EURONOVATE

Security Target
Advanced E-Signature ENsoft v. 1.1

VERSION CONTROL

Version	Date	Author	Changes to Previous Version
1.0	11/02/2013	Giuseppe Mariani	Initial version
1.1	07/03/2013	Giuseppe Mariani	Revisioning par. 2
1.2	27/03/2013	Giuseppe Mariani	Utilization of FDP_RIP instead of an Extended Component
1.3	11/04/2013	Giuseppe Mariani	Revisioning par. 2 – TOE description
1.4	16/04/2013	Giuseppe Mariani	Revisioning par. 2 – TOE description
1.5	19/06/2013	Giuseppe Mariani	Revisioning SFR and other minor changes

Copyright notice

Table of Contents

1. SECURITY TARGET INTRODUCTION (ASE_INT)

This Security Target (ST) describes security objectives, requirements and motivations of the software application **ENSoft**, following named TOE, designed and manufactured by EURONOVATE SA. The TOE is an advanced electronic signature solution compliance to requirements provided by italian *"Codice dell'amministrazione digitale (DL 7 marzo 2005 n. 82 e successive modificazioni), ed alle regole tecniche previste dallo Schema di DPCM ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71, del d. l.gvo 7 marzo 2005 n. 82."*

Security Target identification

Titolo: Advanced E-Signature ENsoft v. 1.1
Data : february 2013

TOE identification

Nome del prodotto: ENSoft versione 1.1

Assurance level

Common Criteria EAL1 augmented with ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1

1.1 *OBJECTIVES OF DOCUMENT*

This document presents the Common Criteria (CC) Security Target (ST) to express the security and evaluation requirements for the EURONOVATE ENsoft product.
The product is designed and manufactured by EURONOVATE SA (http://www.euronovate.com/).
The Sponsor and Developer for the EAL1 evaluation is EURONOVATE SA.
The scope of the Security Target within the development and evaluation process is described in the Common Criteria for Information Technology Security Evaluation [CC]. In particular, a Security Target defines the IT security requirements of an identified TOE and specifies the functional and assurance security measures offered by that TOE to meet stated requirements [CC1, Section C.1].
Security Functional Requirements (SFRs), as defined in [CC2], are the basis for the TOE IT security functional requirements expressed in this Security Target. These requirements describe the desired security behaviour expected of a TOE and are intended to meet the security objectives as stated in this Security Target. Security Functional Requirements express security requirements intended to counter threats in the assumed operating environment of the TOE, and cover any identified organizational security policies and assumptions.

1.2 DOCUMENT ORGANIZATION

The Security Target contains the following additional sections:
TOE description: This section gives an overview of the TOE, describes the TOE in terms of its physical and logical boundaries, and states the scope of the TOE
Security environment definition: This section details the expectations of the environment, the threats that are countered by the TOE and the environment, and the organizational policy that the TOE must fulfill

Security objectives: This section details the security objectives of the TOE and environment
Security requirements: The section presents the security functional requirements (SFR) for the TOE and environment that supports the TOE, and details the assurance requirements
TOE summary specification: The section describes the security functions represented in the TOE that satisfy the security requirements
Rationale: This section closes the ST with the justifications of the security objectives, requirements and TOE summary specifications as to their consistency, completeness, and suitability.

1.3 TERMINOLOGY AND ACRONYMS

CC Common Criteria

DES Data Encryption Standard

ST Security Target

PP Protection Profile

TOE target of evaluation

EAL Evaluation Assurance Level

SAR Security Assurance Requirement

SF Security Function

SFR Security Functional Requirement

TSF TOE Security Function

TSFI TSF interface

IT Information Technology

PC Personal Computer

PDF Portable Document Format

DTBS data to be signed

DTBS/R data to be signed or its unique representation

DCA document creation application

SCA signature creation application

SSCD secure signature creation device

SSL Secure Socket Layer

PKCS Public-Key Cryptography Standards

HSM Hardware security module: a hardware security module is a cryptographic device, which can generate, store and use cryptographic keys within a secure hardware device.

User data PDF document + hash + biometric vector

1.4 REFERENCES

[RF1] Codice dell'amministrazione digitale (DL 7 marzo 2005 n. 82 e successive modificazioni)

[RF2] Schema di DPCM ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71, del d. l.gvo 7 marzo 2005 n. 82.

2. TOE DESCRIPTION

The TOE is a software application, named ENSoft, that have the function of governing to the process of electronic signature of a document.

The TOE is strictly tied to a tablet, that has the function of receiving user's signature and permitting the TOE utilization. Euronovate produces a proper tablet, named Ensign10, but the TOE can works with other tablet having similar characteristics.
Characteristics and functions of Ensign10 are described in the operational environment.

2.1 PHYSICAL SCOPE OF THE TOE

The components of the Euronovate solution are:

- "ENsoft" Sign Software
- Tablet Ensign version 10 inches

The operating models to use the mentioned solution provide:

- Installing the Software ENsoft (1) on the physical client (2) on the operator's position;
- The USB or DVI (3) connection between client and tablet Ensign 10 (4).

