Agence nationale de la sécurité des systèmes d'information

Protection Profile
Electronic Signature Creation Application

Date	:	2nd march 2011
Reference	:	PP-ACSE-CCv3.1
Version	:	1.7

Courtesy Translation

Courtesy translation of the protection profile registered and certified by the French Certification Body under the reference ANSSI-CC-PP-2008/05-M01.

Table of Contents

1 INTRODUCTION 6

1.1 IDENTIFICATION 6
1.2 PROTECTION PROFILE OVERVIEW 6
1.3 DEFINITIONS AND ACRONYMS 7
1.4 REFERENCES 7
1.4.1 Normative references 7
1.4.2 Informative references 8

2 TOE DESCRIPTION 9

2.1 USAGE AND MAJOR SECURITY FEATURES OF A TOE 9
2.1.1 Component managing the interaction with the signatory 9
2.1.2 "What You See is What Is Signed" 11
2.1.3 Component managing/implementing the signature policy 12
2.1.4 Component formatting/hashing the data to be signed 13
2.1.5 Component piloting the interface with the SCDev 13
2.2 NOTE: THE CONFORMITY CHECK OF THE ELECTRONIC SIGNATURE SHALL BE DONE REGARDING THE DATA TO BE SIGNED. IN PARTICULAR, WHEN THE SCDEV PERFORMS ALL OR PART OF THE CALCULATION OF THE HASH VALUE, THE TOE SHALL CHECK THE CONFORMITY OF THE HASH RETURNED BY THE SCDEV. WHEN THE DTBSR SENT BY THE TOE TO THE SCDEV IS A HASH, THE CHECK OF THE ELECTRONIC SIGNATURE CONFORMITY COULD BE DONE REGARDING THAT TRANSMITTED HASH.ENVIRONMENT OF USE OF THE TOE 13

3 CONFORMANCE CLAIMS 15

3.1 CC CONFORMANCE CLAIM 15
3.2 PACKAGE CLAIM 15
3.3 PP CLAIM 15
3.4 CONFORMANCE STATEMENT 15

4 SECURITY PROBLEM DEFINITION 16

4.1 ASSETS 16
4.1.1 User data 16
4.1.2 TOE sensitive assets (TSF data) 17
4.2 ROLES / SUBJECTS 18
4.3 THREATS 18
4.4 ORGANISATIONAL SECURITY POLICIES (OSP) 18
4.4.1 Policies related to the validity of the created signature 18
4.4.2 Control of the invariance of the document's semantics 19
4.4.3 Presentation to the signatory of the document and of the signature attributes 19
4.4.4 Compliance with standards 19
4.4.5 Interaction with the signatory 19
4.4.6 Miscellaneous 20
4.5 ASSUMPTIONS 20
4.5.1 Assumptions on the operational environment 20
4.5.2 Assumptions on the context of operations 22
4.5.3 Conclusion 23

5 SECURITY OBJECTIVES 24

5.1 SECURITY OBJECTIVES FOR THE TOE 24
5.1.1 General objectives 24
5.1.2 Interactions with the signatory 24
5.1.3 Signature policy applications 24
5.1.4 Data protection 25
5.1.5 Cryptographic operations 25
5.1.6 Control of the invariance of the document semantics 25
5.1.7 Presentation of the documents to be signed 26

5.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT 26
5.2.1 Security objectives for the host platform 26
5.2.2 Security objectives for the SCDev and its environment 26
5.2.3 Presence of the signatory 27
5.2.4 Document presentation 27
5.2.5 Miscellaneous 28

6 SECURITY REQUIREMENTS 29

6.1 SECURITY FUNCTIONAL REQUIREMENTS 29
6.1.1 Document stability control 31
6.1.2 Interaction with the signatory 35
6.1.3 Validation rules 35
6.1.4 Application of the Signature policy and generation of the signature 38
6.1.5 Electronic signature export 41
6.1.6 Cryptographic operations 44
6.1.7 User identification and authentication 44
6.1.8 TOE administration 45
6.2 SECURITY ASSURANCE REQUIREMENTS 46

7 RATIONALE 47

7.1 SECURITY OBJECTIVES RATIONALE 47
7.1.1 Organisational security policies (OSP) 47
7.1.2 Assumptions 49
7.1.3 Tables of coverage between Security problem definition and security objectives 50
7.2 SECURITY REQUIREMENTS RATIONALE 53
7.2.1 Objectives 53
7.2.2 Tables of coverage between security objectives and security requirements 58
7.3 DEPENDENCIES 64
7.3.1 Dependencies of the functional security requirements 64
7.3.2 Dependencies of the security assurance requirements 67
7.4 EVALUATION ASSURANCE LEVEL RATIONALE 68
7.5 EAL AUGMENTATION RATIONALE 68
7.5.1 AVA_VAN.3 Focused vulnerability analysis 68
7.5.2 ALC_FLR.3 Systematic flaw remediation 68

APPENDIX A GLOSSARY 69

A.1 COMMON CRITERIA TERMS 69
A.2 ELECTRONIC SIGNATURE TERMS 69

APPENDIX B ACRONYMS 72

Table of Tables

Table 1 Protection profile identification 6
Table2 OSP coverage by security objectives 51
Table3 Security objectives coverage by OSP 51
Table4 Assumptions coverage by security objectives for the operational environment 52
Table5 Security objectives for the operational environment coverage by assumptions 52
Table6 Security objectives for the TOE coverage by functional requirements 60
Table7 Functional requirements coverage by security objectives for the TOE 63
Table8 Dependencies of the functional requirements 66
Table9 Dependencies of the security assurance requirements 67

1 Introduction

This section provides general information and information related to the document management 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.

This section could be used independently as a presentation in catalogues and registers of protection profiles.

1.1 Identification

Title	Protection Profile –Electronic Signature Creation Application
Author	Trusted Labs
CC Version	V3.1 Revision 2
Reference	PP-ACSE-CCv3.1
Version	1.7
Keywords	electronic signature, electronic signature application, electronic signature creation application

Table 1 Protection profile identification

1.2 Protection profile overview

This protection profile was elaborated for the French governmental information security authority (Agence Nationale de la Sécurité des Systèmes d'Information, ANSSI) in order to ease the certification of applications for signature creation usable in particular for the development of the electronic administration.

This protection profile is compliant with the recommendations of the ANSSI for the qualification for security products at the standard level. By making this protection profile available to the products vendors, the ANSSI wishes to encourage the qualification of signature creation applications based on this document.

This protection profile defines security requirements for signature creation applications being able to interface with a Secure Signature Creation Device (SSCD) or a Signature Creation Device (SCDev).

Although the certification of the signature creation application is not 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).

This protection profile relies on the [CWA 14170] document. It defines the security requirements of an electronic signature creation application. “Electronic signature creation” means the generation of a document signature and the generation of attributes related to the signature using a private key associated with a certificate specific to the signatory and confined in a signature creation device (thereafter called *SCDev*).

The application allows to generate at best electronic signatures presumed to be reliable[1] and at least secure electronic signatures[2]. To allow this usage modularity, the use of qualified certificates and of a Secure Signature Creation Device (SSCD) is not required in this protection profile.

The cryptographic operations using the private key of the signatory and allowing to generate the signature are performed by a Signature Creation Device (thereafter SCDev[3]) and not by the application concerned by this protection profile.

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

1.4.1 Normative 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 1.2. ANSSI. See www.ssi.gouv.fr..

[1] Qualified Electronic Signature according to the Directive
[2] Advanced Electronic Signature according to the Directive
[3] the SCDev is also named a SSCD if it has been evaluated compliant with the requirements defined in the Appendix III of the Directive. The protection profile defined in the [CWA 14169] document is recognized as compliant with these requirements.

1.4.2 Informative references

[Directive]	European directive for electronic signature, 13 December 1999, 1999/93/CE.
[CRYPT-STD]	Cryptographic mechanisms – Rules and recommendations about the choice and the parameter's sizes of cryptographic mechanisms. ANSSI. See www.ssi.gouv.fr.
[AUTH-STD]	Authentification - Règles et recommandations concernant les mécanismes d'authentification. ANSSI. See www.ssi.gouv.fr.
[CWA 14169]	Secure signature-creation devices “EAL 4+”, CEN/WS, March 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, 15th December, 2003.

2 TOE Description

The purpose of this part of the protection profile is to describe the TOE, the type of product which it represents as well as the general functionalities that it supports. In addition, this section presents the target of evaluation within a system of signature creation.

2.1 Usage and major security features of a TOE

The target of evaluation (TOE) is the set of software and/or hardware components that creates electronic signatures relying on a SCDev that performs cryptographic operations using the private key of the signatory.

The TOE includes the following functional components:

- the component managing the interaction with the signatory
- the component allowing to launch applications of display
- the component allowing to control the invariance of the document semantics
- the component allowing to display the signature attributes
- the component managing/implementing the signature policy
- the component formatting and hashing the data to be signed
- the component piloting the interface with the SCDev

2.1.1 Component managing the interaction with the signatory

The TOE includes an interface with the signatory, the user of the TOE, allowing him to sign one or more documents.

This interface is either a man-machine interface (MMI) allowing the signatory to interact directly with the TOE, or a programming interface (API) allowing a software component (application, library...) to interact with the TOE.

The interface allows the signatory:

- to select or deselect one or more documents to be signed (already including or not a signature),
- to select the signature policy to be applied,
  If the TOE supports several signature policies, the signature policy to be applied can be selected by the signatory or result from a parameter setting of the application.
- to select the attributes of the signature,
- to select the certificate (and thus the private key) to be used for the signature,
- to express its signature agreement,
- to activate the signature private key,
- at any moment to cancel the process of signature creation, before sending the data to be signed to the SCDev.

The input of the signatory authentication data allowing the SCDev to activate the signature key and their transfer towards the SCDev are under the control of components outside the TOE scope.

2.1.1.1 Selection / deselection of the documents to be signed

The TOE supports a means allowing the signatory to indicate him the document(s) he wishes to sign.

Document to be signed and countersignature

The document to be signed could already contain or not contain signatures.

