Direction centrale de la sécurité des systèmes d'information

Protection Profile Electronic Signature Verification Module

Date	**:**	July 17th, 2008
Reference	**:**	PP-MVSE-CCv3.1
Version	**:**	1.6

Courtesy Translation

Courtesy translation of the protection profile registered and certified by the French Certification Body under the reference DCSSI-PP-2008/06.

Table of Contents

Table of Figures

Table of Tables

1 Introduction

This section provides general information necessary for the registration of the protection profile.

The Section 1.1 "Identification" provides the instructions related to the labeling and the registration of the protection profile (PP).

The Section 1.2 "Protection profile overview" provides an overview of the protection profile, thus allowing the potential user to decide the utility of the protection profile.

1.1 Identification

Title	Protection Profile – Module of Verification for Electronic Signature
Author	Trusted Labs
CC Version	V3.1 Revision 2
Reference	PP-MVSE-CCv3.1
Version	1.6
Key words	electronic signature verification, electronic signature

Table1 Protection profile identification

1.2 Protection Profile overview

This protection profile was elaborate for the French governemental information security authority (Direction Centrale de la Sécurité des Systèmes d'Information, DCSSI) in order to ease the certification of applications of signature verification usable in particular for the development of the electronic administration. This protection profile allows to present all the common security objectives for sponsors of electronic signatures applications. It allows the application providers to edit security targets compliant with expectations of the sponsors of applications and to set the basis of security interoperability.

This protection profile is compliant with the recommendations of the DCSSI for the *qualification standard* process for security products. By making this protection profile available to the product vendors, the DCSSI thus wishes to facilitate and optimize the development, the use and the appreciation of the confidence of the signature verification applications.

This protection profile defines security requirements for a module which is used for electronic signatures verification application. It allows to fulfill the requirements of article 5 (Chapter II: Des dispositifs de vérification de signature électronique) of French decree 2001-272 of March 30th, 2001. The requirements of this decree referring more particularly to the signature verification when performed under the direct control of a person, it is important to note that this protection profile considers in an equivalent way the signature verification performed by an automated system or by a person.

Although the certification of the signature verification application is required to benefit from the presumption of reliability according to the French decree n°2001-272 of the March 30th,

2001, it is recommended to apply to such a certification in order to improve the security of the whole chain of signature and to have complementary evidence in the event of dispute of the signature showing that the used signature method is not reliable (i.e. in the case of a third party providing a contrary proof questioning the presumption of reliability of the signature).

1.3 Definitions and acronyms

The definitions of the various terms used in this document are provided in Appendix A.

The acronyms used in this document are defined in Appendix B.

1.4 References

[CC1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1, Revision 1, September 2006.
[CC2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1, Revision 2, September 2007.
[CC3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements. Version 3.1, Revision 2, September 2007.
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1, Revision 2, September 2007.
[QUA-STD]	Processus de qualification d'un produit de sécurité – Niveau standard. Version 1.1, 18 mars 2008. N°549/SGDN/DCSSI/SDR.
[CRYPT-STD]	Cryptographic mechanisms – Rules and recommendations about the choice and the parameter's sizes of cryptographic mechanisms with standard robustness level. DCSSI. http://www.ssi.gouv.fr/fr/sciences/publications.html
[AUTH-STD]	Authentification - Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse *standard*. DCSSI. http://www.ssi.gouv.fr/fr/sciences/publications.html
[KEYS-STD]	Gestion de clés - Règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques de niveau de robustesse *standard*. DCSSI. http://www.ssi.gouv.fr/fr/sciences/publications.html
[CWA 14169]	Secure signature-creation devices “EAL 4+”, CEN/WS, Mars 2004.
[CWA 14170]	Security requirements for signature creation applications, CEN/WS, May 2004.
[CWA 14171]	General guidelines for electronic signature verification, CEN/WS, May 2004.
[TS 101 733]	Electronic signature formats, ETSI standard, version 1.5.1, 15 december 2003.

2 TOE Overview

The purpose of this part of the protection profile is to describe the target of evaluation (TOE), the type of product which it represents as well as the general functionalities that it supports. Moreover this part presents the target of evaluation for an electronic signature verification application.

The target of evaluation (TOE) is a software or hardware module allowing the verification of electronic signatures.

2.1 Users

The module of electronic signature verification can indifferently be called upon by a person or by an automated system (a calling application).

The term "**Verifier**" used in article 5 of the French decree of the March 30th, 2001 (2001-272) corresponds to a human person who uses a signature verification device evaluated and certified.

In this protection profile, the term "verifier" will include also the case where the verifier is a calling application, although this case is out of the scope of the decree. From the point of view of the requirements stated in this protection profile, no difference will be made between the two possible types of verifiers.

Application note

From a practical point of view, the developers shall be able to define the users of their product as being:

- a person,
- an automated system,
- or indifferently one or the other.

2.2 Signature Policies

In order to understand the various use cases, it is recommended to define what a signature policy is.

According to the ETSI, a signature policy is a set of rules for the creation or the validation of electronic signatures, under which electronic signatures can be determined valid.

It includes rules defining the signature attributes which must be provided by the signatory, as well as rules related to the use of Trusted Third Parties (CA, OSCP servers, time-stamping authorities,...).

A signature policy contains the following elements:

- The identification of one or more "trusted points" and the rules allowing to build a certification path between the signatory's certificate and one of these trusted points;
- Means to obtain a time reference intended to position in time the signature of the signatory (e.g. by time-stamping);

- Means to verify the revocation status of each certificate of the certification path with this time reference;
- The attributes which the signatory's certificate must contain (e.g. OID of the certification policy, *QCStatements*, *key usage*, etc);
- Types of attributes which, in addition to the reference of the signatory's certificate, must be signed jointly with the document (e.g. reference to a signature policy, type of engagement, supposed date of signature, format of the document, supposed role of the signatory, supposed place of signature, etc);
- The set of validation data that the signatory must provide;
- Means to obtain a time reference intended to position in time the validation data (e.g. by time-stamping);
- Cryptographic algorithms (signature and hash) to use within the framework of the digital signature verification of the document and the validation data.

This protection profile defines the minimal set of rules that any compatible module will have to support. For the verification of electronic signatures, the TOE will be able to exert only one subset of all possible rules according to the parameter setting defined by the applied signature policy.

2.3 Use cases

Two use cases are considered: the initial verification and the subsequent verification.

The Initial verification

The initial verification corresponds to a first verification of the electronic signature performed within a time as short as possible after the reception of the electronic signature by the verifier.

The TOE is used in order to perform the control of the electronic signature according to a signature policy chosen by the verifier (cf section 2.4.2) to ensure that the electronic signature is valid. During this operation the validation data necessary to the verification of the signature either are found in the electronic signature or collected by other means. These validation data include a time reference attesting the existence of the digital signature on a specified date. The validity of the other validation data is in particular controlled with respect to this reference date.

The Subsequent verification

The subsequent verification corresponds to a verification of the electronic signature based on the validation data collected during the initial verification by applying a signature policy chosen by the verifier. This verification is performed whereas the time reference (e.g. a time-stamp token) positioning the digital signature in time is still valid.

Note: a third type of verification should be considered if the time reference attached to the digital signature and/or the validation data during the initial verification are no more valid. This type of verification would imply a storing and/or a maintenance of the pieces of evidence. This third use case is not covered by this protection profile.

2.4 Usage and major security features of a TOE

The TOE comprises following functional components:

- The component managing the interaction with the user,
- The component of selection of the signature policy to be applied,
- The component controling the invariance of the document's semantics,
- The component executing the viewer applications of documents,
- The component collecting and processing the validation data,
- The component of verification of digital signatures,
- The component of administration of the signature policies.

2.4.1 Component managing the interaction with the user

Two types of users are considered:

- The Verifier, and
- The Security administrator of the TOE.

It should be noted that the role of administrator of the host platform is different from the role of security administrator of the TOE.

2.4.1.1 Interaction with the verifier

The TOE contains an interface with the verifier.

According to the type of user defined for the TOE, this interface could be a man-machine interface (MMI), a programming interface (API), or a conjunction of both.

This interface allows the following interactions:

- Selection of the document to be verified by the verifier,
- Selection of a signature policy to be applied,
- Communication/presentation of the signature attributes to the verifier,
- Communication of the execution status at the end of the verification process,
- Communication of the validation data to the verifier.

Selection of the document to be verified by the verifier

The TOE offers a means to the verifier enabling him to indicate which document and which electronic signatures he wishes to verify.

Selection of a signature policy to be applied

The TOE offers a means to the verifier allowing him:

- to explicitly select a signature policy to be applied (selected signature policy), or
- to use the signature policy referenced in the electronic signature.

Communication / presentation of the signature attributes to the verifier

The TOE offers a means allowing the verifier to consult the signature attributes present in the electronic signatures.

Communication of the execution status at the end of the verification process

The TOE has a means enabling to communicate the execution status of the verification process to the verifier.

Export of the validation data to the verifier

The TOE has a means enabling to export the validation data used during the verification of the electronic signatures to the verifier.

This allows the verifier to backup (out of the TOE) these data for a later use.

2.4.1.2 Interaction with the Security administrator

This interface is either a man-machine interface (MMI) or a programming interface (API) allowing the security administrator to interact with the TOE. It should be noted that the role of security administrator of the TOE is distinct from the role of host administrator (see *A.Host_platform* assumption).

This interface allows the security administrator:

- to manage the signatures policies (addition/deletion).
- to define the viewer applications to execute according to the supported formats of document
- to initialize the configuration setting allowing to inactivate the function of execution of a viewer application (when the TOE is intended to be used by a machine)

2.4.2 Component of selection of the signature policy to be applied

The controls operated by the module of verification depend on a signature policy.

The TOE determines the signature policy applied in the following way:

- If a signature policy has been explicitly selected by the verifier, then this selected signature policy will be applied, even if a signature policy is referenced in the electronic signature. If the policy referenced by the electronic signatures is different from the signature policy applied, the TOE informs the verifier.
- If the signature policy has not been defined by the application calling the TOE, then the applied signature policy will be the policy referenced in the electronic signature, if such a reference is present. The referenced policy will then be returned to the application calling the TOE in order to verify if necessary that the policy is appropriate for the context of operations.
- If no signature policy were preselected and if no signature policy is referenced in the electronic signatures, then either this constitutes an error, or a default signature

policy will be applied and will have to then be returned to the application calling the TOE in order to verify if necessary that the policy is appropriate for the context of operations.

2.4.2.1 Component controlling the invariance of the document's semantics

A document to be signed can contain variable fields or active code which depends on external parameters and which thus can be different according to the context where the document is viewed. A signatory could thus sign an electronic document whose contents may vary according to the context where it is viewed.

This can mislead the verifier who receives the signature. He could view a document semantically different from the one displayed to the signatory.

Thus, the contents of the documents must be controlled to attest that its semantics does not depend on external parameters.

The TOE relies on an external module to perform this test; the control of the invariance of the semantics of the document is thus out of the evaluation scope.

The TOE must nevertheless inform the verifier:

- when the external module detects that the document's semantics is not invariant,
- when the external module detects that the document's semantics is invariant,
- when the external module is unable to control the invariance of the document's semantics.

Application note

In the absence of qualified external application for controlling the semantics invariance, it is recommended that the product integrates an internal module allowing this control and that this module belongs to the TOE. Only format with contents that cannot vary by construction must be supported.

The product can claim compliance with the requirements of this PP but:

- the security target must contain threats, assumptions, OSP, security objectives and security requirements related to the existence of this module of control,
- the TOE must validate only the documents of the supported format.

2.4.3 Component executing the document viewer applications

To allow a human verifier or an operator supervising an automated system of signature verification to assess the contents of a document during the verification of the electronic signature, the TOE must allow, on request of the verifier/operator, the execution of an application of presentation corresponding to the format of the document.

For this purpose, the TOE defines the formats of document for which it is able to execute an external viewer application. The correspondence between these formats and the viewer applications are defined by the administrator of the TOE. The viewer applications are out of the TOE scope.

A configuration setting, initialized by the security administrator of the TOE, allows to deactivate the execution of the viewer application, for example to facilitate its integration within an automatic process where the view of the signed documents by an operator is not required.

Application note

In the absence of qualified viewer applications, it is recommended that the product integrates an internal module to view the documents. In such a case, this module must be included into the TOE scope. The product can claim compliance with the requirements of this PP but the security target must contain threats, assumptions, OSP, security objectives and security requirements related to the existence of this viewer module.

The provision of the viewing function is necessary for all the products whatever they are intended to be integrated in an automated process or to be used by a person. In the case of the use in an automated process, the product could be configured in order to deactivate this functionality.

2.4.4 Component collecting and processing the validation data

In compliance with the applied signature policy, this component provides the following functions:

- Verification of the compliance of the signed attributes,
- Positioning of the digital signature in time,
- Construction of a valid certification path,
- Verification of the validity of the certification path.

