SECURITY TARGET FOR biocertiX

Common Criteria version 3.1 revision 5 Assurance Level EAL 2

Date	**Revision schedule**
2-06-2025	The version numbers of the ST and Table 1 and 2 have been updated (see Section1.5.1.1: Delivery of the TOE').
23-08-2025	The TOE version number has been updated, and a new assumption has been added, along with its TOE security objective and justification.
24-09-2025	The version number of the TOE (1.2) has been corrected in the ST document. The ST version number was previously been mistakenly inserted in place of the TOE version. The version numbers “AGD_OPE” and “AGD_PRE” in the ST document have also been corrected. The version number of the mobile application has been corrected and a new assumption “A.External_System” has been added, along with its TOE security objective “OE.External_System” and justification. All changes in ST are marked in red.

CONTENTS

Terms 6

1. Introduction 7

1.1. ST Overview 7

1.2. ST Reference 7

1.3. TOE Reference 7

1.4. TOE Overview 8

1.4.1. TOE Type 9

1.4.2. TOE Usage & Major Security Functions 10

1.4.3. Required non-TOE Hardware/Software/Firmware 10

1.5. TOE Description 11

1.5.1. Physical Scope of the TOE 11

1.5.2. Logical Scope of the TOE 12

1.5.2.1. Secure initialization 13

1.5.2.2. Roles & Available Functions 13

1.5.2.3. Secure Administration 13

1.5.2.4. Audit 13

1.5.2.5. Trusted system communication 13

2. Conformance Claims 15

2.1. CC Conformance Claim 15

2.2. PP Conformance Claim 15

3. Security Problem Definition 16

3.1. Assets 16

3.1. Assets 16

3.2. Subjects 16

3.3. Threats 17

3.4. Relation Between Threats & Assets 17

3.5. Organisational Security Policies 19

3.6. Assumptions 19

4. Security Objectives 19

4.1. General 19

4.2 Security objectives for the TOE 19

4.3. Security Objectives for the Operational Environment 20

4.3.1. General 20

4.3.2. Security Problem Definition & Security Objectives 21

4.3.3. Rationale for the Security Objectives ... 23
4.3.3.1. Threats & Objectives ... 23
4.3.3.2. Organizational Security Policies & Objectives ... 23
4.3.3.3. Assumptions & Objectives ... 24
5. Extended Components Definition ... 25
5.1. Class FCS: Cryptographic Support ... 25
5.1.1. Generation of random numbers (FCS_RNG) ... 25
6. Security Requirements ... 26
6.1. Typographical Conventions ... 26
6.2. Subjects, Objects and Operations ... 26
6.3. Security Functional Requirements ... 27
6.3.1. Security Audit (FAU) ... 27
6.3.2. Cryptographic Support (FCS) ... 28
6.3.3. User Data Protection (FDP) ... 31
6.3.4. Identification and Authentication (FIA) ... 33
6.3.5. Security Management (FMT) ... 34
6.3.6. TSF physical protection (FPT) ... 34
6.3.7. TOE Access (FTA) ... 34
6.3.8. Trusted Paths/Channels (FTP) ... 34
6.4. Security Assurance Requirements ... 35
7. Rationale ... 36
7.1. Security Requirements Rationale - Coverage ... 36
7.1.1. Rationale ... 37
7.2. SFR Dependencies ... 37
7.2.1. General ... 37
7.3. Rationales for SARs ... 39
8. TOE Summary Specification ... 40
8.1.1. Security Audit (FAU) ... 41
8.1.2. Cryptographic Support (FCS) ... 41
8.1.3. User Data Protection (FDP) ... 41
8.1.3.1. Access Control ... 41
8.1.4. Identification and authentication (FIA) ... 42
8.1.4.1. User security attribute ... 42
8.1.5. Security Management (FMT) ... 42
8.1.5.4. Management, specification and restrictions on security data ... 42
8.1.6. TSF Physical Protection (FPT) ... 42

8.1.6.1 Basic internal TSF data transfer protection 42
8.1.6.2. Reliable time stamps 42
8.1.7. TOE ACCESS (FTA) 42
8.1.7.1. TSF-initiated termination 42
8.1.8. Trusted Paths/Channels (FTP) 43
8.1.8.1. Inter-TSF trusted channel 43
Bibliography 44

Terms

AC	Authentication Code/Keyboard Input
biocertiX	Business name of the TOE. The TOE consists of biocertiX software (signaturiX Core, signatiruX Admin, Document database, Licence and Configuration database) and biocertiX App accompanied by guidance documentation.
biocertiX server	Server (physical or virtual) where biocertiX software is installed.
ES	External System
Device	Samsung Tablet
HSM	Hardware Security Module
QR	Quick Response Code
QSCD	Qualified Signature Creation Device
Privileged User	The only privileged user is System Administrator
TOTP	Time-based One Time Password
TTP	Trusted Third Party
Vault	Secure Storage of Secrets

1. Introduction

1.1. ST Overview

This ST document defines the security objectives and requirements as well as the scope of the Common Criteria evaluation (according to the Common Criteria methodology) for the biocertiX

biocertiX allows to securely embed handwritten biometric signatures on PDF documents. The signatures are created with a S Pen using a Samsung Tablet (hereinafter referred to as Tablet) on which the biocertiX App mobile application is open. The signing of PDF documents is implemented in accordance with the standard: ETSI EN 319 142-1 V1.1.1 (2016-04) – PadES, signature level B-T [1].

The Target of Evaluation (TOE) is the combination of biocertiX software and the biocertiX App (mobile application). biocertiX software enables the External System to send PDF documents for signing, and users of the signaturiX Core module (the part of biocertiX software) to view the content of the documents and sign them using the biocertiX App (mobile application) open on a Tablet, whereby signing involves sampling the biometric data of the handwritten signature as it is created and embedding it in the PDF document being signed.

TOE is supported by the following software and hardware components to perform its tasks:

- ***External System (ES)*** - A system that allows authenticated users to send PDF documents to the signaturiX Core module for handwritten biometric signatures and receive PDF documents with an embedded biometric signature,
- ***Device (Samsung Tablet)*** - A set of hardware and software for sampling a biometric signature and its cryptographic protection, on which the biocertiX App mobile application is launched,
- ***Certum SimplySign*** - An external environment that enables electronic sealing and time stamping of PDF documents,
- ***Audit Database*** - Software that manages the audit of biocertiX system logs.
- ***Vault: Secret storage -*** A system for securely storing sensitive information (e.g., passwords, private key to decrypt biometrics provided with the biocertiX App, etc.).
- ***Samsung Knox Manage:*** A system that allows the management of Samsung Tablets (including the configuration of the public key involved in encrypting the biometric data on the Tablet before sending it to signaturiX Core module)

To ensure a secure working environment, the biocertiX Core software is delivered as a tamper-proof zip archive for which access (login and password) and the calculated SHA512 hash value is provided via email. The biocertiX software together with an External System and Tablet with the installed biocertiX App provide a handwritten biometric signature service on PDF documents.

1.2. ST Reference

This ST is identified by the following unique reference:

ST Title	SECURITY TARGET FOR biocertiX
ST Version	**2.4-lite**
ST Date	24-09-2025
ST Author	Asseco Data Systems

1.3. TOE Reference

This TOE is identified by the following unique reference:

TOE Name		biocertiX - handwritten biometric signatures on PDF documents
TOE Version		1.2
TOE Component Version	biocertiX System	2.7.0
	biocertiX App	1.012

Evaluation Criteria	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, version 3.1, revision 5, April 2017.
Evaluation Assurance Level	EAL 2
TOE Developer	eXtention
TOE Sponsor	Asseco Data Systems
Evaluation Facility	ITSEF NIT, Poland
Certification Authority	The Center for Standardization and Certification, NASK PIB
Certification ID	1/PC1/AC223/2024

1.4. TOE Overview

biocertiX is a trustworthy system that offers a handwritten biometric signature service on PDF documents. biocertiX ensures that the biometric signature on the document was created by the BioSigner and that the signature is used for its intended purpose - to biometrically sign the document displayed to the BioSigner. The aim of the solution is to enable the expression, in a legally binding manner, of a declaration of intent in electronic form by persons who do not have the means to create an electronic signature or do not have the necessary skills to use such a signature.

biocertiX is a combination of web and mobile applications (biocertiX core software and biocertiX App accordingly) for signing PDF documents (Figure 1).

