by Oakley ([RFC2412]) and SKEME ([SKEME]) protocols.

A.2 Physical location of the TOE within its environment

The aim of this section is to describe, only for illustration, different possible usage scenarios describing operation mode of mobile VPN. For simplification, other network equipments, providing additional services to the VPN (notably: routers, Ethernet switching hubs, firewalls, different areas controlled by firewalls), which could be owned by users are not introduced. Technical aspects bound to high availability and to load balancing which can also exist are not adressed.

The client VPN application is installed on a mobile machine which has a dynamic or static IP address provided by an access provider or gained within a private network of an organization on which the mobile PC is connected. Because of the mobility of a mobile computer, IP address of this one, allocated either dynamically or statically, does not constitute a predictible parameter which can be used to identify the mobile PC. The IP encryptor owns a predictible public IP address. VPN client establishes a VPN link between the mobile equipment and the IP encryptor to be able to access the coorporate private network. In some implementations, IP encryptor can so allocate a private IP address to the client machine (fixed or taken in a set of addresses) independently of the not predictible public address. This private IP adress allows the flows coming from mobile client machine to be restricted and isolated in areas or in applications within the private network. The machine user can then use the private network in a transparent way from outside of the organization.

Data flowing between mobile machine and private network go through non secure networks and the machine can be connected to Internet by various access technologies, from different places and with different operators:

- connection from the personal place of residence by using an ADSL connection;
- connection from a public place (hotel, cafe, train) by using a Wi-Fi access technology;
- connection from the local network of a company or a partner organization.

A.2.1 Encryption system without centralized administration equipment

In the environment illustrated on the figure 1, client VPN application runs in an encryption system context which does not include a « centralized » administration station (neither located on the IP encryptor which ends nomads VPN links, nor located elsewhere on another part of the network).