These functions are implemented in an iterative way as long as a valid certification path could not be constructed.

Verification of the compliance of the signed attributes

The TOE ensures the presence and the compliance of all the signed attributes required by the signature policy.

Examples of verifications:

- Type of engagement is among the types of engagement authorised for this policy
- ...

Positioning of the digital signature in time

To be able to verify the validity of the signatory's certificate as well as other validation data and, *in fine*, to verify the validity of the electronic signatures, the TOE must position the digital signature of the document in time.

"To position the digital signature in time" means "to attest its existence (as a data) on a date provided by a trusted time reference".

The signature policy must define the means to use to position the digital signature in time.

The behavior of the TOE varies according to the modes of use of the TOE:

- In the mode "initial verification", if a "time reference" is not already present, the TOE collects one of them, in accordance with the signature policy.

- In the mode “subsequent verification”, the TOE uses the time reference specified during the initial verification, if provided. It verifies that it is compliant with the signature policy. If the time reference is not compliant or is missing, the electronic signature is declared invalid[1]. This PP doesn’t deal with filing issue and the durability in the time of this first positioning as well as the data used.

Verification of the certificate's compliance

From the reference of the signatory’s certificate contained in the signed attributes, the TOE must ensure that the certificate which will be used as the end of the certification path corresponds to this reference.

Moreover, the characteristics of this certificate must satisfy the requirements of the signature policy.

For examples:

- To control that the identifier of the certification policy of the signatory’s certificate is included in the list defined in the signature policy;
- To control the usage of the private key (*key usage*);
- To control the presence and the value of the extensions necessary for the certificate (*QCstatements*).

Construction of a valid certification path

To ensure the authenticity and the validity of the signatory’s certificate when the digital signature was positioned in time, the TOE searches for a valid certification path between the signatory’s certificate and a trusted point identified in the signature policy.

Two behaviors are possible whether the TOE is performed in “initial verification” mode or in “subsequent verification” mode:

- Initial verification

  In this mode, the TOE implements the functions required by the rules defined in the signature policy until construction of a valid certification path.

  During the construction of the path, the TOE imports validation data (from the network or locally ...) and controls that they are valid according to rules defined in the applied signature policy.

  If it proves that no path can be constructed or that all the constructed paths are invalid, then the electronic signature is declared invalid.

  If it proves that data are not available to attest that an element of the path is not revoked, then the verification is declared incomplete and an initial verification could be reiterated later on.
- Subsequent verification

  In the mode “subsequent verification”, the TOE reconstructs a path and verifies its validity only from the data collected during the initial verification.

  If it proves that no path can be constructed with the available data or if all the paths being able to be constructed with these same data are not valid, then the electronic signature is declared invalid.

[1] In few cases, for example if the time mark is a time-stamp token, the time mark can be not anymore valid because the certificate of the timestamping authority is expired. In that case, it is the responsibility of the verifier to check the validity of the timestamping authority certificate during the signature has been positionned in time.

If it misses data to attest that an element of the certification path is not revoked, then the electronic signature is declared invalid.

According to the cases, the collection of validation data can use network protocols or local accesses to data. The means used to access the data (client applications for the network access or device drivers for local access) are outside of the TOE scope.

The verification of the validity of an element in the certification path consists in checking:

- The integrity and the authenticity of the origin of the element using its associated signature;
- that the date contained in the time reference specified in the signature is included in the validity period of this element;
- the element was not revoked at the date contained in the time reference specified in the digital signature.

All these operations are performed in compliance with the technical elements defined in the signature policy applied.

Verification of the validity of the certificate

The TOE verifies that the certificate is valid by using the time reference specified in the digital signature and the validity period defined in the certificate.

2.4.5 Component of verification of digital signatures

This component is a cryptographic component supporting the algorithms (hash and verification of signature) necessary to the verification of the digital signatures implied in the verification process.

The digital signatures to be verified are, among others:

- The digital signature of the document,
- Digital signatures contained in the certificates constituting the certification path,
- The digital signature of the autosigned root certificate (trusted point),
- Digital signatures associated with the collected validation data (CRL, OCSP answers, ARL,...)

2.4.6 Component of administration of the signature policies

The TOE allows an authenticated administrator to manage all the signature policies supported by the TOE.

Application note

The administration functions supported by the TOE shall be defined by the authors of security targets.

They shall be able to include either none, or some, or all the following functions:

- the addition of a policy,
- the deletion of a policy.

2.5 Available non-TOE hardware/software/firmware

The elements of the technical environment of the TOE are the following:

- The operating system of the physical machine(s) running the TOE;
- A software and/or hardware device allowing to present the document to the verifier and alerting him if its characteristics are not completely compatible with the display characteristics required by the document (use of color, presence of the necessary fonts, etc...) ;
- A software component and/or hardware controlling the invariance of the document's semantics (verifies that its semantics does not depend on external parameters).
- The software or hardware components providing the validation data

These elements are shown in figure 1.

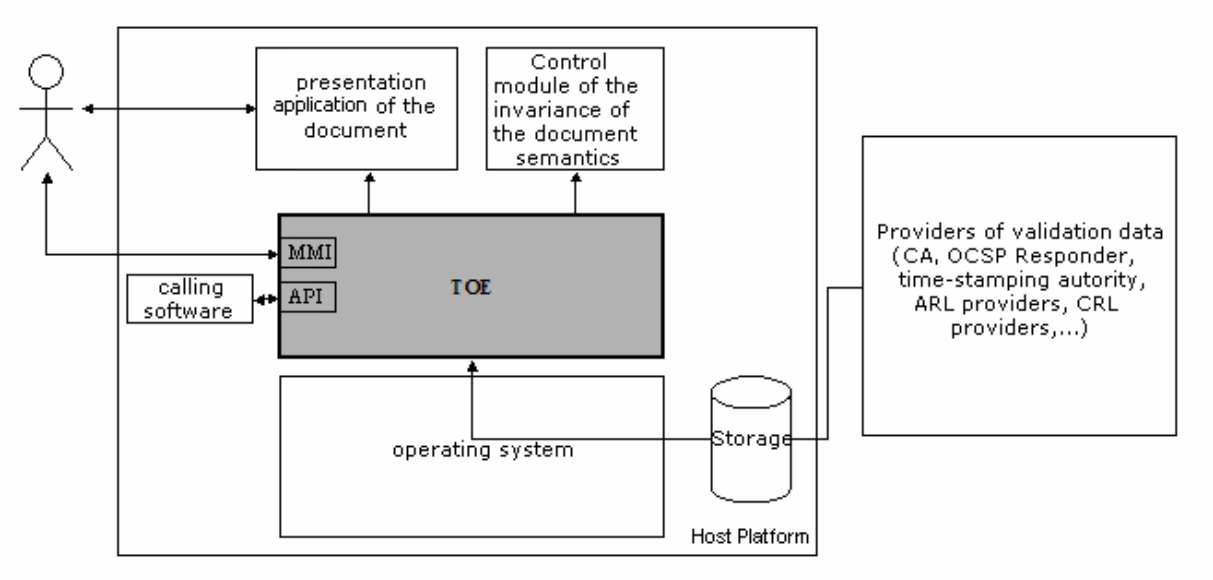

Figure1: The TOE in its environment of use

3 Conformance Claims

This chapter contains the following sections:

CC conformance claim (3.1)

Package claim (3.2)

PP claim (3.3)

Conformance statement (3.4)

3.1 CC conformance claim

This protection profile claims strict conformance with the Common Criteria version 3.1.

It was written in accordance with:

- CC Part 1 [CC1],
- CC Part 2 [CC2],
- CC Part 3 [CC3],
- and the CC evaluation methodology [CEM].

3.2 Package claim

This PP claims conformance with the assurance package defined by the *qualification standard* process [QUA-STD].

3.3 PP claim

This PP does not claim conformance with any other PP.

3.4 Conformance statement

The conformity required for the Security Targets and Protection Profiles which claim conformance with this Protection Profile is **demonstrable** according to the definition in CC Part 1 [CC1].

4 Security Problem Definition

4.1 Assets

This section describes the assets to be protected by the TOE.

4.1.1 User Data

4.1.1.1 Input Data

D.Document

This document is the document signed by the signatory and for whom the TOE must verify the signature.

It can be provided to the TOE either in the same file where the signature is or in an independent file.

Protection: integrity

D.Signature

The electronic signature of a signatory on the document.

Protection: integrity

D.Signed_Attributes

The signed attributes are data signed at the same time as the document. They provide further information to the verifier related to the signature and the circumstances in which it was performed.

The signed attributes include:

- The nonambiguous reference of the signatory‘s certificate or the signatory‘s certificate itself

In option:

- The signature policy or a reference to this one,
- The type of commitment of the signatory,
- The presumed or certified role of the signatory,
- The presumed date and hour of signature,
- The presumed place of signature,
- The format of the document,
- ...

Protection: integrity

D.Validation_Data_In_input

The validation data are the data useful for the verification, they can include:

- The signatory’s certificate,
- Certificates of CA, of CRL publishers, of OCSP servers, of time-stamping units,...
- Certificate Revocation Lists (CRL),

- o OCSP answers,
- o Authority Revocation Lists (ARL)
- o Time-stamping tokens

Protection: integrity

Application note

These data can be obtained from several manners:

- o they can be obtained from a remote server (on a local or open network),
- o they can be stored locally on the machine where the verification is performed,
- o they can be stored within the signature (according to the format).

4.1.1.2 Work data

D.Hash_Data_tobe_Verified

The data to be verified formatted are the data to which the signature relates (signed document and attributes), once hashed by the TOE.

Protection: integrity

4.1.1.3 Output data

D.Return_Status

After the verification, the TOE returns a verification status which depends on the result.

- o Valid signature: all the elements necessary are present and correct.
- o Invalid signature: one or more are incorrect.
- o Incomplete validation: data were not available during the verification.

In the case of the initial verification, an incomplete validation must be considered by the verifier either like an invalid signature, or like the possibility of trying a new initial verification later on. In the case of the subsequent verification, an incomplete validation must be considered by the verifier like an invalid signature.

Protection: integrity

D.Validation_Data_In_Output

The validation data in output are the validation data processed by the TOE.

They are returned by the TOE to the verifier for later use.

These data can be complete or not. If they are, then they could be used for a subsequent verification. Otherwise, they could be re-used and enriched for a new initial verification.

Protection: integrity

4.1.2 TOE sensitive assets (TSF data)

D.Services

This asset represents the executable code implementing the provided services.

The code of the TOE must be protected in integrity.

Protection: integrity

D.Verification_Rules

The main component of the TOE consists of an engine checking rules defined in a signature policy.

The executable code establishing these rules in the application requires a protection in integrity.

Protection: integrity

D.Signature_Policies

The signature policies define the rules to be applied to verify a signature.

The TOE supports one or more signature policies. The list of the signature policies, which is managed by the administrator of the TOE, must be protected in integrity. Moreover, the integrity of each signature policy must also be controlled.

Protection: integrity

Application note

According to the implementations, the signature policies accepted by the TOE can be in two forms:

- in the form of executable code (sequence of execution of rules and decision trees)
- on the one hand in the form of interpretable files (1) by the TOE, and on the other hand in the form of executable code necessary to its interpretation. In this case various formats can be indifferently used: standardized, based on ASN.1 or XML, or proprietary.

D.Data_Representations_Association

The internal data of the module often have a representation different from those displayed to the user or transfered to the module.

The correspondence between the external representation and the internal representation of the same data requires to be protected in integrity.

Ex 1: the type of engagement (ex: “read and approved”) of the signatory could be internally represented by a OID whereas it is displayed explicitly to the signatory in the interface. Ex 2: the format of the document entered in the TOE can also be internally represented in the form of an OID.

Protection: integrity

D.DocFormat_Application_Association

This asset is a parameter managed by the TOE which allows it to decide which external viewer application to execute according to the format of the document having to be displayed to the verifier.

The integrity of this asset must be protected.

Protection: integrity

Application note

The format of the document is:

- either provided by the verifier,
- or present in the signature as a signed attribute.

4.2 Roles / Subjects

S.Verifier

The TOE can be called upon by a person (via MMI) or a calling application (via API). The verifier concerns the entity using the functions of the TOE to verify a signature.

S.Security_Administrator

The security administrator of the TOE is responsible of the following operations:

- o if the TOE allows the configuration of the signature policies, it maintains the signature policies usable (addition, deletion)
- o manages the association between the formats of document and the applications allowing their view from the verifier
- o manages the list of the document formats guaranteeing the invariance of the document's semantics.

Application note

The role of Security Administrator of the TOE is well distinguished from the role of administrator of the host platform on which the TOE is installed (see the *A.Host_Platform* assumption).

4.3 Threats

This section describes the threats to be countered by the TOE. Because all the security objectives are justified by assumptions and OSPs, the statement of the threats is not necessary. In this case the section is not applicable, and is considered as fulfilled.