The figure nr 1 shows the operating context described before:

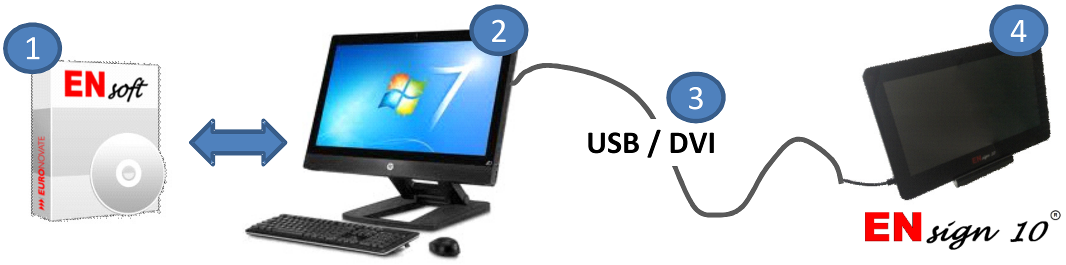

Figure 1 - TOE operational environment

2.2 TOE CHARACTERISTICS

2.2.1 Characteristics of ENSoft

Driver Communication

- Software driven Switch On/Off
- Encrypted communication between PC and Tablet
- Pen as mouse function during document viewing
- Calibration Functions for the device
- Encrypted biometric block
- Scanning on encrypted channel (encryption changes each acquisition) of the samples biometric signature.

PDF Manager

- PDF Scan to convert signature fields (present in PDF file as Hyperlink, Text, Bookmark) into e-signature fields in according to the PDF standard
- Insertion of the encrypted biometric block in the e-signature field of the PDF file

PDF Viewer

- View PDF on Tablet highlighting the signature fields with a dedicated “sensitive area”
- Document scrolling function using the provided pen only
- Document zoom functions

ENSoft includes the following parts:

- Low level Driver for communications with Device
- Layer of manipulation of PDF documents and management of biometric vector
- Reader PDF
- Socket SSL, allowing platform to be integrable by any application.

The architecture of ENSoft is modular. Each DLL solution manages a particular step of the signing process.
The input module is the ENDaemon that as Socket Server handles requests for signing, activating each time the underlying modules that satisfy the request.

The modules that make up the platform ENSoft are:

ENDaemon: This module is the manager of the SW signature. Listening on a port in Localhost is able to receive commands from any client that communicates via socket, turning them into actions on the form below. Receives PDF files to be signed, the public key to encrypt the biometric data, commands for setting the configuration and so on.
Also it is a manager of ENMarketing module, additional product to the platform ENSoft for the management of WebMarketing, DataManager and digital signage.

ENPresenter: Allows the "slideshow" of images contained in a subfolder of ENSoft. This module is the "embedded" release of the most complete module of ENMarketing (Digital Signage). This module is automatically launched by ENDaemon and can be used both to show some images in rotation from the first ignition SW and to put a logo fixed on the screen to identify the customer who uses our signature service.

ENViewer: This is the "core" of the user experience of the signing process. It's a custom PDF reader (does not require the presence of Adobe installed on the workstation) that allows you to view the PDF for signature, shows the signature fields to make them more identifiable by the client, manages the scroll of the document, zoom and navigation general.
This is the form of "FrontEnd" of all the SW solution and is the most impacted by the evolving demands of customers.

ENDocumentManager: This module is the manager of the PDF document. It identifies the signature fields, transforms them to ENViewer, manages the signing of integrity and actually knows the structure of the PDF. Is in charge of this module all processing (PDF/A - PDFFlat - etc ...) related to the production of the PDF.

ENSigner: This module is the only one in the SW structure to manage the customer's signature and the biometric data of this one. Hired directly from ENDocumentManager at the time of the request for a signature, open a box in the tablet that captures the biometric data and draws the customer's signature on the screen. The data are received directly from the tablet 3DES encrypted is decrypted in memory and is built from ENSigner the Biometric vector. Once the signature is done, the ENDocumentManager sends to ENSigner the Hash of the PDF document, which is "joined" to the biometric vector and everything is encrypted with the public key previously provided. At this point the data is returned to the ENDocumentManager that puts them with a signature of integrity in the "dictionary" of the signature field, setting as "apparence" the image of the customer's signature.
Once returned the encrypted biometric lock, the ENSigner overwrites the memory used for processing the data with the "blank" and then frees the memory variables.

ENCommon: This is a library of functions common to all the other modules and contains generic functions such as identification Tablet, window placement, Log management, etc. ...
It is used by all modules except the ENSigner that remains independent in the management of biometric data.

SDK: The software solution ENSoft also provides two other modules (SDK) written in JAVA and. NET that allow you to decouple the "language" of the Socket of the ENDaemon.
These contain a number of methods (API) for the use of the SW which simplify the application integration into the customer's information system.

ENCalligrapher: is a tool for extraction and analysis of signatures biometric data collected by software platform ENSoft.
Through the selection of each signature, the tool allows to visualize:

- information about the tablet used to acquire the data (model, firmware version, etc.);
- information about the software (version);
- information about the document (timestamp acquisition, period of acquisition, number of samples, etc.);

- graphical representation of signature acquired bringing in different colors the signature and movements in air;
- the graphical representation of the main components of a signature: X position, Y position, pressure, behavior, speed and acceleration.