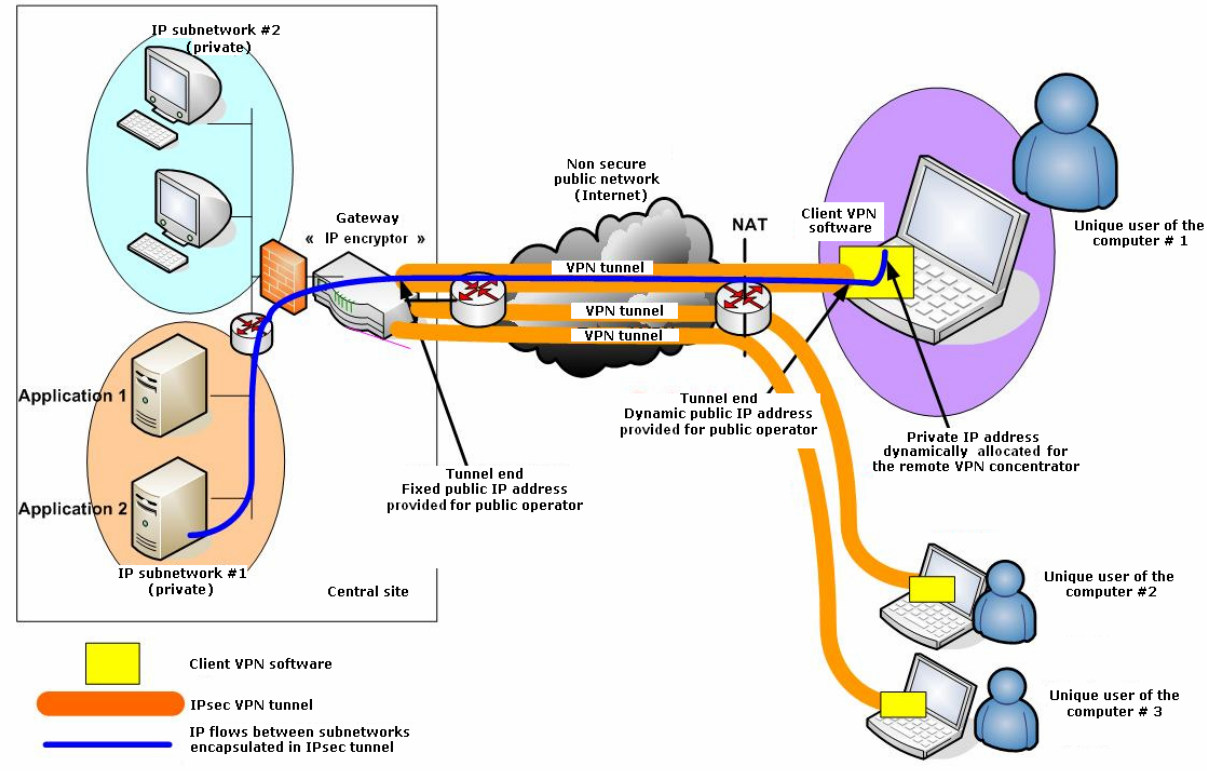

Figure 1. Operation without centralized remote administration equipment

Client VPN application, as well as IP encryptor which receives VPN connections from users, enforces VPN security policies defined on every endpoint. These policies clarify for example, on our figure, that client VPN applications can exchange flows with all IP equipments items

or applications installed within IP subnetwork number 1 of the organization central site (towards applications 1 and 2).

On the other hand, in our example, client VPN applications cannot issue flows towards equipments items or applications located on IP subnetwork number 2 of the central site of this same organization.

A.2.2 Encryption system with specific centralized administration equipment

In the environment illustrated on the figure 2, client VPN application runs in an encryption system context which includes a « centralized » administration station located on a specific network strand.

