Direction centrale de la sécurité des systèmes d'information

Protection Profile - On-the-fly Mass Storage Encryption Application

Creation date	:	August 2008
Reference	:	PP-CDISK-CCv3.1
Version	:	1.4

Courtesy Translation

Courtesy translation of the protection profile registered and certified by the French Certification Body under the reference DCSSI-PP-2008/04.

Table of contents

List of figures

List of tables

1 Protection Profile introduction

1.1 Protection Profile identification

Title:	Protection Profile, On-the-fly mass storage encryption application
Author:	Trusted Labs S.A.S.
Version:	1.4, August 2008
Sponsor:	DCSSI
CC version:	3.1 revision 2

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 aim is to encourage the certification of on-the-fly mass storage encryption applications for public and private sectors qualification requirements.

This document includes two protection profiles (PP), namely:

- On-the-fly mass storage encryption application *with* key generation
- On-the-fly mass storage encryption application *without* key generation

Those two profiles will more simply be called « configuration » in this document, where every section identify, if necessary, one of both profiles . Without any particular distinction, a section is applicable to both configurations.

1.3 Target of evaluation overview

1.3.1 TOE type

The objective is to define security requirements in which an on-the-fly encryption application upon any storage persistent memory (eventually removable) shall comply with the aim of a security evaluation. The target of evaluation (TOE) taken into account in this PP is a software providing the capability to protect confidentiality of recorded data on a part at least of storage persistent memory of a machine (or, more generally, on a storage support possibly removable), in the two following cases:

1. the TOE is out of operation,
2. the TOE is operating but none rightful user is authenticated to the TOE.

Threats relative to the case of the TOE in operation with a rightful user who is authenticated to the TOE will therefore not be considered in the current PP.

The main objective is therefore to cover any machine theft. Nevertheless, operational phase risks related to the confidentiality data protection service provided by the product shall be covered (as, for example, the writing of confidential informations on non ciphered areas or the plaintext writing of the key on a persistent memory). Data confidentiality on the mass memory shall be so ensured whatever the successive states of the machine took place during the operational phase (setting in a stand-by mode, sudden shut-down…).

For simplification, the part of the persistent mass storage memory containing data protected by the TOE will be defined by « disk » later in this PP if no ambiguity is introduced.

1.3.2 TOE usage

The IT hardware of a company or of an administrative department can be subject to theft as well as any other valuables object. Today, this risk is increased by the growth of mobile equipment which is more susceptible to leave workplace contrary to before. The TOE is an on-the-fly encryption application installed on an IT support providing the capability to protect the confidentiality of these data and to reduce the impact of the loss in case of material theft.

1.3.3 Security particularities and security features of the TOE

The TOE, once activated, ciphers and deciphers data which are recorded on and read from the mass memory in a transparent way. This activation requires a user authentication through, for example, the supply of authentication data such as password or passphrase. The TOE also uses, during its operation, encryption keys. The confidentiality of these keys, as the confidentiality of the users authentication data, shall be ensured by the TOE for the cases specified in Section 1.3.1.

Each of both configurations corresponds to a specific product type, depending on whether the TOE generates itself encryption keys (configuration « with key generation ») or whether the TOE receives them from a trusted third party (configuration « without key generation »).

1.3.4 Outside-TOE hardware and software

The TOE is assumed to operate on any type of hardware managing a mass memory. The TOE relies on the operating system (OS) or on the firmware[1] to communicate with the client applications and the user. According to the cases, either OS drivers will be used by the TOE to access mass memory or the TOE itself will serve as a driver, if the TOE is distributed under this shape (applicative library).

Examples of software/hardware covered by the TOE:

- Personal computer running under Windows®, Linux™, Mac OS X®, BSD®, Unix® …
- USB key and its management driver
- Removable hard disk and firmware provided by the builder

1.3.5 Protection Profile use

Requirements introduced into each of both configurations (protection profile) define minimal rules to which a security target of an on-the-fly hard disk encryption application shall comply with, depending on whether this application generates or not its encryption keys; these rules

[1] Software integrated in a material component (hard disk, USB key…). Examples: BIOS, Open Firmware (IEEE-1275), OpenBoot ™…

are not restrictive at all. So, it is allowed to add other functionalities or to refer also to another protection profile. The use of this profile within the context of the certification of an encryption hardware device is another possibility.

However, any modification in the current protection profile is restricted by rules related to the conformance specified in Section 2.4.

2 Conformance claims

This chapter contains the following sections:

CC conformance claim (2.1)

Package conformance claim (2.2)

PP conformance claim (2.3)

PP 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 compliant with the assurance requirements package EAL3 augmented by ALC_FLR.3 and AVA_VAN.3 for the standard level qualification defined in [QUA-STD].

2.3 PP conformance claim

This PP no declares 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 first objective of the TOE is to protect data recorded on the disk by users in the event of theft of the device or of the machine containing the disk. These data are themselves protected on confidentiality via encryption by one or several secret keys (or public), according to mechanisms dependent on the implementation. The description of every asset supplies protection types required for each of those assets (part *Protection*).

3.1.1 Assets protected by the TOE

D.USER_DATA

This asset represents user data to be protected in confidentiality on the disk by the TOE. It is plaintext data (ciphered data are not a sensitive asset).

Protection: confidentiality.

Application note

The writer of security target which is in conformance with this protection profile could also clarify the TOE sensitive assets (for example the encryption keys and the authentication data) which must be distinguished from assets protected by the TOE.

3.2 Users

The operation of the TOE within its operational environment, directly or indirectly handles the roles described below.

User

User of the machine from which some data are to be protected in confidentiality on the machine disk.

Application note

The security administrator role in charge of the TOE installation and configuration does not take place with the security issue in question and the TOE operation does not therefore handle this role. Moreover, in some products administrator and user roles are sometimes not distinguishable.

3.3 Threats

Threats introduced in this section are only those which compromise the TOE security and not those which compromise services provided by the TOE. Therefore, the origin of the different threatening agents is outside of the TOE operational environment, such as any person from outside the organisation who takes advantage of the machine mobility (for example, theft in a public place) or such as a burglar. Administrators and rightful users are not viewed as attackers.

T.DATA_ACCESS

An attacker acquires knowledge of the user sensitive data stored into the disk, for example, after having either collected one or several image(s) of the disk which are partial or total (possibly at different moments) or after having stolen the equipment or the disk.

Application note

According to the implementation, the disk image can also contain other assets, such as some encryption keys.

T.MEMORIES_ACCESS

After the stop of the encryption application by the user, an attacker which have access to storage application memories (for example, RAM) acquires knowledge of the user sensitive data or the cryptographic keys.

3.4 Organisational security policies (OSP)

Organisational security policies introduced in this section are only relative to expected TOE functions and are therefore only relative to services provided by the TOE to the information system.

OSP.CRYPTO

TOE cryptographic mechanisms shall be in conformance with requirements for the standard robustness level of the cryptographic referentials [CRYPTO] and [CRYPTO_GESTION] of the DCSSI.

OSP.NON_REMANENT_2

Organisational measures prevent the eventual re-use of the persistence of memories during the machine shut-down in which runs the product.