Thereafter a “document” either means a simple document, or a document containing one or more overlapping electronic signatures. This second case corresponds to a countersignature of the document.

Signature of one or more documents

If the signature relates to several documents, the same signature attributes are used; in particular:

- identification of the signatory's certificate (thus the same signature private key),
- the same signature policy,
- the same type of commitment,
- the same presumed date,
- etc...

In this case, non-trivial actions will allow the signatory to sign the whole selection of documents. A non-trivial action can for example be performed via a confirmation mechanism (the signatory clicks on the button "sign", the TOE prompts him for a confirmation before executing the action).

Deselecting documents

Moreover, after having viewed a document he has selected, the signatory can refuse to sign it. The TOE thus allows him to deselect one or more already selected documents.

2.1.1.2 Selection of the signature attributes

The TOE allows the signatory to select the signature attributes to be signed jointly with the document.

The signature attributes can be (the list is not exhaustive):

- the reference to the signature policy,
- the type of commitment,
- the presumed place of the signature,
- the presumed date/hour of the signature,
- the format of the contents,
- the role of the signatory
- ...

2.1.1.3 Selection of the certificate to be used

The TOE allows the signatory to indicate which certificate (and thus which private key) to use to create the signature.

2.1.1.4 Signature agreement

The interface with the signatory allows him to express his agreement to sign and this for each document to be signed.

Before creating the signature on one or more documents, the TOE controls that the signatory actually wishes to sign and that the action is not involuntary or accidental. For this purpose, the TOE must force the signatory to perform a sequence of non-trivial operations.

The signature agreement operation is different from the operation of authentication of the signatory to the SCDev. Indeed, the prerequisite of the activation by the signatory of the private key associated with the selected certificate is the signature agreement operation.

2.1.1.5 Interruption of the signature process

The TOE allows the signatory to cancel the signature process of one or more documents at any moment before the TOE transmits the data to be signed to the SCDev.

2.1.2 "What You See is What Is Signed"

As for a paper document, the signatory must be able to view the elements on which he will commit before signing them.

In this protection profile, these problems are treated in three parts:

1) the TOE allows the signatory to view the document to be signed thanks to the component able to execute external viewer applications (see 2.1.2.1).

2) contrary to paper documents, the semantics of electronic documents can in certain cases change according to the environment in which they are visualized. The TOE takes part in the control of the invariance of the semantics of the documents to be signed (see 2.1.2.2).

3) the TOE allows the signatory to view the attributes which will be signed jointly with the document, thanks to the component allowing the view of the signature attributes (see 2.1.2.3)

2.1.2.1 Component allowing to view the documents to be signed

The signatory must be able to view the content of the electronic document to be signed before the creation of the electronic signature.

The TOE must allow, on request of the signatory, the execution of a viewer application corresponding to the format of the document to be viewed. This format is provided to the TOE directly by the user, or is validated by the user.

For this purpose, the TOE manages the association between the supported formats of document and the viewer applications The list of applications to be executed by the TOE are defined by the administrator of the TOE. These viewer applications are out of the TOE scope.

Application note:

In the absence of qualified viewer external applications, it is recommended that the product integrates an internal module for documents viewing and that this module is included in the TOE scope.

In this case, the product is still compliant with the requirements of this PP if its security target contains threats, assumptions, OSP, security objectives and security requirements related to the existence of this viewer module.

2.1.2.2 Component controlling the invariance of the document semantics

The document to be signed can contain variable fields or active code which depends on external parameters and which thus could be different according to the context where the document is viewed.

In some cases, the signatory could thus sign an electronic document which contents may vary according to the context where it is viewed.

In addition, the verifier who will receive the signature can also be misled. He could view a document semantically different from the one presented to the signatory.

Thus, the content of the document to be signed 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 document's semantics is thus out of the evaluation scope.

The TOE must inform the signatory if the external module detects that the semantics of the document is not invariant (i.e. that the document is “unstable”) or that it cannot be controlled.

According to the signature policy, the TOE adopts one of the following behaviors, if the semantics of the document can not be considered as invariant:

- either the signature policy forces to cancel the process of signature,
- or the signature policy does not force to cancel this process, but in this case the TOE must inform the signatory and he can then decide to bypass the warning and to sign anyway.

Application note:

In the absence of external application of control of qualified semantics invariance, it is recommended that the product integrates an internal module allowing this control and that this module belongs to the TOE. The document's format is fixed in the TOE and the content of this format cannot vary by construction.

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

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

2.1.2.3 Component allowing the view of the signature attributes

The TOE allows the signatory to view the signature attributes selected before generating the signature.

2.1.3 Component managing/implementing the signature policy

A signature policy is a set of rules for the creation or the validation of electronic signatures.

At the signature creation, a subset of the signature policy must be applied. This subset defines the necessary minimal requirements so that the signature can be accepted.

Among these requirements, requirements on the signatory's certificate can be found, such as:

- A list of identifiers of certification policies acceptable for the signatory;
- Informations concerning the usage of the private key (*key usage*);
- Extensions required for the certificate (*QCstatements*).

Requirements related to other attributes can also be found:

- Types of commitment authorized for this policy
- ...

The TOE must support one of the two following alternatives:

- it uses one or more signature policies stored in the form of executable code (fixed policies)
- it uses signature policies in the form of interpretable files by the TOE (configurable policies)

2.1.4 Component formatting/hashing the data to be signed

This component formats the data to be signed as well as the attributes of the signature to produce the “Data To Be Signed Representation (DTBSR)” this representation could be

- a formatted hash-value of all the data to be signed,
- or an intermediate hash-value of a first part of the data to be signed and the remaining part of the data to be signed,
- or all the data to be signed.

2.1.5 Component piloting the interface with the SCDev

To be able to interact with the SCDev, this component uses software and/or middleware components. This *middleware* is out of the TOE scope.

The component piloting the interface with the SCDev provides the following functions:

- To obtain from the SCDev the references of the certificates usable by the signatory, or the certificates themselves;
- To indicate to the SCDev the signature key to be activated;
- To transfer the DTBSR to the SCDev;
- For each signed document, to receive from the SCDev the electronic signature as well as the carrying out status indicating the success or the failure of the signature creation process;
- To check the conformity of the electronic signature regarding the data to be signed;
- To manage (open or close) sessions with the SCDev.

Note: The term “session” is defined here as “the period of time during which the private key of the signatory is activated in the SCDev and during which the signatory can generate signatures. A session starts as soon as the signatory correctly authenticates himself to the SCDev (through the TOE) in order to use his pair private key/given certificate. It finishes when the TOE closes it explicitly.”

2.2 Note: The conformity check of the electronic signature shall be done regarding the data to be signed. In particular, when the

SCDev performs all or part of the calculation of the hash value, the TOE shall check the conformity of the hash returned by the SCDev. When the DTBSR sent by the TOE to the SCDev is a hash, the check of the electronic signature conformity could be done regarding that transmitted hash.Environment of use of the TOE

The electronic signature creation application is integrated on a host platform (a personal computer, a public terminal, a personal organizer...).

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

- the operating system of the host platform,
- the software components installed on the operating system allowing to communicate with the SCDev (e.g. PKCS#11 drivers or cryptographic service providers (CSP) defining a cryptographic interface called by the signature application to access a module generating the signature),
- the software allowing to view the document to be signed and alerting the signatory if its characteristics are not completely compatible with the characteristics of display required by the document (use of color, presence of the necessary fonts,...).
- the software and/or hardware component controlling the invariance of the document's semantics (checks if the document's semantics does not depend on external parameters).
- the electronic SCDev (such as a smartcard, a USB token or a software component installed in the host platform).

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 a 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 *standard qualification* process [QUA-STD].

3.3 PP claim

This PP does not claim conformance with any other PP.

3.4 Conformance statement

The conformance 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

This section states the user (the signatory) data which must be protected by the TOE.

4.1.1.1 Document to be signed

D.Signatory's_Document

The signatory's document (SD) during the invocation of the signature process could contain:

- o either a single electronic document, or
- o several electronic documents.

Protection: integrity, confidentiality

Application note

As seen in section 2.1.1.1, a document is defined as

- o either a single electronic document,
- o or an electronic document with one or several signatures attached.

4.1.1.2 Data to be signed

The following assets correspond to successive representations of the data to be signed.

They require an integrity protection.

D.Data_To_Be_Signed

The Data To Be Signed (DTBS) are information for which electronic signature is needed.

They include:

- o the document to be signed,
- o the signature attributes explicitly selected by the signatory or implicitly selected by the application.

The signature attributes must contain:

- o the signatory's certificate or a non-ambiguous reference of this certificate

The signature attributes could contain:

- o the reference to the signature policy,
- o the type of commitment,
- o the presumed place of the signature,
- o the presumed date/hour of the signature,
- o the format of the contents,
- o ...

Protection: integrity, confidentiality

D.DTBS_Formatted

These data correspond to a first formatting of the data to be signed (envelope).

Protection: integrity, confidentiality

D.DTBS_Digest

These data are the hash of the formatted DTBS.

Protection: integrity

D.DTBS_Representation

This asset corresponds to the hash of the data to be signed after having undergone a formatting operation, before its sending to the SCDev.

Protection: integrity

4.1.1.3 Data returned by the TOE

D.Electronic_Signature

The Electronic Signature is an envelope containing:

- the DTBS hash,
- the signature;
- additional data facilitating the verification of the signature

This asset must be to protected by the TOE during its generation before its transmission to the signatory.

Protection: integrity

4.1.2 TOE sensitive assets (TSF data)

This section defines the assets of the TOE involved in the TOE operations.

D.Signature_Policy

The TOE performs the signature operations according to a signature policy.

Protection: integrity

D.Services

This asset represents the executable code implementing the services provided by the TOE.

Protection: integrity

D.Data_Representations_Association

The data within the TOE often have a representation different from those presented to the signatory or input to the TOE.

Example #1: the type of commitment (e.g. “read and approved”) of the signatory could be internally represented by an OID whereas it is presented explicitly to the signatory in the interface.