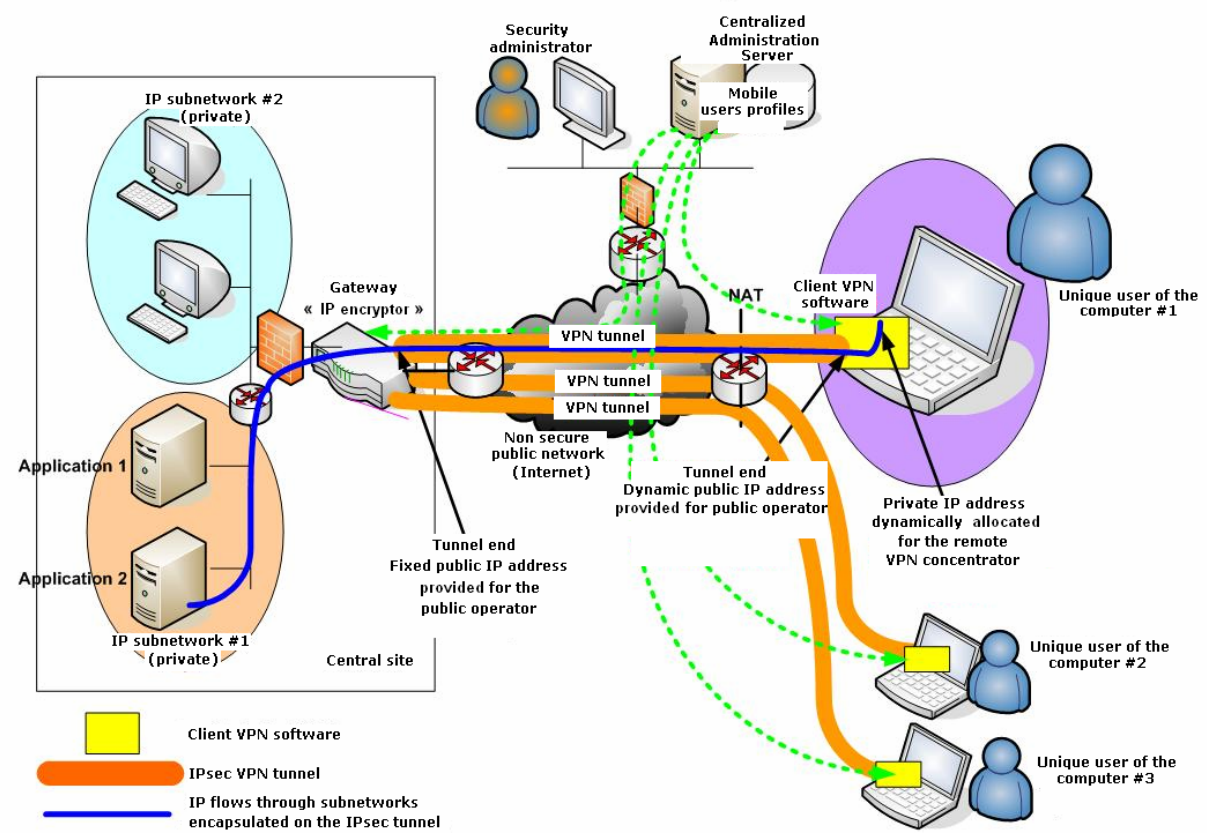

Figure 2. Operation with specific centralized remote administration equipment

Green flows on the figure correspond to administration flows. In this case of use, client VPN applications take their VPN security policy on the administration station (remote administration) centralized (administration station imports configurations towards VPN clients, but these are the VPN clients which take the initiative of the connection towards the administration station because IP addresses of VPN clients are not fixed).

A.2.3 Encryption system with administration centralized on an IP encryptor

In the environment illustrated on the figure 3, client VPN application runs in an encryption system context which includes a « centralized » administration station located on the IP encryptor which ends VPN links with client VPN applications.

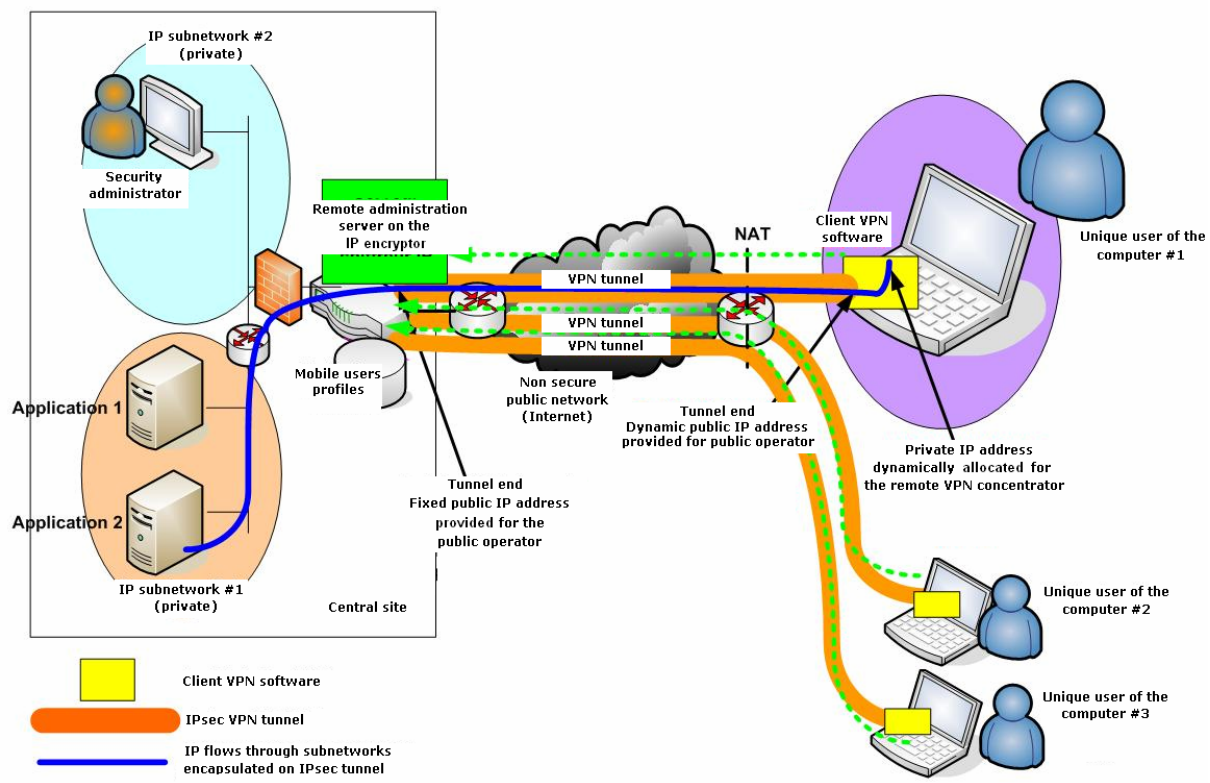

Figure 3. Operation with centralized remote administration equipment on an IP encryptor