4.4 Organisational security policies (OSP)

This section defines the rules applicable to the TOE.

4.4.1 Policies related to the application of a signature policy

P.Signatory_Certificate_Validity

The TOE must control that the signatory's certificate was valid at the time when the signature was positioned in time.

P.Signed_Attributes_Conformity

The TOE must control:

- o that the signed attributes are compliant with the signature policy to be applied, and
- o that all the signature attributes required by the signature policy are present.

P.Signatory_Certificate_Conformity

The TOE must control that all the certificates of the certification path (including the signatory's certificate) are compliant with the signature policy to be applied.

P.Signatory_Certificate_Authenticity

The TOE must control that a valid certification path (1) exists between the signatory's certificate and a trusted point referenced in the signature policy.

(1) The existence of such a validation path proves the authenticity of the signatory's certificate compared to the root certificate (trusted point).

P.Validation_Data_Authenticity/Integrity

The TOE must control the authenticity of the origin and the integrity of the validation data provided.

4.4.2 Communication of the signed attributes

P.Signed_Attributes_Communication

The TOE must allow the signed attributes to be communicated to the verifier.

4.4.3 Presentation of the document to the verifier

P.Document_Presentation

The TOE shall allow the verifier to view the signed document (French Decree 2001-272, Art 5 subparagraph c).

Application note

An administrator of the TOE shall be able to deactivate this feature, for the case where the verifier is a machine (see political P.Administration).

P.Document_Stability_Control

The TOE must inform the verifier if the document's semantics can not or could not be considered as being invariant.

4.4.4 Compliance with standards

P.Hash_Algorithms

The hash algorithms implemented in the TOE must not allow to create two documents producing the same hash.

The algorithms must comply with the DCSSI cryptography requirements [CRYPT-STD].

P.Signature_Algorithms

The supported cryptographic algorithms and the lengths of the keys implemented in the TOE must resist during the validity period of the public-key certificates of these keys.

The algorithms must comply with the DCSSI cryptography requirements [CRYPT-STD].

Application note

The keys used must comply with the DCSSI key management requirements [KEYS-STD].

4.4.5 Export of the validation data

P.Validation_Data_Export

The TOE must allow the verifier to export the validation data used during the verification.

4.4.6 Miscellaneous

P.Administration

The TOE must allow the Security administrator to manage:

- the signature policies [D.Signature_Policy] (to add/remove)
- the table of correspondence between the viewer applications and the document formats in input of the TOE [D.DocFormat_Application_Association].
- deactivate the viewing function of the signed document.

4.5 Assumptions

This section describes the assumptions on the operational environment of the TOE.

A.Host_Platform

It is presumed that the host platform on which the TOE is installed is either directly under the verifier's responsibility or under the responsibility of a legal person or a natural person who guarantees to him that the following measures are applied.

The operating system of the host platform is presumed to offer contexts of execution separated for the various tasks performed.

In addition, it is presumed that the following security measures are implemented:

- the host platform is protected against viruses;
- the data exchange between the host platform and other IT elements via an open network are controlled by a firewall;
- the access to the administration functions of the host platform is restricted to the administrators of the platform (thereafter the “Host administrator”). The user account is different from the host administrator account;
- the installation and the update of the software of the host platform is under the control of the host administrator;
- the operating system of the host platform does not allow the execution of untrusted applications.

Application note

1) The role of host administrator is distinct from the role of security administrator of the TOE.

2) This assumption covers threats where computing process would come to perturb the execution of the services of the TOE and for example to modify the user data such as the certificates and validation data when they are under his control.

A.Signature_Policy_Origin

The origin of the signature policies usable by the TOE is presumed to be authentic.

Application note:

1) This assumption is justified as follows:

To verify the authenticity of the origin of a signature policy, it would be necessary for example to verify the signature associated by its transmitter. With this intention, it would then be necessary to use another signature policy where the authenticity of the origin would remain to prove... This process would be without end.

2) This assumption is automatically filled if the TOE does not use interpreted policies of signature but fixed policies.

A.Document_Presentation

It is presumed that the host platform on which the TOE is installed has one or several viewer applications which:

- o either accurately display the document to be signed,
- o or warn the verifier of possible problems of incompatibilities between the viewer application and the characteristics of the document.

In the case of a countersignature, it is presumed that the signatory has a means at least of knowing the identity of previous signatories and at best of verifying these signatures.

A.Document_Stability_Control

It is presumed that the environment of the TOE provides a module able to determine if the semantics of the signed document is invariant and to communicate the status of this control to the TOE.

A.Services_Integrity

The environment of the TOE is presumed to provide to the Security administrator the means of controlling the integrity of the services and of the parameters of the TOE.

A.Validation_Data_Access

The TOE must have - or to have access to - all the validation data necessary to the verification of the signature of a document according to the signature policy to be applied.

A.Trusted_Security_Administrator

The Security administrator of the TOE is supposed to be trusted, to be trained with the use of the TOE and to have the means necessary to the performance of his tasks.

Application note:

The assumptions must be realistic with respect to the product and its environment. If those are not realistic and cannot be refined into recommendations of usage in the product guidance, then the security target of the product which claims complaince with this PP must transcript them as threats, and corresponding security objectives and requirements.

5 Security Objectives

5.1 Security Objectives for the TOE

5.1.1 General objectives

O.Administration

The TOE shall allow the security administrator to manage:

- the signature policies (to add/remove),
- the table of association between the viewer applications and the document formats in input of the TOE,
- the deactivation of the viewing function of the signed document.

5.1.2 Objectives on the verification rules

O.Time_Reference

In accordance with the signature policy to be applied, the TOE shall ensure the presence of a trusted time reference which allows to attest the existence of the digital signature on a specified date.

Application note

Trusted time reference means here any means allowing to obtain a time reference in a secure way for the context of use of the TOE. This means is defined by the signature policy.

A trusted time reference can for example be:

- a time-stamping stamp signed by a trusted entity, in compliance with the signature policy,
- a mark of time provided by a trusted actor, in compliance with the signature policy.

O.Certification_Path

The TOE shall control that a valid certification path exists between:

- the signatory's certificate whose reference is provided in the signed attributes, and
- a trusted point specified in the signature policy.

O.Certificates_Conformity

The TOE must verify that the certificates of the certification path (including the signatory's certificate) is compliant with the requirements of the signature policy to be applied.

O.Certificates_Validity

In compliance with the RFC 3280, chapter 6.1, and in compliance with the signature policy to be applied, for each certificate of the certification path (including the signatory's certificate), the TOE will have to verify:

- the integrity and the authenticity of the origin of the certificate;

- o that the certificate was valid when the digital signature was positioned in time;
- o that the certificate was not revoked when the digital signature was positioned in time.

O.Validation_Data_Conformity

The TOE must verify that the validation data provided to verify the signature are compliant with the requirements of the signature policy to be applied, in particular that they are signed by their transmitter (integrity and authenticity of the origin).

Application note

The signature of the provided validation data allows to guarantee at the same time the integrity of these data and the authenticity of their origin, in compliance with the signature policy to be applied.

O.Signed_Attributes_Conformity

The TOE must verify the presence and the compliance of the signed attributes with the signature policy.

5.1.3 Objectives related to the display of the signed data

O.Presentation_Application_Execution

The TOE shall be able to execute external applications allowing the verifier to view the document whose signature is to be verified. For that it will be based on the indication of the format of the document provided in the electronic signatures to verify.

A configuration setting shall allow an administrator of the TOE to deactivate this function during the installation of the TOE if the user is an appliance.

O.Signed_Attributes_Communication

The TOE shall allow to communicate the signed attributes to the verifier.

Application note

This objective applies the same way to the cases where the user is a person and where it is a calling application and whatever the means used to communicate them: a man-machine interface (MMI) or a programming interface (API).

O.Validation_Data_Export

The TOE shall allow the exportation of the validation data used during the verification to the verifier.

5.1.4 Objectives related to the control of invariance of the semantics of the document to be verified

O.Document_Stability_Control

For each document to be verified, the TOE shall execute an external module controlling if the document's semantics is invariant.

The TOE shall inform the verifier according to the result transmitted by this module (invariant semantics, variant semantics or control failure).

5.1.5 Compliance with the standards

O.Cryptographic_Operations

The TOE shall implement cryptographic algorithms having the following properties:

- the hash algorithms must not make it possible to create two documents producing the same hash.
- the supported cryptographic algorithms and the lengths of the keys implemented in the TOE must resist during the validity period of the public-key certificates of these keys.

The algorithms must comply with the DCSSI cryptography requirements [CRYPT-STD].

Application note

The keys used must comply with the DCSSI key management requirements [KEYS-STD].

5.2 Security Objectives for operational environment

OE.Signature_Policy_Origin

The administrator of the TOE shall verify the authenticity of the origin of the signature policies before importing them into the TOE.

OE.Host_Platform

The host platform on which the TOE is installed shall be either directly under the responsibility of the verifier or under the control of a legal person or a natural person who guarantees that the following measures are actually applied.

The operating system of the host platform shall provide separated contexts of execution for the various tasks which it performs.

In addition, the following security measures shall be implemented:

- the host platform must be protected from viruses;
- the data exchange between the host platform and other IT elements via an open network must be controlled by a firewall;
- the access to the administration functions of the host platform must be restricted to the administrators of the platform (thereafter the “Host administrator”). The user account must be different from the Host administrator account;
- the installation and the update of the software of the host platform must be under the control of the Host administrator;
- the operating system of the host platform must not allow the execution of untrusted applications.

Application note

The role of Host administrator mentioned above is distinct from the role of Security administrator of the TOE.

OE.Document_Presentation

The host platform on which the TOE is installed shall have viewer applications which:

- either accurately display the document to be signed,
- or warn the verifier of possible problems of incompatibilities between the viewer application and the characteristics of the document.

OE.Document_Stability_Control

The environment of the TOE shall provide a module able to determine if the semantics of the signed document:

- o either is invariant
- o or is not invariant
- o or could not be controled (for example if the document format is not supported).

This module shall communicate the status of the control to the TOE.

OE.Validation_Data_Provision

The environment of the TOE shall provide the validation data necessary to the verification of the signature.

OE.Services_Integrity

The environment of the TOE shall provide to the Security administrator the means of controlling the integrity of the services and of the parameters of the TOE.

OE.Trusted_Security_Administrator

The security administrator of the TOE shall be trusted, shall be trained with the use of the TOE and shall have the means necessary to the performance of his activity.

6 Security Requirements

6.1 Security Functional Requirements

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

- *Editorial Refinement* (term defined in [CC1]): refinement in which a minor modification is performed on a requirement element, like the rewording of a phrase of a requirement for correctness with English grammar. This modification does not change the meaning of the requirement.
- *Refinement*: refinement which allow to add points or to limit the set of acceptable implementations for a requirement element or for all the requirement elements of a component.

The following table lists the subjects, the objects, the operations and their security attributes used in the functional security requirements statement.

Subject	Object / Information	Operation	Security attributes
the Verifier	a signed document	To import the document	the Verifier: - signature policy **the signed document:** - document's stability status
the Verifier	the electronic signature (the signature and the associated signed attributes) and the signed document	import of the electronic signature	the Verifier: - applied signature policy **the electronic signature:** - signature policy - commitment type - claimed role - presumed signature date and time - presumed signature location **the signed document:** - the signed document's content format
the Verifier	the time reference applied to the signature	import of the time reference	the Verifier: - applied signature policy **the time reference applied to the signatory's electronic signature:** - the root keys applicable to verify the time-stamp tokens - time-stamping unit certificate - any needed certificate between the certificate and the root key
- the Verifier	- the certificates belonging to a certification path - the revocation data needed to validate the certification path	import of the certificates and the revocation data	the Verifier: -applied signature policy **the certificates belonging to a certification path** - key usage - QCStatement - the electronic signature status = "correct" - the validity period of the certificate the time reference - certification policy

Subject	Object / Information	Operation	Security attributes
- the Verifier	- validation status "correct signature"	communication of the status to the verifier	validation status: - signatory's public key - document's hash - document's electronic signature

6.1.1 Control during the importation of the document

FDP_IFC.1/Document acceptance Subset information flow control

FDP_IFC.1.1/Document acceptance The TSF shall enforce the **document acceptance information flow control policy** on

- **subjects: the verifier,**
- **information: a signed document**
- **operation: to import the document**

FDP_IFF.1/Document acceptance Simple security attributes

FDP_IFF.1.1/Document acceptance The TSF shall enforce the **document acceptance information flow control policy** based on the following types of subject and information security attributes:

- **subjects: the verifier (signature policy, [assignment: verifier's attributes]),**
- **information: the signed document (document's stability status, [assignment: any other document's attributes])**.

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

Import of the document:

- **either the document's stability status equals "stable", or**
- **the document's stability status is "unstable" or "uncontrolled" but the signature policy allows to bypass the control and the verifier explicitly acknowledges to bypass the control**

The Verifier should be informed only if the document's semantics is unstable.