Application note

It is advised to the user to ensure that the access to the computer after its shut-down is not possible during some time. This time depends on memories characteristics (cf. Assumption A.NON_REMANENT_1). Generally, some dozens seconds are enough. This measure have not to be applied if the product includes a technical function for delete the whole memory while the system is shuting-down or if it is demonstrated that memories are not remanent at all or more generally, if it is demonstrated that the analysis of the memory contents after shut-down of its power supply does not allow to retrieve a useful information for the attacker. Warning: this demonstration shall be made for a given hardware product and not by only using the specifications of the memories manufacturer.

3.5 Assumptions

3.5.1 Assumptions applicable to both configurations

This section describes the assumptions applicable to both configurations: « without key generation » and « with key generation ».

A.OPERATIONAL_ENV

The operational environment doesn't allow an attacker to access the disk when sensitive data are accessible to a rightful user on the equipment.

A.NON_REMANENT_1

Working memories used by the machine where runs the product are not remanent by construction.

Application note

In practice, many theorical non remanent memories are remanent some time after the power off. This phenomenon justifies the OSP.NON_REMANENT_2.

3.5.2 Assumptions applicable to the configuration without key generation

This section describes the assumptions exclusively applicable to the configuration: « without key generation ».

A.KEYS_OPERATIONAL_ENV

The TOE operational environment generates encryption keys with a way and nature which are in conformance with the requirements of the DCSSI referential [CRYPTO].

Moreover, it provides those keys to the TOE by ensuring their integrity, their confidentiality and their authenticity.

4 Security objectives

4.1 Security objectives for the TOE

4.1.1 Objectives applicable to both configurations

This section describes the objectives for the TOE which are applicable to both configurations: « without key generation » and « with key generation ».

O.USER_DEACTIVATE

The TOE shall make sensitive data inaccessible, in particular the cryptographic keys, when the disk is dismantled by the user.

Application note

The meaning of this objective is to allow a user to deactivate a disk, to put the TOE « out of operation », in order to protect its data, in particular on machines which doesn't provide the « switched off » mode (personal digital assistants). Whatever the circumstances, this objective is not related to data secure deletion.

O.CRYPTO

The TOE shall implement cryptographic functions and manage cryptographic keys in conformance with the requirements for the standard robustness level of the cryptographic referentials [CRYPTO] and [CRYPTO_GESTION] of the DCSSI.

O.RECORDED_DATA_PROTECTION

The TOE shall ensure the authentication of the user before providing access to recorded data.

O.ROBUSTNESS

The sudden shut-down (unexpected) of the TOE (of the equipment, of the disk) shall not provide the capability to access sensitive data.

Application note

This objective ensures that, outside of the context of nominal operation, the TOE doesn't record in plain text in a persistent way some data which are supposed to be ciphered. Indeed, a sudden shut-down of the TOE can took place before the theft or the copy of the image. In this case, the support could contain unciphered user data.

4.1.2 Objectives applicable to the configuration with key generation

This section describes the objectives for the TOE exclusively applicable to the configuration « with key generation ».

In addition to previous objectives for the TOE, the configuration « with key generation » includes the objective O.ENCRYPTION_KEYS below.

O.ENCRYPTION_KEYS

The TOE shall generate encryption keys according to requirements for the standard robustness level of the cryptographic referentials [CRYPTO] and [CRYPTO_GESTION] of the DCSSI.

4.2 Security objectives for the operational environment

4.2.1 Objectives applicable to both configurations

This section describes the objectives for the environment applicable to both configurations: « without key generation » and « with key generation ».

OE.OPERATIONAL_ENV.1

When the user is authenticated, the operational environment shall ensure the confidentiality of sensitive data, of keys and of authentication data.

Application note

The equipment shall provide efficient protections against eavesdropping and unauthorised data transmission (correctly configured firewall, antivirus with up-to-date database, « anti-spyware », *etc.*).

Applications installed on the equipment shall not disturb the correct operation of the TOE. Thus, operations that could be done by the user on the files which are protected by the TOE, especially through applications of the user, shall not lead to total or partial copies of these files outside the TOE, except when these copies were clearly required or when it is a clear consequence of the requested operation. The configuration of the machine/system/account user/application shall restrict the storage of protected files within the TOE, in particular as regards the temporary files or working files of the applications.

OE.OPERATIONAL_ENV.2

The user shall access his sensitive data only when he is in a reliable environment (when he is alone or with people having the need to know).

OE.NON_REMANENT_1

Working memories used by the machine which runs the product shall not be remanent by construction.

OE.NON_REMANENT_2

TOE operational environment implements some measures to avoid re-use of the memories remanence during the machine shut-down in which runs the disk encryption application.

4.2.2 Objectives applicable to the configuration without key generation

This section describes the objectives for the environment which are exclusively applicable to the configuration « without key generation ».

Environment objectives which are applicable to the configuration « without key generation » are both objectives OE.OPERATIONAL_ENV.1 and OE.OPERATIONAL_ENV.2 (common to

both configurations), as well as both objectives OE.OPERATIONAL_ENV.3 and OE.OPERATIONAL_ENV.4 below.

OE.OPERATIONAL_ENV.3

The TOE operational environment generates encryption keys with a way and nature which are in conformance with the requirements of the cryptographic referentials [CRYPTO] and [CRYPTO_GESTION] of the DCSSI.

OE.OPERATIONAL_ENV.4

The TOE operational environment provides the keys generated within the context of the objective OE.OPERATIONAL_ENV.3 by ensuring their integrity, their confidentiality and their authenticity.

In a security target compliant with the configuration « without key generation », it is allowed, according to [CC1], section D.3, to integrate the objective on the environment OE.OPERATIONAL_ENV.4 as an objective for the TOE, for example in the form « The TOE shall ensure the integrity, the confidentiality and the authenticity of keys imported by itself ». As a consequence, the target will have to include functional requirements in order to cover these objectives; FDP_ITC, FDP_UIT and FCO_UCT families being quite indicated.

5 Security requirements

5.1 Security functional requirements

In security functional requirements, both following terms are used to indicate a refinement:

- *Editorial refinement* (term defined in [CC1]): refinement in which a minor modification is made on a requirement element, such as a reformulation of a sentence with respect for the English grammar. Whatever the circumstances, this modification must not change the meaning of the requirement.
- *Non-editorial refinement*: refinement which allows to add precision or to limit all acceptable implementations for a requirement element.

The security functional requirements (SFR) model is summarized in Figure 1**.**

Subjects

Security functional requirements (SFR) make reference to the following subjects:

Subject	Security attribute	Possible values
S.API	-	-
S.DISK	Disk status (*AT.STATUS*)	ACTIVATED/DEACTIVATED
S.DISK	Disk identifier (*AT.ID*)	To be clarified in the ST

Remark:

In the SFR model, the following convention was used: the attribute AT.X of the subject Y is called Y.X.

Each disk managed by the TOE is represented by a subject *S.DISK* supporting a security attribute *AT.STATUS* which reflects the fact that this latter is activated or deactivated. The disk is only activated when an authenticated user is bound to this subject. The generic subject *S.API* corresponds to the entry point, accessible by all applications of the host machine, providing the capability to access data of an activated disk.