Green flows on the figure correspond to administration flows. In this case of use, client VPN applications take their VPN security policy on the IP encryptor (in the centralized management module which manages user configurations). In this operation mode, administration flows not flow through VPN tunnels which are not established yet at this step (these administration flows can use, for example, SSL connections in order to secure them).

A.2.4 Encryption system with shared host machine

In the environment illustrated on the figure 4, the multi-users machine hosting the client VPN application connects to a specific application or in all applications included in a specific subnetwork placed within the company with a centralized administration station upon IP encryptor.

This case of use, rarer, is representative of an organization which makes available to its mobile users a set of machines which are not allocated to specific users. Every mobile user has nevertheless an account and a VPN profile which is appropriate for him.

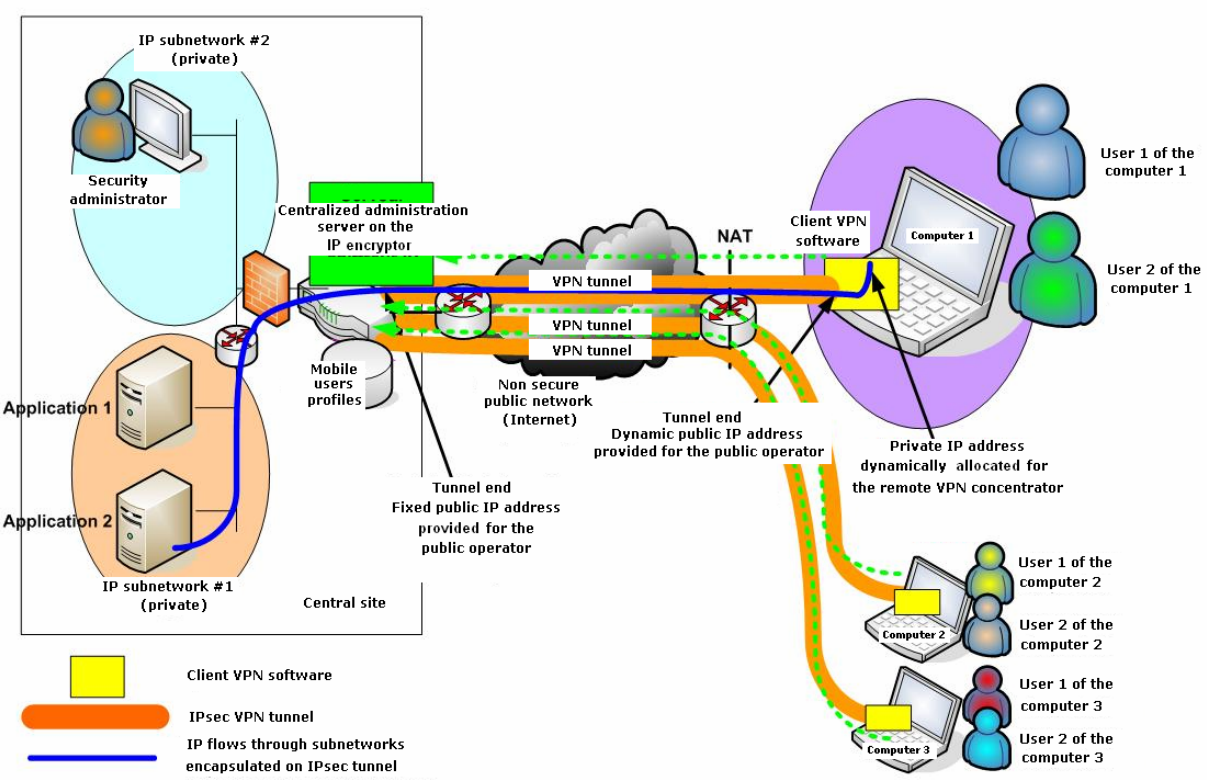

Figure 4. Operation with shared host machine

In this case, every user is authenticated on the centralized administration module and thus automatically gets back his VPN security policy, which is appropriate for him. In this model, VPN security policy of every user is not stored on mobile computer, but on the centralized administration module upon cipher unit.