Example #2: the document format could be internally represented by 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 presented to the signatory.

Protection: integrity

4.2 Roles / Subjects

S.Signatory

The signatory interacts with the TOE to sign one or more documents according to a signature policy.

S.Security_Administrator

The Security Administrator of the TOE is responsible for the following operations:

- management of the association between the supported formats of document and the viewer applications
- management of configuration setting determining if the TOE can sign a document considered to be unstable.
- if the TOE allows the configuration of the signature policies, management of the list of the signature policies usable by the TOE.

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 definition of the threats is not necessary. In this case, the section is not applicable and is therefore 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 validity of the created signature

P.Signatory_Certificate_Conformity

To avoid the creation of invalid signatures, the TOE must control that the certificate selected by the signatory is in compliant with the signature policy to be applied.

P.Signatory_Certificate_Validity

To avoid the creation of invalid signatures, the TOE must control that the certificate selected by the signatory is used during its validity period.

P.Signature_Attributes_Conformity

To avoid the creation of invalid signatures, the TOE must control:

- that the signature attributes selected by the signatory are in compliant with the signature policy to be applied, and
- that all the signature attributes required by the signature policy are present.

4.4.2 Control of the invariance of the document's semantics

P.Document_Stability_Control

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

According to the signature policy, the TOE adopts one of the following behaviors if the document's semantics is not invariant:

- either the signature policy forces to cancel the signature process.
- or the signature policy does not force to cancel it and in this case the TOE must inform the signatory and he can then decide to bypass the warning.

4.4.3 Presentation to the signatory of the document and of the signature attributes

P.Document_Presentation

The TOE must allow the signatory to view a reliable representation of the document to be signed.

The TOE must not allow the signature of a document if it cannot be viewed by the signatory.

P.Signature_Attributes_Presentation

The TOE must allow the signatory to view the signature attributes.

4.4.4 Compliance with standards

P.Hash_Algorithms

The hash algorithm(s) implemented in the TOE must not make it possible to create two documents producing the same hash.

The algorithms must conform to the ANSSI cryptography requirements [CRYPT-STD].

4.4.5 Interaction with the signatory

P.Multiple_Documents_Signature

The TOE must allow to sign in a row a finite number of documents, this number could possibly be one.

The agreement to sign given by the signatory for this or these documents will relate to the same signature attributes.

P.Signature_Process_Interruption

The signatory must be able to interrupt the process of signature before the activation of the signature key.

P.Explicit_Agreement

The TOE must compel the signatory to perform a succession of non-trivial operations to check the agreement of the signatory before executing the process of signature.

4.4.6 Miscellaneous

P.Certificate/Private_Key_Association

The TOE must transfer the necessary information to the SCDev so that it can activate the private key corresponding to the selected certificate.

P.Electronic_Signature_Export

At the end of the process of signature, the TOE must transmit to the signatory the Electronic signature of the document comprising at least:

- the signature of the document;
- the hash of all the data to be signed;
- a reference of the certificate (or the actual certificate) of the signatory;
- a reference of the applied signature policy.

Application note

Other information facilitating the verification of the signature can be added (e.g. the certificate of the signatory, time-stamping tokens, etc).

P.Administration

The TOE must allow the Security administrator to manage (to add/remove) the signature policies [D.Signature_Policy] and the table of association between the viewer applications and the document formats input to the TOE [D.DocFormat_Application_Association].

4.5 Assumptions

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

4.5.1 Assumptions on the operational environment

4.5.1.1 Assumptions on the host platform

A.Host_Platform

It is supposed that the host platform on which the TOE is installed is either directly under the responsibility of the signatory or under the control of the organization to which the signatory belongs or of which he is the customer.

The operating system of the host platform is supposed to provide separate execution contexts for the various processes executed.

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

- the host platform is protected from the 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

The role of Host administrator mentioned above is distinct from the role of Security administrator of the TOE which has particular prerogatives such as management of TOE sensitive assets and configuration parameters.

4.5.1.2 Assumptions on the SCDev

The following assumptions are related to the signature creation device itself and to the possible different interactions of the TOE environment with it.

A.SCDev

It is presumed that the SCDev has the capability to generate a digital signature from the data communicated by the TOE.

It is presumed that the SCDev performs the authentication of the signatory allowing him or not to use the private key corresponding to the selected certificate.

The SCDev is responsible for the protection of the signatory’s data.

The following data are presumed to be stored and used in a secure manner by the SCDev:

- Assets related to the generation of the signature:
  - the private key(s) of the signatory, protected in confidentiality and integrity;
  - the signatory's certificate(s) protected in integrity or, by default, a non ambiguous reference of the signatory's certificate(s);
  - the private key/certificate association, protected in integrity
- Assets related to the authentication of the signatory:
  - the authentication data of the signatory, protected in integrity and confidentiality;
  - the association between authentication data and the private key/certificate pair, protected in integrity (1)

(1) the association can concern an authentication data and private key/certificate pair. Thus, several pairs can be stored in the same SCDev. Their access could be protected by different authentication data.

A.TOE/SCDev_Communications

It is presumed that the software and/or hardware components providing the interface between the TOE and the SCDev is able to manage (to open/close) a secure channel guaranteeing the integrity and the exclusiveness of the communication.

Application note

The components implementing the communication between the TOE and the SCDev can contain various software and/or hardware components installed on the operating system (e.g. PKCS#11 drivers or cryptographic service providers (CSP) defining a cryptographic interface called by the signature application to access a module generating the signature).

A.Signatory_Authentication_Data_Protection

It is presumed that the software and hardware components allowing the signatory to authenticate himself to the SCDev in order to activate the private key corresponding to the selected certificate, guarantee the confidentiality and the integrity of the authentication data during the data entry and during the transfer of these data towards the SCDev.

4.5.1.3 Assumptions on document presentation

A.Document_Presentation

It is presumed that the system of signature creation on which the TOE is installed has one or several viewer applications which:

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

A.Previous_Signatures_Presentation

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

4.5.1.4 Assumption on the control of invariance of the document's semantics

A.Document_Stability_Control

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

4.5.2 Assumptions on the context of operations

A.Signatory_Presence

To avoid the modification of the list of the documents to be signed without his knowledge, the signatory is supposed to remain present between the moments when he wishes to sign the documents and when he enters his authentication data to activate the key of signature.

A.Trusted_Security_Administrator

The Security administrator of the TOE is presumed to be trusted, to be trained for the use of the TOE and to have the means necessary to the execution of his tasks.

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.Signature_Policy_Origin

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

4.5.3 Conclusion

Application note:

The assumptions must be realistic with respect to the product and of 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 compliance with this PP must transcript them as threats, and define corresponding security objectives and requirements.

5 Security objectives

5.1 Security objectives for the TOE

5.1.1 General objectives

O.Certificate/Private_Key_Association

The TOE shall transfer the necessary information to the SCDev so that it can activate the private key corresponding to the selected certificate.

5.1.2 Interactions with the signatory

O.Signature_Attributes_Presentation

The TOE shall present to the signatory an exact representation of the attributes that will be signed.

O.Explicit_Agreement

The TOE shall provide to the signatory the means of explicitly expressing (i.e., in a voluntary and non-ambiguous way) its agreement to select document(s) and to start the process of signature of the selected documents.

O.Signature_Process_Interruption

The TOE shall provide to the signatory the means to cancel the process of signature before the activation of the signature key.

O.Documents_To_Be_Signed

After the signatory's agreement for signature, the TOE shall guarantee that the actually processed documents correspond exactly to the documents selected to be signed.

If the signatory gives his agreement for several documents, the signature attributes used for the signature of each document shall to be identical.

5.1.3 Signature policy applications

O.Signatory_Certificate_Conformity

The TOE shall check that the certificate selected by the signatory is compliant with the signature policy to be applied.

O.Signatory_Certificate_Validity

The TOE shall control that the certificate selected by the signatory is used during its validity period.

Application note

The time reference used for this purpose is the time provided by the operating system of the host platform.

O.Signature_Attributes_Conformity

The TOE shall control the presence and the compliance of the signature attributes selected by the signatory with the signature policy to be applied.

O.Electronic_Signature_Export

At the end of the process of signature, the TOE shall transmit to the signatory the Electronic signature of the document containing at least:

- the signature of the document;
- the hash of all the data to be signed;
- a reference of the certificate (or the actual certificate) of the signatory;
- a reference of the applied signature policy.

Application note

Other information facilitating the verification of the signature can be added (e.g. the certificate of the signatory, time-stamping tokens, etc).

5.1.4 Data protection

O.Administration

The TOE shall allow the Security administrator to manage (to add/remove) the signature policies [D.Signature_Policy] and the table of association between the viewer applications and the document formats input to the TOE [D.DocFormat_Application_Association].

5.1.5 Cryptographic operations

O.Cryptographic_Operations

The TOE shall implement cryptographic algorithms having the following properties:

- the hash algorithms must not allow to create two documents producing the same hash
- the algorithms must conform to the ANSSI cryptography requirements [CRYPT-STD].

5.1.6 Control of the invariance of the document semantics

O.Document_Stability_Control

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

The TOE shall inform the signatory if this module determines that the document's semantics is unstable.

In this case, according to the signature policy, the TOE shall adopt one or the other of the following behaviors:

- if the signature policy forces to cancel the process of signature, TOE shall cancel the process of signature;
- if the signature policy does not force to cancel the process of signature, the TOE shall inform the signatory and he can then decide to bypass the warning.

5.1.7 Presentation of the documents to be signed

O.Viewer_Application_Execution

The TOE shall be able to execute an external application allowing the signatory to view the document to be signed.

To identify which viewer application to execute, the TOE shall manage the association between formats for which the TOE allows the signature and the associated viewer applications.

The TOE shall not allow the signature of a document if it cannot determine which viewer application to execute.

5.2 Security objectives for the operational environment

5.2.1 Security objectives for the host platform

OE.Host_Platform

The host platform on which the TOE is installed shall be either directly under the responsibility of the signatory or under the control of the organization to which the signatory belongs or of which he is the customer.