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

FDP_IFF.1.4/Document acceptance The TSF shall explicitly authorise an information flow based on the following rules:

- **controls succeed**

- **or controls bypassed**.

FDP_IFF.1.5 / Document acceptance The TSF shall explicitly deny an information flow based on the following rules:

- **controls fail**
- **and controls cannot be bypassed**.

Application note

The TOE shall provide means:

- to execute an external module controlling if the document's semantics is invariant,
- to warm the signatory if the document's semantics is not invariant.

FDP_ITC.1 / Document acceptance Import of user data without security attributes

FDP_ITC.1.1 / Document acceptance The TSF shall enforce the **document acceptance information flow control policy** when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.1.3 / Document acceptance The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **determine whether the document's semantics is invariant or not by invoking a dedicated external module**.

Refinement:

The TOE shall inform the verifier when the document's semantics is unstable or cannot be checked.

Application note

The document semantics could vary for example if the document includes fields or active code that uses information external to the document.

FMT_MSA.3 / Document's acceptance Static attribute initialisation

FMT_MSA.3.1 / Document's acceptance The TSF shall enforce the **document acceptance access control policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

Refinement:

If the signature policy does not explicitly include a parameter specifying what to do in case the document is not detected as stable, then the default behavior will be to stop the signature process when the document is not detected as stable.

FMT_MSA.3.2/Document's acceptance [Editorial Refinement] The TSF shall allow **nobody** to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.1/Document's semantics invariance status Management of security attributes

FMT_MSA.1.1/Document's semantics invariance status [Editorial refinement] The TSF shall enforce the **document acceptance access control policy** to restrict the ability to **modify** the security attribute **document's stability status** to **nobody**.

FMT_SMF.1/Getting document's semantics invariance status Specification of Management Functions

FMT_SMF.1.1/Getting document's semantics invariance status The TSF shall be capable of performing the following management functions:

- **invoking an external module to get the status indicating whether the document's semantics is invariant or not**.

6.1.2 Presentation of the signed document

FMT_MTD.1/Document format/viewer association table Management of TSF data

FMT_MTD.1.1/Document format/viewer association table The TSF shall restrict the ability to **modify** the **document format/viewer association table** to **the administrator**.

FMT_SMF.1/Management of the document format/viewer association table Specification of Management Functions

FMT_SMF.1.1/Management of the document format/viewer association table The TSF shall be capable of performing the following management functions:

- **an administrator of the TOE shall be permitted to manage the document format/viewer association table**.

FMT_MTD.1/Viewer activation parameter Management of TSF data

FMT_MTD.1.1/Viewer activation parameter The TSF shall restrict the ability to **initialize** the **viewer activation parameter** to **the administrator**.

Global refinement:

This configuration parameter initialization shall be performed upon the TOE installation.

FMT_SMF.1/Management of the viewer activation parameter Specification of Management Functions

FMT_SMF.1.1/Management of the viewer activation parameter The TSF shall be capable of performing the following management functions:

- **the TOE installation procedure shall include the initialization the viewer activation parameter**.

6.1.3 Signature policies

6.1.3.1 Selection of the signature policy to be applied

FMT_MTD.1/Selection of the applied signature policy Management of TSF data

FMT_MTD.1.1/Selection of the applied signature policy The TSF shall restrict the ability to **select** the **applied signature policy** to **the verifier**.

FMT_SMF.1/Selection of the applied signature policy Specification of Management Functions

FMT_SMF.1.1/Selection of the applied signature policy The TSF shall be capable of performing the following management functions:

- **the verifier shall be permitted to select the signature policy to be applied**.

6.1.4 Verification of the signature

The following requirements are related to the verification process of the signature of a document.

6.1.4.1 Importation of the electronic signature and of the signed attributes

The following requirements are related to the importation of the electronic signature and of the signed attributes.

FDP_IFC.1/Electronic signature Subset information flow control

FDP_IFC.1.1/Electronic signature The TSF shall enforce the **electronic signature information flow control policy** on

- **subjects: the verifier,**
- **information: the electronic signature (the electronic signature and related signed attributes, and the signed document)**
- **operation: import of the electronic signature (i.e. acceptance as signed attributes conforming to the signature policy)**.

Application note

Authorizing the import the electronic signature and related signed attributes means that signed attributes meet the rules defined in the applied signature policy.

FDP_IFF.1/Electronic signature Simple security attributes

FDP_IFF.1.1/Electronic signature The TSF shall enforce the **electronic signature information flow control policy** based on the following types of subject and information security attributes:

- **subjects: the verifier (applied signature policy, [assignment: other verifier's attributes, if any])**
- **information: the electronic signature (signature policy, commitment type, claimed role, presumed signature date and time, presumed signature location, [assignment: list of supported signed attributes]) and the signed document (the signed document's content format, [assignment: list of document's attributes])**.

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

Signature import:

- **launch the document viewer corresponding to the document's format, according to the document format/viewer association table, if the viewer activation parameter is set;**
- **inform the verifier if the referenced signature policy is not the applied signature policy, when the electronic signature includes a reference to a signature policy.**
- **if the signed attribute "signature policy" is present in the electronic signature, then its value is conformant to the signature policy;**
- **if the signed attribute "commitment type" is present in the electronic signature, then its value is conformant to the signature policy;**
- **if the signed attribute "claimed role" is present in the electronic signature, then its value is conformant to the signature policy;**
- **if the signed attribute "presumed signature date and time" is present in the electronic signature, then its value is conformant to the signature policy;**

- o **if the signed attribute "presumed signature location" is present in the electronic signature then its value is conformant to the signature policy**
- o **[assignment: any other supported rule on signed attributes]**.

FDP_IFF.1.3/Electronic signature The TSF shall enforce the **other rules explicitly defined in the Signature SFP**.

FDP_IFF.1.4/Electronic signature The TSF shall explicitly authorise an information flow based on the following rules:

- o **the signed attributes are compliant with the Signature SFP**
- o **and the signed document is stable**.

FDP_IFF.1.5/Electronic signature The TSF shall explicitly deny an information flow based on the following rules:

- o **the signed attributes are not compliant with the Signature SFP**
- o **or the signed document is unstable**.

Application note

The TOE shall provide means:

- to execute an external module controlling if the document's semantics is invariant

FMT_MSA.3/Electronic signature Static attribute initialisation

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

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

FMT_MSA.1/Electronic signature Management of security attributes

FMT_MSA.1.1/Electronic signature The TSF shall enforce the **electronic signature access control policy** to restrict the ability to **modify** the security attributes **signature and its signed attributes** to **nobody**.

FDP_ITC.2/Electronic signature Import of user data with security attributes

FDP_ITC.2.1/Electronic signature The TSF shall enforce the **electronic signature information flow control policy** when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.2.3/Electronic signature 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/Electronic signature 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/Electronic signature The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

- **invoke an external module in charge of controlling the document's semantic invariance (using 1/ the signed document's content format provided by the electronic signature and 2/ the documents' content itself).**
- **transmit the result of the module's analysis to the verifier**.

6.1.4.2 Importation of a valid time reference

FDP_IFC.1/Time reference Subset information flow control

FDP_IFC.1.1/Time reference The TSF shall enforce the **time reference acceptance information flow control policy** on

- **subjects: the verifier,**
- **information: the time reference applied to the signature**
- **operation: import of the time reference**.

FDP_IFF.1/Time reference Simple security attributes

FDP_IFF.1.1/Time reference The TSF shall enforce the **time reference acceptance information flow control policy** based on the following types of subject and information security attributes:

- **subjects: the verifier (applied signature policy, [assignment: other verifier's attributes, if any])**
- **information: the time reference applied to the signatory's electronic signature (attributes: the root keys applicable to verify the time-stamp**

tokens, time-stamp unit certificate, any needed certificate between the certificate and the root key).

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

Operation: import of the time reference applied to the signatory's electronic signature:

- **the key usage of the time-stamping unit certificate indicates that this certificate is only usable for timestamping purposes**
- **there exists a certification path between the time-stamping unit certificate and a root certificate dedicated to the verification of time-stamping tokens**
- **each rule applied to the previously mentioned certification path defined in requirement *FDP_IFF.1/Certification path* is met for the date/time included in the time reference**.

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

FDP_IFF.1.4/Time reference The TSF shall explicitly authorise an information flow based on the following rules:

- **controls succeed**.

FDP_IFF.1.5/Time reference The TSF shall explicitly deny an information flow based on the following rules:

- **controls fail**.

FMT_MSA.3/Time reference Static attribute initialisation

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

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

FMT_MSA.1/Time reference Management of security attributes

FMT_MSA.1.1/Time reference The TSF shall enforce the **time reference acceptance access control policy** to restrict the ability to **modify** the security attributes **of the time reference** to **nobody**.

FDP_ITC.2/Time reference Import of user data with security attributes

FDP_ITC.2.1/Time reference The TSF shall enforce the **time reference acceptance information flow control policy** when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.2.3/Time reference 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/Time reference 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/Time reference The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **[assignment: additional importation control rules]**.

6.1.4.3 Importation of a valid certification path

The following requirements are related to the verification rules which apply on the certificates of a certification path and allowing to determine if the certification path is valid or not.

Certificates

FMT_MSA.1/Certificates Management of security attributes

FMT_MSA.1.1/Certificates The TSF shall enforce the **certification path acceptance information flow control policy** to restrict the ability to **modify** the security attributes **of the imported certificates** to **nobody**.

Validation data of the certificates

FMT_MSA.1/Certificates validation data Management of security attributes

FMT_MSA.1.1/Certificates' validation data The TSF shall enforce the **certification path acceptance information flow control policy** to restrict the ability to **modify** the security attributes **of the certificates' revocation data** to **nobody**.

Miscellaneous

FDP_IFC.1/Certification path Subset information flow control

FDP_IFC.1.1/Certification path The TSF shall enforce the **certification path acceptance information flow control policy** on

- **subjects: the verifier,**
- **information:**
  - **the certificates belonging to a certification path**
  - **the revocation data needed to validate the certification path**
- **operation: import of the information (i.e. meaning that the path is accepted as a valid certification path according to the signature policy)**.

Application note

Authorizing the export of certificates and related validation data means that the path is accepted as a valid certification path according to the signature policy.

FDP_IFF.1/Certification path Simple security attributes

FDP_IFF.1.1/Certification path The TSF shall enforce the **certification path acceptance information flow control policy** based on the following types of subject and information security attributes:

- **subjects: the verifier (applied signature policy, [assignment: other verifier's attributes, if any])**
- **information: certification path validation data, including:**
  - **the certificates belonging to the certification path (certificates' fields): key usage, QCStatement, the electronic signature status, the period of validity, the time reference, certification policy.**
  - **the revocation data of each certificate in the certification path ([assignment: revocation data attributes]),**
  - **[assignment: list of other information checked and, for each, the security attributes]**.

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

Import of the certification path components and related validation data:

- **the certification path binds the signatory's certificate to a root certificate defined in the applied signature policy,**

The following rules are met at the date/time included in the imported time reference.

Certification path:

- **for each certificate of the certification path, the electronic signature of the certificate is correct**
- **for each certificate of the certification path, the period of validity of the certificate includes the date included in the time reference**

- **for each revocation data, the electronic signature of the revocation data is correct**
- **for each certificate of the certification path, the certificate is not revocated at the date included in the time reference**
- **for each certificate of the certification path, except the leaf certificate, the key usage indicate that the certificate is a CA certificate**
- **for each certificate of the certification path, the certification policy is conformant with the applied signature policy (application note: there may be different requirements for the CA certificates and for the leaf certificate).**
- **[assignment: any other supported rule on the certification path].**

The following rules are met.

Signatory's certificate:

- **the key usage of the signatory's certificate indicates that this certificate is usable for non repudiation purposes (Application note: bit 1 of keyUsage set)**
- **the certificate is a Qualified Certificate (Application note: information available using a QCStatement, see RFC 3739),**
- **the private key corresponding to public key is protected by an SCDev (Application note: information available using a QCStatement, see RFC 3739)**
- **[assignment: any other supported rule on signatory's certificate fields]**.

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

FDP_IFF.1.4/Certification path The TSF shall explicitly authorise an information flow based on the following rules:

- **controls succeed**.

FDP_IFF.1.5/Certification path The TSF shall explicitly deny an information flow based on the following rules:

- **controls fail**.

FMT_MSA.3/Certification path Static attribute initialisation

FMT_MSA.3.1/Certification path The TSF shall enforce the **certification path acceptance information flow control policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

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

FDP_ITC.2/Certification path Import of user data with security attributes

FDP_ITC.2.1/Certification path The TSF shall enforce the **certification path acceptance information flow control policy** when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.2.3/Certification path 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/Certification path 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/Certification path The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

- **a valid time reference has been imported (see *FDP_IFC.1/Time reference* and associated requirements), in conformance to the applied signature policy;**
- **any data needed to control certificates non repudiation have been imported, in conformance to the applied signature**.