2.3 IT ENVIRONMENT REQUIRED BY THE TOE

2.3.1 Workstation

The solution ENSoft has been developed for Windows systems. It is currently compatible with Windows XP SP3, Windows 7 and we are currently working on full compatibility with Windows 8. The drivers have been written in Visual C + + 2010 which then becomes a prerequisite for the functioning of the solution. All the "top" part of the SW was written in .NET 2.0, the SW was tested with all subsequent versions .NET successfully.

2.3.2 Characteristics and functionality of the tablet ENsign

General Specification

- Color Display 10.1 inch
- "USB to VGA" for Microsoft Windows XP/VISTA/7©
- Dimension ~263x173x16 mm
- Weight ~750gr

Signature characteristics

- Electromagnetic technology
- Battery-free pen
- Min resolution 1000 LPI
- Active area 222 x 125 mm
- 1024 level of pressure (10bit)
- Force applicable : 30g – 500g
- 150 samples per second
- Significant movements flying up to 10mm

Screen

- Panel 16:9 LCD 10.1 inch TFT
- Video resolution 1024 x 600
- 262K colors
- LED backlighting
- Surface safety glass

Software and Hardware security

- Single-shell container sealed and no screws, tempered glass front immovable
- USB and DVI cable are not detachable from the tablet
- Standard 3DES comunication encryption

The tablet ENsign is covered by a patent.
The tablet is composed by a electromagnetic digitizer, by a LCD display, by an USB hub, by electronics for control interfacing and advanced system of coding.
The digitizer recognizes movements of electronic pen, supplied with the digitizer.

The USB hub is integrated inside the tablet, and has the duty of sending the data of the digitizer to a PC and receiving from PC data for the display.

The electronics for control/interface and coding has two principal duty:

1- convert the data flow from USB interface into electric signal for displaying. The electronics for control/interface receives data from USB port and converts them in electronic signals for the display.

2- Coding data coming from digitizer so that cannot be captured in the case of a fraudulent interception, with an high level of coding.

The tablet looks as a single-shell container sealed and no screws, with tempered glass front immovable and USB cable not detachable from the tablet.

The user read from tablet display the information and, after the decision of signing, with a specific command activates the coding od graphometric data, sending them to the PC for interpreting and elaboration.

After the decoding of graphomertric data, it’s created a “bitmap” image of the signature, that is put in the PDF document and showed on the tablet display for confirmation and for operation ending.

The Tablet Ensign is also usable in connection with other software having the same functions of ENsoft.

2.4 LOGICAL SCOPE OF THE TOE

The TOE realizes a solution of advanced electronic signature, since comply requirements of [RF2] art. 56.

Besides, TOE recognizes and accept documents PDF (Portable Document Format - RFC 3778) or PDF/A, international standard ISO 19005, included among PAS Format (Publicly Available Specification).

TOE offers a complete management of the signature process, since the production of PDF document required by the customer, until the document will be signed and returned unmodifiable.

TOE hashes the PDF document with algorithm SHA-1, before sending it to tablet.

End users, after an examination of document, sign on the tablet and confirm the signature.

The TOE makes the registration of biometric parameters (acceleration, speed, pressure and interruption), and creates a graphometric vector that is joined to the hash of document.

After, the graphometric block (hash of document + graphometric vector) so created is coded with a public key given by a certification authority and whose private key (necessary to decode the document in case of refuse to acknowledge from the customer and intervention of the magistracy) is kept care of a public officer or in a HSM.

Moreover to the graphometric block it is put a further signature of integrity at level sw (the graphometric data, coded together with the hash of the original document and the image of the signature, are integral part of the signature of integrity. In case it is modified, even if only a bit of that document, when opened, it will be seen a message saying that the document has been modified after the putting of the signature itself).

At the end of operation, TOE provides a secure deletion of temporary data of each signing session, so that no misleading data is used for any other operation, and avoid misuse.

2.5 TOE FUNCTIONALITY

The TOE, in junction with its environment, claim the conformance to art. 56 of DPCM [RF2]. Hereunder are noticed the main points of national law on electronic signature. Each point shows how the Ensoft's Features, Ensign10 (signature device) and the identified process respects the European dictates regulatory:

1. Signer Identification

As with paper documents the signer, before to apply his own sign, comes identified from teller or from anyone supply the sign service by an identity document.

2. The unique connection to the signature of the signer

The signer checks the document, shown on the tablet, before to sign. This document contains all the same features of the paper document.

The electronic signature made on the tablet is linked to the document in secure and not editable mode, ensuring the unique connection of the signature to the signer. Basically:

a) The system will perform the registration of biometric parameters (acceleration, velocity, pressure and jumps in the air) creating a biometric vector that is joined to the hash (fingerprint) of the document;
b) The biometric block (hash of the document + biometric vector) thus registered is encrypted by a public key supplied by a certification authority and whose private key (which is necessary to decrypt the document in case of disavowal by the customer and judiciary intervention) is kept from a public official or in a HSM (hardware security module);
The biometric block is also marked with a further signature of integrity (the biometrics data, encrypted with the hash of the original document and the image of the signature, are integral parts of the integrity signature affixed on the PDF, by Ensoft, against each signature customer. In case it is changed, even just a bit of that document, a message is displayed each one the document is opened, this message will indicate that the document was modified after the date of affixing the signature itself.