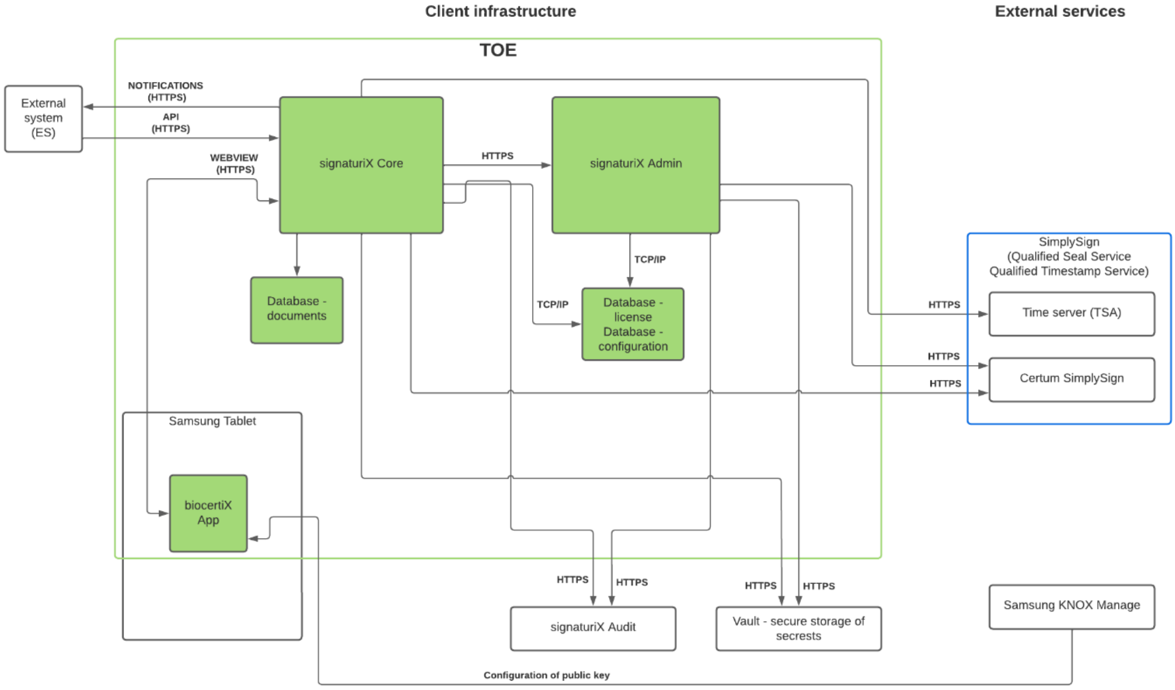

Figure 1: biocertiX – Secure Biosignature System

biocertiX software and biocertiX App are components of the TOE (biocertiX) that reside in a tamper-proof environment, providing the necessary functionality to protect the BioSigner attributes needed to securely create a handwritten biometric signature. Other elements are part of the system environment (elements outside the TOE, e.g. External System needed by the user to interact with the TOE, trusted third party services, etc.). Biometric signatures require a biocertiX App (mobile application) installed on the Tablet with the ability to record the degree of S Pen pressure during the handwritten biometric signature creation.

The user interacts with the ES, which communicates with the TOE using encrypted HTTPS. The user is an individual who has at its disposal the Tablet equipped with S Pen. The ES using the signed digitally API of the signaturiX Core system sends the user a PDF document(s) to be displayed to BioSigner for signing on Tablet. The user and the BioSigner are not necessarily the same person. In response to the sent document(s), the signaturiX Core system generates and sends back to the ES a time-limited one-time QR/AC code. The ES displays this QR/AC code to the user. The user launches the biocertiX App on the Tablet and scans the QR code displayed on the ES or inputs AC code via the Tablet keyboard. This QR/AC code includes a unique authentication identifier of the PDF document(s) to be signed biometrically. The PDF document(s) is displayed on the Tablet in the biocertiX App and the BioSigner can review the content and sign it by providing a handwritten biometric signature on the Tablet.

The biometrics sample of the submitted signature is encrypted on the Tablet with a one-time symmetric key generated using a cryptographically strong random number generator [2, 3, 4] with hardware enhanced entropy provided by Samsung technology that complies with the statistical random number generator tests specified in NIST SP 800-90A [5]. The symmetric key is then encrypted with a public key configured on the Tablet during system initialization, and the corresponding private key is stored on the biocertiX server in a keystore file protected by a password stored in Vault. Each biocertiX instance has a pre-installation generated key pair, of which the public key is installed on the biocertiX App and private key is installed on signaturiX Core during initialization. The biometric signature secured in this way is sent to the signaturiX Core, where it is decrypted, converted to a standardized format and re-encrypted with a one-time symmetric key, which is encrypted with an HSM public key issued by a trusted third party – Certum SimplySign; The HSM public key is a 4096-bit RSA key generated for a given consumer by trusted third party (it is included in the TOE delivery in the license file). The corresponding RSA private key is held only by the TTP. Please note that the actual seal is performed by a TTP using a different pair of keys[1].

The user authentication process is provided by ES, therefore the TOE (signaturiX Core) does not store the credentials of individual users Through the signaturiX Core configuration service, a list of users (logins) who are authorised to use signaturiX Core is sent from the ES. When performing operations for service calls that have the login of a user in the request parameters, signaturiX Core checks whether this user is in the list of authorised users. It is the role of ES to ensure that only an authenticated user of the external system can send a request to signaturiX Core containing the login of this user.

All interactions of the BioSigner with signaturiX Core via ES must be carried out using HTTPS. The TOE receives the document(s) to be signed from the ES using the API of signaturiX Core (SOAP and/or REST). Each document or package of documents sent to the TOE (signaturiX Core) has a unique 'document/package token' assigned to it by the ES. In response to the uploaded document(s), the signaturiX Core returns to the ES a unique, one-time credentials in the form of a QR/AC code, based on which the ES user accesses the document(s) in signaturiX Core by scanning the QR code or input AC code via the Tablet keyboard in the biocertiX App. The biocertiX App presents the selected document(s) to the BioSigner and allows him/her to sign it. Once the signature is affixed, the TOE (signaturiX Core) generates audit records/logs and transfers them to an external audit database to store and secure these records/logs. The content of each audit record/log is electronically signed with a dedicated private key separate from the key used to sign/seal the signed document itself, and the auditor can verify signatures of the audit records/logs. The audit database is protected (record/log integrity is ensured) in the TOE environment.

1.4.1. TOE Type

The TOE type is "none" (undefined), as the TOE is not of a readily available type[2].

Additional note:

The TOE allows to securely embed handwritten biometric signatures on PDF documents The TOE is the combination of web and mobile applications (biocertiX core software and biocertiX App accordingly). signaturiX Core the part of biocertiX software communicates with the biocertiX App using HTTPS.

The TOE implements a protocol (described in Section 1.4) for fetching and embedding signature biometrics into a PDF document.

[1] The certificate of the public key corresponding to the Certum SimplySign private key used to create the qualified electronic seal is available according to Certification Policy of Certum SimplySign concerning QSCD.

[2] According to Annex A - Specification of Security Targets subsection A.4.2.2 [7] the TOE type may be defined as "none" if the TOE is not of a readily available type.

1.4.2. TOE Usage & Major Security Functions

signaturiX Core ensures that the signature operation must be authorized using the ES.

Usage of the TOE includes the following steps:

1) Secure receipt from ES of PDF documents for biometric signature,
2) Authentication of PDF document(s) using QR/AC code,
3) Secure embedding of biometric data (captured form external S_Pen) in a PDF document,
4) Sealing and time-stamping a PDF document with embedded encrypted biometric data,
5) A biometrically signed document is securely made available for download by the ES.

The main utility and security functions of the TOE are:

- TOE initialization
  - ➢ TOE works in the client-server architecture. The client part of the TOE's located on the Tablet (biocertiX App). Its initialization is performed using Knox Manage software, which provides automatic configuration of the public key certificate, security policies and biocertiX App on managed tablets. During initialization of the server part of the TOE, the corresponding private key used by signaturiX Core is installed in keystore on biocertiX server and password to this keystore is stored in Vault. The public key used to create the cryptogram of biometrics decryption key is placed in the license file as part of the license.
- TOE Administration (server part of the TOE)

➢ The System Administrator is allowed to manage users and to configure the system.