6.1.4.4 Capacity to interpret the imported data

The following requirements are related to the capacity of the TOE to interpret the imported data.

FPT_TDC.1/Electronic signature Inter-TSF basic TSF data consistency

FPT_TDC.1.1/Electronic signature The TSF shall provide the capability to consistently interpret **the electronic signature** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/Electronic signature The TSF shall use **[assignment: list of interpretation rules to be applied by the TSF]** when interpreting the TSF data from another trusted IT product.

Application note

To realize this '"assignment", the authors of security targets shall specify the acceptable standards of the TOE to interpret the imported electronic signatures (formats of acceptable signatures).

FPT_TDC.1/Time reference Inter-TSF basic TSF data consistency

FPT_TDC.1.1/Time reference The TSF shall provide the capability to consistently interpret **time references** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/Time reference The TSF shall use **[assignment: list of interpretation rules to be applied by the TSF]** when interpreting the TSF data from another trusted IT product.

Application note

To realize this '"assignment", the authors of security targets shall specify the acceptable standards of the TOE allowing to interpret the imported time reference.

FPT_TDC.1/Certificates Inter-TSF basic TSF data consistency

FPT_TDC.1.1/Certificates The TSF shall provide the capability to consistently interpret **certificates** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/Certificates The TSF shall use **[assignment: list of interpretation rules to be applied by the TSF]** when interpreting the TSF data from another trusted IT product.

Application note

To realize this '"assignment", the authors of security targets shall specify the acceptable standards of the TOE allowing to interpret the imported certificates.

FPT_TDC.1/Certificate revocation data Inter-TSF basic TSF data consistency

FPT_TDC.1.1/Certificate revocation data The TSF shall provide the capability to consistently interpret **certificates' revocation data** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/Certificate revocation data The TSF shall use **[assignment: list of interpretation rules to be applied by the TSF]** when interpreting the TSF data from another trusted IT product.

Application note

To realize this '"assignment", the authors of security targets shall specify the acceptable standards of the TOE allowing to interpret the imported validation data.

6.1.4.5 Return of the verification status

FDP_IFC.1/Electronic signature validation Subset information flow control

FDP_IFC.1.1/Electronic signature validation The TSF shall enforce the **electronic signature validation information flow policy** on

- **subject: the verifier**
- **information: validation status "correct signature"**
- **operations: communication of the status to the verifier**.

FDP_IFF.1/Electronic signature validation Simple security attributes

FDP_IFF.1.1/Electronic signature validation The TSF shall enforce the **electronic signature validation information flow policy** based on the following types of subject and information security attributes:

- **subject: the verifier ([assignment: verifier's security attributes]]**
- **information: validation status "correct signature" (signatory's public key, document's hash, document's electronic signature)**.

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

Communication of the status to the verifier:

- **there exists a valid certification path binding the signatory's certificate to a root certificate referenced in the applied signature policy and therefore authenticating the signatory's public key;**
- **the document's electronic signature, verified using the signatory's public key, is correct**
- **to communicate the status "wrong signature" in case at least one rule among the information control policy rules is false**.

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

FDP_IFF.1.4/Electronic signature validation The TSF shall explicitly authorise an information flow based on the following rules:

- **controls succeed**.

FDP_IFF.1.5/Electronic signature validation The TSF shall explicitly deny an information flow based on the following rules:

- **controls fail**.

FMT_MSA.3 / Signature validation status Static attribute initialisation

FMT_MSA.3.1 / Signature validation status The TSF shall enforce the **electronic signature validation information flow policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 / Signature validation status The TSF shall allow the **nobody** to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.1 / Signature validation status Management of security attributes

FMT_MSA.1.1 / Signature validation status The TSF shall enforce the **electronic signature validation information flow policy** to restrict the ability to **modify** the security attributes **signature validation status** to **nobody**.

FDP_ETC.2 / Verification status Export of user data with security attributes

FDP_ETC.2.1 / Verification status The TSF shall enforce the **electronic signature validation information flow policy** when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2 / Verification status The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 / Verification status The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4 / Verification status The TSF shall enforce the following rules when user data is exported from the TOE:

- **data exported as security attributes of the verification status are:**
  - **the validation data contributing to prove the verification status correctness,**
  - **the signed attributes,**
  - **the limit on the value of transactions for which the signatory's certificate can be used, if it is specified in the signatory's certificate, and**
  - **the result of the analysis of the document's semantics invariance to the verifier**.

Application note

The validation data are intended to be possibly used during a subsequent verification.

The signed attributes, the limitation on the amount of the transaction and the stability of the semantics of the document are communicated to the verifier with a programming interface or a man-machine interface.

6.1.5 Cryptographic support

FCS_COP.1 / Signature verification Cryptographic operation

FCS_COP.1.1 / Signature verification The TSF shall perform

- **electronic signature verification** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **CRYPT-STD, [assignment: list of standards]**.

Global refinement:

The ST author must choose cryptographic algorithms having key lengths resistant to a cryptanalysis attacks. The public-private key pairs used by those algorithms shall be strong enough to thwart attacks during the validity period of the certificate to which the public key is linked.

Application note

The keys used must comply with the DCSSI key management requirements [KEYS-STD].

FCS_COP.1 / Hash Cryptographic operation

FCS_COP.1.1 / Hash The TSF shall perform

- **hash generation** in accordance with a specified cryptographic algorithm **[assignment: hash algorithm]** and cryptographic key sizes **[assignment: hash size]** that meet the following: **CRYPT-STD, [assignment: list of standards]**.

Global refinement:

The ST author must select a hash generating algorithm which does not produce identical message-digests out of two distinct documents.

6.1.6 User identification and authentication

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles

- **Verifier**
- **Security administrator**

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

FIA_UID.2 User identification before any action

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

Application note

The authentication mechanism must be compliant with the DCSSI authentication requirements [AUTH-STD].

6.2 Security Assurance Requirements

The required evaluation level is EAL3 augmented with ALC_FLR.3 and AVA_VAN.3.

7 Rationale

7.1 Security objectives / security problem

7.1.1 Organisational security policies (OSP)

7.1.1.1 Policies related to the application of a signature policy

P.Signatory_Certificate_Validity the organisational security policy *P.Signatory_Certificate_Validity* is covered by the security objectives:

- *O.Time_Reference* which requires that the signature is positioned in time
- *O.Certificates_Validity* which requires that the TOE verifies that the signatory's certificate used for the signature was valid when the signature was positioned in time.

P.Signed_Attributes_Conformity the organisational security policy *P.Signed_Attributes_Conformity* is completely covered by the security objective *O.Signed_Attributes_Conformity* which takes the same terms.

P.Signatory_Certificate_Conformity the organisational security policy *P.Signatory_Certificate_Conformity* is covered by the security objective *O.Certificates_Conformity* which takes the same terms.

P.Signatory_Certificate_Authenticity the organisational security policy *P.Signatory_Certificate_Authenticity* is covered by the security objective *O.Certification_Path* which requires that the TOE controls that a valid certification path exists to attest the authenticity of the signatory's certificate used for the signature.

P.Validation_Data_Authenticity/Integrity the organisational security policy *P.Validation_Data_Authenticity/Integrity* is covered by the security objective *O.Validation_Data_Conformity* which requires in particular that these data are signed by their transmitter.

7.1.1.2 Communication of the signed attributes

P.Signed_Attributes_Communication the organisational security policy *P.Signed_Attributes_Communication* is covered by the objective *O.Signed_Attributes_Communication* which requires that the TOE presents the attributes signed to the verifier.

7.1.1.3 Presentation of the document to the verifier

P.Document_Presentation the organisational security policy *P.Document_Presentation* is covered by the following security objectives:

- *OE.Document_Presentation* which requires that the environment of the TOE provides an application allowing the verifier to view the signed document.

- o *O.Presentation_Application_Execution* which requires on the one hand that the TOE can execute a viewer application provided by the environment of the TOE on request of the verifier, on the other hand that this functionality can be inhibited during the installation.

P.Document_Stability_Control the organisational security policy *P.Document_Invariant_Semantic* is covered on the one hand by the security objective *O.Document_Stability_Control* which requires that the TOE relies on an external module controlling the invariance of the semantics of the signed document and communicates the result of control to the verifier, on the other hand by the security objective *OE.Document_Stability_Control* which requires that the environment of the TOE provides such a module.

7.1.1.4 Compliance with the standards

P.Hash_Algorithms the organisational security policy *P.Hash_Algorithms* is directly covered by the security objective *O.Cryptographic_Operations* which, on this point, takes the same terms.

P.Signature_Algorithms the organisational security policy *P.Signature_Algorithms* is directly covered by the objective security *O.Cryptographic_Operations* which, on this point, takes all the same terms.

7.1.1.5 Export of the validation data

P.Validation_Data_Export This policy is covered by the objective *O.Validation_Data_Export* which takes all the elements of this one.

7.1.1.6 Miscellaneous

P.Administration This policy is covered by the objective *O.Administration* which takes the same terms and in addition by the security objective *OE.Trusted_Security_Administrator* which ensures that the administrator of the TOE is not a threat agent.

7.1.2 Assumptions

A.Host_Platform the assumption *A.Host_Platform* is covered by the security objective *OE.Host_Platform* which takes the same terms.

A.Signature_Policy_Origin the assumption *A.Signature_Policy_Origin* is covered by the security objective *OE.Signature_Policy_Origin* requiring of the administrators of the TOE to make sure the authenticity of the origin of the signature policies usable by the TOE.

A.Document_Presentation the assumption *A.Document_Presentation* is covered by the security objective *OE.Document_Presentation* which takes the same terms.

A.Document_Stability_Control the assumption *A.Document_Stability_Control* is covered by the security objective *OE.Document_Stability_Control* which takes the same terms.

A.Services_Integrity the assumption *A.Services_Integrity* is covered entirely by the objective *OE.Services_Integrity* which takes the same terms.

A.Validation_Data_Access the assumption *A.Validation_Data_Access* is covered by the objective *OE.Validation_Data_Provision* which requires that this one provides the validation data necessary to the verification of the signature.

A.Trusted_Security_Administrator the assumption *A.Trusted_Security_Administrator* is covered entirely by the objective *OE.Trusted_Security_Administrator* which takes the same terms.

7.1.3 Tables of coverage between Security problem definition and security objective

Organisational security policies (OSP)	Security objectives	Rationale
P.Signatory_Certificate_Validity	O.Time_Reference, O.Certificates_Validity	Section 7.1.1
P.Signed_Attributes_Conformity	O.Signed_Attributes_Conformity	Section 7.1.1
P.Signatory_Certificate_Conformity	O.Certificates_Conformity	Section 7.1.1
P.Signatory_Certificate_Authenticity	O.Certification_Path	Section 7.1.1
P.Validation_Data_Authenticity/Integrity	O.Validation_Data_Conformity	Section 7.1.1
P.Signed_Attributes_Communication	O.Signed_Attributes_Communication	Section 7.1.1
P.Document_Presentation	OE.Document_Presentation, O.Presentation_Application_Execution	Section 7.1.1
P.Document_Stability_Control	O.Document_Stability_Control, Signed OE.Contrôle_Sémantique_Document	Section 7.1.1
P.Hash_Algorithms	O.Cryptographic_Operations	Section 7.1.1
P.Signature_Algorithms	O.Cryptographic_Operations	Section 7.1.1
P.Validation_Data_Export	O.Validation_Data_Export	Section 7.1.1
P.Administration	O.Administration, OE.Trusted_Security_Administrator	Section 7.1.1

Table2 OSP coverage by security objectives

Security objectives	Organisational security policies (OSP)
O.Administration	P.Administration
O.Time_Reference	P.Signatory_Certificate_Validity
O.Certification_Path	P.Signatory_Certificate_Authenticity
O.Certificates_Conformity	P.Signatory_Certificate_Conformity
O.Certificates_Validity	P.Signatory_Certificate_Validity
O.Validation_Data_Conformity	P.Validation_Data_Authenticity/Integrity
O.Signed_Attributes_Conformity	P.Signed_Attributes_Conformity
O.Presentation_Application_Execution	P.Document_Presentation
O.Signed_Attributes_Communication	P.Signed_Attributes_Communication
O.Validation_Data_Export	P.Validation_Data_Export
O.Document_Stability_Control	P.Document_Stability_Control
O.Cryptographic_Operations	P.Hash_Algorithms, P.Signature_Algorithms
OE.Signature_Policy_Origin	
OE.Host_Platform	
OE.Document_Presentation	P.Document_Presentation
OE.Document_Stability_Control	P.Document_Stability_Control
OE.Validation_Data_Provision	
OE.Services_Integrity	
OE.Trusted_Security_Administrator	P.Administration