3. The sole control of the signer on the signature generation system

The technology used to collect the signature on the tablet allows to records all the individual characteristics of the signer in the act of signing. In fact, at the moment in which the person signing the document, Ensoft records a series of behavioral parameters such as:

- the pressure of the pen,
- the speed at which you are signing
- the acceleration during the writing phase,
- sections where the pen is raised during the signing.

The registration process allows customer to view, even after a long time, the signature on the "document" and, if necessary, to be able to compare with other signatures by the same person on the tablet. In particular:

- the tablet is assembled in such a way that any tampering would compromise the structure and is therefore easily identifiable;
- the tablet uses hardware encryption components, in this way all data transmitted that can only be interpreted by the software of the manufacturer of the tablet; are used multiple levels of encryption between hardware and software components so as to maximize the level of security of all components that managing biometric data;
- temporary data of each signing session are destroyed at the end of the operation.

The solution Euronovate allows the signer to have complete control over what is displayed on the tablet at the time of signature, in particular the customer is able to:

- review on the tablet all parts of the document;
- use the appropriate controls to zoom in/out on the text of the document;
- identify intuitively all parts of the document where there is a signature;
- repeat several times each signature before confirmation;
- cancel the operation after it has been the last signature.

4. The ability to verify that the "document" signed has not been altered since you signed it

The "documents", after being signed by signer, shall be signed by the provider signature solution through the application of a digital signature using the PDF format for their representation. This is an international standard ISO 19005, subset of PDF, specially designed for the storage and reference long-term electronic document also through different software. This in order to ensure the integrity of the document in terms of non-modifiability and inalterability of its contents. The documents thus generated are stored according to the rules on conservation of documents (electronic storage) provided in the Digital Administration Code (hereafter CAD).

5. The ability of the signer to obtain evidence of the signed

It 'also important that:

- the signer may request a paper copy of the document which was placed the operation or, alternatively, to receive a copy of the document in electronic format by e-mail;

- The choices about the will to receive copies of documents relating to transactions and operating procedures of such transactions is sole responsibility of the customer to will express such choices.

In all cases, the documents can be retrieved, viewed, printed, or upon request of the person concerned, throughout the storage period.

6. The identification of the signature solution provider

The provider produces a copy of the "document" on letterhead and after the signature of the customer shall affix his electronic signature, associated with an administrator with authority to sign, according to the regulations in place the Digital Administration Code.

7. The absence of any element, in the signature, act to amend the acts, facts or data represented

The provider shall take all the modern mechanisms of manipulation of the "document". In particular, with regard to the service, as noted earlier in this document, TOE accept also the PDF/A static, with the endorsement of the qualified electronic signature of the customer and stored according to the rules of the CAD, allows to determine that the same has undergone changes over time.

8. The unique connection of the signature to the document signed

Each "document" after signing on the tablet by the signer, it assumes a unique feature that allows to trace, with certainty, the will expressed at the time of signature. The biometric data, detected by the tablet, are sent to Ensoft in a safe and encrypted way and will be destroyed at the end of their use after signing the document. At the end of the signature in fact, the data held by the operator are destroyed so as to avoid misuse.

Above functionalities give developer indications for the identification of threats and determination of security objectives.

3. CC CONFORMANCE CLAIM

ST and TOE are conformant to version 3.1 (Revision 4) of the Common Criteria for Information Technology Security Evaluation.
The following conformance claims are made for the TOE and ST:

- Common Criteria for Information Technology Security Evaluation. Version 3.1 Rev.4 Part 1 september 2012
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, Version 3.1 Rev. 4 september 2012
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, Version 3.1 Rev. 4 september 2012

The claimed assurance package is EAL1 augmented with ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1.

This ST does not claim conformance to any PPs.

4. SECURITY PROBLEM DEFINITION

This section summarizes assets, threats addressed by the TOE and assumptions about the intended environment of the TOE. Note that while the identified threats are mitigated by the security functions implemented in the TOE, the overall assurance level (EAL1+) also serves as an indicator of whether the TOE would be suitable for a given environment.

4.1 ASSETS

DTBS and DTBS/R
Set of data, or its representation, which the signatory intends to sign. Their integrity and the unforgeability of the link to the signatory provided by the digital signature must be maintained.

Signature creation function
Function of the TOE to create digital signature for the DTBS/R with the SCD.

4.2 TOE USER

Signatory - User who holds the TOE and uses it on his own behalf or on behalf of the natural or legal person or entity he represents.
Operator - End user of the TOE acting in connection with signatory.
Administrator - User who is in charge to perform the TOE initialization, TOE personalization or other TOE administrative functions.

4.3 THREATS

T.User: signatory identification.
Unauthorized people may present as an authorized signatory to use SSCD for gaining access to TOE functions.
T.Repudiate: action repudiation.
Signatory denies having signed data or verifying data before signing.
T.SigF_Misuse: misuse of the signature creation function of the TOE.
An attacker misuses the signature creation function of the TOE to create a digital signature for data the signatory has not decided to sign.
T.DTBS_Forgery: forgery of the DTBS.
An attacker modifies the DTBS/R. Thus the DTBS/R used by the TOE for signing does not match the DTBS the signatory intended to sign.

4.4 ORGANIZATIONAL SECURITY POLICIES

There are no organizational security policies.