➢ signaturiX Admin - configuration. is created in the administration application and each System Administrator is identified by a login and password and TOTP. The administration application is inside the TOE

- Signing operation

➢ The user can indicate (using ES) PDF documents for signing in signaturiX Core. Indicated documents are transferred from ES to signaturiX Core with user login via API. Upon acceptance of a time-limited QR/AC code provided by the TOE, the user is given access to a document(s) on which he/she can provide handwritten signatures or submit an open document for handwritten signature to another person.

- Audit

➢ An audit trail is produced of all security relevant events within the TOE. Access to the Audit Database requires prior authentication using a login and password and TOTP. Management access to audit trail is outside the scope of the TOE.

TOE shall manage the Data Assets as defined in Section 3.1.

1.4.3. Required non-TOE Hardware/Software/Firmware

The following non-TOE software-based elements (accompanied by necessary hardware for this software/services) are required for the operation of the TOE (they are excluded from the scope of the TOE delivery):

- ***External System (ES)***: A Web application that integrates with biocertiX using the API of biocertiX. The ES sends PDF documents to signaturiX Core and presents to the user the authentication QR/AC code received in response. The QR code is scanned or AC code is inputted via the Tablet keyboard on a Tablet where the user is presented with the document(s) (based on the QR/AC code, the view of the biocertiX App is redirected to the document transferred from ES to signaturiX Core). Once the documents are approved in signaturiX Core, the ES receives the signed document(s) from the user using the API of biocertiX.
  The TOE consumer is responsible to either development or acquire the ES.
- ***Certum SimplySign:*** Qualified electronic seal and qualified Timestamps service. As part of this service, SimplySign signs the sent document digest/hash. The digest/hash signed in this way together with the seal's public key certificate and timestamp is saved in the PDF document by the biocertiX system. The access to both of the SimplySign services provided by Certum is required for TOE operation.
  The TOE consumer is responsible for obtaining access to Certum SimplySign: Qualified electronic seal and qualified Timestamps services that are used by the TOE.

- ***Samsung Knox Manage:*** A system that allows the management of Samsung Tablets (including the configuration of the public key involved in encrypting the biometric data on the Tablet before sending it to signaturiX Core). The access to Samsung Knox Manage service provided by Samsung is required for TOE operation. Samsung Knox Manage is a part of Samsung Knox Suite
  The TOE consumer is responsible for acquiring license Samsung Knox Suite.

Additionaly, the following non-TOE hardware-based elements are required for the operation of the TOE (all hardware elements are excluded from the scope of the TOE delivery):

- ***Samsung Tablet:*** A mobile device (S3 upwards) that allow to use a hardware enhanced entropy in a cryptographically strong random number generator.
- Server hosting the biocertiX software together with vault. Minimum requirement for that server:
  - ✓ CPU 4 Core 2.4 GHz Intel(R) Xeon(R) CPU E5-2680 v4 or equivalent
  - ✓ RAM 4 GB
  - ✓ HDD 30 GB
  - ✓ OS Debian 10
- Server hosting signaturiX Audit where the signaturiX Audit is installed (the signaturiX Audit itself is included in to scope of the TOE delivery). It must be a different server than the server hosting biocertiX software together with vault. Minimum requirements for that server:
  - ✓ 2 Core 2.4 GHz Intel(R) Xeon(R) CPU E5-2680 v4 or equivalent
  - ✓ RAM 2 GB
  - ✓ HDD 20 GB
  - ✓ OS Debian 10

1.5. TOE Description

The TOE is a software component connected to external services (signaturiX Audit, Vault, Qualified Seal Service, Qualified Timestamp Service and ES[3]) using HTTPS. The TOE is located in a tamper-proof environment. In regards to biometric data processing the TOE meets the requirements of ISO / IEC 19794-7 for biometrics and standards for PDF documents ISO 32000-1.

1.5.1. Physical Scope of the TOE

The TOE consists of the following elements (see Table 1 section 1.5.1.1):

- ***biocertiX App*** **–** mobile application (for devices) that responsible for sampling a biometric signature and its cryptographic protection. The biocertiX App. shall be acquired from Google Play Store.
- ***signaturiX Core***: software element that enables the embedding of biometric data (collected and encrypted handwritten biometric signature data using device) in PDF documents according to the protocol described in section 1.4.
- ***Document database***: A postgres database that stores documents in memory for the duration of their processing in signaturiX Core. This ensures that documents are not stored on the signaturiX Core server file system.
- ***Database (licenses and configuration)***: A postgres database that stores information about the logins of users who have been authorized by the API of biocertiX to access the biocertiX system and use its functionalities (including, for example, qualified seals). The configuration of the biocertiX appearance (colours, logos) and the current values of the biocertiX system parameters are also stored there. The logins of users authorized to use the biocertiX system are transmitted via the secure API of biocertiX.
- ***signaturiX Admin:*** An administration application that allows trusted System Administrators to configure the system parameters (tomcat 9 with the signaturix-admin web application).

The following guidance documentation are needed for compliant TOE setup::

- Installation, Configuration and Maintenance of TOE

The following non-TOE elements are provided together with the TOE:

[3] The Samsung Knox Manage, depicted in Figure 2, is not connected to the TOE during its operation. It is used solely utilized during the installation procedure (specifically during the TOE initialization).

- ***Vault: Secret storage*** - A system for securely storing sensitive information (e.g., passwords, private key to decrypt biometrics provided with the biocertiX App, etc.)
- ***signaturix-audit***: an auditing system with a database that stores audit records/logs (tomcat 9 with the signaturix-audit web application)
- ***signaturix-starter*** (alpine Linux with initialisation script)

1.5.1.1. Delivery of the TOE

The TOE comprises two components:

- The biocertiX Software is delivered in a tamper-protected file, the biocertiX Software along with the documentation and non-TOE elements defined in section 1.5.1 are placed in a zip-archive protected by SHA512 digest/hash (see Table 1].

biocertiX Software elements	**Version**
signaturiX Core	2.7.0
Document database	2.2
Database (licenses and configuration)	17.2
signaturiX Admin	2.7.0
Installation, Configuration and Maintenance of TOE	**Version**
AGD_PRE	0.99
AGD_OPE	1.3
Non TOE elements	**New version**
Vault: Secret storage	1.18
signaturix-audit	2.7.0
signaturix-starter	2.7.0

Table. 1. biocertiX software and non TOE elements

Link to this elements [table 1] is sent to the Customer leading to the file distribution system (hosted by the Xtension provider). Access to the file is secured by a password, which is sent by SMS to a designated person (an employee of the Client).

- The biocertiX App. shall be acquired from Google Play Store [table 2].

biocertiX Application	**version**
biocertiX App	1.012

Table. 2. biocertiX Application

1.5.2. Logical Scope of the TOE

After installation and configuration, TOE creates a signature prototype (raw biometric data) using a device, This data are encrypted with AES-256 key. The encryption key is then encrypted with a public key configured on the Tablet during system initialization (the corresponding private key is stored on the biocertiX server in a keystore file protected by a password stored in Vault). The encrypted raw biometric data together with the encrypted AES-256 biometrics encryption key are sent to the signaturiX Core where they are decrypted, i.e. firstly biometrics encryption key and then with its usage raw biometrics data. The raw biometrics data are converted into a standardized format (ISO 19794-7:2014 compliant [6]) and then encrypted with a random one-time symmetric AES-256 key generated in the signaturiX Core application. The product of this encryption is referred to as the cryptogram of biometrics. The AES-256 key is encrypted with a public HSM key (RSA 4096-bit) and the result of this encryption is referred to as the cryptogram of biometrics decryption key. The cryptogram of biometrics and the cryptogram biometrics decryption key are embedded in the signed PDF document. The whole PDF document (with encrypted biometrics embedded) is hashed and the hash value as the data to be signed (DTBS/R) is sealed by using a Certum SimplySign (TTP). Additionally the electronically sealed PDF document is time-stamped using the qualified timestamp service offered by Certum SimplySign TTP).

This chapter describes the logical security features offered by the TOE.

1.5.2.1. Secure initialization

When the system is installed, it is configured according to the 'administrator manual' documentation guidelines. The TOE initialization is performed using Knox Manage software, which provides automatic configuration of the public key certificate, security policies and biocertiX App on managed tablets. The corresponding private key used by signaturiX Core is installed in keystore on biocertiX server and password to this keystore is stored in Vault. The public key used to create the cryptogram of biometrics decryption key is placed in the license file as part of the license.