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

The following security measures shall be implemented:

- the host platform must be protected from the 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 which has particular prerogatives such as management of TOE sensitive assets and configuration paramaters.

5.2.2 Security objectives for the SCDev and its environment

The following security objectives are related to the signature creation device itself or the components of its environment allowing the interactions of the signatory or the TOE with it.

OE.SCDev

The SCDev shall have at least the capability to generate a signature of the data transmitted by the TOE. Moreover, the SCDev shall perform the authentication of the signatory allowing him to use the private key corresponding to the selected certificate.

The SCDev is responsible for the protection of the signatory data. The following data shall be stored and used in a secure manner by the SCDev:

- Assets related to the generation of the signature:
  - the private key(s) of the signatory, protected in confidentiality and integrity;
  - the actual certificate(s) protected in integrity or, by default, a reference to the certificate(s) of the signatory;
  - the private key/certificate association, protected in integrity
- Assets related to the authentication of the signatory:
  - the authentication data of the signatory, protected in integrity and confidentiality;
  - the association between authentication data and the private key/certificate pair, protected in integrity

OE.TOE/SCDev_Communications

The software and/or hardware components providing the interface between the TOE and the SCDev shall be able to manage (to open/close) a secure channel guaranteeing the integrity and the exclusiveness of the communication.

OE.Signatory_Authentication_Data_Protection

The software/hardware components allowing the signatory to authenticate himself to the SCDev in order to activate the private key corresponding to the selected certificate, shall guarantee the confidentiality and the integrity of the authentication data of during the data input and during the transfer of these data towards the SCDev.

5.2.3 Presence of the signatory

OE.Signatory_Presence

The signatory shall remain present between the moments when he agrees to sign the documents and when he enters his authentication data to activate the key of signature.

Application note

If for any reason the signatory cannot remain present, he must start again the process from the beginning: selection of the documents to be signed, selection of the attributes, etc

5.2.4 Document presentation

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,
- either warn the signatory of possible problems of incompatibilities between the viewer application and the characteristics of the document.

In case the document to be signed already contains signatures, the environment of the TOE allows the signatory at least to know the identity of previous signatories, at best to verify the validity of these signatures.

5.2.5 Miscellaneous

OE.Document_Stability_Control

The environment of the TOE shall provide a module able to determine if the semantics of the document to be signed is invariant and to communicate the status of this analysis to the TOE.

OE.Signature_Policy_Origin

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

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.

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.

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 item, such as the rewording of a sentence for correctness with English grammar. This modification must not change the meaning of the requirement.
- *Refinement*: refinement which allow to add precisions or to limit the set of acceptable implementations for a requirement item or for all the requirement items 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 Signatory	a document to be signed	To import the document	**The Signatory:** - signature policy - signatory's explicit agreement to sign the document if is not stable **a document to be signed:** - document's identifier - document's stability status
the Signatory	the signatory's certificate	To import the signatory's certificate	**The Signatory:** - applied signature policy **the signatory's certificate:** - key usage status - QCStatement if required by the signature policy - certificate identifier
- the Signatory - the SCDev	- the formatted DTBS - the electronic signature	To transfer the formatted DTBS to the SCDev	**The Signatory:** - applied signature policy - signatory's certificate - signatory's explicit agreement to sign an unstable document **the formatted DTBS:** - the formatted DTBS **the Electronic signature:** - signature policy identifier - commitment type - claimed role - presumed signature date and time - presumed signature location

Subject	Object / Information	Operation	Security attributes
- the Signatory - the SCDev	the Electronic signature	To export the Electronic signature to the Signatory	**The SCDev** - the status of signature generation process **the Electronic signature:** - the generated electronic signature - the signed document's hash - the reference to the signatory's certificate - the reference of the applied signature policy

6.1.1 Document stability control

The following requirements are related to the control of the invariance of the signed document's semantics.

6.1.1.1 Control during 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 signatory,**
- **information: a document to be signed**
- **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 signatory (signature policy, signatory's explicit agreement to sign the document if is not stable)**
- **information: a document to be signed (document's identifier, document's stability status)**
- **operation: to import the document**

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:

Importation 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 signatory explicitly acknowledges to bypass the control**.

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 the means:

- to execute an external module controlling if the semantics of the document to be signed is invariant,
- to warn the signatory of the document if the semantics is not invariant,
- to ask the signatory's explicit agreement to continue the signature process if the semantics of the document is not invariant and if the security policy authorises to bypass the control.

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,**
- **the document shall invoque an external module in charge of controlling that the semantics of the document to be signed is invariant,**
- **the document shall inform the signatory when the document's semantics is not stable**.

Refinement:

The TOE shall inform the signatory 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/Selected documents Management of security attributes

FMT_MSA.1.1/Selected documents The TSF shall enforce the **document acceptance information flow control policy** to restrict the ability to ***select*** the security attributes ***documents' to be signed identifiers*** to **the signatory**.

FMT_SMF.1/Selection of a list of documents Specification of Management Functions

FMT_SMF.1.1/Selection of a list of documents The TSF shall be capable of performing the following management functions:

- **selecting a list of documents to be signed**.

Refinement:

The TSF shall allow the selection of documents to be signed until the signatory has given his agreement to sign.

Application note

The list of the documents to be signed can not change after the signatory's signature agreement. Nevertheless he can cancel the signature process at any moment (see *FDP_ROL.2/Abort of the signature process*).

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 information flow 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**.

FMT_MSA.1/Signatory agreement to sign an unstable document Management of security attributes

FMT_MSA.1.1/Signatory agreement to sign an unstable document The TSF shall enforce the **document acceptance information flow control policy** to restrict the ability to ***modify*** the security attributes **signatory agreement to sign an unstable document** to **the signatory**.

FMT_SMF.1/Getting signatory agreement to sign an unstable document Specification of Management Functions

FMT_SMF.1.1/Getting signatory agreement to sign an unstable document The TSF shall be capable of performing the following management functions:

- **get the explicit agreement of the signatory to sign a document whose semantics is unstable**.

6.1.2 Interaction with the signatory

FDP_ROL.2/Abort of the signature process Advanced rollback

FDP_ROL.2.1/Abort of the signature process The TSF shall enforce **the signature generation information flow control policy** to permit the rollback of all the operations on the **electronic signature and its related attributes**.

FDP_ROL.2.2/Abort of the signature process [Editorial refinement] The TSF shall permit operations to be rolled back **[before the formatted DTBS are transferred to the SCDev**.

6.1.3 Validation rules

6.1.3.1 Validation rules related to the signature attributes

The following requirements deal with the signature attributes.

FMT_MSA.1/Signature attributes Management of security attributes

FMT_MSA.1.1/Signature attributes The TSF shall enforce the **signature generation information flow control policy** to restrict the ability to ***select*** the security attributes **signature attributes** to **the signatory**.

FMT_SMF.1 / Modification of signature attributes Specification of Management Functions

FMT_SMF.1.1 / Modification of signature attributes The TSF shall be capable of performing the following management functions:

- **permit the signatory to change the value of the signature attributes required by the applied signature policy**.

Refinement:

The TSF shall allow the modification of signature attributes until the signatory has given his agreement to sign.

6.1.3.2 Rules related to the signatory's certificate

The following requirements deal with the verification rules on the signatory's certificate.

FDP_IFC.1 / Signatory's certificate import Subset information flow control

FDP_IFC.1.1 / Signatory's certificate import The TSF shall enforce the **signatory's certificate information flow control policy** on

- **subjects: the signatory**
- **information:**
  - **the signatory's certificate**
- **operations:**
  - **to import the signatory's certificate**

FDP_IFF.1 / Signatory's certificate import Simple security attributes

FDP_IFF.1.1 / Signatory's certificate import The TSF shall enforce the **signatory's certificate information flow control policy** based on the following types of subject and information security attributes:

- **subjects: the signatory (applied signature policy)**
- **information: the signatory's certificate (key usage, Signature SFP)**.

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

To import the signatory's certificate

- **the "key usage" of the selected 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 if required by the signature policy (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)**.

FDP_IFF.1.3/Signatory's certificate import The TSF shall enforce the **other rules explicitly defined in the Signature SFP (eventually including the QCStatement)**.

FDP_IFF.1.4/Signatory's certificate import The TSF shall explicitly authorise an information flow based on the following rules:

- **controls succeed**.

FDP_IFF.1.5/Signatory's certificate import The TSF shall explicitly deny an information flow based on the following rules:

- **controls fail**.

FMT_MSA.3/Signatory's certificate import Static attribute initialisation

FMT_MSA.3.1/Signatory's certificate import The TSF shall enforce the **signatory's certificate information flow control policy** to provide ***restrictive*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/Signatory's certificate import [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/Signatory's certificate Management of security attributes

FMT_MSA.1.1/Signatory's certificate The TSF shall enforce the **signatory's certificate information flow control policy** to restrict the ability to ***select*** the security attributes **certificate identifier** to **the signatory**.

FDP_ITC.2/Signatory's certificate Import of user data with security attributes

FDP_ITC.2.1/Signatory's certificate The TSF shall enforce the **signatory's certificate information flow control policy** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2/Signatory's certificate The TSF shall use the security attributes associated with the imported user data.

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

FPT_TDC.1/Signatory's certificate Inter-TSF basic TSF data consistency

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

FPT_TDC.1.2/Signatory's certificate 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

The ST authors must here defines standards supported by the TOE.

FMT_SMF.1/Signatory's certificate selection Specification of Management Functions

FMT_SMF.1.1/Signatory's certificate selection The TSF shall be capable of performing the following management functions:

- **allow the signatory to select a certificate among the list of certificates suitable for the applied signature policy**.

6.1.4 Application of the Signature policy and generation of the signature

FDP_IFC.1/Signature generation Subset information flow control

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

- **subjects: the signatory, the SCDev**
- **information:**
  - **the formatted DTBS**
  - **the electronic signature (once generated)**
- **operations:**
  - **to transfer the formatted DTBS to the SCDev**.