Later in this PP, the TSF will play the role of a subject but, by definition, it does not have to appear in the above table.

Objects

Security functional requirements (SFR) make reference to the following objects:

Object	Security attribute	Possible values
S.DISK	*cf.* Subjects	*cf.* Subjects
Encryption key (*OB.KEY*)	Associated disk identifier (*AT.ID*)	To be clarified in the ST
Ciphered user data (*OB.UD*)	Associated disk identifier (*AT.ID*)	To be clarified in the ST
Authentication data (*OB.AD*)	Associated disk identifier (*AT.ID*)	To be clarified in the ST

Remark: in the SFR model, the following convention was used: the attribute AT.X of the object Y is called Y.X.

Subjects *S.DISK* are also objects, thus there are some operations for which objects are *S.DISK*.

An encryption key implicitly corresponds to a disk. Thus, the recording of user data (D.USER_DATA) on a disk results in the creation or the modification of an object *OB.UD* whose security attribute *associated disk identifier (AT.ID)* allows to know with which key (in other words, on which disk) the data are ciphered. So, the object OB.UD represents the same data as the asset D.USER_DATA, but once ciphered by the TOE.

Authentication data *(OB.AD)* associated to a disk represents the data used to authenticate the disk user, when these are managed by the TOE.

Operations

Security functional requirements (SFR) make reference to the following operations:

Operation	Subject	Object
Creation (*CREATE*)	TSF	S.DISK, OB.AD, OB.KEY
Activation (*MOUNT*)	S.DISK	S.DISK
Deactivation (*DISMOUNT*)	S.API, TSF	S.DISK
Access (*ACCESS*)	S.DISK	OB.AD
Use (*USE*)	S.API	OB.KEY
Reading/writing/Erase (*DECIPHER/CIPHER/ERASE*)	S.API	OB.UD

The *CREATE* operation corresponds intuitively to the creation of a disk: an encryption key is implicitly associated to it, whether the key is either randomly generated, or derivated from data provided by the user (configuration « with key generation ») or imported (configuration « without key generation »). Likewise, there is no requirement on encryption keys storage.

In the same way, the creation of a disk also creates (*CREATE*) some authentication data (OB.AD) which allow to authenticate later the owner of the disk. Once created, those data can only be handled (*ACCESS*) by their creator, with the *ACCESS* operation which can be defined in a security target (deletion, modification, reading…).

The *MOUNT* operation corresponds to the disk activation by the user. To activate the disk, he has to provide authentication data OB.AD. The implementation of this operation leads to a modification of the security attribute S.DISK.STATUS which takes the value ACTIVATED.

The *DISMOUNT* operation allows to dismantle a disk. The implementation of this operation leads to a modification of the security attribute S.DISK.STATUS which takes the value DEACTIVATED.

The USE operation corresponds to the use of a key in purposes of disk encryption or decryption. It is a TOE « internal » operation which is not a part of the TOE external interface.

The *DECIPHER* operation corresponds to the reading of data on a disk managed by the TOE. As the TOE only reads data on « its » disk on a ciphered way, it is a cryptographic operation of decryption.

The *CIPHER* operation corresponds to the writing of data on a disk managed by the TOE. As the TOE only writes data on « its » disk on a ciphered way, it is an encryption cryptographic operation.

The *ERASE* operation corresponds to the deletion of data on a disk managed by the TOE.

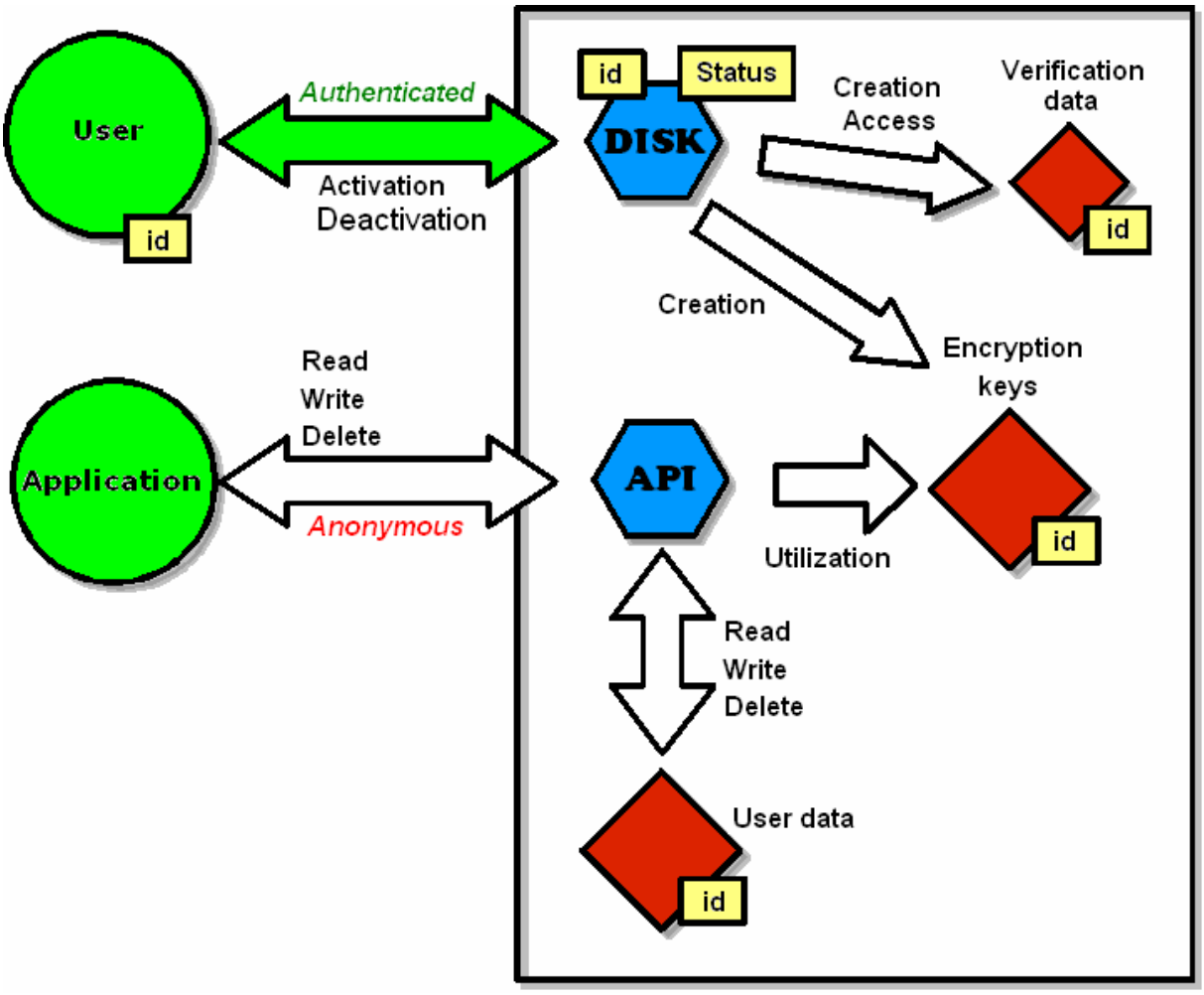

Figure 1 : TSP summary

Users

U.User represents the machine user whose some data must be protected in confidentiality on the disk.