1.5.2.2. Roles & Available Functions

signaturiX System Administrator

> They are users who administer the signaturiX Core software (the part of TOE)). They access through the signaturiX Admin application to perform various TOE-specific operations, e.g. making changes to the TOE configuration, etc. Trusted System Administrators are created in the signaturiX Admin application and each is identified by a login and password and TOTP.

biocertiX User

> They are users who can indicate in the signaturiX Core module (using ES) PDF documents for signing. Users are identified by a user ID. In response to the uploaded document (s), the API returns a one-time, time-limited credentials (in the form of a QR/AC code). Using this QR/AC code, the user is given access to the document(s) via the biocertiX App, where he/she can provide handwritten signatures on the document or submit the open document to another person for signature.

1.5.2.3. Secure Administration

Once installed and initialized, the TOE can only be modified (e.g. changes to configuration files, biocertiX system parameters) by authorized System Administrator(s). The System Administrator should be authenticated before any change made to the system. All administrative activities (carried out in the TOE) are recorded by audit.

signaturiX System Administrator is authenticated with a login, a strong password and TOTP before is authorized to perform any actions in the signaturiX Admin application. The signaturiX Admin application must provide strict access control to all system components (System Administrator(s) are first identified and authenticated and then after successful authentication, access to system objects is controlled based on assigned activities according to the procedure guidelines).

1.5.2.4. Audit

All TOE security events are recorded in external database (c). This event log includes all changes to the TOE, including changes induced by System Administrators, which may affect its security. Inside the signaturiX Audit each entry is protected to prevent changes, entries are protected against deletion (their integrity is ensured). All audit records resulting from the actions of the TOE System Administrators and the execution of requests in the TOE are stored in the signautriX Audit database. The connection between the TOE and signaturiX Audit component is provided via TCP secure protocol TLS 1.3. Access to the Audit Database is possible only after prior authentication (only by authorized auditor who can't be a TOE System Administrator). The Audit records do not contain any data that allows the recovery or decryption of confidential user data.

1.5.2.5. Trusted system communication

The TOE implements and enforces the following trusted communication methods and protocols:

- ***External System - ES***: connects to the TOE using HTTPS. The ES sends to the TOE, via the TOE API, a document(s) to be signed. In response, the TOE returns to the ES a unique, one-time credentials in the form of a QR/AC code, based on which the ES user accesses the document(s) in the signaturiX Core module using the biocertiX App.
- ***Certum SimplySign:*** connects to the TOE using HTTPS. A qualified electronic seal and qualified timestamps are provided by the Certum SimplySign.
- ***signaturiX Audit:*** connects to the TOE using HTTPS. A database that stores audit records/logs
- The 'primary biometric data' in a format appropriate for the biometric sampling device used is encrypted by the biocertiX App using a session AES-256 key generated by cryptographically strong random number generator with hardware enhanced entropy provided by Samsung technology that complies with the statistical random number generator tests specified in NIST SP 800-90A and sent in encrypted form to the signaturiX Core. The symmetric key is then encrypted with a public key configured on the Tablet

during system initialization. The private key used for session AES key decryption is stored on the biocertiX server in a keystore file protected by a password stored in Vault.

Additionally, communication between signaturiX Core and biocertiX App is provided using the HTTPS protocol with mutual authentication.

2. Conformance Claims

2.1. CC Conformance Claim

This security target is conformant to Common Criteria version 3.1 revision 5.

More precisely, this security target is:

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017 [7].
- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017 [8].
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017 [9].

as follows:

- Part 2 extended; and
- Part 3 conformant.

The following must be considered:

- Common Methodology for Information Technology Security Evaluation, Evaluation methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017 [15]

The assurance requirement of this security target is **EAL2 Conformant**

2.2. PP Conformance Claim

This ST does not claim conformance to any PP for the TOE.

3. Security Problem Definition

3.1. Assets

3.1. Assets

The TOE has the following assets, which are to be protected in integrity and some of them in confidentiality as described below. The TOE must ensure that whenever the asset is persisted outside the TOE, the TOE has performed the necessary cryptographic operations to enforce confidentiality and integrity i.e., to detect if an asset has been modified. Access control to TOE assets outside the TOE are to be enforced by the environment.

R.Document - a PDF-formatted document sent by the user to the TOE. It is returned to the user with an embedded and encrypted scan of a biometric signature. It shall be protected in integrity and authenticity. The authenticity means that the document is processed in reliable manner in TOE, what is confirmed by the qualified electronic seal service. Non-repudiation in the case of Biosigner is not managed in TOE and its environment, because it is not the objective of TOE.

R.EmbeddedBioSignature: biometrics binaries scanned by BioSigner on the Tablet with the use of S Pen and converted to ISO 197 94-7:2014 compliant format and embedded in PDF document. It shall be protected in integrity and confidentiality.

R.Reference_User_Authentication_Data: the set of data used by TOE to authenticate the ~~R.~~User. It contains login list used by the TOE to authenticate the ~~R.~~User (who are authorised to use signaturiX Core). The R.Reference_User_Authentication_Data shall be protected in integrity and confidentiality.

Application Note 1

Any change of login list requires re-initialization of the TOE Core by System Administrator.

R.Reference_Device_Authentication_Data: is the set of data used by the TOE to authenticate the Device. It contains all the data used by the TOE to authenticate the Device. The R.Reference_Device_Authentication_Data shall be protected in integrity and confidentiality.

Application Note 2

The tablet is bound to the user only during the working session on the document(s) (from scanning the QR code or by input AC code via the Tablet keyboard to approving or rejecting the document(s)). It is not necessary to bind the tablet with the user longer than it is required to present and sign all the documents indicated by the user in ES. The device is additionally authenticated through the customer's network infrastructure (e.g. VPN or secure WiFi) and only then is it given network access to communicate with biocertiX.

R.TSF_DATA: is the set of TOE data (executable and configuration) used to operate the TOE. It shall be protected in integrity.

R.Privileged_User: is the set of data that uniquely identifies a Privileged User (System Administrator (s)) within the TOE. It shall be protected in integrity.

Application Note 3

It is assumed that TOE System Administrator and operating System Administrator (root) is the same subject with unique authentication data. Another attempt requires at least two different subjects with different authentication data for administrative tasks purposes (the principle of two eyes).

R.Reference_Privileged_User_Authentication_Data: is the set of data used by the TOE to authenticate the Privileged User. It shall be protected in integrity and confidentiality.

R.Audit: audit records containing logs of events requiring to be audited. The logs are produced by the TOE and stored externally. The R.Audit shall be protected in integrity.

R.Random random secrets, e.g. AES keys used by the TOE to encrypt biometric sample, QR/AC for Device authentication. It shall be protected in integrity and confidentiality.

3.2. Subjects

This following list of subjects interact with the TOE:

- User is the natural or legal person who uses the TOE through the secure protocol (HTTPS) where they provide the documents for Signing by the BioSigner.
- BioSigner is the person who use S Pen to sign documents on the Tablet.
- Privileged User is only the System Administrator who manages and implements changes to the TOE.

- System Auditor review audit archives and logs to verify system performance against security rules.
- **Attacker** is a human, or process acting on their behalf, located outside the TOE. An attacker is a threat agent (a person with the aim of manipulating user data, or a process acting on their behalf) trying to undermine the TOE security functions, especially to change properties of the maintained assets.

Application Note 5

System Auditor is user of a separate system with a separate user account. System Auditor is identified by a login and password and TOTP.

3.3. Threats

The following threats are defined for the TOE. An attacker described in each of the threats is a subject that is not authorised for the relevant operation, but may present himself as an unknown user or as one of the other defined subjects.

T.BIOSIGNER_IMPERSONATION: Attacker impersonates a BioSigner and binds R. EmbeddedBioSignature created by the BioSigner with R.Document unaccepted by BioSigner. The assets R.Document and R. EmbeddedBioSignature are threatened.
This threat covers the following attacks:

- An attacker may attempt to access to the R.EmbeddedBioSignature provided by a BioSigner, which can be replayed to impersonate the BioSigner (e.g. signing another document(s) on behalf of the BioSigner) or another BioSigner.
- An attacker may try to record and imitate or generate the biometric characteristic of the BioSigner.
- An attacker modifies R. Embedded**BioSignature** during or after creation before its embedding in R.Document.

T. USER_IMPERSONATION

An attacker impersonates User. As examples, it could be:

- ~~by transferring wrong User to TOE from ES; or~~
- by transferring wrong R.Reference_User_Authentication_Data to TOE from ES.