FDP_IFF.1/Signature generation Simple security attributes

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

- **subjects: the signatory (applied signature policy, signatory's certificate, [assignment: any other signatory's attribute]), signatory's explicit agreement to sign the present non invariant document (see *FDP_IFF.1.2/Signature generation*, the SCDev ([assignment: SCDev's attribute])**
- **information: the formatted DTBS (the data to be signed format), the electronic signature (signature policy identifier, commitment type, claimed role, presumed signature date and time, presumed signature location, [assignment: list of supported signature attributes])**.

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

To transfer of the formatted DTBS:

- **to communicate the signature attributes to the signatory before the signature generation**
- **to launch the viewer corresponding to the document's format according to the document format/viewer association table**
- **to activate the signing key corresponding to the selected signatory's certificate.**

Electronic signature:

- **if the signature policy requires the inclusion of the signature attribute "signature policy identifier", then its value shall be included;**
- **if the signature policy requires the inclusion of the signature attribute "commitment type", then its value shall be included;**
- **if the signature policy restricts the values to be taken by the "commitment type" attribute, then its value shall be conformant to the signature policy;**

- **if the signature policy requires the inclusion of the signature attribute "claimed role", then its value shall be included;**
- **if the signature policy restricts the values to be taken by the "claimed role" attribute then its value shall be conformant to the signature policy;**
- **if the signature policy prevents the inclusion of the signature attribute "presumed signature date and time", then its value shall not be included;**
- **if the signature policy requires the inclusion of the signature attribute "presumed signature location", then its value shall be included;**
- **[assignment: any other supported rule on signature attributes]**.

FDP_IFF.1.3/Signature generation The TSF shall enforce the **others rules explicitly defined in the applied signature policy**.

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

- **Security attributes are compliant with Signature SFP**
- **and the formatted DTBS semantic control succeed**.

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

- **Security attributes are not compliant with the Signature SFP**
- **or the formatted DTBS semantics control fails**.

Application note

The TOE must provide the means for:

- the communication of the signature attributes to the signatory before the generation of the signature,
- the execution of a viewer application for the format of the document to be signed according to the association table “format/viewer”
- the activation of the signature private key associated with the selected signatory’s certificate.

Note that the conformance of the signatory's certificate with respect to the applied signature policy is not check in the present policy but in the *signatory's certificate information flow control policy* that is the subject of component *FDP_IFC.1/Signatory's certificate import*. In the present component the conformance of the signatory's certificate is assumed established.

FMT_MSA.3/Signature generation Static attribute initialisation

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

FMT_MSA.3.2/Signature generation [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.1/Explicit signatory agreement Import of user data without security attributes

FDP_ITC.1.1/Explicit signatory agreement The TSF shall enforce the **signature generation information flow control policy** when importing user data, controlled under the SFP, from outside of the TOE.

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

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

Application note

FDP_ITC.1.3: the ST author must identify the list of actions that the TOE will consider as a proof of agreement for signature.

6.1.5 Electronic signature export

FDP_IFC.1/Electronic signature export Subset information flow control

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

- **subjects:**
  - **the signatory,**
  - **the SCDev**
- **information:**
  - **the Electronic signature**
- **operations:**
  - **to export the Electronic signature to the signatory**.

FDP_IFF.1/Electronic signature export Simple security attributes

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

- **subjects:**
  - **the signatory ([assignment: signatory's security attributes])**
  - **the SCDev (the status of signature generation process, [assignment: any other SCDev attributes])**
- **information:**
  - **the Electronic signature (the generated electronic signature, the signed document's hash, the reference to the signatory's certificate, the reference of the applied signature policy, [assignment: list of signature attributes]**.

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

Export of the electronic signature to the signatory is allowed if the signature generation (performed by the SCDev) succeeded.

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

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

- **Signature generation succeeds**.

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

- **Signature generation fails**.

FDP_ETC.2/Electronic signature export Export of user data with security attributes

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

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

FDP_ETC.2.3/Electronic signature export 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/Electronic signature export The TSF shall enforce the following rules when user data is exported from the TOE: **[assignment: additional exportation control rules]**.

FMT_MSA.3/Electronic signature export Static attribute initialisation

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

FMT_MSA.3.2/Electronic signature export [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/SCDev signature generation status Management of security attributes

FMT_MSA.1.1/SCDev signature generation status The TSF shall enforce the **electronic signature export information flow control policy** to restrict the ability to ***modify*** the security attributes **SCDev's signature generation status** to **nobody**.

FMT_SMF.1/Getting SCDev's signature generation status Specification of Management Functions

FMT_SMF.1.1/Getting SCDev's signature generation status The TSF shall be capable of performing the following management functions:

- **getting the SCDev's signature generation status (discriminate whether the signature generation process completed or failed)**.

6.1.6 Cryptographic operations

FCS_COP.1 / Hash function Cryptographic operation

FCS_COP.1.1 / Hash function The TSF shall perform

- **hash generation** 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]**.

Application note:

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

6.1.7 User identification and authentication

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles

- **Signatory**
- **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 authentication reference document of the ANSSI [AUTH-STD].

6.1.8 TOE administration

6.1.8.1 Capability to view the document to be signed

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:

- **allow the administrator of the TOE to manage [assignment: management operations] the document format/viewer association table**.

Application note

In the "assignment", the ST author must define the operations on the document format/viewer association table allowed by the TOE to the security administrator. The possible operations could be addition and deletion of entries, the modification of the viewer application, etc.

6.1.8.2 Signature policy management

FMT_MTD.1/Management of the signature policies Management of TSF data

FMT_MTD.1.1/Management of the signature policies The TSF shall restrict the ability to ***[assignment: list of allowed management operations]*** the **signature policies** to **the security administrator of the TOE**.

Application note

The assignment must be consistent with the assignment of the component *FMT_SMF.1/Management of the signature policies*.

FMT_SMF.1/Management of the signature policies Specification of Management Functions

FMT_SMF.1.1/Management of the signature policies The TSF shall be capable of performing the following management functions: **[assignment: list of management functions to be provided by the TSF]**.

Application note

The assignment must be consistent with the assignment of the component *FMT_MTD.1/Management of the signature policies*.

6.2 Security Assurance Requirements

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

7 Rationale

7.1 Security objectives rationale

7.1.1 Organisational security policies (OSP)

7.1.1.1 Policies related to the validity of the created signature

P.Signatory_Certificate_Conformity This policy is covered by the *O.Signatory_Certificate_Conformity* objective which requires that the TOE controls the compliance of the certificate selected by the signatory with respect to the requirements of the signature policy.

P.Signatory_Certificate_Validity This policy is covered by the *O.Signatory_Certificate_Validity* objective which requires that the TOE controls that the certificate selected by the signatory is valid.

P.Signature_Attributes_Conformity This policy is covered by the *O.Signature_Attributes_Conformity* objective by requiring that the TOE controls the presence and the compliance of all the signature attributes required by the signature policy.

7.1.1.2 Control of the invariance of the document's semantics

P.Document_Stability_Control the organisational security policy *P.Document_Stability_Control* is covered:

- on the one hand by the security objective for the TOE *O.Document_Stability_Control* which requires that the TOE interacts with an external module in charge of controlling the invariance of the semantics of the signed document, and which defines the two alternative behaviors compliant with those defined in this policy;
- on the other hand, by the security objective for the TOE environment *OE.Document_Stability_Control* which requires that the environment of the TOE provides such a module.

7.1.1.3 Presentation of the document and of the signature attributes to the signatory

P.Document_Presentation the security policy is covered by the objectives *O.Viewer_Application_Execution* and *OE.Document_Presentation* which require:

- on the one hand that the TOE can execute an external viewer application related to the format of the document to be signed,
- in the other hand that the TOE prevents the signature of documents for which a viewer application cannot be executed.

P.Signature_Attributes_Presentation This policy is covered completely by the *O.Signature_Attributes_Presentation* objective which requires that the TOE offers to the

signatory a representation of the signature attributes compliant with those which will be signed.

7.1.1.4 Compliance with standards

P.Hash_Algorithms the organisational security policy is covered entirely by the *O.Cryptographic_Operations* objective which uses the same terms.

7.1.1.5 Interaction with the signatory

P.Multiple_Documents_Signature the policy is covered by the *O.Documents_To_Be_Signed* objective which requires that:

- o the TOE guarantees that the signed documents are those selected by the signatory (no addition, no suppression, no substitution of documents in the list);
- o that identical signature attributes are used when the signatory's agreement is related to a set of documents.

P.Signature_Process_Interruption This policy is covered by the *O.Signature_Process_Interruption* objective by requiring that the TOE provides the means of canceling the process of signature at any moment before the activation of the signature private key.

P.Explicit_Agreement This organisational security policy is covered by the *O.Explicit_Agreement* objective. This objective requires the signatory to express without ambiguity his agreement to sign.

7.1.1.6 Miscellaneous

P.Certificate/Private_Key_Association the organisational security policy *P.Certificate/Private_Key_Association* is completely covered by the security objective *O.Certificate/Private_Key_Association* which uses the same terms.

P.Electronic_Signature_Export the organisational security policy is covered entirely by the *O.Electronic_Signature_Export* objective which uses the same terms.

P.Administration the organisational security policy is covered on the one hand by the *O.Administration* objective which uses the same terms and on the other hand by the security objective on the environment *OE.Trusted_Security_Administrator* which ensures that the administrator of the TOE is not a threatening agent.

7.1.2 Assumptions

7.1.2.1 Assumptions on the operational environment

Assumptions on the host platform

A.Host_Platform This assumption is covered completely by the *OE.Host_Platform* objective which reuses all its elements.

Assumptions on the SCDev

A.SCDev the assumption is covered completely by the *OE.SCDev* objective which reuses all its elements.

A.TOE/SCDev_Communications This assumption is covered entirely by the *OE.TOE/SCDev_Communications* objective which reuses all its elements.

A.Signatory_Authentication_Data_Protection This assumption is covered entirely by the *OE.Signatory_Authentication_Data_Protection* objective which reuses all its elements.