4.5 ASSUMPTIONS

User assumptions

**A.Operator - **It is assumed that Operators are well trained in order to use correctly TOE and chosen among the trustworthy staff of the organization.
A.Administrator_IT - It is assumed that Administrator are chosen among the trustworthy staff and well trained to use correctly TOE and all elements of the environment IT.

Environment non-IT assumptions

A.Physical - It is assumed that TOE is installed in a physically secure location that can only be accessed by authorised personel.

Environment IT assumptions

A.Authentication – It is assumed that Operators and Administrators must be authenticated by the IT system. Authentication requirements in the IT system shall be configured according to the risks in the operational environment.
A.Protect - It is assumed that IT environment will provide adequate protection of documents against forgery attacks and malware.
A.DCA - The signatory uses only a trustworthy DCA. The DCA sends to signatory data that signatory wishes to sign in a format appropriate for signing.
A.PDF - It is assumed that IT sends to TOE PDF or PDF/A document.

5. SECURITY OBJECTIVES

5.1 TOE SECURITY OBJECTIVES

This section defines TOE security objectives. Security objectives establish the behaviour expecting from TOE to contrast threats and support the assumptions and the security policies of the organization.

OT.Doc_Integrity - TOE must assure the integrity of documents. This objective isn’t in conflict with the process of creation of a signature if applied to a cryptographic function of hash on the same document.
OT.Crypto - TOE must assure the quality of the cryptographic process so that the probability that data of creation of a signature can be modified is completely slight.

OT.Delete - As soon as the signature's operation ends, TOE must delete every trace of the signature.
OT.Sig_Integrity - TOE must assure the integrity of a document signed.

5.2 IT ENVIRONMENT SECURITY OBJECTIVES

OE.Authentication - IT environment must identify and authenticate administrators and operators of the TOE.
OE.Code - IT environment must be able to protect documents against forgery and discover and reject documents containing a code which can modify the object of the subscription.
OE.Visio - DTBS/R sent to signatory has a format that permits to signatory to see the entire document.
OE.Form - IT must change in PDF or PDF/A format any document or data to be signed, before sending to TOE.

5.3 NON-IT ENVIRONMENT SECURITY OBJECTIVES

These security objectives are on charge of TOE environment. They are necessary to support TOE security objectives to oppose security problems and to support assumptions established in TOE security environment.

OE.Protect – Organization must ensure that only authorized people can access to TOE.
OE.Noevil – Operators must be trustworthy and trained on TOE and IT environment right use.
OE.Administrator - Administrator must be trustworthy and trained on TOE and IT environment right use.
OE.Identification - Operators must identify the signatories according to the rules established by the organization, before permitting the access to TOE.

6. EXTENDED COMPONENTS DEFINITION

There are no extended components.

7. SECURITY REQUIREMENTS

7.1 OVERVIEW

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 of the Common Criteria, part 2 providing functional requirements and part 3 providing assurance requirements.

7.2 SFR CONVENTIONS

Assignment. The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows [**assignment**].

Selection. The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows [***selection***].

Refinement. The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for **additions**, and strike-through, for deletions.

Iteration. The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a slash "/" at the end of the component identifier and a unique name for the iteration.

7.3 SECURITY FUNCTIONAL REQUIREMENTS (SFR)

Functional Requirements
FDP_DAU.1 Basic Data Authentication
FDP_RIP.1 Subset residual information protection
FDP_UIT.1 Data Exchange Integrity
FCS_COP.1 Cryptographic operation/EnDec
FCS_COP.1 Cryptographic operation/HASH
FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction
FTP_ITC.1 Inter-TSF trusted channel

Table 1: TOE Security Functional Components (SFR)

FDP_DAU.1 Basic Data Authentication

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [assignment: **document signed**].

FDP_DAU.1.2 The TSF shall provide [assignment: **signatory**] with the ability to verify evidence of the validity of the indicated information.

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *deallocation of the resource from*] the following objects: [assignment: **SSCD**].

FDP_UIT.1 Data exchange integrity

FDP_UIT.1.1 The TSF shall enforce the [assignment: **access control**] to [selection: *receive*] user data in a manner protected from [selection: *modification*] errors.

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

FCS_COP.1 Cryptographic operation/En-Dec

FCS_COP.1.1 The TSF shall perform [assignement: **data encryption and decryption**] in accordance with a specified cryptographic algorithm [
a) AES,
b) 3DES,
] and cryptographic key sizes [
a) 128 bit (AES),
b) 168 bit (3DES)
] that meet the following: [
a) [AES],
b) [3DES]].

FCS_COP.1 Cryptographic operation/HASH

FCS_COP.1.1 The TSF shall perform [assignement*:* **secure hashing**] in accordance with a specified cryptographic algorithm [assignement: **SHA-1**] and cryptographic key sizes [assignement: **160 bit**] that meet the following:[assignement: **SHA-1**].

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm[
a) AES,
b) 3DES,
] and cryptographic key sizes [
a) 128 bit (AES),
b) 168 bit (3DES)
] that meet the following: [
a) [AES],
b) [3DES]].

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**memory overwrite**] that meets the following: [**none**].

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [selection: *the TSF*] to initiate communication via the trusted channel.
FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: **sign creation and verification**].