The assets User and R.Reference_User_Authentication_Data are threatened

T.BYPASS: An attacker may be able to bypass TOE protection mechanisms through unprotected interfaces in order to inappropriately access protected data and services (illicitly use the TOE's management functions). All the assets are threatened.
T.EXCESS_AUTHORITY: An attacker may be able to exercise System Administrator authorities to inappropriately manage the TOE. The assets R.Privileged_User, R.Reference_Privileged_User_Authentication_Data and R.TSF_Data are threatened.
T.TAMPER: An attacker may be able to inappropriately modify or otherwise tamper R.TSF_Data. R.TSF_Data is threatened.
T.TSF_COMPROMISE: System Administraqtor (Privileged_User) may cause R.TSF_Data (e.g. executable code) to be inappropriately accessed (viewed, modified, or deleted). R.TSF_Data is threatened.
T.UNAUTHORIZED_ACCESS: An attacker may gain access to R.TSF_Data and/or user data for which they are not authorized according to the TOE security policies All the assets are threatened.
T.UNDETECTED_ACTIONS: The System Administrator may not have the ability to detect potential security violations thus limiting the System Administrator's ability to identify and take action against a possible security breach. All the assets are threatened.
T.AUDIT: An attacker may be able to cause the lost or destruction of R.Audit before transferring it to the external signaturiX Audit module. The asset R.Audit is threatened.
T.CRYPTO: Weakness of crypto considering parameters values and known cryptanalysis attacks. All the assets requiring integrity and/or confidentiality and/or authenticity protection are threatened.

3.4. Relation Between Threats & Assets

This following table provides an overview of the relationships between asset, associated security properties and threats. For details consult the individual threats in the previous sections.

Asset	Security Dimensions	Threats
R.Document	Integrity	T.BYPASS T.UNAUTHORIZED_ACCESS T.UNDETECTED_ACTIONS

		T.CRYPTO
	Authenticity	T.BIOSIGNER_IMPERSONATION T.BYPASS T.UNAUTHORIZED_ACCESS T.UNDETECTED_ACTIONS T.CRYPTO
R.EmbeddedBioSignature	Integrity	T.BIOSIGNER_IMPERSONATION T.BYPASS T.UNAUTHORIZED_ACCESS T.UNDETECTED_ACTIONS T.CRYPTO
	Confidentiality	T.BIOSIGNER_IMPERSONATION T.BYPASS T.UNAUTHORIZED_ACCESS T.UNDETECTED_ACTIONS T.CRYPTO
R.Reference_User_Authentication_ Data	Integrity	T.BYPASS T.UNAUTHORIZED_ACCESS T.UNDETECTED_ACTIONS T.CRYPTO T.USER_IMPERSONATION
	Confidentiality	T.BYPASS T.UNAUTHORIZED_ACCESS T.UNDETECTED_ACTIONS T.CRYPTO T.USER_IMPERSONATION
R.Reference_Device_Authentication_Data	Integrity	T.BYPASS T.UNAUTHORIZED_ACCESS T.UNDETECTED_ACTIONS T.CRYPTO
	Confidentiality	T.BYPASS T.UNAUTHORIZED_ACCESS T.UNDETECTED_ACTIONS T.CRYPTO
R.TSF_DATA	Integrity	T.BYPASS T.EXCESS_AUTHORITY T.TAMPER T.TSF_COMPROMISE T.UNAUTHORIZED_ACCESS T.UNDETECTED_ACTIONS T.CRYPTO
R.Privileged_User	Integrity	T.BYPASS T.EXCESS_AUTHORITY T.UNAUTHORIZED_ACCESS T.UNDETECTED_ACTIONS T.CRYPTO
R.Reference_Privileged_Authentication_Data	Integrity	T.BYPASS T.EXCESS_AUTHORITY T.UNAUTHORIZED_ACCESS T.UNDETECTED_ACTIONS T.CRYPTO
	Confidentiality	T.BYPASS T.EXCESS_AUTHORITY T.UNAUTHORIZED_ACCESS T.UNDETECTED_ACTIONS T.CRYPTO
R.Audit	Integrity	T.BYPASS T.UNAUTHORIZED_ACCESS T.UNDETECTED_ACTIONS T.AUDIT T.CRYPTO
R.Random	Integrity	T.BYPASS T.UNAUTHORIZED_ACCESS T.UNDETECTED_ACTIONS T.CRYPTO
	Confidentiality	T.BYPASS T.UNAUTHORIZED_ACCESS T.UNDETECTED_ACTIONS T.CRYPTO

Table 3-1 Relation between Assets, security properties & threats

3.5. Organisational Security Policies

TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

OSP.ACCOUNTABILITY

The users of the TOE shall be held accountable for security-relevant actions within the system.

OSP.CRYPTOGRAPHY

FIPS-approved or SOGIS agreed cryptographic functions shall be used to perform all cryptographic operations.

3.6. Assumptions

A. PRIVILEGED_USER: It is assumed that all personnel administering the TOE are trusted, competent and possesses the resources and skills required for his/her tasks and is trained to conduct the activities he/she is responsible for.

A.BIOSIGNER: It is assumed that the BioSigner is conscious of what he/she is signing and the responsibility resulting from it.

A.SAMPLING_BIOMETRIC_DATA: It is assumed that data sampled by S Pen are reliable and protected before it is transferred to TOE for encryption purposes

A.BIOSIGNER_DEVICE: It is assumed that the device used by the User and BioSigner to interact with TOE is under the User control for the signature operation, e.g. protected against malicious code, protected against physical interception by unauthorized entities.

A.TRUSTED_USER: It is assumed that the User of the biocertiX system is not malicious, and exercises appropriate precautions.

A. COMMUNICATION PROTECTED: It is assumed that the communication between the TOE and external entities providing services to the TOE must be protected from eavesdropping and modification through physical or logical means.

A. EXTERNAL_SYSTEM: It is assumed that each user must first be authenticated in ES before they can use the biocertiX system

A.ACCESS_PROTECTED: It is assumed that the signaturiX Core part of the TOE operates in a protected environment. Only Privileged Users have access to TOE. The TOE software and hardware environment is installed, configured and managed by Privileged Users in a secure state that mitigates against the specific risks applicable to the deployment environment.

A.AUDIT: It is assumed that any audit generated by the TOE are only handled by authorised personal. The personal that carries these activities should act under established practices.

A.TRUSTED_PKI: It is assumed that PKI service providers that exchange data with the TOE are trusted.

A.TIME_STAMPS: It is assumed that reliable time stamps for audit logs are provided by operating system's clock configured in such a way that it is regularly synchronized with trusted server based on the NTP protocol.

Application Note 4

The timestamp mentioned above applies to the dating of events log.

4. Security Objectives

4.1. General

This section identifies and defines the security objectives for the TOE and its operational environment. These security objectives reflect the stated intent, counter the identified threats, and take into account the assumptions.

4.2 Security objectives for the TOE

The following security objectives describe security functions to be provided by the TOE.

OT.USER_MANAGEMENT

The TOE shall ensure that any modification to R.Reference_User_Authentication_Data is performed under control of the Privileged User

OT. BIOSIGNATURE_INTEGRITY_CONFIDENTIALITY

The TOE shall ensure that a R.EmbeddedBioSignature can't be modified when using by the TOE and that it is confidential during transmission between biocertiX App and signaturiX Core.

Application Note 5

It is assumed Tablet operating system ensures that the biosignature capturing application is protected against another applications influence. The user should ensure the physical security of the Tablet. Before sending to signaturiX Core biometric data is encrypted with AES256 in the biocertiX App.

OT.SELF_PROTECTION: The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure**.**

OT.ROBUST_TOE_ACCESS: The TOE will provide secure mechanisms that control a user's (System Administrator and User) logical access to the TOE and explicitly denies access for unauthorized subjects, i.e. attackers .

OT.IDENTIFICATION_AUTHENTICATION: The TOE must ensure that only identified and authenticated users gain access to protected resources.

OT.SECURE_CHANNEL: The TSF shall communicate externally (with all non-TOE Software) and internally (between separate parts of the TOE software) using a trusted channel that protects the confidentiality and integrity of user data being transmitted

OT.INTEGRITY: The TOE will provide the capability to perform self-tests to ensure the integrity of critical functionality, software/firmware and data has been maintained. The TOE will also provide a means to verify the integrity of downloaded updates and control the download and launch of executables.

