EURONOVATE
best digital transformation solutions

Security Target

Advanced E-Signature ENsoft v.2

Version	Date	Author	Changes from previous version
1.0	17 June 2021	Conte Andrea	Initial version
1.1	01 July 2021	Conte Andrea	Minor changes
1.2	30 October 2021	Conte Andrea	Corrections and clarifications
1.3	13 January 2022	Conte Andrea	Corrections and clarifications

SUMMARY

1. SECURITY TARGET INTRODUCTION

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, where applicable, 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.2
Data: 13 January 2022
Versione: 1.3

TOE identification

Product name: ENSoft version 2.0

Sponsor and Developer: Euronovate SA

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 version 2.0 product.

The product is designed and manufactured by EURONOVATE SA (http://www.euronovategroup.com).

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

DCA document creation application

DES Data Encryption Standard

DTBS data to be signed

DTBS/R data to be signed or its unique representation

EAL Evaluation Assurance Level

IT Information Technology

PC Personal Computer

PDF Portable Document Format

PKCS Public-Key Cryptography Standards

PP Protection Profile

SAR Security Assurance Requirement

SF Security Function

SFR Security Functional Requirement

SSL Secure Socket Layer

ST Security Target

TOE target of evaluation

TSF TOE Security Function

TSFI TSF interface

User data PDF document + hash + biometric vector

1.4. INDEX TABLES

1.5. INDEX IMAGES

1.6. 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 OVERVIEW

2.1 TOE type, usage and major security features of the TOE

The TOE is a software application, named “ENSoft version 2.0” , that has the function of governing the process of electronic signature of a document.

The TOE is strictly tied to a tablet that has the function of receiving the user's signature and permitting the TOE utilization. Euronovate produces proper tablets, named ENSign11, but the TOE can work with other tablets having similar characteristics.
Characteristics and functions of ENSign11 are described in the operational environment.

These are the TOE’s security functions.

TOE_Crypto
The TOE performs decryption of the data exchanged with the tablet using the SDK provided by the tablet manufacturer and AES plus RSA to encrypt them before adding into the pdf.
TOE_Sign
The TOE, in order to protect data and signatures of signers, will destroy data of each signing session at the end of the operation.
TOE_SHA256
The TOE can generate hashes using the algorithms SHA-256.
TOE_Integrity
The TOE put an integrity sign on a document at the end of operations.

2.2 Non-TOE hardware/software/firmware required by the TOE

Workstation

The solution ENSoft version 2.0 has been developed for Windows systems. It is currently compatible with Windows 7,8 and 10.

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 4.5.2, the SW was tested with all subsequent versions .NET successfully.

Tablet

The tablet (Ensign 11 or equivalent) is composed of an electromagnetic digitizer, a LCD display, an USB hub and electronics for control interfacing and advanced system of coding.
The digitizer recognizes movements of the 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 the USB interface into an electric signal for displaying. The electronics for control/interface receives data from the USB port and converts them into electronic signals for the display.
2. Coding data coming from digitizer so that cannot be captured in the case of a fraudulent interception, with a high level of coding.

The tablet looks as a single-shell container sealed, with tempered glass front immovable and USB cable not detachable from the tablet.
The user reads from the tablet screen the information and, after the decision of signing, with a specific command activates the coding of graphometric data, sending them to the PC for interpreting and elaboration.
After the decoding of graphometric data, it's created a "bitmap" image of the signature, that is put in the PDF document and shown 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 version 2.0.

3. TOE DESCRIPTION

3.1 physical scope of the TOE

The components of the Euronovate solution are:

- "ENSoft version 2.0" signature software
- a 10 inch tablet (like ENSign 11)

The operating models to use the mentioned solution provide:

- Installing the Software ENSoft version 2.0(1) on the physical client (2) on the operator's position
- The USB connection (3) between client and tablet ENSign11 (4).

The Figure 1 shows the operating context described before:

Figure 1 TOE operational environment

3.2 logical scope of the TOE

The TOE, in conjunction with its environment, realizes a solution of advanced electronic signature..
Besides, TOE recognizes and accepts 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, from the production of PDF documents required by the customer, until the document will be signed and returned unmodifiable.

TOE hashes the PDF document with algorithm SHA-256, before sending it to the tablet.