U.Application represents applications performing reading writing and deletion operations, by calling the entry point enabling to access data of an activated disk.

5.1.1 Requirements applicable to both configurations

5.1.1.1 Requirements bound to the users authentication

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow

- **CREATE,**
- **DISMOUNT,**
- **USE, DECIPHER, CIPHER and ERASE**

on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 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:

TSF-mediated actions include MOUNT and ACCESS.

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow

- **CREATE,**
- **DISMOUNT,**
- **USE, DECIPHER, CIPHER and ERASE**

on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 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:

TSF-mediated actions include MOUNT and ACCESS.

The authentication mechanism must meet the DCSSI's requirements [AUTH].

Application note

The users authentication could be performed by a passphrase, etc.

5.1.1.2 Requirements bound to the TOE robustness

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

- **hot / warm / cold reset of the host machine**
- **when the host machine is switched off (power shortage)**
- **[assignment: other list of failures or types of failures]**.

5.1.1.3 Miscellaneous

FMT_MSA.3 Static attribute initialisation

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

Non-editorial refinement:

The restrictive values of security attributes shall be assigned according to the following rules:

- Rule STATUS: The TSF shall assign the value DEACTIVATED to the security attribute AT.STATUS whenever a S.DISK is created.
- Rule VD: Upon creation of an object OB.AD by a subject S.DISK, the TSF shall assign the value of the attribute AT.ID of S.DISK to the security attribute AT.ID of OB.AD.
- Rule KEY: Upon creation of an object OB.KEY by a S.DISK, the TSF shall assign the value of the attribute AT.ID of S.DISK to the security attribute AT.ID of OB.KEY.
- Rule DU: Upon creation of an object OB.UD, the TSF shall assign the value referencing the associated encryption key (OB.KEY) to the security attribute AT.ID of OB.UD.

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

Application note

The value of the security attribute AT.ID shall be specified in the product security target in conformance with this protection profile. For example, this value can corresponds to a hash of the user passphrase allowing to activate the disk.

For OB.UD, this requirement simply expresses the fact that ciphered user data (OB.UD) are implicitly associated to the used encryption key (OB.KEY).

FMT_MSA.1/Disk_Status Management of security attributes

FMT_MSA.1.1/Disk_Status The TSF shall enforce the **TOE access control policy** to restrict the ability to **modify** the security attributes **S.DISK.STATUS** to **the TSF itself**.

Application note

No subject is authorized to configure the security attribute S.DISK.STATUS as ACTIVATED.

FMT_MSA.1/ID Management of security attributes

FMT_MSA.1.1/ID The TSF shall enforce the **TOE access control policy** to restrict the ability to **modify** the security attributes **OB.UD.ID, OB.KEY.ID, OB.AD.ID and S.DISK.ID** to **the TSF itself**.

Application note

No subject is authorized to configure security attributes OB.UD.ID, OB.KEY.ID, OB.AD.ID and S.DISK.ID.

FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the **TOE access control policy** on **subjects, objects and operations identified by this table:**

Subjects	TSF, S.API, S.DISK
Objects	OB.KEY, OB.UD, OB.AD
Operations	CREATE, MOUNT, DISMOUNT, USE, DECIPHER, CIPHER, ERASE

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **TOE access control policy** to objects based on the following:

Type	Element	relevant security attributes(s)
Subjects	TSF, S.API, S.DISK	AT.ID, and AT.STATUS (for S.DISK)
Objects	S.DISK, OB.KEY, OB.UD, OB.AD	AT.ID

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

Rule	Operation	Condition
Rule1	The TSF is allowed to CREATE a S.DISK and the associated OB.KEY and OB.AD	no condititon
Rule2	a subject S.DISK is allowed to MOUNT a S.DISK	The user is authenticated by the TSF based on OB.AD, the values of security attributes S.DISK.ID and OB.AD.ID are the same and the value of the security attribute S.DISK.STATUS is DEACTIVATED
Rule3	a subject S.API is allowed to DISMOUNT a S.DISK	the value of the security attribute S.DISK.STATUS is ACTIVATED
Rule4	a subject S.API is allowed to USE an object OB.KEY	the values of the security attributes S.DISK.ID and OB.KEY.ID are the same and the value of the security attribute S.DISK.STATUS is ACTIVATED
Rule5	a subject S.API is allowed to CIPHER, DECIPHER, ERASE an object OB.UD	the values of the security attributes OB.KEY.ID and OB.UD.ID are the same and S.API is allowed to USE OB.KEY (cf. Rule4)
Rule6	a subject S.DISK is allowed to ACCESS an object OB.AD	The user is authenticated by the TSF based on OB.AD and the values of the security attributes S.DISK.ID and OB.AD.ID are the same

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

- **Rule7: The TSF shall perform DISMOUNT operation on S.DISK after [selection: completion of [assignment: operation], [assignement: time interval of user inactivity], [assignement: other condition]] provided the value of the security attribute S.DISK.STATUS is ACTIVATED.**
- **[assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects]**.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the **following rule(s):**

- **[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]**.

Application note

The TSF forbids the access to data of a ciphered disk (CIPHER, DECIPHER and ERASE) if this disk was not activated by an authentication using the object OB.AD associated to the disk.

The author of a ST which is compliant with this profile will have to specify the conditions under which the TOE operation is ended (so determining the deactivation of all disks).

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's cryptographic requirements ([CRYPTO] and [CRYPTO_GESTION])**.

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects: **cryptographic keys and any sensible user data**.

Non-editorial refinement:

"Resource" stands for any memory (e.g. RAM) and "deallocation" occurs upon DISMOUNT of the disk by the user.

5.1.2 Requirements applicable to the PP with key generation

Besides the previous TOE requirements, the configuration « with key generation » includes the requirements below.

5.1.2.1 Requirements bound to the key generation

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment: cryptographic key generation algorithm]** and specified cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **DCSSI's cryptographic requirements ([CRYPTO] and [CRYPTO_GESTION])**.

Application note

The generation mentioned can be a derivation from authentication data.

5.2 Security assurance requirements

Assurance requirements are applicable to both configurations without change. The evaluation assurance level of this protection profile is EAL3 augmented by ALC_FLR.3 and AVA_VAN.3 according to the standard level qualification process defined in [QUA-STD].

6 Rationales

6.1 Security objectives / security problem

6.1.1 Threats

T.DATA_ACCESS

The TOE records on the disk user sensitive data (asset D.USER_DATA) under a ciphered form (object OB.UD). Thus, the asset protection is the protection of the ciphered data.

This threat is countered by O.RECORDED_DATA_PROTECTION which ensures the confidentiality of recorded data (ciphered) on the disk. O.ROBUSTNESS also contributes to counter this threat by ensuring that no data user is recorded, even temporarily, in plain text on the disk.

On the other hand, O.USER_DEACTIVATE ensures that the user can explicitly protect his data by disabling the disk in which they are stored.