OT.CRYPTOGRAPHIC_FUNCTIONS: The TOE shall provide cryptographic functions (i.e., encryption/decryption and digital signature operations) to maintain the confidentiality and allow for detection of modification of TSF data that is transmitted between physically separated portions of the TOE, or stored outside the TOE. The TOE must implement approved cryptographic algorithms for encryption/decryption, authentication, and signature generation/verification and approved key generation techniques meeting the FIPS or SOGIS requirements.

OT.MANAGE: The TOE will provide all the functions exchanging TSF data (e.g. changes to configuration files, biocertiX system parameters) necessary to support the System Administrators in their management of the security of the TOE, and restrict these functions from unauthorized use.

OT.AUDIT: The TOE shall ensure that all users can be held accountable for their security relevant actions. In this context the TOE shall log all security relevant events and react in order to keep the TOE in a secure state. All this logs are immediately and securely transferred to the external signaturiX Audit.

OT.ROLES The TOE will support users roles and separately System Administrator roles. Users not being System Administrators are not allowed to perform administrative operations.

4.3. Security Objectives for the Operational Environment

4.3.1. General

OE.RELIABILITY: The authorized User is responsible for linking visible R.Document only with the person using S Pen at the moment. The authorized User is the sole entity to operate the Tablet.

OE.TIME_STAMPS: The operational environment shall provide reliable time stamps according to NTP protocol for audit logs. System Administrator shall be capable to set the time incoming from Operation system (using NTP protocol).

OE.PERSONNEL: Personnel working as TOE System Administrators shall be carefully selected and possesses the resources and skills required for his tasks and trained for proper operation of the TOE.

OE.BIOSIGNER: BioSignerm placing his/her signature in the area pointed on the Tablet screen, shell be conscious of what he/she is signing and the responsibility resulting from it.

OE.SAMPLING_BIOMETRIC_DATA: The data sampled by S Pen are reliable and protected before it is transferred to TOE for encryption purposes.

OE.BIOSIGNER_DEVICE: The device (tablet) containing the biocertiX App and which is used by the BioSigner to interact within the TOE shall be protected against malicious code and protected against physical interception by unauthorized entities. The device may be used to view the document(s) to be signed.

OE.COMMUNICATION PROTECTION: The communication between the TOE and external entities providing services to the TOE must be protected from eavesdropping and modification through physical or logical means.

OE. EXTERNAL SYSTEM: Before using the biocertiX system, each user must first be authenticated in ES.

OE.ENVIRONMENT: The signaturiX Core part of the TOE shall operate in a protected environment that limits physical access to the TOE to authorised privileged users. The TOE software and hardware environment shall be installed and maintained by System Administrators in a secure state that mitigates against the specific risks applicable to the deployment environment.

OE.AUDIT: Any audit generated by the TOE are only handled by authorised personal. The personal that carries these activities should act under established practices.

OE.TRUSTED_PKI: The TOE exchanges data with trusted PKI service providers for Qualified Seal and Qualified Timestamp purposes. .

4.3.2. Security Problem Definition & Security Objectives

The following tables map security objectives with the security problem definition.

	OT.USER_MANAGEMENT	OT. BIOSIGNATURE_INTEGRITY_CONFIDENTIALITY	OT.SELF_PROTECTION	OT.ROBUST_TOE_ACCESS	OT.IDENTIFICATION_AUTHENTICATION	OT.SECURE_CHANNEL	OT.INTEGRITY	OT.CRYPTOGRAPHIC_FUNCTIONS	OT.MANAGE	OT. AUDIT	OT. ROLES
T.BIOSIGNER_IMPERSONATION		x						x		x	
T.USER_IMPERSONATION	x										
T.BYPASS			x								
T.EXCESS_AUTHORITY											x
T.TAMPER			x								
T.TSF_COMPROMISE									x		
T.UNAUTHORIZED_ACCESS				x	x						
T.UNDETECTED_ACTIONS				x	x	x	x			x	
T.AUDIT			x							x	
T.CRYPTO								x			
Organizational Security Policies											
OSP.ACCOUNTABILITY				x	x					x	
OSP.CRYPTOGRAPHY								x			

Table 4.1 TOE Security objectives & (threats, Organizational Security Policies)

	OE.RELIABILITY	OE.TIME_STAMPS	OE.PERSONNEL	OE.BIOSIGNER	OE.SAMPLING_BIOMETRIC_DATA	OE.BIOSIGNER_DEVICE	OE.COMMUNICATION PROTECTION	OE.ENVIRONMENT	OE.AUDIT	OE.TRUSTED_PKI	OE EXTERNAL SYSTEM
T.BIOSIGNER_IMPERSONATION	x										
T.BYPASS											
T.EXCESS_AUTHORITY											
T.TAMPER											
T.TSF_COMPROMISE											
T.UNAUTHORIZED_ACCESS											
T.UNDETECTED_ACTIONS											
T.AUDIT									x		
T.CRYPTO											
Organizational Security Policies											
OSP.ACCOUNTABILITY		x									
OSP.CRYPTOGRAPHY											

Table 4.2 TOE Security Objectives for the Operational Environment & (threats, Organizational Security Policies)

	OE.RELIABILITY	OE.TIME_STAMPS	OE.PERSONNEL	OE.BIOSIGNER	OE.SAMPLING_BIOMETRIC_DATA	OE.BIOSIGNER_DEVICE	OE.COMMUNICATION PROTECTION	OE.ENVIRONMENT	OE.AUDIT	OE.TRUSTED_PKI	OE EXTERNAL SYSTEM
A. PRIVILEGED_USER			x								
A.TIME_STAMPS		x									
A.TRUSTED_USER	x										
A.BIOSIGNER				x							
A.SAMPLING_BIOMETRIC_DATA					x						
A.BIOSIGNER_DEVICE						x					
A.COMMUNICATION PROTECTED							x				
A.ACCESS_PROTECTED								x			
A.AUDIT									x		
A.TRUSTED PKI										x	
A.EXTERNAL SYSTEM											x

Table 4.3 TOE Assumptions and Security Objectives for the environment

4.3.3. Rationale for the Security Objectives

This section provides a rationale objective that covers each threat, organizational security policy and assumption.

4.3.3.1. Threats & Objectives

T.BIOSIGNER_IMPERSONATION is covered by **OT.AUDIT** requiring that audit detect access attempts to TOE protected resources.

It is also covered by ***OT.CRYPTOGRAPHIC_FUNCTIONS*** requiring the usage of endorsed algorithms.

It is also covered by ***OT. BIOSIGNATURE_INTEGRITY_CONFIDENTIALITY*** requiring that the R.EmbeddedBioSignature is protected in integrity and confidentiality during transfer between the parts of the TOE (from biocertiX App to sygnaturiX Core).

It is also covered by **OE. RELIABILITY** requiring that only the authorized User can operate Tablet.

T.USER_IMPERSONATION is covered by ***OT.SIGNER_MANAGEMENT*** requiring the User to be securely created.

T.BYPASS is covered by **OT.SELF_PROTECTION** requiring that the TSF will maintain a domain for its own execution so that it can protect itself at the interfaces it offers.

T.EXCESS_AUTHORITY is covered by ***OT.ROLES*** requiring that The TOE distinguishes administrative roles that are differentiated from users.

T.TAMPER is covered by **OT.SELF_PROTECTION** requiring that the TSF will maintain a domain for its own execution so that it can protect itself at the interfaces it offers.

T.TSF_COMPROMISE is covered by **OT.MANAGE** requiring that the TOE ensures that System Administrator functions are protected from unauthorized use.

T.UNAUTHORIZED_ACCESS is covered by **OT.ROBUST_TOE_ACCESS** requiring that the TOE provide a mechanism to explicitly denies access for unauthorized subjects .

It is also covered by **OT.IDENTIFICATION_AUTHENTICATION** requiring to implement identification and authentication mechanisms in the TOE.

T.UNDETECTED_ACTIONS is covered by **OT.ROBUST_TOE_ACCESS** requiring that the TOE provide a mechanism to deny access to specific users when appropriate.

It is also covered by **OT.IDENTIFICATION_AUTHENTICATION** requiring to implement identification and authentication mechanisms in the TOE.

It is also covered by **OT.SECURE_CHANNEL** requiring the protection of the integrity and confidentiality through the use of a trusted channel

It is also covered by **OT.INTEGRITY** requiring the integrity of software that is installed onto the system from the network.

It is also covered by **OT. AUDIT** requiring that audit detect access attempts to TOE protected resources.