Presentation of the document

A.Document_Presentation This assumption is covered entirely by the *OE.Document_Presentation* objective which reuses all its elements.

A.Previous_Signatures_Presentation This assumption is covered completely by the *OE.Document_Presentation* objective which reuses all its elements.

Assumption on the control of the invariance of the document's semantics

A.Document_Stability_Control the *A.Document_Stability_Control* assumption is covered by the security objective *OE.Document_Stability_Control* which reuses its elements.

7.1.2.2 Assumptions on the context of operations

A.Signatory_Presence the *A.Signatory_Presence* assumption is completely covered by the security objective *OE.Signatory_Presence* which reuses its elements.

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

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

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

7.1.3 Tables of coverage between Security problem definition and security objectives

Organisational security policies (OSP)	Security objectives	Rationale
P.Signatory_Certificate_Conformity	O.Signatory_Certificate_Conformity	Section 7.1.1
P.Signatory_Certificate_Validity	O.Signatory_Certificate_Validitylidity	Section 7.1.1
P.Signature_Attributes_Conformity	O.Signature_Attributes_Conformity	Section 7.1.1
P.Document_Stability_Control	O.Document_Stability_Control, OE.Document_Stability_Control	Section 7.1.1
P.Document_Presentation	O.Viewer_Application_Execution, OE.Document_Presentation	Section 7.1.1
P.Signature_Attributes_Presentation	O.Signature_Attributes_Presentation	Section 7.1.1
P.Hash_Algorithms	O.Cryptographic_Operations	Section 7.1.1
P.Multiple_Documents_Signature	O.Documents_To_Be_Signed	Section 7.1.1
P.Signature_Process_Interruption	O.Signature_Process_Interruption	Section 7.1.1
P.Explicit_Agreement	O.Explicit_Agreement	Section 7.1.1
P.Certificate/Private_Key_Association	O.Certificate/Private_Key_Association	Section 7.1.1
P.Electronic_Signature_Export	O.Electronic_Signature_Export	Section 7.1.1

Organisational security policies (OSP)	Security objectives	Rationale
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.Certificate/Private_Key_Association	P.Certificate/Private_Key_Association
O.Signature_Attributes_Presentation	P.Signature_Attributes_Presentation
O.Explicit_Agreement	P.Explicit_Agreement
O.Signature_Process_Interruption	P.Signature_Process_Interruption
O.Documents_To_Be_Signed	P.Multiple_Documents_Signature
O.Signatory_Certificate_Conformity	P.Signatory_Certificate_Conformity
O.Signatory_Certificat_Validity	P.Signatory_Certificate_Validity
O.Signature_Attributes_Conformity	P.Signature_Attributes_Conformity
O.Electronic_Signature_Export	P.Electronic_Signature_Export
O.Administration	P.Administration
O.Cryptographic_Operations	P.Hash_Algorithms
O.Document_Stability_Control	P.Document_Stability_Control
O.Viewer_Application_Execution	P.Document_Presentation
OE.Host_Platform	
OE.SCDev	
OE.TOE/SCDev_Communications	
OE.Signatory_Authentication_Data_Protection	
OE.Signatory_Presence	
OE.Document_Presentation	P.Document_Presentation
OE.Document_Stability_Control	P.Document_Stability_Control
OE.Signature_Policy_Origin	
OE.Trusted_Security_Administrator	P.Administration
OE.Services_Integrity	

Table3 Security objectives coverage by OSP

Assumptions	Security objectives for the operational environment	Rationale
A.Host_Platform	OE.Host_Platform	Section 7.1.2
A.SCDev	OE.SCDev	Section 7.1.2
A.TOE/SCDev_Communications	OE.TOE/SCDev_Communications	Section 7.1.2
A.Signatory_Authentication_Data_Protection	OE.Signatory_Authentication_Data_Protection	Section 7.1.2
A.Document_Presentation	OE.Document_Presentation	Section 7.1.2
A.Previous_Signatures_Presentation	OE.Document_Presentation	Section 7.1.2
A.Document_Stability_Control	OE.Document_Stability_Control	Section 7.1.2
A.Signatory_Presence	OE.Signatory_Presence	Section 7.1.2
A.Trusted_Security_Administrator	OE.Trusted_Security_Administrator	Section 7.1.2
A.Services_Integrity	OE.Services_Integrity	Section 7.1.2
A.Signature_Policy_Origin	OE.Signature_Policy_Origin	Section 7.1.2

Table4 Assumptions coverage by security objectives for the operational environment

Security objectives for the operational environment	Assumptions
OE.Host_Platform	A.Host_Platform
OE.SCDev	A.SCDev
OE.TOE/SCDev_Communications	A.TOE/SCDev_Communications
OE.Signatory_Authentication_Data_Protection	A.Signatory_Authentication_Data_Protection
OE.Signatory_Presence	A.Signatory_Presence
OE.Document_Presentation	A.Document_Presentation, A.Previous_Signatures_Presentation
OE.Document_Stability_Control	A.Document_Stability_Control
OE.Signature_Policy_Origin	A.Signature_Policy_Origin
OE.Trusted_Security_Administrator	A.Trusted_Security_Administrator
OE.Services_Integrity	A.Services_Integrity

Table5 Security objectives for the operational environment coverage by assumptions

7.2 Security requirements rationale

7.2.1 Objectives

7.2.1.1 Security objectives for the TOE

General objectives

O.Certificate/Private_Key_Association the objective is covered by the requirement *FDP_IFF.1/Signature generation*. This requirement requires that the TOE is able to activate the private key of signature corresponding to the certificate selected by the signatory.

Interaction with the signatory

O.Signature_Attributes_Presentation the objective is covered by the *FDP_IFF.1/Signature generation* requirement which requires in particular that the TOE can present the signature attributes to the signatory before the beginning of the signature process.

O.Explicit_Agreement the objective is covered by the *FDP_ITC.1/Explicit signatory agreement* requirement by which the TOE requires that a succession of non-trivial operations is carried out before considering the effective agreement to sign.

O.Signature_Process_Interruption the objective is covered by the *FDP_ROL.2/Abort of the signature process* requirement which ensures that the signatory has the possibility of canceling the signature before sending the data to the SCDev.

O.Documents_To_Be_Signed the objective is covered by the functional requirements:

- *FMT_MSA.1/Selected documents* which restricts the capacity to select documents to be signed to the signatory only.
- *FMT_SMF.1/Selection of a list of documents* which requires that the TOE allows to select documents to be signed as long as the signatory did not give his agreement to sign.
- *FMT_MSA.1/Signature attributes* which restricts to the signatory only the capacity to select the signature attributes.
- *FMT_SMF.1/Modification of signature attributes* which requires that the TOE makes it possible to modify the value of the signature attributes as long as the signatory did not give his agreement to sign.

As a consequence, the same signature attributes will be applied to all the selected documents.

Application of a signature policy

O.Signatory_Certificate_Conformity the objective is covered in the following way:

The TOE must apply a flow control policy during the importation of a certificate (*FDP_IFC.1/Signatory's certificate import*). The functional component *FDP_IFF.1/Signatory's certificate import* defines that this policy allows the importation of

the certificate in the TOE if the rules defined in the signature policy are fulfilled. These rules are related to the signatory's certificate. The compliance of the selected certificate is guaranteed if its attributes fulfill the rules defined in the signature policy.

The functional components *FDP_ITC.2/Signatory's certificate* and *FPT_TDC.1/Signatory's certificate* ensure on the one hand that the TOE applies the rules of the flow control policy during the importation of the selected certificate and on the other hand that the TOE is able to exploit the data contained in the imported 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/Signatory's certificate importation* guarantees that the default values assigned to the attributes of security concerned in the flow control policy take restrictive values.
- The functional components *FMT_MSA.1/Signatory's certificate* and *FMT_SMF.1/Signatory's certificate selection* guarantee to the signatory the exclusive right to select the suitable certificate for electronic signatures he wishes to perform.
- 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 realization of any operation before having identified successfully the user.

O.Signatory_Certificat_Validity the objective is covered in the following way:

The TOE must apply a flow control policy during the importation of a certificate (*FDP_IFC.1/Signatory's certificate import*). The functional component *FDP_IFF.1/Signatory's certificate import* defines that this policy allows the importation of the certificate in the TOE if the rules defined in the signature policy are fulfilled. These rules are related to the signatory's certificate. The compliance of the selected certificate is guaranteed if its attributes fulfill the rules defined in the signature policy.

The functional components *FDP_ITC.2/Signatory's certificate* and *FPT_TDC.1/Signatory's certificate* ensure on the one hand that the TOE observes the rules of the flow control policy during the importation of the selected certificate and on the other hand that the TOE is able to exploit the data contained in the imported 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/Signatory's certificate importation* guarantees that the default values assigned to the security attributes concerned in the flow control policy take restrictive values.
- The functional components *FMT_MSA.1/Signatory's certificate* and *FMT_SMF.1/Signatory's certificate selection* guarantee to the signatory the exclusive right to select the suitable certificate for electronic signatures he wishes to perform.
- Component *FMT_SMR.1* requires 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.

O.Signature_Attributes_Conformity the objective is covered in the following way:

The TOE must apply a flow control policy during the generation of a signature (*FDP_IFC.1/Signature generation*). The functional component *FDP_IFF.1/Signature generation* defines that this policy allows the generation of the signature (i.e. the sending of the formatted DTBS to the SCDev) if the rules defined in the signature policy are fulfilled. This component also defines rules related to the signature attributes. The compliance of the signature attributes is guaranteed if these attributes fill the rules defined in the 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/Signature generation* guarantees that the default values of the attributes concerned in the flow control policy have restrictive values.
- The functional component *FMT_MSA.1/Signature attributes* and *FMT_SMF.1/Modification of signature attributes* guarantee to the signatory the exclusive right to select the suitable certificate for electronic signatures he wishes to perform.
- Component *FMT_SMR.1* requires 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 realization of any operation before having identified successfully the user.