A.3 TOE features

The TOE main functionality is to provide to the information system a secured communication link with an IP encryptor by offering the following services to protect the applicative dataflow (IP packets flowing between the machine hosting the client VPN application and an IP encryptor in front end of an organization):

- VPN security policies enforcement,
- confidentiality protection of applicative data,
- authenticity protection of applicative data,
- confidentiality protection of topologic informations,
- authenticity protection of topologic informations.

Furthermore, for its correct operation, the TOE requires the following services:

- Authentication:
  - authentication check on the encryption system.
- VPN security policies management:
  - VPN security policies import,
  - VPN security policies export,
  - access protection to the VPN security policies.
- Cryptographic keys management:
  - cryptographic keys import,

  - o access protection to the cryptographic keys,
  - o correct use of cryptographic keys.
- Administration:
  - o remote administration flows protection.

A.3.1 Services provided by the TOE

VPN security policies enforcement

VPN security policies specify security rules which determine the processing to apply to data. These latters correspond to data which are provided by information system applications and which are transported by network. They are called applicative data which flow between the TOE and an IP encryptor.

The client VPN application applies implicit filtering functions. So if no any VPN security policy is defined on a given VPN link, incoming or outgoing packets are rejected (default filtering rule).

Security services which can be enforced by a VPN security policy are:

- confidentiality protection of applicative data,
- authenticity protection of applicative data.

These policies are stored at the TOE and the IP encryptor concerned level to be enforced locally.

Confidentiality protection of applicative data

Ensure confidentiality of applicative data provides the capability to prevent the disclosure of these data when they flow through a non secure public network. For that purpose, these data can be ciphered before flowing through the public network and deciphered at the other end of the tunnel.

The encryption/decryption algorithm and used keys characteristics are defined in the security context associated to the enforced VPN security policy.

Authenticity protection of applicative data

To ensure authenticity of applicative data, it is required to ensure at the same time on-the-fly integrity of these data as well as authentication of the origin of these. Ensure data integrity provides the capability to detect that they were not modified accidentally or voluntarily during their transmission between the TOE and an IP encryptor. Ensure data authenticity ensures that the data origin is correct.

The algorithm used for generate authenticity informations and for check them as well as used keys characteristics are defined in the security context associated to the enforced VPN security policy.

Confidentiality protection of topologic informations

Ensure confidentiality of topologic data provides the capability to prevent disclosure of these data when they flow through a non secure public network. For that purpose, these data can

be ciphered before flowing through the public network and deciphered at the other end of the tunnel.

The encryption/decryption algorithm and used keys characteristics are defined in the security context associated to the enforced VPN security policy.

Authenticity protection of topologic informations

To ensure authenticity of topologic data, it is required to ensure at the same time on-the-fly integrity of these data as well as authentication of the origin of these. Ensure data integrity provides the capability to detect that they were not modified accidentally or voluntarily during their transmission between the TOE and an IP encryptor. Ensure data authenticity ensures that the data origin is correct.

The algorithm used for generate authenticity informations and for check them as well as used keys characteristics are defined in the security context associated to the enforced VPN security policy.

A.3.2 Required services for the correct operation of the TOE

A.3.2.1 Authentication

Check of the authentication on the encryption system

This service provides the capability to check that the user and the administrator are correctly authenticated towards the encryption system before being able to use client VPN application.