7.4 ROBUSTNESS DECLARATION

TOE described in this ST is designed to be used in an IT environment well protected by unauthorizated access and to be used by operators and administrators well trained.
It is assumed that in this environment attackers have a low level of danger, so it results adequate a level of robustness “LOW”.
The only element for which is adequate a claim of robustness is the SFR FCS_COP.1.

7.5 SECURITY ASSURANCE REQUIREMENTS (SAR)

The security assurance requirements for the TOE (Table 2) are the EAL1 components, augmented with ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.
EAL1+ was selected as the assurance level because the TOE is a commercial product whose users require a low level of independently assured security. The TOE is targeted at a relatively benign environment with good physical access security and competent administrators. Within such environments it is assumed that attackers will have a very limited attack potential. As such, EAL1+ is appropriate to provide the assurance necessary to counter the limited potential for attack.

Assurance Class	**Assurance components**
ADV: Development	ADV_FSP.1Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.1Labelling of the TOE
	ALC_CMS.1TOE CM coverage
ATE: Tests	ATE_IND.1Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1Vulnerability survey
ASE: Security Target Evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Stated security requirements
	ASE_SPD.1 Security Problem Definition
	ASE_TSS.1 TOE summary specification

Table 2: Security Assurance Requirements (SAR)

ADV_FSP.1 Basic functional specification

Dependencies: None.
Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.
ADV_FSP.1.2D The developer shall provide a tracing from the functional specification to the SFRs.

AGD_OPE.1 Operational user guidance

Dependencies: ADV_FSP.1 Basic functional specification
Developer action elements:
AGD_OPE.1.1D The developer shall provide operational user guidance.

AGD_PRE.1 Preparative procedures

Dependencies: None.
Developer action elements:
AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

ALC_CMC.1 Labelling of the TOE

Dependencies: ALC_CMS.1 TOE CM coverage
Developer action elements:
ALC_CMC.1.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMS.1 TOE CM coverage

Dependencies: None.
Developer action elements:
ALC_CMS.1.1D The developer shall provide a configuration list for the TOE.

ASE_INT.1 ST introduction

Dependencies: None.
Developer action elements:
ASE_INT.1.1D The developer shall provide an ST introduction.

ASE_CCL.1 Conformance claims

Dependencies:
ASE_INT.1 ST introduction
ASE_ECD.1 Extended components definition
ASE_REQ.1 Stated security requirements
Developer action elements:
ASE_CCL.1.1D The developer shall provide a conformance claim.
ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

ASE_OBJ.2 Security objectives

Dependencies:
ASE_SPD.1 Security problem definition
Developer action elements:
ASE_OBJ.1.1D The developer shall provide a statement of security objectives.
ASE_OBJ.2.2D The developer shall provide a security objectives rationale

ASE_ECD.1 Extended components definition

Dependencies: No dependencies.

Developer action elements:

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

ASE_REQ.2 Derived security requirements

Dependencies:

ASE_OBJ.2 Security objectives

ASE_ECD.1 Extended components definition

Developer action elements:

ASE_REQ.2.1D The developer shall provide a statement of security requirements.

ASE_REQ.2.2D The developer shall provide a security requirements rationale.

ASE_SPD.1 Security problem definition

Dependencies: No dependencies

Developer action elements:

ASE_SPD.1.1D The developer shall provide a security problem definition

ASE_TSS.1 TOE summary specification

Dependencies: ASE_INT.1 ST introduction

ASE_REQ.1 Stated security requirements

ADV_FSP.1 Basic functional specification

Developer action elements:

ASE_TSS.1.1D The developer shall provide a TOE summary specification.

ATE_IND.1 Independent testing - conformance

Dependencies:

ADV_FSP.1 Basic functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

Developer action elements:

ATE_IND.1.1D The developer shall provide the TOE for testing.

AVA_VAN.1 Vulnerability survey

Dependencies:

ADV_FSP.1 Basic functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

Developer action elements:

AVA_VAN.1.1D The developer shall provide the TOE for testing.

8. TOE SUMMARY SPECIFICATION (ASE_TSS)

This section provides the TOE summary specification, a high-level definition of the security functions claimed to meet the functional and assurance requirements.

8.1 TOE SECURITY FUNCTIONS

TOE_Crypto
The TOE performs encryption and decryption using the algorithm 3DES for the exchange of data with SSCD.
TOE_Sign
The TOE, in order to protect data and signature of signer, will destroy data of each signing session at the end of the operation.
TOE_SHA1
The TOE can generate hashes using the algorithms SHA-1.
TOE_Integer
The TOE put an integrity sign on a document at the end of operations.

8.2 SAR DOCUMENTS

The following *Table 3* connects the assurance components provided by CC with the documents drawn up in the TOE evaluation contest.

Assurance Components	Documents	Contents
ADV_FSP.1	Functional specification	In the document the functional specifications to cover up TOE requirements are identified.
AGD_OPE.1	Operational user guidance Functional specification	In the document the operations for a correct and safe use of TOE are described.
AGD_PRE.1	Developers delivery procedures	The document contains the instructions for a safe TOE initialization.
ALC_CMC.1	Configuration Management Plan	The document describes the configuration management plan.
ALC_CMS.1	Configuration list	The document contains TOE configuration list.
ATE_IND.1	Document relative to TOEs test performed by developers	The document described test plan performed by the developers, and results from test execution.
AVA_VAN.1	Vulnerability analisys	Documents contain a detailed analisys of TOE vulnerabilites.