Finally, O.CRYPTO ensures that operated cryptographic functions and cryptographic keys management which are used, enable to prevent unauthorized access to disk data by cryptanalysis. The quality of used keys is ensured by this objective.

In the case of the configuration « with key generation », O.ENCRYPTION_KEYS ensures the availability of cryptographic keys as well as the quality of their generation (being able to generate keys which it needs, according to DCSSI cryptographic referentials, the TOE is ensured that they will be available and of quality) leading so to cryptanalysis resistance of user data ciphered on the disk.

In the case of the configuration « without key generation », the availability of encryption keys used by the TOE as well as the quality of their generation is ensured by the objective on the environment OE.OPERATIONAL_ENV.3. In addition, OE.OPERATIONAL_ENV.4 ensures the confinement and the protection (integrity, confidentiality and authenticity) of keys outside of the TOE and during their transmission to the TOE.

In both configuration cases, keys management quality is ensured by O.CRYPTO.

In other words, OE.OPERATIONAL_ENV.3 and OE.OPERATIONAL_ENV.4 cover, in the case of « without key generation » configuration, nearly the same security aspects than the objective O.ENCRYPTION_KEYS in the case of « with key generation »configuration.

T.MEMORIES_ACCESS

This threat is covered by the objective O.USER_DEACTIVATE which ensures the unavailability of sensitive data, in particular in working memories, after the shut-down by the user of the application.

6.1.2 Organisational security policies (OSP)

OSP.CRYPTO

This OSP is directly covered by the objectives O.CRYPTO and O.ENCRYPTION_KEYS in the case of « with key generation » configuration. In the configuration « without key generation», the security objective O.ENCRYPTION_KEYS is replaced by the two following objectives on the environment: OE.OPERATIONAL_ENV.3 and OE.OPERATIONAL_ENV.4

OSP.NON_REMANENT_2

This organisational policy is directly covered by the objective OE.NON_REMANENT_2 which ensures the implementation by the operational environment of measures against the remanence.

6.1.3 Assumptions

6.1.3.1 Assumptions applicable to both configurations

A.OPERATIONAL_ENV

This assumption is directly covered by OE.OPERATIONAL_ENV.1 and OE.OPERATIONAL_ENV.2.

When the TOE is operating and when a rightful user has activated a disk, the client workstation applications are freely likely to handle data included into this disk. The objective OE.OPERATIONAL_ENV.1 ensures that those applications don't create any copies of these data on the same support as the disk without user being aware of it, and in a general manner that the client workstation cannot be the source of a data confidentiality loss.

OE.OPERATIONAL_ENV.2 ensures that the rightful users are aware and trained to the correct security practices so that they access their sensitive data only when they are in a reliable environment. Therefore, the users participate to the trust which we can give to the TOE operational environment.

A.NON_REMANENT_1

This assumption is directly covered by OE.NON_REMANENT_1 which ensures the absence of remanence into the working memories of the product.

6.1.3.2 Assumptions applicable to the configuration without key generation

A.KEYS_OPERATIONAL_ENV

This assumption is directly covered by OE.OPERATIONAL_ENV.3 and OE.OPERATIONAL_ENV.4.

6.1.4 Coverage between problem definition and security objectives

Threats	Security objectives	Rationale
T.DATA_ACCESS	O.ROBUSTNESS, O.RECORDED_DATA_PROTECTION, O.CRYPTO, O.ENCRYPTION_KEYS, O.USER_DEACTIVATE, OE.OPERATIONAL_ENV.3, OE.OPERATIONAL_ENV.4	Section 6.1.1
T.MEMORIES_ACCESS	O.USER_DEACTIVATE	Section 6.1.1

Table 1 Mapping threats to security objectives

The Table 1 concerns the « with key generation » configuration. In the case of the « without key generation » configuration, according to the rationale, the security objective O.ENCRYPTION_KEYS is replaced by the both following objectives on the environment: OE.OPERATIONAL_ENV.3 and OE.OPERATIONAL_ENV.4.

Security objectives	Threats
O.USER_DEACTIVATE	T.DATA_ACCESS, T.MEMORIES_ACCESS
O.CRYPTO	T.DATA_ACCESS
O.RECORDED_DATA_PROTECTION	T.DATA_ACCESS
O.ROBUSTNESS	T.DATA_ACCESS
O.ENCRYPTION_KEYS	T.DATA_ACCESS
OE.OPERATIONAL_ENV.1	
OE.OPERATIONAL_ENV.2	
OE.NON_REMANENT_1	
OE.NON_REMANENT_2	

Table 2 Mapping security objectives to threats

The Table 2 is about the « with key generation » configuration. In the case of the « without key generation » configuration, according to the rationale, the security objective O.ENCRYPTION_KEYS is no more applicable and the (greyed out) line relative to this objective must be replaced by the both following lines:

OE.OPERATIONAL_ENV.3	T.DATA_ACCESS
OE.OPERATIONAL_ENV.4	T.DATA_ACCESS

Organisational security policies (OSP)	Security objectives	Rationale
OSP.CRYPTO	O.CRYPTO, O.ENCRYPTION_KEYS	Section 6.1.2
OSP.NON_REMANENT_2	OE.NON_REMANENT_2	Section 6.1.2

Table 3 Mapping organisational security policies to security objectives

The Table 3 concerns the « with key generation » configuration. In the case of the « without key generation » configuration, according to the rationale, the security objective O.ENCRYPTION_KEYS is replaced by the both following objectives on the environment: OE.OPERATIONAL_ENV.3 and OE.OPERATIONAL_ENV.4.

Security objectives	Organisational security policies (OSP)
O.USER_DEACTIVATE	
O.CRYPTO	OSP.CRYPTO
O.RECORDED_DATA_PROTECTION	
O.ROBUSTNESS	
O.ENCRYPTION_KEYS	OSP.CRYPTO
OE.OPERATIONAL_ENV.1	
OE.OPERATIONAL_ENV.2	
OE.NON_REMANENT_1	
OE.NON_REMANENT_2	OSP.NON_REMANENT_2
OE.OPERATIONAL_ENV.3	
OE.OPERATIONAL_ENV.4	

Table 4 Mapping security objectives to organisational security policies

The Table 4 concerns the « with key generation » configuration. In the case of the « without key generation » configuration, according to the rationale, the security objective O.ENCRYPTION_KEYS is no more applicable and the (greyed out) line relative to this objective must be replaced by the both following lines:

OE.ENV_OPERATIONNEL.3	OSP.CRYPTO
OE.ENV_OPERATIONNEL.4	OSP.CRYPTO

Assumptions	Security objectives for the operational environment	Rationale
A.OPERATIONAL_ENV	OE.OPERATIONAL_ENV.1, OE.OPERATIONAL_ENV.2	Section 6.1.3
A.NON_REMANENT_1	OE.NON_REMANENT_1	Section 6.1.3
A.KEYS_OPERATIONAL_ENV	OE.OPERATIONAL_ENV.3, OE.OPERATIONAL_ENV.4	Section 6.1.3

Table 5 Mapping assumptions to security objectives for the operational environment

The greyed out line of Table 5 only applies to the « without key generation » configuration. Other lines apply to both configurations.