A.3.2.2 VPN security policies management

VPN security policies import

This service provides the capability to ensure the import in a secure way of VPN security policies within the TOE by ensuring their authenticity and their confidentiality. Generated outside of the TOE, they are imported by two ways:

- Locally:

  The administrator connects directly and physically himself to the TOE. This method is generally done during initialization phase to distribute initial security policies and their context. During the operational phase, it allows the security administrator to directly operate upon the TOE.

- Remotely:

  Policies are imported via a dataflow between the TOE and the administrator; the dataflow is protected on authenticity and confidentiality. This remote administration provides the capability to import new security policies with their context at the level of a machines workset, and this remote administration is generally used only during operational phase.

VPN security policies export

This service provides the capability to export VPN security policies towards an authenticated remote administrator by ensuring their authenticity. It allows a remote administrator to review the enforced VPN security policies and so it is easier to solve problems met during operational phase.

Access protection to VPN security policies

This service provides the capability to prevent export of VPN security policies, in an unauthorized way, outside of the TOE. It also enables ascertaining that a given security policy is usable (accessible) only by services which need it, and only after prior user authentication.

VPN security policies are so subject to access control dependent of the authentication of machine user.

A.3.2.3 Cryptographic keys management

Access protection to cryptographic keys

This service provides the capability to prevent secret and private keys to be exported in an unauthorized way outside of the TOE. It also enables ascertaining that a given key is usable (accessible) only by services which need it, and only after prior user authentication (keys are unlocked under the condition of check of authentication data provided by the user).

Cryptographic keys import

This service provides the capability to import in a secure way cryptographic keys, generated outside of the TOE, within the host machine:

- Locally by a security administrator:

  The administrator connects himself directly to the TOE. This method is generally performed during initialization phase to distribute initial cryptographic keys. During operational phase, it permits the security administrator to operate directly on the TOE.

- Remotely, with a user or via a remote administration mechanism:

  Cryptographic keys are imported via a dataflow between the TOE and the administrator or a remote administration equipment.

- Locally by the user:

  When keys are on an external support (smart card or USB key for example), this method allows the user to directly import keys on client VPN application during operational phase.

During the import, this service protects the integrity and/or confidentiality of keys according to the kind of keys.

Correct use of cryptographic keys

This service provides the capability to correctly manage cryptographic keys validity period: generation, bypass, regular renewal, destruction.

A.3.2.4 Administration

Remote administration flows protection

This service provides the capability to protect the authenticity and the confidentiality of remote administration flows for the renewal of keys or of VPN security policies and for the renewal of their security context. This service so provides the capability to ensure protection of TOE sensitive data, by only allowing access to reliable services which are authorized to proceed to these operations.

This service also protects against the replay of remote administration operation sequences flowing through links between client VPN application and update service which is on the corporate private network.

A.4 Possible additional functionalities for the client VPN application

This appendix introduces additional functionalities which can be proposed by the manufacturers in answers to users specific needs.

Local audit

Recording by the TOE of local audit data on the host machine was not retained in the considered security issue. This audit would provide the capability to log the eventual events which could not be audited at the level of IP encryptors or of centralized remote administration equipment.

Confidentiality protection of VPN security policies

This service would provide the capability to ensure, in addition to the integrity, the confidentiality of VPN security policies during their storage on the host machine hosting the TOE.

Annex B Definitions and acronyms

B.1 Definitions

This appendix provides the definition of the main terms used in this document. For the definition of Common Criteria terminology, refer to [CC1], §4.

Term	Definition
Administrator	User authorized to manage whole or part of the TOE. He can own particular privileges which provide the capability to modify security policies and cryptographic keys of the TOE.
Authenticity	Security property ensuring integrity and authentication of the origin for data in question.
Authentication	Security measure which checks the declared identity.
IP encryptor	Device placed backward a private network and intended to cipher communications exchanged between equipments of this network and external equipments by ensuring confidentiality and/or authenticity protection of data (via the use of VPN channel).
Session key	Key with short validity period generated randomly and used to ensure confidentiality, authenticity and integrity of data.
Security context	Security parameters which permit to know which security characteristics must be used to enforce the given VPN security policy. These parameters include cryptographic algorithms, keys sizes...
Operational environment	TOE environment during its operational phase.
Centralized remote administration equipment	Automatic equipment playing the role of the administrator and responsible of TOE remote administration.
Optional	In the case of this protection profile, « optional » means that the service or the security property in question shall be implanted within the TOE, but that their application or their use is not mandatory.
VPN security policy	Security policy providing the capability to specify security services (confidentiality and/or authenticity) to enforce on informations which flow between client VPN application and an IP encryptor.