Table 3: SAR to documents mapping

9. RATIONALE

9.1 OBJECTIVES/SFRs RATIONALE

The following table provides a summary of the relationship between the security objectives and threats/assumptions. The rationale is in the following section.
This section proves that every security objective counters at least a threats or supports an assumption, and every threats or assumption is linked to a security objective.

	OT.Doc_Integrity	OT.Crypto	OT.Delete	OT.Sig_Integrity	OE.Identification	OE.Administrator	OE.Noevil	OE.Protect	OE.Form	OE.Visio	OE.Code	OE.Authentication
A.Operator							X					X
A.Administrator_IT						X						X
A.Physical								X				
A.Authentication												X
A.Protect											X	
A.DCA										X		
A.PDF									X			
T.User					X							
T.Repudiate		X		X						X	X	
T.SigF_Misuse		X	X									
T.DTBS_Forgery	X	X									X	

Table 4: Relationship between objectives and threats/assumptions

A.Operator
It’s assumed that operators are trustworthy appropriately trained to use correctly TOE; assumption supported by OE. Noevil. Personnel reliability is in charge of the organization while the training is appropriately supported by specific manual.

A.Administrator_IT
The Administrators of the IT environment are responsible for the right usage of the devices composing the IT environment to which some important security functions are assigned, as previously said. For this reason it’s necessary that Administrators are well trained to use correctly all the devices composing the IT environment and chosen among a trustworthy personnel as described by OE.Administrator who therefore supports the A.Administrator_IT assumption.

A.Physical
The assumption A.Physical is supported by the Organization objective OE.Protect that considers the use of the hardware in an environment guarded by an operator or an authorized personnel and in protected areas where nobody can have the access unless clearly authorized.

A.Authentication
TOE hasn’t identification and authentication functions of Operators and Administrators.
This fundamental function is delegate to IT environment, and is applied conforming to company regulations for accessing to applications, as described in OE.Authentication, which supports the assumption.

A.Protect
Documents that signatory wants to sign are prepared by It environment and sent to TOE. It’s necessary that IT environment provide adequate protection of documents against forgery attacks and malware. OE.Code provides that IT environment must be able to protect documents against forgery and discover and reject documents containing a code which can modify the object of the subscription.

So the assumption is well supported.

A.DCA
Signatory must receive the documents to be signed in a predefined format, so that he can see the whole document also through the scrolling function and using the provided pen only. This assumption is supported by OE.Visio.

A.PDF
TOE supports only documents in PDF and PDF/A format. So it's necessary that IT change in PDF format any document to be signed, before sending to TOE. The format PDF (Portable Document Format - RFC 3778), is become the international standard ISO 19005 and is included among the formats PAS (Publicly Available Specification). This assumption is supported by OE.Form.

T.User
People not authorized might use the TOE.
The objective OE.Identification provides that Operators must identify the signatories according to the rules established by the organization, before permitting the access to TOE. So OE.Identification oppose the threat.

T.Ripudiate
This threat concerns the possibility that signatory denies having signed data or verifying data before signing. The threat is opposed by OT.Crypto that assure the quality of the cryptographic process, by OE.Code that protects documents against forgery, by OE.Visio that provides to send to signatory documents with a format that permits to signatory to see the entire document, and by OT.Sig_Integrity, that assures the integrity of document at the end of operation.

T.SigF_Misuse
This threat concerns the possibility that an attacker use a digital signature of an identified signatory for fraudulent purposes. The threats is opposed by OT.Crypto, that assure the quality of the cryptographic process, and by OT.Delete that assure the cancellation of every trace of the signature after the signing operation.

T.DTBS_Forgery
This threats concerns the possibility that a document is modified after the signing operation. The threat is opposed by OE.Code that protects documents against forgery, by OT.Crypto that assure the quality of the cryptographic process, and by OT.Doc_Integrity that assures the integrity of document.

9.2 SECURITY REQUIREMENTS RATIONALE

9.2.1 Tracing of SFRs to security objectives

The below *Table 5* provides the mapping of the TOE SFRs and the security objectives for the TOE. From the Table we deduce how the security requirements map all the security objectives: each security requirement faces at least an objective and each TOE objective is faced by at least a security objective.

	OT.Doc_Integrity	OT.Crypto	OT.Delete	OT.Sig_Integrity
FDP_DAU.1				X
FDP_RIP.1			X	
FDP_UIT.1	X			
FCS_COP.1/En-Dec		X		
FCS_COP.1/HASH	X			
FCS_CKM.1		X		
FCS_CKM.4		X	X	
FTP_ITC.1	X			X

Table 5: SFRs to security objectives mapping

OT.Doc_Integrity
The signatory of a document must have the possibility of verify that the document has not be modified after the signing operation. This objective isn't in conflict with the process of creation of a signature if applied to a cryptographic function of hash on the same document, and is supported by FDP_UIT.1.
This objective is also supported by the SFR FCS_COP.1/HASH, for having the capability to verify the integrity of document signed, and by the SFR FTP_ITC.1 in order to provide a secure communication channel.