T.AUDIT is covered by **OT.SELF_PROTECTION** requiring that the TSF will maintain a domain for its own execution so that it can protect itself at the interfaces it offers.

It is also covered by **OT. AUDIT** requiring that audit detect access attempts to TOE protected resources.

It is also covered by OE.AUDIT requiring that **a**ny audit generated by the TOE are only handled by authorised personal which acts under established practices.

T.CRYPTO is covered by **OT.CRYPTOGRAPHIC_FUNCTIONS** requiring that the cryptographic mechanisms shall provide cryptographic functions (i.e., encryption/decryption and digital signature operations) to maintain the confidentiality and allow for detection of modification of TSF data that is transmitted between physically separated portions of the TOE, or stored outside the TOE The TOE must implement approved cryptographic algorithms for encryption/decryption, authentication, and signature generation/verification and approved key generation techniques meeting the FIPS or SOGIS requirements.

4.3.3.2. Organizational Security Policies & Objectives

OSP.ACCOUNTABILITY is covered by **OT.ROBUST_TOE_ACCESS** requiring that the TOE provide a mechanism to deny access to specific users when appropriate.

It is also covered by **OT.IDENTIFICATION_AUTHENTICATION** requiring to implement identification and authentication mechanisms in the TOE

It is also covered by **OT. AUDIT** requiring that audit detect access attempts to TOE protected resources.

It is also covered by **OE.TIME_STAMPS** requiring the operational environment to provide a reliable timestamps (settable by the System Administrator in the case of audit logs timestamping with NTP protocol). The audit mechanism is required to include the current date and time in each audit record.

OSP.CRYPTOGRAPHY is covered by **OT.CRYPTOGRAPHIC_FUNCTIONS** requiring that the cryptographic mechanisms shall provide cryptographic functions (i.e., encryption/decryption and digital signature operations) to maintain the confidentiality and allow for detection of modification of TSF data that is transmitted between physically separated portions of the TOE, or stored outside the TOE. The TOE must implement approved cryptographic algorithms for encryption/decryption, authentication, and signature generation/verification and approved key generation techniques meeting the FIPS or SOGIS requirements.

4.3.3.3. Assumptions & Objectives

A.PRIVILEGED_USER is covered by **OE.PERSONNEL** requiring that the TOE System Administrators shall be carefully selected and well trained and non-hostile.

A.BIOSIGNER is covered by ***OE.BIOSIGNER*** requiring that the BioSigner, placing his/her signature in the area pointed on the Tablet screen, is conscious of what he/she is signing and the responsibility resulting from it

A.SAMPLING_BIOMETRIC_DATA is covered by OE. SAMPLING_BIOMETRIC_DATA requiring the data sampled by S Pen are reliable and protected before it is transferred to TOE for encryption purposes.

A.BIOSIGNER_DEVICE is covered by ***OE.BIOSIGNER_DEVICE*** requiring the Signer's device to be protected against malicious code and protected against physical interception by unauthorized entities.

A.TRUSTED_USER is covered by **OE.RELIABILITY** requiring that only the authorized User can operate the Tablet.

A.COMMUNICATION_PROTECTED is covered by **OE.COMMUNICATION PROTECTION** requiring that the communication between the TOE and External services are protected against eavesdropping and protected against modification through physical or logical means.

A.EXTERNAL_SYSTEM is covered by **OE.EXTERNAL_SYSTEM** requiring that each user must first be authenticated in ES before they can use the biocertiX system.

A.ACCESS_PROTECTED is covered by ***OE.ENVIRONMENT*** requiring the TOE be operated in an environment with physical access controls..

A.AUDIT is covered by **OE.AUDIT requiring a**ny audit generated by the TOE are only handled by authorised personnel which acts under established practices.

A.TRUSTED PKI is covered by ***OE.TRUSTED_PKI*** requiring that the TOE exchanges data with trusted PKI service providers.

A.TIME_STAMPS is covered by **OE.TIME_STAMPS** requiring the operational environment to provide a reliable time stamps according NTP protocol (settable by the System Administrator).

5. Extended Components Definition

5.1. Class FCS: Cryptographic Support

5.1.1. Generation of random numbers (FCS_RNG)

Family behaviour

This family defines quality requirements for the generation of random numbers which are intended to be use for cryptographic purposes.

Components levelling and description

Figure shows the component leveling for this family.

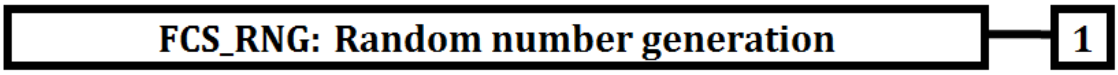

Figure 3 — FCS_RNG: Component levelling

FCS_RNG.1 Random number generation requires that random numbers meet a defined quality metric.

Management of FCS_RNG.1

The following actions can be considered for the management functions in FCS_RNG.1:

a) there are no management activities foreseen.

Audit of FCS_RNG.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) there are no actions defined to be auditable.

FCS_RNG.1 Random number generation

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1.1

The TSF shall provide a [selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic] random number generator that implements: [assignment: list of security capabilities].

FCS_RNG.1.2

The TSF shall provide [selection: bits, octets of bits, numbers [assignment: format of the numbers]] that meet [assignment: a defined quality metric].

6. Security Requirements

6.1. Typographical Conventions

The following conventions are used in the definitions of the SFRs:

- Selections made in this ST are written in **bold text and double underlined**, and the original text is indicated in a footnote.
- Assignments made in this ST are written in **italics and underlined**, and the original text is indicated in a footnote.
- Iterations are denoted by a slash "/" and the iteration indicator after the component identifier.

6.2. Subjects, Objects and Operations

This section describes the subjects, objects and operations support by the TOE.

Subject	Description
R.Document	Represents a PDF document with an embedded and encrypted scan of a biometric signature
R.EmbeddedBioSignature	Biometrics binaries scanned on the Tablet with the use of S Pen and converted to ISO 197 94-7:2014 compliant format and embedded in PDF document
R.Reference_User_Authentication_Data	Data used by the TOE to authenticate a User
R.Privileged_User	Represents within the TOE a privileged user that can administrate the TOE.
R.Reference_Privileged_User_Authentication_Data	Data used by the TOE to authenticate a Privileged_User
R.Reference_Device_Authentication_Data	Data used by the TOE to authenticate a Device
R.TSF_DATA	TOE Core Part Configuration Data

Table 6.1. Subjects and description

Subject	Operation	Object	Description
R.Privileged_User	Create_New_User	User R.Reference_User_ Authentication_Data	A new User can be created which covers the object representing the new User as well as the object used to authenticate the newly created User.
R.Privileged_User	User_Maintenance	User	System Administrator can change the set of Users and related Reference_User_ Authentication_Data in the TOE.

Table 6.2. Subject, object, operation and description

6.3. Security Functional Requirements

The individual security functional requirements are specified in the sections below.

6.3.1. Security Audit (FAU)

FAU_GEN.1 Audit Generation

FAU_GEN.1.1: The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions

b) All auditable events for the **minimum**[4] level of audit,

c) And:

- ✓ ***Privileged User management;***
- ✓ ***Privileged User authentication;***
- ✓ ***User management;***
- ✓ ***User authentication;***
- ✓ ***Biometrics binaries generation;***
- ✓ ***Signing document;***
- ✓ ***change of TOE configuration***[5].

Application Note 6

Management of R.Privileged User and User objects shall include all events, which creates, modifies or deletes the User or R.Privileged User objects.

TOE configuration shall include all events, which creates, modifies and deletes the configuration object.

Application Note 7

The audit log for the signing operation contain the R. EmbeddedBioSignature in encrypted form.

[4] [selection, choose one of: minimum, basic, detailed, not specified]

[5] [assignment: other specifically defined auditable events]

FAU_GEN.1.2: The TSF shall record within each audit record at least the following information:

a. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b. For each audit event type, based on the auditable event definitions of the functional components included in the ST:

- ✓ ***Type of action performed (success or failure),***
- ✓ ***identity of the role which performs the operation,***
- ✓ ***logID,***
- ✓ ***operation status,***
- ✓ ***None***[6]

Application Note 8

Audit trail shall not include any data which allow to retrieve sensitive data like (biometrics binary data).

FAU_GEN.2 User identity association

FAU_GEN.2.1: For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.3.2. Cryptographic Support (FCS)

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 ***defined in Table6.3*** [7] and specified cryptographic key sizes ***defined in Table6.3*** [8] that meet the following: ***defined in Table6.3*** [9].