Term	Definition
Editorial refinement	Refinement where a small change is made in a requirement, i.e. rephrasing a sentence due to adherence to proper English grammar. This change is not allowed to modify the meaning of the requirement in any way.
Non-editorial refinement	Refinement allowing to make a requirement more precise or to limit the scope of its acceptable implementations.
Private network	Internal network of an entity (as a company or a service) which shall be protected from flows coming from the outside but not from its own flows. This network is considered secure.
Public network	Accessible network to any entity and any person which cannot be considered secure.
Encryption system	Equipments workset sharing the same public key infrastructure and being able to contribute in particular to the establishment of ciphered communications between its different members.

B.2 Acronyms

CC	*Common Criteria*
EAL	*Evaluation Assurance Level*
IP	*Internet Protocol*
IT	*Information Technology*
OSP	*Organisational Security Policy*
PP	*Protection Profile*
SPD	*Security Problem Definition*
SSL	*Secure Sockets Layer*
ST	*Security Target*
TOE	*Target Of Evaluation*
VPN	*Virtual Private Network*

Annex C References

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1, revision 1, September 2006. CCMB-2006-09-001.

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1, revision 2, September 2007. CCMB-2007-09-002.

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements. Version 3.1, revision 2, September 2007. CCMB-2007-09-003.

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1, revision 2, September 2007. CCMB-2007-09-004.

[CRYPTO] Cryptographic mechanisms - Rules and recommendations about the choice and parameters sizes of cryptographic mechanisms with standard robustness level. DCSSI.

[CRYPTO_GESTION] Gestion des clés cryptographiques : Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques de niveau de robustesse standard. DCSSI.

[AUTH] Authentification : Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard. DCSSI.

[QUA-STD] Processus de qualification d'un produit de sécurité – niveau standard. Version 1.1, 18 mars 2008. N°549/SGDN/DCSSI/SDR.

[PP-VPNC] Profil de Protection « Application VPN cliente », version cc3.0, ref. « pp0602 »

[PB-INT] Problématique d'interconnexion des réseaux IP. Version 1.8, mai 2003. Premier Ministre, Secrétariat général de la défense nationale, Direction centrale de la sécurité des systèmes d'information, Sous-direction scientifique et technique, Laboratoire Technologies de l'Information.

[PP-FIR] Profil de Protection, Firewall d'interconnexion de réseaux IP. Version 1.07, mars 2004. AQL. http://meleze.arkoon.net/pps.html.

[PPnc0502] Profil de Protection, Chiffreur IP. Version 1.5, février 2005. DCSSI. http://www.ssi.gouv.fr/site_documents/pp/ppnc0502.pdf.

[PRIS] Politique de Référencement Intersectorielle de Sécurité (PRIS), Préambule, version 2.0, juin 2002, OID 1.2.250.1.137.2.2.1.2.1.1

[RFC2401] Security Architecture for the Internet Protocol. RFC 2401. November 1998. S. Kent, R. Atkinson. http://www.ietf.org/rfc/rfc2401.

[RFC2402] IP Authentication Header (AH). RFC 2402. November 1998. S. Kent, R. Atkinson. http://www.ietf.org/rfc/rfc2402.

[RFC2406] IP Encapsulating Security Payload (ESP). RFC 2406. November 1998. S. Kent, R. Atkinson. http://www.ietf.org/rfc/rfc2406.

[RFC2408] Internet Security Association and Key Management Protocol (ISAKMP). RFC 2408. November 1998. D. Maughan, M. Schertler, M. Schneider, J. Turner. http://www.ietf.org/rfc/rfc2408.