End users, after an examination of the document, signs on the tablet and confirms 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 the document.

After, the graphometric block (hash of document + graphometric vector) created is encrypted first with AES and then with a public key given by a certification authority (RSA) 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, encrypted 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, a message will be presented 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 avoids misuse.

Characteristics of ENSoft version 2.0

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

PDF Manager

- PDF elaboration to convert signature fields (present in PDF file as Text or 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 or finger
- Document zooming functions

The architecture of ENSoft version 2.0 is modular and customizable.
Modular means that the suite is divided into libraries (DLL) and each of them manage a specific function of the process. These libraries are named “core modules”.
Customizable means that the suite can be extended by writing custom modules which can handle specific behaviours of a customer (like pre-processing documents, acquiring data from a scanner/ocr, sending signed documents to a document system and so on). These libraries are named “process plugins”.

The core of the solution is called *ENMonitor*: it is a Windows Service that is launched automatically when the user does the login on the workstation:

- It is the container of all process plugin required by the solution
- It is the orchestrator of the suite: it will start, stop and restart in case of error each single process plugin in order to assure the business continuity

ENSoft version 2.0 is a process plugin and includes the following parts:

- Low level driver for communications with the device
- Layer for PDF manipulation and management of biometric vector
- Viewer PDF
- Communication channels (https, tcp/ip, websocket) that allow the signature suite to be used by any application with a proper SDK

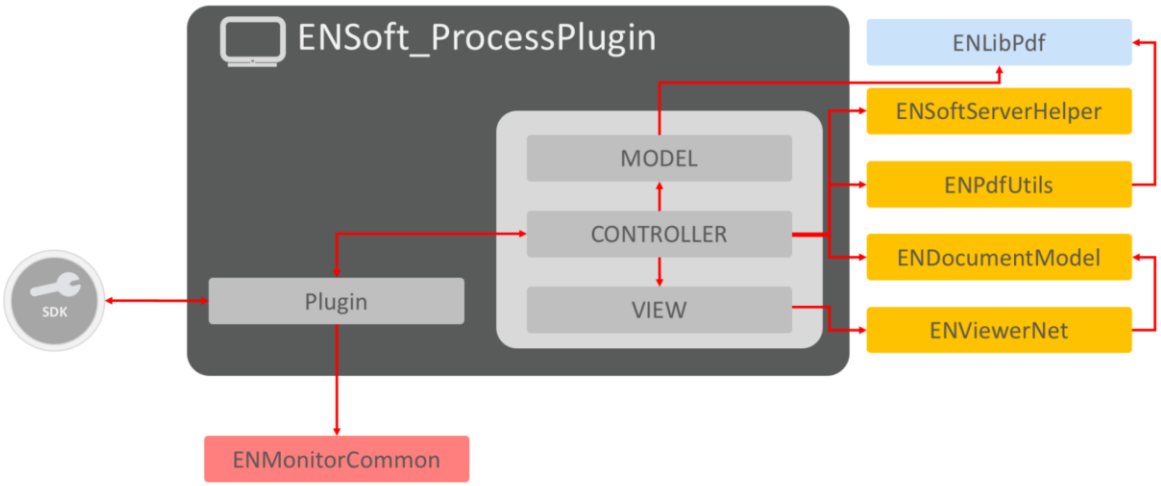

Figure 2 internal design of ENSoft version 2.0

As shown in Figure 2, the modules that make up the platform ENSoft version 2.0 are:

- *ENLibPDF*: an-internally developed library that manipulates the PDF at low-level according to the ISO/IEC 32000-2. This component adds the signature field, applies the encrypted biometric block into the signature fields with the incremental signature flow.
- *ENPdfUtils*: a tool library which lets ENLibPDF usable inside the process plugin
- *ENSoftServerHelper*: a tool library in charge of handling the communication with the remote signature server (SoftServer)

- *ENDocumentModel*: a tool library which describes the model of the signing document (how many signatures there are, where are the signatures located, how many signers there are…)
- *ENViewerNet*: a tool library in charge of presenting the PDF to the final user inside the tablet and handling click and gestures on it. 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 in general.
  It is composed of several “handlers”:
  - *touch* handler: to handle touch event raised by the user with the finger on the tablet screen
  - *keyboard* handler: to handle keyboard-like event raised by the user with the pen on the tablet screen
  - timer handler: to handle the timeout for inactivity
  - *inertial scroll* handler: to handle the scrolling of the document
  - *JSFunction* handler: to handle the usage of javascript inside the presented document on the tablet
  - *HookCallback* handler: to handle the communication with other internal components (callbacks)