Table3 Security objectives coverage by OSP

Assumptions	Security objectives	Rationale
A.Host_Platform	OE.Host_Platform	Section 7.1.2
A.Signature_Policy_Origin	OE.Signature_Policy_Origin	Section 7.1.2
A.Document_Presentation	OE.Document_Presentation	Section 7.1.2
A.Document_Stability_Control	OE.Document_Stability_Control	Section 7.1.2
A.Services_Integrity	OE.Services_Integrity	Section 7.1.2
A.Validation_Data_Access	OE.Validation_Data_Provision	Section 7.1.2
A.Trusted_Security_Administrator	OE.Trusted_Security_Administrator	Section 7.1.2

Table4 Assumptions coverage by security objectives

Security objectives	Assumptions
OE.Signature_Policy_Origin	A.Signature_Policy_Origin
OE.Host_Platform	A.Host_Platform
OE.Document_Presentation	A.Document_Presentation
OE.Document_Stability_Control	A.Document_Stability_Control
OE.Validation_Data_Provision	A.Validation_Data_Access
OE.Services_Integrity	A.Services_Integrity
OE.Trusted_Security_Administrator	A.Trusted_Security_Administrator

Table5 Security objectives coverage by assumptions

7.2 Security requirements rationale

7.2.1 Objectives

7.2.1.1 Security objectives for the TOE

General objectives

O.Administration This objective is covered by the following functional requirements:

- *FMT_SMF.1/Management of the document format/viewer association table* which defines the administration function of association data between the signed document formats and the viewer applications.
- *FMT_SMF.1/Management of the viewer activation parameter* which defines the function making it possible to inhibit the viewing function of the signed document

Objectives on the verification rules

O.Time_Reference the security objective *O.Time_Reference* is covered in the following way:

The TOE must apply an information flow control policy (*FDP_IFC.1/Time reference*) during the importation of the time reference associated with the digital signature to accept this reference as valid. The functional component *FDP_IFF.1/Time reference* defines the rules to be applied to the various data concerned to determine if the time reference is valid; few rules are related to the time reference itself, others are related to the validation data of this reference. This component lists in addition the rules applicable to the validation data defined within the functional component; according to the signature policy applied, a subset of these rules will be actually applied.

The functional components *FMT_MTD.1/Selection of the applied signature policy* and *FMT_SMF.1/Selection of the applied signature policy* define that only the verifier can select the signature policy to be applied.

The functional components *FDP_ITC.2/Time reference* and *FPT_TDC.1/Time reference* ensure on the one hand that the TOE applies the flow control policy during the importation of the time reference and on the other hand that the TOE is able to interpret the imported data and thus to exploit them.

The following functional components, related to the management of the security attributes of the subjects and information concerned in the flow control policy also contribute to cover this objective:

- The functional component *FMT_MSA.3/Time reference* guarantees that the default values defined for the security attributes concerned in the flow control policy take restrictive values.
- The functional component *FMT_MSA.1/Time reference* guarantees that the security attributes of the time reference cannot be modified.
- The functional component *FMT_MSA.1/Certificates* guarantees that the certificates attributes implied in the verification of the validity of the time reference cannot be modified.
- The functional component *FMT_MSA.1/Certificates validation data* guarantees that the attributes of the validation data of the certificates implied in the validity verification of the time reference cannot be modified.
- Component *FMT_SMR.1* requires of the TOE to distinguish the role of verifier from the role of administrator.
- Component *FIA_UID.2* requires that the TOE does not allow the execution of any operation before having identified successfully the user.

O.Certification_Path the security objective *O.Certification_Path* is covered in the following way:

The TOE must apply an information flow control policy (*FDP_IFC.1/Certification path*) during the importation of a set of certificates constituting a certification path between the signatory's certificate and a root certificate defined in the signature policy.

The functional component *FDP_ITC.2/Certification path* ensures that the TOE applies the flow control policy during the importation of certificates. The components *FPT_TDC.1/Certificates* and *FPT_TDC.1/Certificate revocation data* ensure that the TOE is able to exploit these data.

The rules of the flow control policy are defined in the functional component *FDP_IFF.1/Certification path*. This component defines the rules having to be implemented.

The verification rules which ensure the validity of the certification path are defined by the signature policy applied. This policy can be selected only by the verifier (*FMT_MTD.1/Selection of the applied signature policy* and *FMT_SMF.1/Selection of the applied signature policy*).

The following functional components, related to the management of the security attributes of the subjects and information concerned in the flow control policy also contribute to cover this objective:

- The functional component *FMT_MSA.3/Certification path* guarantees that the default values defined for the security attributes concerned in the flow control policy take restrictive values.
- The functional component *FMT_MSA.1/Certificates* guarantees that the imported certificates attributes essential to build the certification path cannot be modified.
- The functional component *FMT_MSA.1/Certificates validation data* guarantees that the attributes of the validation data of the signatory's certificate cannot be modified.

Finally the following components contribute to the good application of the information flow control policy:

- Component *FMT_SMR.1* requires of the TOE to distinguish the role of verifier from the role of administrator.
- Component *FIA_UID.2* requires that the TOE does not allow the execution of any operation before having identified successfully the user.

O.Certificates_Conformity the security objective *O.Certificates_Conformity* is covered in the following way:

The TOE must apply an information flow control policy (*FDP_IFC.1/Certification path*) during the importation of a set of certificates constituting a certification path between the signatory's certificate and a root certificate defined in the signature policy.

The functional component *FDP_ITC.2/Certification path* ensures that the TOE applies the information flow control policy during the importation of the certificates. The components *FPT_TDC.1/Certificates* and *FPT_TDC.1/Certificate revocation data* ensure that the TOE is able to exploit these data.

The rules of the flow control policy are defined in the functional component *FDP_IFF.1/Certification path* which indicates the rules having to be implemented.

The verification rules which ensure the validity of the certification path are defined by the signature policy applied. This policy can be selected only by the verifier (*FMT_MTD.1/Selection of the applied signature policy* and *FMT_SMF.1/Selection of the applied signature policy*).

The following functional components, related to the management of the security attributes of the subjects and information concerned in the flow control policy also contribute to cover this objective:

- The functional component *FMT_MSA.3/Certification path* guarantees that the default values defined for the security attributes concerned in the flow control policy take restrictive values.
- The functional component *FMT_MSA.1/Certificates* guarantees that the attributes of the imported certificates essential to build the certification path cannot be modified.
- The functional component *FMT_MSA.1/Certificates validation data* guarantees that the attributes of the validation data of the signatory's certificate cannot be modified.

Finally the following components contribute to the good application of the flow control policy:

- Component *FMT_SMR.1* requires of the TOE to distinguish the role of verifier from the role of administrator.
- Component *FIA_UID.2* requires that the TOE does not allow the execution of any operation before having identified successfully the user.

O.Certificates_Validity the security objective *O.Certificates_Validity* is covered in the following way:

The TOE must apply an information flow control policy (*FDP_IFC.1/Certification path*) during the importation of a set of certificates constituting a certification path between the signatory's certificate and a root certificate defined in the signature policy.

The functional component *FDP_ITC.2/Certification path* ensures that the TOE applies the flow control policy during the importation of the certificates and of the information of non-revocation.

The components *FPT_TDC.1/Certificates* and in particular *FPT_TDC.1/Certificate revocation data* ensure that the TOE is able to exploit these data.

The rules of the flow control policy are defined in the functional component *FDP_IFF.1/Certification path*. This component indicates the set of rules which shall be implemented. This requirement comprise in particular rules allowing the TSF to make sure that the certificates of the path are valid and that their state is not revoked.

The rules to verify to actually ensure the validity of the certificates of the path are defined by the signature policy applied. This policy can be selected only by the verifier (*FMT_MTD.1/Selection of the applied signature policy* and *FMT_SMF.1/Selection of the applied signature policy*).

The following functional components, related to the management of the security attributes of the subjects and information concerned in the flow control policy also contribute to cover this objective:

- The functional component *FMT_MSA.3/Certification path* guarantees that the default values defined for the security attributes concerned in the flow control policy take restrictive values.
- The functional component *FMT_MSA.1/Certificates* guarantees that the attributes of the imported certificates essential to build the certification path cannot be modified.
- The functional component *FMT_MSA.1/Certificates validation data* guarantees that the attributes of the validation data of the signatory's certificate cannot be modified.

Finally the following components contribute to the good application of the flow control policy:

- Component *FMT_SMR.1* requires of the TOE to distinguish the role of verifier from the role of administrator.
- Component *FIA_UID.2* requires that the TOE does not allow the execution of any operation before having identified successfully the user.

O.Validation_Data_Conformity the security objective *O.Validation_Data_Conformity* is covered in the following way:

The TOE must apply an information flow control policy (*FDP_IFC.1/Certification path*) during the importation of a set of certificates constituting a certification path between the signatory's certificate and a root certificate defined in the signature policy. This flow control policy also applies to information of non-revocation associated with the certificates.

The functional component *FDP_ITC.2/Certification path* ensures that the TOE applies the flow control policy during the importation of the certificates and information of non revocation.

The components *FPT_TDC.1/Certificates* and in particular *FPT_TDC.1/Certificate revocation data* ensure that the TOE is well able to exploit these data.

The rules of the flow control policy are defined in the functional component *FDP_IFF.1/Certification path*. This last component indicates the set of rules having to be implemented and comprises rules allowing the TSF to make sure of the validity certificates revocation data.

The rules to be checked in order to ensure the validity of revocation-data of the certificates of the certification path are defined by the signature policy applied. This policy can be selected only by the verifier (*FMT_MTD.1/Selection of the applied signature policy* and *FMT_SMF.1/Selection of the applied signature policy*).

The following functional components, related to the management of the security attributes of the subjects and information concerned in the flow control policy also contribute to cover this objective:

- The functional component *FMT_MSA.3/Certification path* guarantees that the default values defined for the security attributes concerned in the flow control policy take restrictive values.
- The functional component *FMT_MSA.1/Certificates* guarantees that the attributes of the imported certificates essential to build the certification path cannot be modified.
- The functional component *FMT_MSA.1/Certificates validation data* guarantees that the attributes of the validation data of the signatory's certificate cannot be modified.

Finally the following components contribute to the good application of the flow control policy:

- Component *FMT_SMR.1* requires of the TOE to distinguish the role of verifier from the role of administrator.
- Component *FIA_UID.2* requires that the TOE does not allow the execution of any operation before having identified successfully the user.

O.Signed_Attributes_Conformity the security objective *O. Signed_Attributes_Conformity* is covered in the following way:

The TOE must apply an information flow control policy during the importation of the electronic signatures (*FDP_IFC.1/Electronic signature*). The functional component *FDP_IFF.1/Electronic signature* defines the rules to be applied in particular to control the compliance of the attributes signed with respect to the signature policy. This last component also defines the rules which shall be implemented by the TOE. The signature policy applied uses a subset of these rules.

The functional components *FMT_MTD.1/Selection of the applied signature policy* and *FMT_SMF.1/Selection of the applied signature policy* define that only the verifier can select the signature policy to be applied.

The functional components *FDP_ITC.2/Electronic signature* and *FPT_TDC.1/Electronic signature* ensure on the one hand that the TOE applies the flow control policy during the importation of the electronic signatures (including signed attributes) and on the other hand that the TOE is able to interpret and thus to exploit these data.

The following functional components, related to the management of the security attributes of the subjects and information concerned in the flow control policy also contribute to cover this objective:

- The functional component *FMT_MSA.3/Electronic signature* guarantees that the default values defined for the security attributes concerned in the flow control policy take restrictive values.
- The functional component *FMT_MSA.1/Electronic signature* guarantees that the attributes of the signature cannot be modified.

Finally the following components contribute to the good application of the flow control policy:

- Component *FMT_SMR.1* requires of the TOE to distinguish the role of verifier from the role of administrator.
- Component *FIA_UID.2* requires that the TOE does not allow the execution of any operation before having identified successfully the user.

Objectives related to the display of the signed data

O.Presentation_Application_Execution the security objective *O.Presentation_Application_Execution* is covered by the following components of requirement:

- *FDP_IFF.1/Electronic signature*, which ensures that the user will be able to view the document through an external viewer application. The TOE automatically launches the viewer application associated with the format of the document to be signed by using a *list of associations document format/viewer*.
- *FMT_MTD.1/Document format/viewer association table* and *FMT_SMF.1/Management of the document format/viewer association table* which guarantee that the contents of the *list of associations document format/viewer* can be modified only by an administrator.
- *FMT_MTD.1/Viewer activation parameter* and *FMT_SMF.1/Management of the viewer activation parameter* which guarantee that the *activation parameter of the viewing function of the signed document* can be modified only by an administrator.

O.Signed_Attributes_Communication the security objective *O.Signed_Attributes_Communication* is covered by the following components of requirement:

- *FDP_IFF.1/Electronic signature*, which requires that the TOE is able to export the attributes of the signature.

O.Validation_Data_Export the security objective *O. Validation_Data_Export* is covered in the following way:

The TOE must apply an information flow control policy during the exportation of the result of the signature verification (*FDP_IFC.1/Electronic signature validation* and *FDP_IFF.1/Electronic signature validation*).