Security objectives for the operational environment	Assumptions
OE.OPERATIONAL_ENV.1	A.OPERATIONAL_ENV
OE.OPERATIONAL_ENV.2	A.OPERATIONAL_ENV
OE.NON_REMANENT_1	A.NON_REMANENT_1
OE.NON_REMANENT_2	
OE.OPERATIONAL_ENV.3	A.KEYS_OPERATIONAL_ENV
OE.OPERATIONAL_ENV.4	A.KEYS_OPERATIONAL_ENV

Table 6 Mapping security objectives for the operational environment to assumptions

The greyed out lines in table 6 only apply to the « without key generation » configuration. Other lines apply to both configurations.

6.2 Security requirements / security objectives

6.2.1 Objectives

6.2.1.1 Security objectives for the TOE

Objectives applicable to both configurations

O.USER_DEACTIVATE

This objective is covered by the requirements which define the access control policy FDP_ACC.1, FDP_ACF.1 and the unavailability policy of residual data FDP_RIP.1 which ensure that:

- A user can explicitly deactivate a disk,
- The deactivation effectively protects data because, in accordance with the access control policy of the TOE, disk data are only accessible if the disk state is *ACTIVATED*,
- The disk deactivation by the user involves sensitive data deletion.

O.CRYPTO

This objective is covered by FCS_COP.1, which ensures that all cryptographic operations shall be in compliance with requirements of DCSSI cryptographic referentials for the standard robustness level ([CRYPTO] and [CRYPTO_GESTION]).

O.RECORDED_DATA_PROTECTION

The TOE records user sensitive data (D.USER_DATA) under a ciphered form (object OB.UD) on the disk . The asset protection is therefore the protection of these ciphered data.

Access control (FDP_ACC.1 and FDP_ACF.1) ensures that only objects which are accessible at the fixed time are associated to an activated disk. In addition, this control forces the encryption of user data recorded on the disk (without which the protection could not be effective).

On the other hand, the requirements bound to mandatory authentication of a user before activation of a disk (FIA_UID.1 and FIA_UAU.1) ensure that only the rightful user checks access to data which are recorded. The access itself doesn't require authentication (FIA_UID.1).

Finally, the definitive association, to a given disk (S.DISK), of recorded user sensitive data (OB.UD) and authentication data (OB.AD, OB.KEY) enabling his authentication, avoids information « leakage » from a disk to another one without any activation of the disks. Indeed, all of these objects and subjects are connected by a security attribute AT.ID definitely fixed during their creation (FMT_MSA.3, FMT_MSA.1/Disk_Status and FMT_MSA.1/ID).

O.ROBUSTNESS

This objective is covered by the requirements which ensure that any interruption of the TOE which is accidental (FPT_FLS.1), automatic or intentional (FDP_ACF.1), let the TOE, and especially data protected by the TOE, in a secure state, that is to say a state where the disks in question are deactivated; in other words, encryption keys are not accessible out of operation.

Objectives applicable to the configuration with key generation

O.ENCRYPTION_KEYS

This objective is directly covered by the requirement FCS_CKM.1.

6.2.2 Coverage between objectives and security requirements

Security objectives	Functional requirements for the TOE	Rationale
O.USER_DEACTIVATE	FDP_ACC.1, FDP_ACF.1, FDP_RIP.1	Section 6.2.1
O.CRYPTO	FCS_COP.1	Section 6.2.1
O.RECORDED_DATA_PROTECTION	FDP_ACF.1, FIA_UID.1, FIA_UAU.1, FMT_MSA.3, FMT_MSA.1/Disk_Status, FMT_MSA.1/ID, FDP_ACC.1	Section 6.2.1
O.ROBUSTNESS	FPT_FLS.1, FDP_ACF.1	Section 6.2.1
O.ENCRYPTION_KEYS	FCS_CKM.1	Section 6.2.1

Table 7 Mapping security objectives for the TOE to functional requirements

The greyed out line in table 7 only applies to the « with key generation » configuration. Other lines apply to both configurations.

Functional requirements for the TOE	Security objectives
FIA_UID.1	O.RECORDED_DATA_PROTECTION
FIA_UAU.1	O.RECORDED_DATA_PROTECTION
FPT_FLS.1	O.ROBUSTNESS
FMT_MSA.3	O.RECORDED_DATA_PROTECTION
FMT_MSA.1/Disk_Status	O.RECORDED_DATA_PROTECTION
FMT_MSA.1/ID	O.RECORDED_DATA_PROTECTION
FDP_ACC.1	O.USER_DEACTIVATE, O.RECORDED_DATA_PROTECTION
FDP_ACF.1	O.USER_DEACTIVATE, O.RECORDED_DATA_PROTECTION, O.ROBUSTNESS
FCS_COP.1	O.CRYPTO
FDP_RIP.1	O.USER_DEACTIVATE
FCS_CKM.1	O.ENCRYPTION_KEYS

Table 8 Mapping functional requirements to security objectives for the TOE

The greyed out line in table 8 only applies to the « with key generation » configuration. Other lines apply to both configurations.

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/Disk_Status, FMT_MSA.1/ID
FMT_MSA.1/Disk_Status	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1
FMT_MSA.1/ID	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1
FDP_ACC.1	(FDP_ACF.1)	FDP_ACF.1
FDP_ACF.1	(FDP_ACC.1) and (FMT_MSA.3)	FMT_MSA.3, FDP_ACC.1
FCS_COP.1	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1
FDP_RIP.1	No dependency	
FIA_UID.1	No dependency	
FIA_UAU.1	(FIA_UID.1)	FIA_UID.1
FPT_FLS.1	No dependency	
FCS_CKM.1	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_COP.1

Table 9 Functional requirements dependencies

The greyed out line in table 9 only applies to the « with key generation » configuration. Other lines apply to both configurations.

6.3.1.1 Rationale for unsatisfied dependencies

The dependency FMT_SMR.1 of FMT_MSA.3 is not satisfied. This dependency is not required because the model does not use the role notion.

The dependency FMT_SMF.1 of FMT_MSA.1/Disk_Status is not satisfied. The TOE does not manage a management function. This dependency is therefore not required.

The dependency FMT_SMR.1 of FMT_MSA.1/Disk_Status is not satisfied. This dependency is not required because the model does not use the role notion.

The dependency FMT_SMF.1 of FMT_MSA.1/ID is not satisfied. The TOE does not manage a management function. This dependency is therefore not required.

The dependency FMT_SMR.1 of FMT_MSA.1/ID is not satisfied. This dependency is not required because the model does not use the role notion.

The dependency FCS_CKM.4 of FCS_COP.1 is not satisfied. The keys destruction phase is not included into the scope of the TOE; therefore this requirement does not need to be satisfied.

The dependency FCS_CKM.4 of FCS_CKM.1 is not satisfied. The keys destruction phase is not included into the scope of the TOE; therefore this requirement does not need to be satisfied.

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 necessary in conformance 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 necessary in conformance 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 according to the standard level qualification process defined in [QUA-STD].