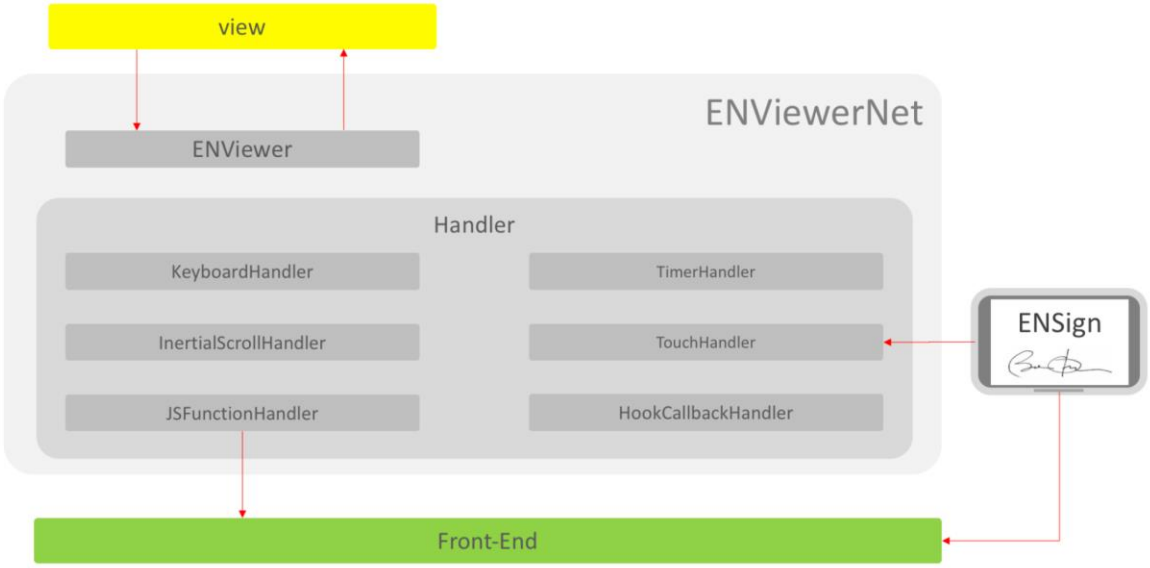

Figure 3 internal design of ENViewerNet process plugin with all handlers

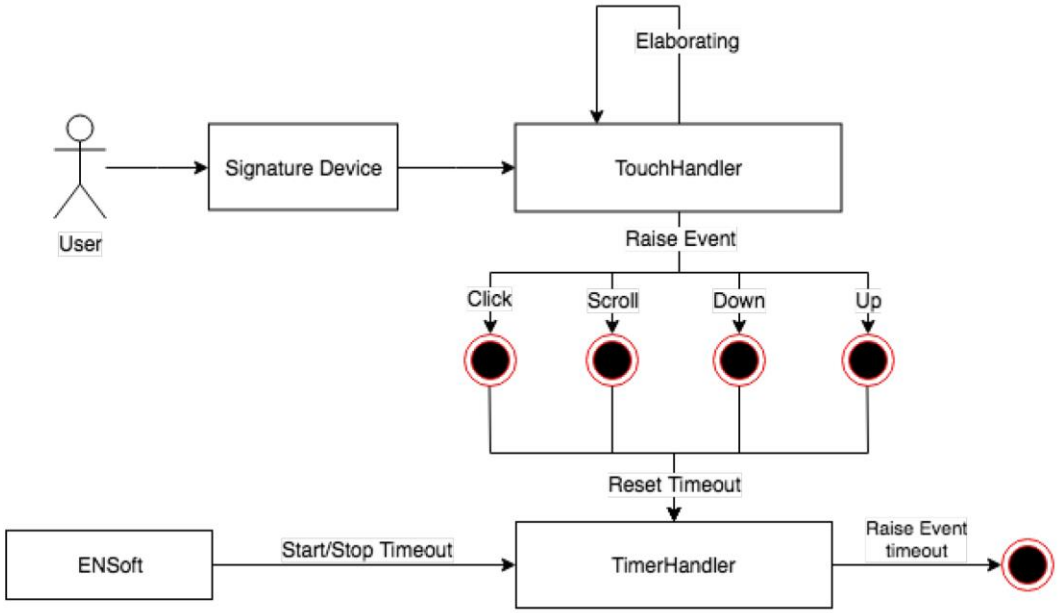

Figure 4 sequence diagram of the user interaction (touch) and timeout handler

There are others process plugins involved in the process, used for acquiring biometric data from an external device in a secure way, for marketing purposes and for better user experience:

- *ENSigner:* this module shows a signature box inside the tablet allowing the user to draw the signature with the pen. It also handles secure communication over the USB channel using the proper SDK provided by the manufacturer of the tablet.
- *ENContentsPlayer*: allows the "slideshow" of images contained in a subfolder of ENSoft version 2.0. This module is automatically launched by ENMonitor 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.
- *ENVirtualTablet*: this plugin shows a virtual tablet in the primary monitor of the workstation in order to see what the user saw inside the tablet (mirroring function).
- *ENCalligrapher*: a tool for extraction and analysis of signatures of biometric data collected by software platform ENSoft version 2.0. 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.

Standard cryptographic methods

Below there is a description of the encryption systems used in various software modules:

Communication with external world:

ENMonitor exposes various kinds of listeners (https, tcp, websocket) protected with certificates (TLS 1.2) to receive and send data from/to applications that require the use of the tablet's signature.

Encryption of biometrics data:

The collection of biometric data acquired from the tablet is encrypted with the AES algorithm (256 bits key), and both the encryption key that the seed is encrypted with RSA (the asymmetric key pair is provided by client uses only the public for encryption, while the private key is held in a safe place). For additional security, both seed and key are randomly generated at the time of the encryptions of biometric data.

Communication with ENsign11 or equivalent tablet:

Communication with the tablet ENSign11 is secured by the manufacturer of the tablet. ENSign11 has an internal Cryptographic Engine that provides a set of data security options (like AES Cipher Support for 256-Bit Keys) and performs NIST Standard Encryption/Decryption Operations without CPU Intervention.

3.3 TOE ENVIRONMENT FUNCTIONALITY

The TOE, in conjunction with its environment, claims 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 version 2.0's Features, the signature device and the identified process respects the European dictates regulatory:

Signer Identification

As with paper documents, the signer before applying his own sign, is identified from the teller or from anyone supplying the sign service by an identity document.

The unique connection to the signature of the signer

The signer checks the document, shown on the tablet, before signing. This document contains 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) acquired 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 judicial 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 version 2.0, 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.

The sole control of the signer on the signature generation system

The technology used to collect the signature on the tablet allows records of 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 version 2.0 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 customers 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.

Euronovate's solution 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.

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).

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 accepts 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.

The unique connection of the signature to the document signed

Each "document" after signing on the tablet by the signer, 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 version 2.0 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.

4. CC CONFORMANCE CLAIM

ST and TOE are conformant to version 3.1 Revision 5 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.5 Part 1 April 2017

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.

5. 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.

5.1 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 signatures for the DTBS/R.

5.2 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 the signatory.

Administrator: User who is in charge to perform the TOE initialization, TOE personalization or other TOE administrative functions.

5.3 THREATS

T.User: signatory identification.

Unauthorized people may present as an authorized signatory to use the tablet 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.

5.4 ORGANIZATIONAL SECURITY POLICIES

There are no organizational security policies.

5.5 ASSUMPTIONS

User assumptions

A.Operator: It is assumed that Operators are well trained in order to use TOE correctly and chosen among the trustworthy staff of the organization.

A.Administrator_IT: It is assumed that administrators are chosen among the trustworthy staff and well trained to correctly use TOE and all elements of the IT environment.

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 personnel.

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 the 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 the 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.

6. SECURITY OBJECTIVES

6.1 TOE SECURITY OBJECTIVES

This section defines TOE security objectives. Security objectives establish the behaviour expected 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.

6.2 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 the 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.

6.3 NON-IT ENVIRONMENT SECURITY OBJECTIVES

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

OE.Protect: Organization must ensure that only authorized people can access 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.