[RFC2409] The Internet Key Exchange (IKE). RFC 2409. November 1998. D. Harkins, D. Carrel. http://www.ietf.org/rfc/rfc2409.

[RFC2412] The OAKLEY Key Determination Protocol. RFC 2412. November 1998. H. Orman. http://www.ietf.org/rfc/rfc2412.

[SKEME] SKEME: A Versatile Secure Key Exchange Mechanism for Internet. IEEE Proceedings of the 1996 Symposium on Network and Distributed Systems Security. Krawczyk, H.

Index

A

A.ACCESS 18
A.ADMIN 16
A.AUTHENTICATING_COMPONENT 16
A.COMM 17
A.CONFIGURATION 17
A.IP_ENCRYPTER 16
A.KEYS_EXPORT 17
A.MACHINE 16
A.MULTI-USERS 17
A.REMOTE_ADMIN_EQUIPMENT 16
A.RESET 17
A.USER 16
A.USER_RIGHTS 17

D

D.APPLICATIVE_DATA 12
D.CRYPTO_KEYS 12
D.SOFTWARE 13
D.TOPOLOGIC_DATA 12
D.VPN_POLICIES 12

F

FCO_NRO.1/DATA 29
FCS_CKM.3 38
FCS_COP.1 38
FDP_ETC.1/EXPORT 27
FDP_ETC.1/VPN_POL 36
FDP_IFC.1/DATA 27
FDP_IFC.1/KEY_IMPORT 33
FDP_IFC.1/VPN_POL 37
FDP_IFF.1/DATA 28
FDP_IFF.1/KEY_IMPORT 33
FDP_IFF.1/VPN_POL 37
FDP_ITC.1/IMPORT 27
FDP_ITC.1/KEY_IMPORT 35
FDP_ITC.2/VPN_POL 36
FDP_UCT.1/DATA 30
FDP_UCT.1/KEY_IMPORT 35
FDP_UCT.1/VPN_POL 36
FDP_UIT.1/DATA 29
FDP_UIT.1/KEY_IMPORT 35
FDP_UIT.1/VPN_POL 36
FIA_UAU.2/ADMIN 32
FIA_UAU.2/USER 31
FIA_UID.2/ADMIN 32
FIA_UID.2/USER 31
FIA_USB.1/ADMIN 32
FIA_USB.1/USER 31
FMT_MSA.1/MODIFY 33
FMT_MSA.1/QUERY 33
FMT_MSA.3 33

O

O.ADMIN_AUTHENTICATION 19
O.ADMIN_FLOWS_PROTECTION 21
O.APPLI_AUTHENTICITY 19
O.APPLI_CONFIDENTIALITY 19
O.CRYPTO 21
O.KEYS_IMPORT 20
O.KEYS_PROTECTION 20
O.POL_ENFORCEMENT 19
O.POL_IMPORT 20
O.POL_PROTECTION 20
O.REPLAY_PROTECTION 21
O.TOPO_AUTHENTICITY 19
O.TOPO_CONFIDENTIALITY 19
O.USER_AUTHENTICATION 19
OE.ACCESS 23
OE.ADMIN 21
OE.AUTHENTICATING_COMPONENT 22
OE.COMM 22
OE.CONFIGURATION 22
OE.CRYPTO 23
OE.IP_ENCRYPTER 21
OE.KEYS_EXPORT 22
OE.MACHINE 22
OE.MULTI-USERS 22
OE.REMOTE_ADMIN_EQUIPMENT 21
OE.RESET 22
OE.USER 21
OE.USER_RIGHTS 22
OSP.CRYPTO 15
OSP.POL_EXPORT 16
OSP.PROVIDED_SERVICES 15

S

Security administrator 13
System and network administrator 13

T

T.ADMIN_USURPATION 14
T.KEYS_DISCLOSURE 15
T.KEYS_MODIFICATION 14
T.POL_DISCLOSURE 15
T.POL_MODIFICATION 15
T.REPLAY 14
T.USER_USURPATION 14

U

User 13