6.5 Rationale for 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].

Additional description of the TOE and its environment

This appendix is informative.

A.1 Application domain

The term « disk » shall be understood as any **persitent mass memory**, independently from the underlying electronic support (USB key, RAMDisk, *etc.*).

We shall also speak about « support » to define the hardware which hosts the disk.

Table 11 introduces different data allocation units of a disk viewed as a data storage space, from the largest to the most reduced units.

Table 11 : Allocation units

Name	*Definition*	*Scope of the PP*
Complete disk	The physical disk, without distinction of different potential platters (RAID disks).	Included
Partition	Division of the disk in different pseudo-disks. At the BIOS level. For example, Windows identifies partitions and disks under the name of « volume ».	Included
Sub-partition	Only exist on some OS (for example, *slices* of the BSD systems). Below the file system.	Included
Directory	At the level of the OS file system. For example, the OS of the Unix family do not distinguish between directories and (sub-)partitions.	Included
Files group	Files group « marked » on one way or another, generally an attribute of the file, managed by the TOE or the OS. The notion of group is independent from the hierarchy of the file system.	Included
File	Contains user data and is identified by a name.	Out of scope
Cluster	Allocation unit of the files management system. The cluster is generally an abstraction of the sector.	Out of scope
Sector	Elementary allocation unit of a formatted disk containing the useful data.	Out of scope
Track	For a disk, data contained on a circumference of a disk platter. Typically, a track contains sectors, informations of disk management (number of sector, CRC of sector, number of track, etc.), spaces intersectors (GAP) and space of the track end (GAP) not normally containing useful informations.	Out of scopet

The TOE relative to this PP is an application which ciphers in a transparent way (« on-the-fly ») one or several allocation units among the five biggest: disk, partition, sub-partition, directory or files group. In this PP it is called, by a stretch of language, « disk » the space of storage ciphered by the TOE, regardless of the type of allocation unit in question.

An application offering « RAM disks » which record ciphered data into an OS file, but display them to the user as separate disks, is also included within the framework of this profile.

It is important to not confuse this disk notion with the encryption logical unit used by cryptographic algorithms of the application. For example, the TOE can cipher complete partitions, but by cluster or by sector, by using a derivated key for every cluster or every sector. The encryption logical unit only impacts the evaluation of the product (vulnerability analysis) and its implementation.

A.2 TOE usage

A.2.1 Safe analogy

To better understand the TOE usage, it can be useful to compare an on-the-fly encryption application to a safe or to a strengthened cupboard. The first objective of a safe is to protect, **once closed,** its contents against the theft. Likewise, an encryption application aims to protect software data once these are ciphered and once the disk is « deactivated ».

To put the analogy further, during day, when the staff is present in premises, the safe may be opened and its contents handled by persons present. The access to the safe contents is then regulated by organisational and hardwre measures (access control to the premises containing the safe, monitoring cameras, *etc.*). Therefore it clearly seems that the safe provided protection is not related to data under use but it is only related to data during their storage (data recorded on the disk). In particular, this means that safe security critical aspects are about its opening and its closing:

- Who can open it? In what circumstances?
- Who can close it? In what circumstances?
- What is it about?

In the same way, it is possible that a disk encryption application doesn't protect recorded data once this disk is « activated » or when they are handled by an application (in the workstation memory). In particular, disk sharing questions are often within the scope of operating system rights management or the scope of network management. Although it is not excluded that the application also integrates such mechanisms, those mechanisms are not included into the scope of the TOE.

A.2.2 Authentication keys and authentication data

Authentication data enable users (and eventuals administrators) to be authenticated towards the TOE to either activate a disk or configure it.

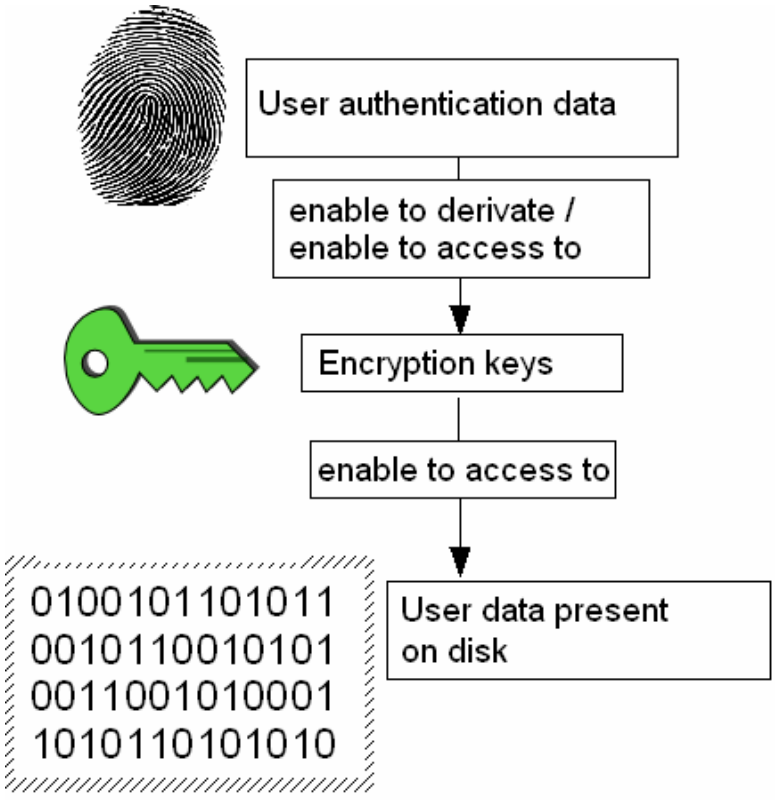

Figure 2 : Illustrative principle of disk activation.

Keys are cryptographic data used by the TOE to cipher (and decipher) data recorded on the disk.

The knowledge of some of these keys gives access to the disk contents or to a part of this disk, regardless of the TOE, and the knowledge of authentication data gives access to keys[2].

The distinction between both notions relies on the following properties:

- Authentication data are normally known by the user whereas keys have only to be known by the TOE.
- Authentication data should be easily modifiable (for example, a change of password should not require to cipher again all the disk), it is not the case for keys.
- Authentication data are only occasionally used (notably to activate the disk) whereas encryption keys stay on memory to decipher data when it is requested by an authenticated user.

In practice, relation between those data can be extremely variable from an implementation to another one. Thus, authentication data can either be used to directly derivate the encryption key or only be used for cipher (decipher) the disk encryption key, *etc.* In the first case, a change of authentication data will require to « transcipher » the disk while in the second case, only the disk encryption key will have to be « transciphered ».

A.2.3 TOE operation

The TOE is a transparent intermediary between applications used by a user for handle his data (reading, modification, backup), and the storing support containing the ciphered disk.

[2] According to the Kerchoff's principle, we suppose that the relation between authentication data and keys is an information known by the attacker.

The user explicitly interacts with the TOE under only two ways: when he is accessing the ciphered disk for the first time by activating the disk and when he explicitly deactivates the disk.

The disk activation requires the user authentication. Once activated, nothing distinguishes the ciphered disk to other mass memories to which the user has access.