O.Electronic_Signature_Export the objective is covered in the following way:

The TOE must apply an information flow control policy during the importation of a document into the TOE (*FDP_IFC.1/Electronic signature export*). The functional component *FDP_IFF.1/Electronic signature export* defines the rules to be applied by the TOE to export the created Electronic signatures.

The component *FDP_ETC.2/Electronic signature export* requires that the TOE executes an external module to determine if the document's semantics is invariant or not, when it imports the document to be signed.

The following 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 export* guarantees that the default values of the security attributes concerned in the flow control policy have restrictive values.
- The functional component *FMT_SMF.1/Getting SCDev's signature generation status* requires that the TOE is able to receive from the SCDev the status of the operation of generation of the digital signature.
- The functional component *FMT_MSA.1/SCDev signature generation status* which does not allow anybody to modify the status of the operation of generation of the signature returned by the SCDev.
- 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.

Data protection

O.Administration the objective is covered by the following functional components:

- *FMT_SMR.1* which requires that the TOE distinguishs the role of Security administrator from the role of signatory;
- *FMT_MTD.1/Document format/viewer association table* and *FMT_SMF.1/Management of the document format/viewer association table* which allows the Security administrator of the TOE (and only him) to modify the table of association between the document formats and the viewer applications;
- *FMT_SMF.1/Management of the signature policies* which defines the operations of management of the signature policies and *FMT_MTD.1/Management of the signature policies* which restricts their use to the Security administrator of the TOE.

Cryptographic operations

O.Cryptographic_Operations the objective is covered by the requirement *FCS_COP.1/Hash function* which allows the security targets authors to define the hash algorithms implemented in the TOE.

Control of the invariance of the document's semantics

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

The TOE must apply a flow control policy during the importation of a document into the TOE (*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 execute an external module to determine if the document's semantics is invariant or not when it imports the document.

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's acceptance* guarantees that the default values of the security attributes concerned in the flow control policy have restrictive values.
- The functional components *FMT_MSA.1/Document's semantics invariance status* and *FMT_SMF.1/Getting document's semantics invariance status* which require on the one hand that the TOE has a means of executing 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.
- The functional components *FMT_MSA.1/Signatory agreement to sign an unstable document* and *FMT_SMF.1/Getting signatory agreement to sign an unstable document* guarantee that only the signatory can modify the attribute allowing the TOE to continue the signature process of a document whose semantics is not considered as invariant.
- Component *FMT_SMR.1* requires 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 realization of any operation before having identified successfully the user.

Presentation of the documents to be signed

O.Viewer_Application_Execution the objective is covered by the following components:

- *FDP_IFF.1/Signature generation*, which ensures that the user will be able to view the document through an external viewer application. The TOE automatically executes 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* guarantees that the contents of the *list of associations document format /viewer* can be modified only by an administrator.

7.2.2 Tables of coverage between security objectives and security requirements

Security objectives	Functional requirements	Rationale
O.Certificate/Private_Key_Association	FDP_IFF.1/Signature generation	Section 7.2.1
O.Signature_Attributes_Presentation	FDP_IFF.1/Signature generation	Section 7.2.1
O.Explicit_Agreement	FDP_ITC.1/Explicit signatory agreement	Section 7.2.1
O.Signature_Process_Interruption	FDP_ROL.2/Abort of the signature process	Section 7.2.1
O.Documents_To_Be_Signed	FMT_MSA.1/Selected documents, FMT_SMF.1/Selection of a list of documents, FMT_MSA.1/Signature attributes, FMT_SMF.1/Modification of signature attributes	Section 7.2.1
O.Signatory_Certificate_Conformity	FDP_IFC.1/Signatory's certificate import, FDP_IFF.1/Signatory's certificate import, FDP_ITC.2/Signatory's certificate, FPT_TDC.1/Signatory's certificate, FMT_MSA.3/Signatory's certificate import, FMT_MSA.1/Signatory's certificate, FMT_SMF.1/Signatory's certificate selection, FMT_SMR.1, FIA_UID.2	Section 7.2.1

Security objectives	Functional requirements	Rationale
O.Signatory_Certificate_Validity	FDP_IFC.1/Signatory's certificate import, FDP_IFF.1/Signatory's certificate import, FDP_ITC.2/Signatory's certificate, FPT_TDC.1/Signatory's certificate, FMT_MSA.3/Signatory's certificate import, FMT_MSA.1/Signatory's certificate, FMT_SMF.1/Signatory's certificate selection, FMT_SMR.1, FIA_UID.2	Section 7.2.1
O.Signature_Attributes_Conformity	FDP_IFC.1/Signature generation, FDP_IFF.1/Signature generation, FMT_MSA.3/Signature generation, FMT_MSA.1/Signature attributes, FMT_SMF.1/Modification of signature attributes, FMT_SMR.1, FIA_UID.2	Section 7.2.1
O.Electronic_Signature_Export	FDP_IFC.1/Electronic signature export, FDP_IFF.1/Electronic signature export, FDP_ETC.2/Electronic signature export, FMT_MSA.3/Electronic signature export, FMT_MSA.1/SCDev signature generation status, FMT_SMR.1, FMT_SMF.1/Getting SCDev's signature generation status, FIA_UID.2	Section 7.2.1

Security objectives	Functional requirements	Rationale
O.Administration	FMT_SMF.1/Management of the document format/viewer association table, FMT_MTD.1/Document format/viewer association table, FMT_SMR.1, FMT_MTD.1/Management of the signature policies, FMT_SMF.1/Management of the signature policies	Section 7.2.1
O.Cryptographic_Operations	FCS_COP.1/Hash function	Section 7.2.1
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_MSA.1/Signatory agreement to sign an instable document, FMT_SMR.1, FMT_SMF.1/Getting document's semantics invariance status, FMT_SMF.1/Getting signatory agreement to sign an instable document, FIA_UID.2	Section 7.2.1
O.Viewer_Application_Execution	FDP_IFF.1/Signature generation, FMT_MTD.1/Document format/viewer association table, FMT_SMF.1/Management of the document format/viewer association table	Section 7.2.1

Table6 Security objectives for the TOE coverage by functional requirements

Functional requirements	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/Selected documents	O.Documents_To_Be_Signed
FMT_SMF.1/Selection of a list of documents	O.Documents_To_Be_Signed
FMT_MSA.1/Document's semantics invariance status	O.Document_Stability_Control
FMT_SMF.1/Getting document's semantics invariance status	O.Document_Stability_Control
Unstable FMT_MSA.1/Signatory agreement to sign year document	O.Document_Stability_Control
FMT_SMF.1/Getting signatory agreement to sign an unstable document	O.Document_Stability_Control
FDP_ROL.2/Abort off the signature process	O.Signature_Process_Interruption
FMT_MSA.1/Signature attributes	O.Documents_To_Be_Signed, O.Signature_Attributes_Conformity
FMT_SMF.1/Modification of signature attributes	O.Documents_To_Be_Signed, O.Signature_Attributes_Conformity
FDP_IFC.1/Signatory's certificate import	O.Signatory_Certificate_Conformity, O.Signatory_Certificate_Validity
FDP_IFF.1/Signatory's certificate import	O.Signatory_Certificate_Conformity, O.Signatory_Certificate_Validity
FMT_MSA.3/Signatory's certificate importation	O.Signatory_Certificate_Conformity, O.Signatory_Certificate_Validity
FMT_MSA.1/Signatory's certificate	O.Signatory_Certificate_Conformity, O.Signatory_Certificate_Validity
FDP_ITC.2/Signatory's certificate	O.Signatory_Certificate_Conformity, O.Signatory_Certificate_Validity

Functional requirements	Security objectives
FPT_TDC.1/Signatory's certificate	O.Signatory_Certificate_Conformity, O.Signatory_Certificate_Validity
FMT_SMF.1/Signatory's certificate selection	O.Signatory_Certificate_Conformity, O.Signatory_Certificate_Validity
FDP_IFC.1/Signature generation	O.Signature_Attributes_Conformity
FDP_IFF.1/Signature generation	O.Certificate/Private_Key_Association, O.Signature_Attributes_Presentation, O.Signature_Attributes_Conformity, O.Viewer_Application_Execution
FMT_MSA.3/Signature generation	O.Signature_Attributes_Conformity
FDP_ITC.1/Explicit to sign agreement	O.Explicit_Agreement
FDP_IFC.1/Electronic signature export	O.Electronic_Signature_Export
FDP_IFF.1/Electronic signature export	O.Electronic_Signature_Export
FDP_ETC.2/Electronic signature export	O.Electronic_Signature_Export
FMT_MSA.3/Electronic signature export	O.Electronic_Signature_Export
FMT_MSA.1/SCDev signature generation status	O.Electronic_Signature_Export
FMT_SMF.1/Getting SCDev's signature generation status	O.Electronic_Signature_Export
FCS_COP.1/Hash function	O.Cryptographic_Operations
FMT_SMR.1	O.Signatory_Certificate_Conformity, O.Signatory_Certificate_Validity, O.Signature_Attributes_Conformity, O.Electronic_Signature_Export, O.Administration, O.Document_Stability_Control
FIA_UID.2	O.Signatory_Certificate_Conformity, O.Signatory_Certificate_Validity, O.Signature_Attributes_Conformity, O.Electronic_Signature_Export, O.Document_Stability_Control
FMT_MTD.1/Document format/viewer association table	O.Administration, O.Viewer_Application_Execution

Functional requirements	Security objectives
FMT_SMF.1/Management of the document format/viewer association table	O.Administration, O.Viewer_Application_Execution
FMT_MTD.1/Management of the signature policies	O.Administration
FMT_SMF.1/Management of the signature policies	O.Administration