6.4 OBJECTIVES/THREATS 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 threat or supports an assumption, and every threat or assumption is linked to a security objective.

	OT.Doc_Integrity	OT.Crypto	OT.Delete	OT.Sig_Integrity
A.Operator				
A.Administrator_IT				
A.Physical				
A.Authentication				
A.Protect				
A.DCA				

A.PDF				
T.User				
T.Repudiate		X		X
T.SigF_Misuse		X	X	
T.DTBS_Forgery	X	X		

Table 1: Relationship between TOE objectives and threats/assumptions

	OE.Identification	**OE.Administrator**	**OE.Noevil**	**OE.Protect**
A.Operator			X	
A.Administrator_IT		X		
A.Physical				X
A.Authentication				
A.Protect				
A.DCA				
A.PDF				
T.User	X			
T.Repudiate				
T.SigF_Misuse				
T.DTBS_Forgery				

Table 2: Relationship between ENV objectives and threats/assumptions – Part 1

	OE.Form	**OE.Visio**	**OE.Code**	**OE.Authentication**
A.Operator				X
A.Administrator_IT				X
A.Physical				
A.Authentication				X
A.Protect			X	
A.DCA		X		
A.PDF	X			
T.User				
T.Repudiate		X	X	
T.SigF_Misuse				
T.DTBS_Forgery			X	

Table 3: Relationship between ENV objectives and threats/assumptions - Part 2

A.Operator

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

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 correctly use 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 fun+
damental function is delegated to the 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 a signer wants to sign are prepared by It environment and sent to TOE. It's necessary that the IT environment provide adequate protection of documents against forgery attacks and malware. OE.Code provides that the 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 it to TOE. The format PDF (Portable Document Format - RFC 3778), has 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 opposes the threat.

T.Ripudiate

This threat concerns the possibility that the signer 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 may use a digital signature of an identified signatory for fraudulent purposes. The threat is opposed by OT.Crypto, that assures the quality of the cryptographic

process, and by OT.Delete that assures the cancellation of every trace of the signature after the signing operation.

T.DTBS_Forgery

This threat 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 documents.

7. EXTENDED COMPONENTS DEFINITION

There are no extended components.

8. SECURITY REQUIREMENTS

8.1 OVERVIEW

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 of the Common Criteria v.5, part 2 providing functional requirements and part 3 providing assurance requirements.

8.2 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***].

Iteration: The iteration operation allows you to use a component more than once to perform different operations. An iteration is carried out by placing a slash "/" at the end of the component followed by a unique string that identifies the iteration.

8.3 SECURITY FUNCTIONAL REQUIREMENTS (SFR)

Functional Requirements
FDP_DAU.1 Basic Data Authentication
FDP_RIP.1 Subset residual information protection
FCS_COP.1 Cryptographic operation/AES
FCS_COP.1 Cryptographic operation/RSA
FCS_COP.1 Cryptographic operation/HASH
FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

Table 4: 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 [**document signed**].
FDP_DAU.1.2 The TSF shall provide [**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 [***deallocation of the resource from***] the following objects: [**tablet and ENSigner**].

FCS_COP.1 Cryptographic operation/AES

FCS_COP.1.1 The TSF shall perform [**data encryption and decryption**] in accordance with a specified cryptographic algorithm [**AES**] and cryptographic key sizes [**256 bit**] that meet the following: [**FIPS PUB 197**].

FCS_COP.1 Cryptographic operation/RSA

FCS_COP.1.1 The TSF shall perform [**data encryption and decryption**] in accordance with a specified cryptographic algorithm [**RSA**] and cryptographic key sizes [**4096 bit**] that meet the following: [**PKCS #1 v2.1**].

FCS_COP.1 Cryptographic operation/HASH

FCS_COP.1.1 The TSF shall perform [**secure hashing**] in accordance with a specified cryptographic algorithm [**SHA-256**] and cryptographic key sizes [**256 bit**] that meet the following: **[FIPS PUB 180-4].**

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall use cryptographic keys, provided by [**A.Administrator_IT]** in accordance with a specified cryptographic key generation algorithm [**RSA**] and cryptographic key sizes [**4096 bit**] that meet the following: [**FIPS PUB 186-4**].

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**].