OT.Crypto
TOE's developer has required an high quality of the cryptographic process so that the probability that data of creation of a signature can be modified is completely slight. This objective is supported by SFR FCS_COP.1/En-Dec, and by FCS_CKM.1 and FCS_CKM.4 in order to create and destroy cryptographic keys.

OT.Delete
In order to avoid misuse, it's important that, at the end of signature's operation, TOE could delete every trace of the signature. This objective is supported by SFR FDP_RIP.1 and by FCS_CKM.4.

OT.Sig_Integrity
TOE software must certificate with an integrity sign that hash of the document, joined with graphometric data the picture of user's signature, is protected by alterations. In the case of any change, at the opening of the document, a security message will notify that the document has been modified after the signature.
This objective is supported by SFR FDP_DAU.1 and by the SFR FTP_ITC.1 in order to provide a secure communication channel.

9.2.2 Satisfaction of dependencies

Following *Table 6* shows dependencies required by Common Criteria for SFR and SAR (assurance level EAL1).

ST requirements	Dependencies required by CC	Dependencies satisfaction
SFR		
FDP_DAU.1	None	None
FDP_RIP.1	None	None
FDP_UIT.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]	Note 1 FTP_ITC.1 Inter-TSF trusted channel
FCS_COP.1	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1 Cryptographic key generation FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1 Cryptographic operation FCS_CKM.4 Cryptographic key destruction
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	FCS_CKM.1 Cryptographic key generation
FTP_ITC.1	None	None
SAR		
ADV_FSP.1	None	None
AGD_OPE.1	ADV_FSP.1 Basic functional specification	ADV_FSP.1 Basic functional specification
AGD_PRE.1	None	None
ALC_CMC.1	ALC_CMS.1 TOE CM coverage	ALC_CMS.1 TOE CM coverage
ALC_CMS.1	None	None
ATE_IND.1	ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational user guidance	ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational

	AGD_PRE.1 Preparative procedures	user guidance AGD_PRE.1 Preparative procedures
AVA_VAN.1	ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures	ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
ASE_INT.1	None	None
ASE_CCL.1	ASE_INT.1 ST introduction ASE_REQ.1 Stated security requirements ASE_ECD.1 Extended components definition	ASE_INT.1 ST introduction ASE_REQ.1 Stated security requirements There are no extended components
ASE_OBJ.2	ASE_SPD.1 Security problem definition	ASE_SPD.1 Security problem definition
ASE_ECD.1	None	None
ASE_REQ.2	ASE_OBJ.2 Security objectives ASE_ECD.1 Extended components definition	ASE_OBJ.2 Security objectives There are no extended components
ASE_SPD.1	None	None
ASE_TSS.1	ASE_INT.1 ST introduction ASE_REQ.1 Stated security requirements ADV_FSP.1 Basic functional specification	ASE_INT.1 ST introduction ASE_REQ.1 Stated security requirements ADV_FSP.1 Basic functional specification

Table 6: Verification of dependencies

Note 1: The TOE does’nt implement policies or functions of access control and flow control; consequently the dependencies FDP_ACC or FDP_IFC are not required.

9.3 TOE SUMMARY SPECIFICATION

The table below provides a summary of SFRs satisfied by TOE security functions. The sections describe how the TOE security functions satisfy the SFR.

	TOE_Crypto	**TOE_SHA1**	**TOE_Sign**	**TOE_Integer**
FDP_DAU.1				**X**
FDP_RIP.1			**X**	
FDP_UIT.1	**X**	**X**		
FCS_COP.1/En-Dec	**X**			
FCS_COP.1/HASH		**X**		
FCS_CKM.1	**X**			
FCS_CKM.4	**X**		**X**	

FTP_ITC.1			**X**	**X**

Table 7: Summary of SFRs satisfied by TOE Functions

FDP_DAU.1
The TOE put a warranty signature on the document at the end of all operation in order to guarantee the authenticity of document. This family provides a method of providing a guarantee of the validity of a specific unit of data that can be subsequently used to verify that the information content has not been forged or fraudulently modified. The security function TOE_Integer performs this operation.

FDP_RIP.1
The SSCD stores biometric characteristics of signature and, after an operation of coding, send them to a PC. IN order to avoid misuse of data stored, it's necessary the deleting of all data of biometric characteristics of signature. The security function TOE_Sign performs this operation.

FDP_UIT.1
The communications between SSCD and SCA requires an high level of protection. This family defines the requirements for providing integrity for user data in transit between the element of TOE. TOE_Crypto performs encryption and decryption using the algorithm 3DES for the exchange of data between SSCD and SCA.

FCS_COP.1
It's important communicate with the SSCD in a secure way, so the developer has decided to implement cryptographic operation for this communication channel.
These SFR's must be correctly performed in accordance with a specified algorithm and with a cryptographic key. TOE_Crypto and TOE_SHA1 performs encryption and decryption using the algorithm 3DES for the exchange of data with SSCD, and SHA1 to grant the unmodifiability of data.

FCS_CKM.1
The TOE generates keys only for signing a document PDF and protect user's biometric vector, but these keys are not readable outside the TOE and are immediatly overwritten at the end of signing operation.

FCS_CKM.4
The TOE ensures that keys are overwritten before a resource is deallocated from a key object.

FTP_ITC.1
TOE shall provide a secure communication channel in order to establish a secure exchange of data with SSCD.

LIST OF FIGURES

LIST OF TABLES