Table7 Functional requirements coverage by security objectives for the TOE

7.3 Dependencies

7.3.1 Dependencies of the functional security requirements

Requirements	CC Dependencies	Satisfied Dependencies
FDP_ROL.2/Abort off the signature process	(FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.1/Signature generation
FDP_IFC.1/Signature generation	(FDP_IFF.1)	FDP_IFF.1/Signature generation
FDP_IFF.1/Signature generation	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Signature generation, FMT_MSA.3/Signature generation
FMT_MSA.3/Signature generation	(FMT_MSA.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_MSA.1/Signature attributes, FMT_MSA.1/Signatory's certificate
FDP_ITC.1/Explicit to sign agreement	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Signature generation, FMT_MSA.3/Signature generation
FDP_IFC.1/Electronic signature export	(FDP_IFF.1)	FDP_IFF.1/Electronic signature export
FDP_IFF.1/Electronic signature export	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Electronic signature export, FMT_MSA.3/Electronic signature export
FDP_ETC.2/Electronic signature export	(FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.1/Electronic signature export
FMT_MSA.3/Electronic signature export	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/SCDev signature generation status, FMT_SMR.1
FMT_MSA.1/SCDev signature generation status	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_IFC.1/Electronic signature export, FMT_SMF.1/Getting SCDev's signature generation status, FMT_SMR.1
FMT_SMF.1/Getting SCDev's signature generation status	No dependence	
FCS_COP.1/Hash function	(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	
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's acceptance

Requirements	CC Dependencies	Satisfied Dependencies
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's acceptance
FMT_MSA.3/Document's acceptance	(FMT_MSA.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_MSA.1/Selected documents, FMT_MSA.1/Document's semantics invariance status
FMT_MSA.1/Selected documents	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FDP_IFC.1/Document acceptance, FMT_SMF.1/Selection of a list of documents
FMT_SMF.1/Selection of a list of documents	No dependence	
FMT_MSA.1/Document's semantics invariance status	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FDP_IFC.1/Document acceptance, FMT_SMF.1/Getting document's semantics invariance status
FMT_SMF.1/Getting document's semantics invariance status	No dependence	
Unstable FMT_MSA.1/Signatory agreement to sign year document	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FDP_IFC.1/Document acceptance, FMT_SMF.1/Getting signatory agreement to sign an unstable document
FMT_SMF.1/Getting signatory agreement to sign an unstable document	No dependence	
FMT_MSA.1/Signature attributes	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_IFC.1/Signature generation, FMT_SMR.1, FMT_SMF.1/Modification of signature attributes
FMT_SMF.1/Modification of signature attributes	No dependence	
FDP_IFC.1/Signatory's certificate import	(FDP_IFF.1)	FDP_IFF.1/Signatory's certificate import
FDP_IFF.1/Signatory's certificate import	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Signatory's certificate import, FMT_MSA.3/Signatory's certificate importation
FMT_MSA.3/Signatory's certificate importation	(FMT_MSA.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_MSA.1/Signatory's certificate
FMT_MSA.1/Signatory's certificate	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FDP_IFC.1/Signatory's certificate import, FMT_SMF.1/Signatory's certificate selection

Requirements	CC Dependencies	Satisfied Dependencies
FDP_ITC.2/Signatory's certificate	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/Signatory's certificate import, FPT_TDC.1/Signatory's certificate
FPT_TDC.1/Signatory's certificate	No dependence	
FMT_SMF.1/Signatory's certificate selection	No dependence	
FMT_MTD.1/Document format/viewer association table	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1/Management of the document format/viewer association table
FMT_SMF.1/Management of the document format/viewer association table	No dependence	
FMT_MTD.1/Management of the signature policies	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1/Management of the signature policies
FMT_SMF.1/Management of the signature policies	No dependence	

Table8 Dependencies of the functional requirements

7.3.1.1 Rationale for the unsatisfied Dependencies

Dependence FCS_CKM.4 of FCS_COP.1/Hash function is not supported. The dependence with FCS_CKM.4 is not satisfied because the hash function does not require any cryptographic key.

Dependence FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 of FCS_COP.1/Hash function is not supported. The dependence with FCS_CKM.1, FDP_ITC.1 or FDP_ITC.2 is not satisfied because the hash function requires neither the generation nor the importation of keys in the TOE.

Dependence FTP_ITC.1 or FTP_TRP.1 of FDP_ITC.2/Signatory's certificate is not supported. The dependence between the component *FDP_ITC.2/Signatory's certificate* and one of components *FTP_ITC.1* or *TFP_TRP.1* is not satisfied because the protocols used in the public key infrastructures are self-protected and guaranteed, not immediately, but during the verification of the signature:

- the integrity of the certificates of the certification chain is guaranteed thanks to the self-signed certificate (or trusted point) defined in the signature policy whose integrity is maintained by the environment of the TOE
- during the verification of the signature, the fact of building a valid certification chain between the signatory's certificate and the trusted point defined in the

signature policy allows to guarantee the authenticity of the origin of the various certificates composing this chain.

- finally, the signatory's certificate does not require any confidentiality protection.

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 security 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 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 component AVA_VAN.3.

7.4 Evaluation assurance level rationale

The assurance level of this PP is EAL3+, because it is required by the ANSSI *qualification standard* process [QUA-STD].

7.5 EAL augmentation rationale

7.5.1 AVA_VAN.3 Focused vulnerability analysis

Augmentation required by the *qualification standard* process.

7.5.2 ALC_FLR.3 Systematic flaw remediation

Augmentation required by the *qualification standard* process.

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 Certification 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 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 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 a programming interface (API) provided by the operating system of the host platform.

Signature Creation Device (SCDev)

Hardware or software intended to apply the *signature-creation data 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 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.

Signature Verification Device

Hardware or software intended to apply the *signature-verification data 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 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

CSP Cryptographic Service Provider

CWA CEN Workshop Agreements

DTBS Data To Be Signed

DTBSR Data To Be Signed Representation

ETSI European Telecommunications Standards Institute

MMI Man-Machine Interface

OID Object Identifier

PKCS#11 Public Key Cryptography Standards

PP Protection profile

SCDev Signature Creation Device

SD Signatory's Document

SSCD Secure Signature Creation Device

TOE Target of Evaluation

Index

A

A.Document_Presentation 22
A.Document_Stability_Control 22
A.Host_Platform 20
A.Previous_Signatures_Presentation 22
A.SCDev 21
A.Services_Integrity 23
A.Signatory_Authentication_Data_Protection 22
A.Signatory_Presence 22
A.Signature_Policy_Origin 23
A.TOE/SCDev_Communications 22
A.Trusted_Security_Administrator 23

D

D.Data_Representations_Association 17
D.Data_To_Be_Signed 16
D.DocFormat_Application_Association 18
D.DTBS_Digest 17
D.DTBS_Formatted 17
D.DTBS_Representation 17
D.Electronic_Signature 17
D.Services 17
D.Signatorys_Document 16
D.Signature_Policy 17

F

FCS_COP.1/Hash__function 44
FDP_ETC.2/Electronic__signature__export 42
FDP_IFC.1/Document__acceptance 31
FDP_IFC.1/Electronic__signature__export 41
FDP_IFC.1/Signatory's__certificate__import 36
FDP_IFC.1/Signature__generation 38
FDP_IFF.1/Document__acceptance 31
FDP_IFF.1/Electronic__signature__export 41
FDP_IFF.1/Signatory's__certificate__import 36
FDP_IFF.1/Signature__generation 39
FDP_ITC.1/Document__acceptance 32
FDP_ITC.1/Explicit__signatory__agreement 41
FDP_ITC.2/Signatory's__certificate 37
FDP_ROL.2/Abort__of__the__signature__process 35
FIA_UID.2 44
FMT_MSA.1/Document's__semantics__invariance__status 34
FMT_MSA.1/SCDev__signature__generation__status 43
FMT_MSA.1/Selected__documents 33
FMT_MSA.1/Signatory__agreement__to__sign__an__unstable__document 34
FMT_MSA.1/Signatory's__certificate 37
FMT_MSA.1/Signature__attributes 35
FMT_MSA.3/Document's__acceptance 33
FMT_MSA.3/Electronic__signature__export 43
FMT_MSA.3/Signatory's__certificate__import 37
FMT_MSA.3/Signature__generation 40
FMT_MTD.1/Document__format/viewer__association__table 45
FMT_MTD.1/Management__of__the__signature__policies 46
FMT_SMF.1/Getting__document's__semantics__invariance__status 34
FMT_SMF.1/Getting__SCDev's__signature__generation__status 43
FMT_SMF.1/Getting__signatory__agreement__to__sign__an__unstable__document 35
FMT_SMF.1/Management__of__the__document__format/viewer__association__table 45
FMT_SMF.1/Management__of__the__signature__policies 46
FMT_SMF.1/Modification__of__signature__attributes 35
FMT_SMF.1/Selection__of__a__list__of__documents 34
FMT_SMF.1/Signatory's__certificate__selection 38
FMT_SMR.1 44
FPT_TDC.1/Signatory's__certificate 38

O

O.Administration 25
O.Certificate/Private_Key_Association 24
O.Cryptographic_Operations 25
O.Document_Stability_Control 25
O.Documents_To_Be_Signed 24
O.Electronic_Signature_Export 25
O.Explicit_Agreement 24
O.Signatory_Certificate_Conformity 24
O.Signatory_Certificate_Validity 24
O.Signature_Attributes_Conformity 25
O.Signature_Attributes_Presentation 24
O.Signature_Process_Interruption 24
O.Viewer_Application_Execution 26
OE.Document_Presentation 27
OE.Document_Stability_Control 28
OE.Host_Platform 26
OE.SCDev 26
OE.Services_Integrity 28
OE.Signatory_Authentication_Data_Protection 27
OE.Signatory_Presence 27
OE.Signature_Policy_Origin 28
OE.TOE/SCDev_Communications 27
OE.Trusted_Security_Administrator 28

P

P.Administration 20
P.Certificate/Private_Key_Association 20
P.Document_Presentation 19
P.Document_Stability_Control 19
P.Electronic_Signature_Export 20
P.Explicit_Agreement 20
P.Hash_Algorithms 19
P.Multiple_Documents_Signature 19

P.Signatory_Certificate_Conformity..... 18
P.Signatory_Certificate_Validity..... 19
P.Signature_Attributes_Conformity..... 19
P.Signature_Attributes_Presentation..... 19
P.Signature_Process_Interruption..... 20

S

S.Security_Administrator..... 18
S.Signatory..... 18