The functional component *FDP_ETC.2/Verification status* requires that the verification status of the signature is communicated with the validation data proving its accuracy and with the necessary information for the verifier to process the signature (signed attributes, fields of the signatory's certificate,...)

The following functional components, related to the management of the security attributes of the subjects and information concerned in the flow control policy also contribute to cover this objective:

- The functional component *FMT_MSA.3/Signature validation status* guarantees that the default values defined for the security attributes concerned in the flow control policy take restrictive values.
- The functional component *FMT_MSA.1/Signature validation status* guarantees that the status of the signature cannot be modified.

Finally the following components contribute to the good application of the flow control policy:

- Component *FMT_SMR.1* requires of the TOE to dinstinguish the role of verifier from the role of administrator.
- Component *FIA_UID.2* requires that the TOE does not allow the execution of any operation before having identified successfully the user.

Objectives related to the control of invariance of the semantics of the document to be verified

O.Document_Stability_Control the security objective *O.Document_Stability_Control* is covered in the following way:

The TOE must apply an information flow control policy during the importation of a document (*FDP_IFC.1/Document acceptance*). The functional component *FDP_IFF.1/Document acceptance* defines the rules to be applied by the TOE to accept the document.

The component *FDP_ITC.1/Document acceptance* requires that the TOE invokes an external module to determine if the document's semantics is invariant or not, when the document is imported.

The following functional components, related to the management of the security attributes of the subjects and information concerned in the flow control policy also contribute to cover this objective:

- The functional component *FMT_MSA.3/Document acceptance* guarantees that the default values defined for the security attributes concerned in the flow control policy take restrictive values.
- The functional components *FMT_MSA.1/Document semantics invariance status* and *FMT_SMF.1/Getting document semantics invariance status* which require on the one hand that the TOE has a means of invoking an external module to determine whether the document's semantics is invariant, on the other hand that nobody can modify the result of the control.
- Component *FMT_SMR.1* requires of the TOE to distinguish the role of signatory from the role of administrator.
- Component *FIA_UID.2* requires that the TOE does not allow the execution of any operation before having identified successfully the user.

Compliance with standards

O.Cryptographic_Operations the security objective *O.Cryptographic_Operations* is covered by the requirements:

- *FCS_COP.1/Hash* concerning the collision-resistant property between the digests produced by the application of the hash algorithm.
- *FCS_COP.1/Signature verification* which guarantees that all the cryptographic algorithms used in the verification process of the electronic signatures are resistant to cryptanalysis attacks. In particular the size of the keys shall be sufficiently large to ensure the resistance of the public key present in a certificate during the validity period of this certificate.

7.2.2 Tables of coverage between security objectives and security requirements

Security objectives	Functional requirements	Rationale
O.Administration	FMT_SMF.1/Management of the viewer activation parameter, FMT_SMF.1/Management of the document format/viewer association table	Section 7.2.1
O.Time_Reference	FDP_IFC.1/Time reference, FDP_IFF.1/Time reference, FMT_MTD.1/Selection of the applied signature policy, FMT_SMF.1/Selection of the applied signature policy, FDP_ITC.2/Time reference, FPT_TDC.1/Time reference, FMT_MSA.3/Time reference, FMT_MSA.1/Time reference, FMT_MSA.1/Certificates, FMT_MSA.1/Certificates validation data, FMT_SMR.1, FIA_UID.2	Section 7.2.1
O.Certification_Path	FDP_IFC.1/Certification path, FDP_ITC.2/Certification path, FPT_TDC.1/Certificates, FPT_TDC.1/Certificate revocation data, FMT_MTD.1/Selection of the applied signature policy, FMT_SMF.1/Selection of the applied signature policy, FMT_MSA.3/Certification path, FMT_MSA.1/Certificates, FMT_MSA.1/Certificates validation data, FMT_SMR.1, FDP_IFF.1/Certification path, FIA_UID.2	Section 7.2.1

Security objectives	Functional requirements	Rationale
O.Certificates_Conformity	FDP_IFC.1/Certification path, FDP_ITC.2/Certification path, FPT_TDC.1/Certificates, FPT_TDC.1/Certificate revocation data, FDP_IFF.1/Certification path, FMT_MTD.1/Selection of the applied signature policy, FMT_SMF.1/Selection of the applied signature policy, FMT_MSA.3/Certification path, FMT_MSA.1/Certificates, FMT_MSA.1/Certificates validation data, FMT_SMR.1, FIA_UID.2	Section 7.2.1
O.Certificates_Validity	FDP_IFC.1/Certification path, FDP_ITC.2/Certification path, FPT_TDC.1/Certificates, FPT_TDC.1/Certificate revocation data, FDP_IFF.1/Certification path, FMT_MTD.1/Selection of the applied signature policy, FMT_SMF.1/Selection of the applied signature policy, FMT_MSA.3/Certification path, FMT_MSA.1/Certificates, FMT_MSA.1/Certificates validation data, FMT_SMR.1, FIA_UID.2	Section 7.2.1
O.Validation_Data_Conformity	FDP_IFC.1/Certification path, FDP_ITC.2/Certification path, FPT_TDC.1/Certificates, FPT_TDC.1/Certificate revocation data, FDP_IFF.1/Certification path, FMT_MTD.1/Selection of the applied signature policy, FMT_SMF.1/Selection of the applied signature policy, FMT_MSA.3/Certification path, FMT_MSA.1/Certificates, FMT_MSA.1/Certificates validation data, FMT_SMR.1, FIA_UID.2	Section 7.2.1

Security objectives	Functional requirements	Rationale
O.Signed_Attributes_Conformity	FDP_IFC.1/Electronic signature, FDP_IFF.1/Electronic signature, FMT_MTD.1/Selection of the applied signature policy, FMT_SMF.1/Selection of the applied signature policy, FDP_ITC.2/Electronic signature, FPT_TDC.1/Electronic signature, FMT_MSA.3/Electronic signature, FMT_MSA.1/Electronic signature, FMT_SMR.1, FIA_UID.2	Section 7.2.1
O.Presentation_Application_Execution	FMT_MTD.1/Document format/viewer association table, FMT_MTD.1/Viewer activation parameter, FDP_IFF.1/Electronic signature, FMT_SMF.1/Management of the document format/viewer association table, FMT_SMF.1/Management of the viewer activation parameter	Section 7.2.1
O.Signed_Attributes_Communication	FDP_IFF.1/Electronic signature	Section 7.2.1
O.Validation_Data_Export	FDP_IFC.1/Electronic signature validation, FDP_IFF.1/Electronic signature validation, FDP_ETC.2/Verification status, FMT_MSA.3/Signature validation status, FMT_MSA.1/Signature validation status, FMT_SMR.1, FIA_UID.2	Section 7.2.1

Security objectives	Functional requirements	Rationale
O.Document_Stability_Control	FDP_IFC.1/Document acceptance, FDP_IFF.1/Document acceptance, FDP_ITC.1/Document acceptance, FMT_MSA.3/Document's acceptance, FMT_MSA.1/Document's semantics invariance status, FMT_SMF.1/Getting document's semantics invariance status, FMT_SMR.1, FIA_UID.2	Section 7.2.1
O.Cryptographic_Operations	FCS_COP.1/Signature verification, FCS_COP.1/Hash	Section 7.2.1

Table6 Security objectives for the TOE coverage by functional requirements

Functional requirements of the TOE	Security objectives
FDP_IFC.1/Document acceptance	O.Document_Stability_Control
FDP_IFF.1/Document acceptance	O.Document_Stability_Control
FDP_ITC.1/Document acceptance	O.Document_Stability_Control
FMT_MSA.3/Document's acceptance	O.Document_Stability_Control
FMT_MSA.1/Document's semantics invariance status	O.Document_Stability_Control
FMT_SMF.1/Getting document semantics invariance status	O.Document_Stability_Control
FMT_MTD.1/Document format/viewer association table	O.Presentation_Application_Execution
FMT_SMF.1/Management of the document format/viewer association table	O.Administration, O.Presentation_Application_Execution
FMT_MTD.1/Viewer activation parameter	O.Presentation_Application_Execution
FMT_SMF.1/Management of the viewer activation parameter	O.Administration, O.Presentation_Application_Execution
FMT_MTD.1/Selection of the applied signature policy	O.Time_Reference, O.Certification_Path, O.Certificates_Conformity, O.Certificates_Validity, O.Validation_Data_Conformity, O.Signed_Attributes_Conformity
FMT_SMF.1/Selection of the applied signature policy	O.Time_Reference, O.Certification_Path, O.Certificates_Conformity, O.Certificates_Validity, O.Validation_Data_Conformity, O.Signed_Attributes_Conformity
FDP_IFC.1/Electronic signature	O.Signed_Attributes_Conformity
FDP_IFF.1/Electronic signature	O.Signed_Attributes_Conformity, O.Presentation_Application_Execution, O.Signed_Attributes_Communication

Functional requirements of the TOE	Security objectives
FMT_MSA.3/Electronic signature	O.Signed_Attributes_Conformity
FMT_MSA.1/Electronic signature	O.Signed_Attributes_Conformity
FDP_ITC.2/Electronic signature	O.Signed_Attributes_Conformity
FDP_IFC.1/Time reference	O.Time_Reference
FDP_IFF.1/Time reference	O.Time_Reference
FMT_MSA.3/Time reference	O.Time_Reference
FMT_MSA.1/Time reference	O.Time_Reference
FDP_ITC.2/Time reference	O.Time_Reference
FMT_MSA.1/Certificates	O.Time_Reference, O.Certification_Path, O.Certificates_Conformity, O.Certificates_Validity, O.Validation_Data_Conformity
FMT_MSA.1/Certificates validation data	O.Time_Reference, O.Certification_Path, O.Certificates_Conformity, O.Certificates_Validity, O.Validation_Data_Conformity
FDP_IFC.1/Certification path	O.Certification_Path, O.Certificates_Conformity, O.Certificates_Validity, O.Validation_Data_Conformity
FDP_IFF.1/Certification path	O.Certification_Path, O.Certificates_Conformity, O.Certificates_Validity, O.Validation_Data_Conformity
FMT_MSA.3/Certification path	O.Certification_Path, O.Certificates_Conformity, O.Certificates_Validity, O.Validation_Data_Conformity
FDP_ITC.2/Certification path	O.Certification_Path, O.Certificates_Conformity, O.Certificates_Validity, O.Validation_Data_Conformity
FPT_TDC.1/Electronic signature	O.Signed_Attributes_Conformity

Functional requirements of the TOE	Security objectives
FPT_TDC.1/Time reference	O.Time_Reference
FPT_TDC.1/Certificates	O.Certification_Path, O.Certificates_Conformity, O.Certificates_Validity, O.Validation_Data_Conformity
FPT_TDC.1/Certificate revocation data	O.Certification_Path, O.Certificates_Conformity, O.Certificates_Validity, O.Validation_Data_Conformity
FDP_IFC.1/Electronic signature validation	O.Validation_Data_Export
FDP_IFF.1/Electronic signature validation	O.Validation_Data_Export
FMT_MSA.3/Signature validation status	O.Validation_Data_Export
FMT_MSA.1/Signature validation status	O.Validation_Data_Export
FDP_ETC.2/Verification status	O.Validation_Data_Export
FCS_COP.1/Signature verification	O.Cryptographic_Operations
FCS_COP.1/Hash	O.Cryptographic_Operations
FMT_SMR.1	O.Time_Reference, O.Certification_Path, O.Certificates_Conformity, O.Certificates_Validity, O.Validation_Data_Conformity, O.Signed_Attributes_Conformity, O.Validation_Data_Export, O.Document_Stability_Control
FIA_UID.2	O.Time_Reference, O.Certification_Path, O.Certificates_Conformity, O.Certificates_Validity, O.Validation_Data_Conformity, O.Signed_Attributes_Conformity, O.Validation_Data_Export, O.Document_Stability_Control

Table7 Functional requirements coverage by security objectives for the TOE

7.3 Dependencies

7.3.1 Dependencies of the security functional requirements

Requirements	CC dependencies	Satisfied dependencies
FDP_IFC.1/Document acceptance	(FDP_IFF.1)	FDP_IFF.1/Document acceptance
FDP_IFF.1/Document acceptance	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Document acceptance, FMT_MSA.3/Document acceptance
FDP_ITC.1/Document acceptance	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Document acceptance, FMT_MSA.3/Document acceptance
FMT_MSA.3/Document acceptance	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/Document semantics invariance status, FMT_SMR.1
FMT_MSA.1/Document semantics invariance status	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_IFC.1/Document acceptance, FMT_SMF.1/Getting document semantics invariance status, FMT_SMR.1
FMT_SMF.1/Getting document semantics invariance status	No dependence	
FMT_MTD.1/Document format/viewer association table	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1/Management of the document format/viewer association table, FMT_SMR.1
FMT_SMF.1/Management of the document format/viewer association table	No dependence	
FMT_MTD.1/Viewer activation parameter	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1/Management of the viewer activation parameter, FMT_SMR.1
FMT_SMF.1/Management of the viewer activation parameter	No dependence	
FCS_COP.1/Signature verification	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.2/Certification path
FCS_COP.1/Hash	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	
FMT_SMR.1	(FIA_UID.1)	FIA_UID.2
FIA_UID.2	No dependence	
FMT_MTD.1/Selection of the applied signature policy	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1/Selection of the applied signature policy