In operation mode, the TOE ciphers (respectively, deciphers) in a transparent way for the user, the recorded data (respectively, read) on the disk. Encryption process features depend on the implementation (primitives and cryptographic algorithms, keys size, *etc.*).

A.3 TOE functionalities

The TOE main functionality is to protect the confidentiality of recorded data on a persistent mass storage memory to cope with the theft of a support or a machine containing it, while enabling an authenticated user to access them:

- Confidentiality protection of data stored on the disk

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

- Authentication
  - o User authentication

A.3.1 Services provided by the TOE

Confidentiality protection of sensitive data stored on the disk

The main service provided by the TOE is the confidentiality protection of sensitive data recorded on the disk. This confidentiality protection shall notably apply to temporary versions of data managed by other applications or by the operating system of the machine.

A.3.2 Services required for the TOE correct operation

User authentication

The use of the disk encryption application requires a prior user authentication (for example, through the entry of a passphrase). This authentication allows to activate the disk and to access the data which are stored.

A.4 Elements related to the design

A.4.1 TOE physical and logical scope

The TOE defined in this PP runs on any type of IT hardware having a persistent storing memory (possibly removable). The users authentication procedure and the TOE operation (encryption and decryption) can call upon specific hardware (USB keys, smart cards, *etc.*) according to the implementation but this PP puts no particular requirement relative to hardware which is outside of the TOE.

In addition, it will be assumed that applications hosted on the machine can be configured so that they can back up user data in a transparent way on the persistent memory protected and managed by the TOE.

A.4.2 About the configurations

Both configurations introduced into this document aim to cover two types of current products while keeping a maximum of flexibility for the security target writing: « single-station » products which generate themselves encryption keys, and « big organization » products which run in cooperation with a centralized keys server, for example being able to act as escrow (cf. following section).

In every case, the principle is to ensure a sufficient quality level of generated keys so that the TOE can counter the threat of disk theft. In the case of the « with generation » configuration, keys generation algorithms are included into the scope of the TOE and are therefore evaluated with the product; in the case of « without generation » configuration, the assumptions redaction explicitly indicate the keys generation importance, and it is reasonable to think that the user will have to rely on a trusted product, possibly independently certified.

A.5 Additional services

This section introduces various additional services likely to be implemented by a product in conformance with this PP.

A.5.1 Auto-lock

The product automatically deactivates the disk after an inactivity time limit defined by a security administrator during initial configuration. A user re-authentication is then required to activate again the disk.

This type of mechanism provides the capability to improve data protection either in the case of a more or less prolonged user absence far from its workstation or in the case of a user neglect of disk desactivation. Some implementations are coordinated with other similar softwares, such as the screensaver of the host machine.

A.5.2 Escrow and recovery

Within the context of a professional use, data recovery can be as important as their protection. Products then offer the possibility to export one or several escrow keys or recovery keys for a remote storage. The purpose is to ensure the availability of those data in the following cases:

- loss/neglect of authentication data by the user,
- on request within the organization body (in case of letter of request, for example).

Recovery solutions can be various. For example, it can be a plaintext export of encryption keys or of users authentication data enabling their storage on another support. It can also be an encryption on the disk of encryption keys copies thanks to of a escrow key.

At an organizational level, it is important to exactly define the roles of different actors who are involved in the recovery procedure, notably to avoid the bypass of this procedure by attackers (*i.e.* an attacker having stolen a disk making himself out to be a rightful user at the recovery service).

A.5.3 Backup

Data encryption is sometimes opposed to backup requirements[3]. The product can provides or not the capability to backup ciphered data (disk image) or to backup plain text data (what means having several users on the same disk).

A.5.4 Roles management

The product can distinguish various users categories for allocate to them specific rights. Within the context of a deployment, of an administration or of a company, persons which install, which configure and which use a workstation can be different (system administrator, security administrator, user), and the product can reflect this tasks separation by distinguishing following roles:

- **User:** machine user who has some data to be protected in confidentiality on the machine persistant mass memory.
- **System and network administrator:** administrator in charge of the machine. He configures machine parameters (user accounts and volume names for example), but he does not install nor configure the encryption application.
- **Security administrator:** administrator in charge of installation and configuration of the encryption application. The security administrator defines data which must be ciphered and in which place.

Among the exclusively controllable parameters by one of those roles, let us quote:

- the keys size and the nature of encryption algorithms used by the product,
- the control by the product of the quality of authentication data chosen by users (minimal size, presence of non-alphanumeric characters, *etc.*)
- the mandatory renewal of keys or authentication data after a specific period
- the possibility to deactivate or not the product
- the workstation configuration, as the fact that *swap* partitions are under the control of the TOE, the management of the temporary files by client applications, the deactivation of the stand-by mode of the host machine...

A.5.5 Secure deletion

The TOE specified in this profile describes a data deletion operation on an activated disk. A product can specify requirements relative to data secure deletion applying to this operation, for example to ensure the impossibility to review assumed deleted data.

In the same idea, it can be necessary to define a procedure which specify how and conditions under which a security administrator shall destroy in an irreversible way data contained on the user disk. For example, this procedure may be applied in the case of a user left or a user resignation from the organization, or this procedure may be applied when the disk is allocated to a new usage or a new user. The way data are destroyed or made unavailable can rely on mechanisms of the product as, for example, disk transciphering or disk deletion by systematic destruction (noise).

These requirements can be express by using the component FDP_RIP.2 (*Full residual information protection*).

[3] Thus, ciphered data do not generally enable to incrementaly back up data in an effective way.

Annex B Definitions and acronyms

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

B.1 Abbreviations and acronyms

BIOS	*Basic Input Output System*
CC	*Common Criteria*
EAL	*Evaluation Assurance Level*
IT	*Information Technology*
OS	*Operating System*
OSP	*Organisational Security Policy*
PP	*Protection Profile*
RAID	*Redundant Array of Independent Disks*
SFR	*Security Function Requirement*
ST	*Security Target*
TOE	*Target Of Evaluation*

B.2 Definitions

Target Of Evaluation (TOE)

The product to evaluate and its associated documentation.

Security Target (ST)

Document used as a reference for the evaluation of the TOE: the certificate delivered (by the DCSSI) will prove the conformance of the product and its documentation with the requirements specified into the security target.

Disk

Persistent mass memory containing data ciphered by the TOE.

Disk image

Set of (ciphered) data in the persistent mass memory.

Machine

Equipment which hosts the persitent mass memory encryption application (laptop computer, network server, *etc.*).

Device

Physical device hosting the persistent mass memory. The support is not totally necessarily under the control of the TOE, that is the protected memory can only form part of this support.

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. http://www.ssi.gouv.fr/fr/sciences/publications
[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. http://www.ssi.gouv.fr/fr/sciences/publications
[AUTH]	Authentification : Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard. DCSSI. http://www.ssi.gouv.fr/fr/sciences/publications
[QUA-STD]	Processus de qualification d'un produit de sécurité – niveau standard. Version 1.1, 18 march 2008. N°549/SGDN/DCSSI/SDR.
[PP-CDISK]	Protection profile « Application de chiffrement de données à la volée sur mémoire de masse », version CC 3.0.

Index