8.4 ROBUSTNESS DECLARATION

TOE described in this ST is designed to be used in an IT environment well protected by unauthorized 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 in an adequate level of robustness “LOW”.
The only element for which is adequate a claim of robustness is the SFR FCS_COP.1.

8.5 SECURITY ASSURANCE REQUIREMENTS (SAR)

The security assurance requirements for the TOE (Table 5) 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 5: Security Assurance Requirements (SAR)

9. RATIONALE

9.1 SECURITY REQUIREMENTS RATIONALE

The below Table 6 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	
FCS_COP.1/AES		X		
FCS_COP.1/RSA		X		
FCS_COP.1/HASH	X			
FCS_CKM.1		X		
FCS_CKM.4		X	X	

Table 6: SFRs to security objectives mapping

OT.Doc_Integrity
The signatory of a document must have the possibility of verifying that the document has not been 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,. This objective is supported by FCS_COP.1/HASH, for having the capability to verify the integrity of documents signed.

OT.Crypto
TOE's developer has required a 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 FCS_COP.1/RSA and FCS_COP.1/AES, 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 FDP_RIP.1 and by FCS_CKM.4.

OT.Sig_Integrity
TOE software must certify with an integrity sign that the hash of the document, joined with graphometric data and the picture of the 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 FDP_DAU.1.

9.2 SATISFACTION OF DEPENDENCIES

Following Table 7 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
FCS_COP.1/AES	[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_COP.1/RSA	[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_COP.1/HASH	[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
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 AGD_PRE.1 Preparative procedures	ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational 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 7: Verification of dependencies

10. TOE SUMMARY SPECIFICATION

This section provides the TOE summary specification, a high-level definition or the security functions claimed to meet the functional and assurance requirements.
The table below provides a summary of SFRs satisfied by TOE security functions.

	TOE_Crypto	TOE_SHA256	TOE_Sign	TOE_Integrity
FDP_DAU.1				X
FDP_RIP.1			X	
FCS_COP.1/AES	X			
FCS_COP.1/RSA	X			
FCS_COP.1/HASH		X		
FCS_CKM.1	X			
FCS_CKM.4	X		X	

Table 8: Summary of SFRs satisfied by TOE Functions

TOE_Crypto

FCS_COP.1/AES
ENSigner process plugin
It's important to communicate with the tablet 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 performs encryption of the acquired data from the tablet using the algorithm AES-256 . ENSigner process Plugin and ENDocumentModel implement such level of encryption.

FCS_COP.1/RSA
ENSigner process plugin
It's important to communicate with the tablet 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 performs encryption of the previously AES-256 encrypted data acquired data using the algorithm RSA. ENSigner process Plugin and ENDocumentModel implement such level of encryption.

FCS_CKM.1
ENSigner process plugin
The TOE generates keys only for signing a document PDF and protecting the user's biometric vector, but these keys are not readable outside the TOE and are immediately overwritten at the end of signing operation. ENPdfUtils and ENLibpdf implement such level of encryption.

FCS_CKM.4

ENSigner process plugin

The TOE ensures that keys are overwritten before a resource is deallocated from a key object. The deallocation and destruction of memory areas where keys are stored is guarantee by Invoking standard methods of .NET framework.

TOE_SHA256

FCS_COP.1/HASH

ENLibPDF + ENPdfUtils

The TSF shall perform secure hashing in accordance with cryptographic algorithm SHA-256 which is required by ISO/IEC 32000-2. ENLibPdf implements such algorithm and uses it each time a signature is added.

TOE_Sign

FDP_RIP.1

ENSigner process plugin

The tablet acquires biometric characteristics of signatures and, after an operation of coding, sends them to a PC. In order to avoid misuse of data stored, it's necessary to delete all data of biometric characteristics of signatures. The security function TOE Sign performs this operation. The ENSigner process plugin assures the deletion of acquired data.

FCS_CKM.4

ENSigner process plugin

The TOE ensures that keys are overwritten before a resource is deallocated from a key object.
The deallocation and destruction of memory areas where keys are stored is guarantee by Invoking standard methods of .NET framework.

TOE_Integrity

FDP_DAU.1

ENLibPDF + ENPdfUtils

The TOE put a warranty signature on the document at the end of all operations in order to guarantee the authenticity of the 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 Integrity performs this operation using ENLibPdf method