Requirements	CC dependencies	Satisfied dependencies
FMT_SMF.1/Selection of the applied signature policy	No dependence	
FDP_IFC.1/Electronic signature	(FDP_IFF.1)	FDP_IFF.1/Electronic signature
FDP_IFF.1/Electronic signature	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Electronic signature, FMT_MSA.3/Electronic signature
FMT_MSA.3/Electronic signature	(FMT_MSA.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_MSA.1/Electronic signature
FMT_MSA.1/Electronic signature	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FDP_IFC.1/Electronic signature
FDP_ITC.2/Electronic signature	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/Electronic signature, FPT_TDC.1/Electronic signature
FDP_IFC.1/Time reference	(FDP_IFF.1)	FDP_IFF.1/Time reference
FDP_IFF.1/Time reference	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Time reference, FMT_MSA.3/Time reference
FMT_MSA.3/Time reference	(FMT_MSA.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_MSA.1/Time reference, FMT_MSA.1/Certificates, FMT_MSA.1/Certificates validation data
FMT_MSA.1/Time reference	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FDP_IFC.1/Time reference
FDP_ITC.2/Time reference	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/Time reference, FPT_TDC.1/Time reference, FPT_TDC.1/Certificates, FPT_TDC.1/Certificate revocation data
FDP_IFC.1/Certification path	(FDP_IFF.1)	FDP_IFF.1/Certification path
FDP_IFF.1/Certification path	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Certification path, FMT_MSA.3/Certification path
FMT_MSA.3/Certification path	(FMT_MSA.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_MSA.1/Certificates, FMT_MSA.1/Certificates validation data

Requirements	CC dependencies	Satisfied dependencies
FDP_ITC.2/Certification path	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/Certification path, FPT_TDC.1/Certificates, FPT_TDC.1/Certificate revocation data
FPT_TDC.1/Electronic signature	No dependence	
FPT_TDC.1/Time reference	No dependence	
FPT_TDC.1/Certificates	No dependence	
FPT_TDC.1/Certificate revocation data	No dependence	
FDP_IFC.1/Electronic signature validation	(FDP_IFF.1)	FDP_IFF.1/Electronic signature validation
FDP_IFF.1/Electronic signature validation	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Electronic signature validation, FMT_MSA.3/Signature validation status
FMT_MSA.3/Signature validation status	(FMT_MSA.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_MSA.1/Signature validation status
FMT_MSA.1/Signature validation status	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FDP_IFC.1/Electronic signature validation
FDP_ETC.2/Verification status	(FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.1/Electronic signature validation
FMT_MSA.1/Certificates	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FDP_IFC.1/Certification path
FMT_MSA.1/Certificates validation data	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FDP_IFC.1/Certification path

Table8 Dependencies of the functional requirements

7.3.1.1 Rational for the unsatisfied dependencies

Dependence FCS_CKM.4 of FCS_COP.1/Signature verification is not supported. The dependence between *FCS_COP.1/Signature verification* and *FCS_CKM.4* is not satisfied, since the keys used being public-keys they do not require protected method for their destruction.

Dependence FCS_CKM.4 of FCS_COP.1/Hash is not supported. The dependence between the *FCS_COP.1/Hash* component and component *FCS_CKM.4* is not satisfied

because a hash algorithm does not require a key, therefore does not require requirements describing the methods of destruction of the keys.

Dependence FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 of FCS_COP.1/Hash is not supported. The dependence between the FCS_COP.1/Hash component and one of three components FCS_CKM.1, FDP_ITC.1 and FDP_ITC.2 are not satisfied because a hash algorithm does not require a key, therefore does not require requirements describing the methods of generation or importation of keys

Dependence FMT_SMF.1 of FMT_MSA.1/Electronic signature is not supported. The component *FMT_MSA.1/Electronic signature* not defining new management feature, the dependence between this component and component *FMT_SMF.1* does not need to be satisfied.

Dependence FTP_ITC.1 or FTP_TRP.1 of FDP_ITC.2/Electronic signature is not supported. The dependence between the requirement component *FDP_ITC.2/Electronic signature* and one of component FTP_ITC.1 or TFP_TRP.1 is not satisfied because:

- these data do not require confidentiality protection;
- the validity of the digital signature contained in the electronic signatures guarantees the integrity of all the signed data;
- finally, the validity of the electronic signatures (if it is attested at the end of the verification process) proves the authenticity of the origin of information.

Dependence FMT_SMF.1 of FMT_MSA.1/Time reference is not supported. The dependence between the component *FMT_MSA.1/Time reference* and the component FMT_SMF.1 is not satisfied because this first component does not define a new management function of the security attributes.

Dependence FTP_ITC.1 or FTP_TRP.1 of FDP_ITC.2/Time reference is not supported. The dependence between the requirement component *FDP_ITC.2/Certificates validation data* and one of components FTP_ITC.1 or FTP_TRP.1 does not have to be satisfied because the data conveyed by the protocols used in the public key infrastructures are autoprotected:

- the integrity of the time reference is guaranteed by the digital signature which is associated to it;
- the authenticity of the origin of the time reference is guaranteed by the construction of a valid certification path between the key of the time-stamping unit and a trusted point dedicated to the time-stamping defined in the signature policy.
- finally, the data received by the TOE do not require protection in terms of confidentiality.

Dependence FTP_ITC.1 or FTP_TRP.1 of FDP_ITC.2/Certification path is not supported. The dependence between the requirement component *FDP_ITC.2/Certification path* and one of component FTP_ITC.1 or FTP_TRP.1 does not have to be satisfied because the protocols used in the public key infrastructures are autoprotected:

- the integrity of each certificate of the certification path and information of non-revocation is guaranteed by a digital signature appended by a higher authority, the

autosigned root certificate being referenced in the signature policy (protected in integrity by the TOE).

- Building a valid certification path between the signatory's certificate and a trusted point defined in the signature policy allows to guarantee the authenticity of the origin of the various certificates composing this path.
- the data received by the TOE do not require protection in terms of confidentiality.

Dependence FMT_SMF.1 of FMT_MSA.1/Signature validation status is not supported. The dependence between the component *FMT_MSA.1/Signature validation status* and the component FMT_SMF.1 is not satisfied because this first component does not define a new management function of the security attributes.

Dependence FMT_SMF.1 of FMT_MSA.1/Certificates is not supported. *The FMT_MSA.1/Certificated* component not defining new management feature, the dependence between this component and component *FMT_SMF.1* do not need to be satisfied.

Dependence FMT_SMF.1 of FMT_MSA.1/Certificates validation data is not supported. The component *FMT_MSA.1/Certificates validation data* not defining new management feature, the dependence between this component and component *FMT_SMF.1* does not need to be satisfied.

7.3.2 Dependencies of the security assurance requirements

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 dependence	
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 dependence	
ALC_DEL.1	No dependence	
ALC_DVS.1	No dependence	
ALC_FLR.3	No dependence	
ALC_LCD.1	No dependence	
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 dependence	
ASE_INT.1	No dependence	
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 dependence	
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

Table9 Dependencies of the assurance requirements

7.3.2.1 Rationale for the unsatisfied dependencies

Dependence ADV_IMP.1 of AVA_VAN.3 is not supported. The dependence with ADV_IMP.1 is not satisfied because this requirement is covered by the requirement component AVA_VAN.3.

Dependence ADV_TDS.3 of AVA_VAN.3 is not supported. The dependence with ADV_TDS.3 is not satisfied because this requirement is covered by the requirement component AVA_VAN.3.

7.4 EAL rationale

The assurance level of this protection profile is EAL3 augmented, because it is required by the *qualification standard* process [QUA-STD].

7.5 Rationale for the EAL augmentation

7.5.1 ALC_FLR.3 Systematic flaw remediation

Augmentation required by the process of *qualification standard*.

7.5.2 AVA_VAN.3 Focused vulnerability analysis

Augmentation required by the process of *qualification standard*.

Appendix A Glossary

This glossary gives the definition of terms used in this document.

The glossary is composed of two parts. The first part is related to the Common Criteria terms, the second clarifies the terms related to the electronic signature.

A.1 Common Criteria terms

Evaluation Assurance Level (EAL)

A package of assurance components from the part 3 which represents the level of the evaluation.

Target Of Evaluation (TOE)

A set of software, firmware and/or hardware possibly accompanied by an administrator and user guidance.

TOE Security Policy (TSP)

A set of rules controlling how the assets are managed, protected and distributed in a TOE.

A.2 Electronic signature terms

Qualified Certificate Authority

Entity providing certificates fulfilling the requirements defined in appendix II of the Directive.

Certificate

An electronic attestation which links *signature-verification data* to a *signatory*.

A certificate must contain:

(a) the identification of the certification-service-provider and the State in which it is established;

(b) the name of the signatory or a pseudonym, which shall be identified as such;

(c) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;

(d) signature-verification data which correspond to signature-creation data under the control of the signatory;

(e) an indication of the beginning and end of the period of validity of the certificate;

(f) the identity code of the certificate;

(g) the electronic signature of the certification-service-provider issuing it;

If necessary, scope of use of the certificate, and limits on the value of transactions for which the certificate can be used.

Qualified Certificate

A certificate fulfilling the requirements defined in article 6 of the French Decree No 2001-272 of March 30th, 2001 defined for the application of article 1316-4 of the French civil code and related to the electronic signatures.

I.e., in addition to the elements defined above, a qualified certificate must contain:

a) A mention indicating that this certificate is issued as qualified certificate;

b) the *secure electronic signature* of the certification service provider of which issues the certificate.

Digest / Hash value

Result of a one-way hash function, i.e. of a function calculating an imprint of a message so that an even a minor modification of the message involves the modification of the imprint.

Cryptographic Service Provider (CSP)

Software layer allowing an application to use cryptographic services thanks to an programming interface (API) provided by the operating system of the host platform.

Signature Creation Device (SCDev)

Hardware or software intended to apply the *data for creation of electronic signatures* to generate electronic signature.

Secure Signature Creation Device (SSCD)

A Signature creation Device which satisfy the requirements defined in the I of article 3 of the Decree No 2001-272 of March 30th, 2001 defined for the application of article 1316-4 of the civil code and related to the electronic signatures.

Signature Verification Device

Hardware or software intended to apply the *data for verification of electronic signatures*.

Directive

Directive 1999/93/EC of the European Parliament and of the Council of December 13rd, 1999 on a Community framework for electronic signatures.

Signature-creation data

Elements specific to the *signatory*, such as private cryptographic keys, used by him to create *electronic signatures*.

Signature-verification data

Elements, such as public cryptographic keys, used to verify the *electronic signatures*.

Contents format

An identifier allowing to determine the type of application able to display the document correctly.

Object Identifier (OID)

A sequence of characters or numbers, stored in compliance with ISO/IEC 9834, that uniquely references an object or a class of objects in the electronic signature envelope.

Signature policy

Set of rules for the creation or the validation of electronic signatures, under which a signature can be considered as valid.

Certification Service Provider

An entity or a legal or natural person who issues certificates or other services related to electronic signatures.

Accreditation of the Electronic certification service providers

The act by which a third part, known as accreditation body, attests that an *electronic certification service provider* provides services compliant with particular requirements for quality.

Signatory

Any natural person, acting for his own account or for the natural person or legal person he represents, who uses a *signature creation device.*

Electronic signatures

Data in electronic form attached to, or logically associated with other electronic data and which serves as a method of authentication of that data.

Secure electronic signatures

Electronic signatures which satisfy, moreover, with the following requirements:

- to be specific to the signatory;
- to be created by means which the signatory can keep under his exclusive control;
- to guarantee with the related act a link such as any later modification of the act is detectable;

Digital signature

Result of the cryptographic operation of signature on data to be signed and using a signature private key.

System of signature creation

The complete system which allows the creation of electronic signatures and which includes the application of creation of signature and the signature creation device.

Appendix B Acronyms

API Application Programming Interface

ARL Authority Revocation List

CA Certification Authority

CRL Certificate Revocation List

CSP Cryptographic Service Provider

CWA CEN Workshop Agreements

ETSI European Telecommunications Standards Institute

MMI Man-Machine Interface

OCSP Online Certificate Status Protocol

OID Object Identifier

PKCS#11 Public Key Cryptography Standards #11

PP Protection profile

SCDev Signature Creation Device

SSCD Secure Signature Creation Device

TOE Target of Evaluation

Index