Table 6.3. Key Generation Table

Key generation algorithm	Key size(s)	Standard
Symmetric key generation	AES-256	[FIPS197[10]]

Application Note 9

This SFR covers the generation of encryption keys for biometric data encryption in signaturiX App and signaturiX Core.

FCS_CKM.1.1/1: The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ***defined in Table*6.4**[10] and specified cryptographic key sizes ***defined in Table* 6.4**[11] that meet the following: ***defined in Table* 6.4**[12].

Table 6.4. Key Generation Table

Key generation algorithm	Key size(s)	Standard
Symmetric key generation	AES-256	[FIPS197]

Application Note 10

This SFR covers the generation of the client and server encryption keys and client and server MAC keys for the TLS protocol (derived from the master secret).

[6] [assignment: Type of action performed (success or failure), identity of the role which performs the operation. [assignment: other audit relevant information]]
[7] [assignment: cryptographic key generation algorithm]
[8] [assignment: cryptographic key sizes]
[9] [assignment: list of standards]
[10] [assignment: cryptographic key generation algorithm]
[11] [assignment: cryptographic key sizes]
[12] [assignment: list of standards]

FCS_CKM.2 Cryptographic key distribution

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method ***defined in Table* 6.5**[13] that meets the following: ***defined in Table* 6.5**[14]**.**

Table 6.5. Key Distribution Table

Key generation algorithm	**Standard**
Key exchange of encryption keys	Conformant to [RFC8446[11]]

Application Note 11

This SFR covers the symmetric key transport protocol from signaturiX App to signaturiX Core and wrapping of AES-256 biometrics decryption key.

FCS_CKM.2.1/1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method ***defined in Table 6.6***[15] that meets the following: ***defined in Table 6.6***[16]**.**

Table 6.6. Key Distribution Table

Key generation algorithm	**Standard**
Key agreement of session	(EC) Diffie-Hellman conformant to [RFC8446]
Exchange of X509 v3 certificates	Conformant to [RFC8446] and [RFC5280 [12]]

Application Note 12

This SFR covers the key establishment of session keys and exchange of client and server X.509 v3 certificates in the TLS protocol.

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 ***Secure erasing-zeroization***[17] that meets the following: ***no standards***[18]

Application Note 13

Private keys are zeroized when they are deleted by the System Administrator. Zeroization is done by overwriting once with zeroes.

FCS_COP.1 Cryptographic operation

FCS_COP.1.1: The TSF shall perform ***the operation defined in table 6.7***[19] in accordance with a specified cryptographic algorithm ***defined in table 6.7***[20] and cryptographic key sizes ***defined in table 6.7***[21] that meet the following:***defined in table6.7***[22].

Table 6.7. Cryptographic operations for biometric data protection

Cryptographic operations	**Algorithm**	**Key size(s)**	**Standards**
Raw biometric data encryption	AES	256	[FIPS197]
Standardized biometric data encryption	AES	256	[FIPS197]

[13] [assignment: cryptographic key distribution method]
[14] [assignment: list of standards]
[15] [assignment: cryptographic key distribution method]
[16] [assignment: list of standards]
[17] [assignment: cryptographic key destruction method]
[18] [assignment: list of standards]
[19] [assignment: list of cryptographic operations]
[20] [assignment: cryptographic algorithm]
[21] [assignment: cryptographic key sizes]
[22] [assignment: list of standards]

Wrapping of data encryption key in signaturiX App	RSA	4096	PKCS#1 v2.2
Wrapping of data encryption key in signaturiX Core	RSA	4096	OAEPWITHSHA512ANDMGF1PADDING [RFC8017 [13]]

Application Note 14

This SFR covers biometric data encryption and data encryption keys wrapping in signaturiX App and signaturiX Core.

FCS_COP.1.1/1 The TSF shall perform ***the operation defined in table 6.8***[23] in accordance with a specified cryptographic algorithm ***defined in table 6.8***[24] and cryptographic key sizes ***defined in table 6.8***[25] that meet the following:***defined in table 6.8***[26].

Table 6.8. Cryptographic operations for the TLS protocol

Cryptographic operations	**Algorithm**	**Key size(s)**	**Standards**
Asymmetric encryption and decryption	RSA	4096	RSA Encryption Scheme with PKCS#1 v2.2 (RSAES-PKCS1-v2.2) conformant to [RFC8446] and [RFC8017],
Symmetric encryption and decryption	AES (GCM_mode)	128, 256	Conformant to [FIPS197] and [SP800-38A[14]]
Digital signature generation and verification	RSA	4096	RSA Signature Scheme with PKCS#1 v12.2

Application Note 15

This SFR covers cryptographic operations used by the TLS protocol.

FCS_COP.1.1/2 The TSF shall perform ***the operation defined in table 6.9***[27] in accordance with a specified cryptographic algorithm ***defined in table 6.9***[28] and cryptographic key sizes ***defined in table 6.9***[29] that meet the following:***defined in table 6.9***[30].

Table 6.9 Cryptographic signatures for REST and SOAP API

Cryptographic operations	**Algorithm**	**Key size(s)**	**Standards**
Digital signature generation and verification for REST API	RSA + SHA-256	4096	[RFC8017]
Digital signature generation and verification for SOAP API	RSA + SHA-256	4096	[RFC8017]

Application Note 16

[23] [assignment: list of cryptographic operations]
[24] [assignment: cryptographic algorithm]
[25] [assignment: cryptographic key sizes]
[26] [assignment: list of standards]
[27] [assignment: list of cryptographic operations]
[28] [assignment: cryptographic algorithm]
[29] [assignment: cryptographic key sizes]
[30] [assignment: list of standards]

This SFR covers cryptographic operations used by signing of API. The API is secured with asymmetric cryptography in such a way that requests are signed with a dedicated private key and verified with a dedicated public key (independently of the encryption provided by HTTPS).

FCS_COP.1.1/3 The TSF shall perform ***the operation defined in table 6.10***[31] in accordance with a specified cryptographic algorithm ***defined in table 6.10***[32] and cryptographic key sizes ***defined in table 6.10***[33] that meet the following: ***defined in table 6.10***[34].

Table 6.10. Cryptographic hashing

Cryptographic operations	**Algorithm**	**Key size(s)**	**Standards**
Hashing for the purpose of integrity control	SHA-256, SHA-512	256, 512	FIPS PUB 180-4

Application Note 17

This SFR covers cryptographic operations for cryptographic hashing.

FCS_RNG.1 Random number generation

FCS_RNG.1.1 The TSF shall provide a **deterministic**[35] random number generator that implements: ***unique QR/AC code for device authentication***[36].

FCS_RNG.1.2 The TSF shall provide **bits**[37] that meet ***NIST SP 800/90A***[38].

Application Note 18

This SFR covers generation of QR/AC code. The RNG/PRNG should be resistant to manipulation or analysis of its sources, or any attempts to predictably influence its states by applying checksums over the sources.

6.3.3. User Data Protection (FDP)

FDP_ACC.1/User Maintenance - Subset access control

FDP_ACC.1.1/ User Maintenance: The TSF shall enforce the ***User Maintenance SFP***[39] on:

Subjects: Privileged User

Objects: The security attributes User_Authentication_Data of User

Operations: User_Maintenance:

The Privilegded User updates the R.User_Authentication_Data of User.

The Privileged User deletes the R. User_Authentication_Data[40]***.***

FDP_ACF.1/User Maintenance - Security attribute based access control

FDP_ACF.1.1/ User Maintenance: The TSF shall enforce the ***User Maintenance SFP***[41] to objects based on the following:

1) ***Whether the subject is a Privileged User authorized to maintain the User security attributes***[42].

[31] [assignment: list of cryptographic operations]
[32] [assignment: cryptographic algorithm]
[33] [assignment: cryptographic key sizes]
[34] [assignment: list of standards]
[35] [selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic]
[36] [assignment: list of security capabilities]
[37] [selection: bits, octets of bits, numbers [assignment: format of the numbers]]
[38] [assignment: a defined quality metric]
[39] [assignment: access control SFP]
[40] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]
[41] [assignment: access control SFP]
[42] [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]

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

1) ***None***[43].

FDP_ACF.1.3/ User Maintenance : The TSF shall explicitly authorize access of subjects to objects based on the following additional rules:

1) ***None***[44].

FDP_ACF.1.4/ User Maintenance : The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

1) ***None***[45].

FDP_ACC.1/Signing - Subset access control

FDP_ACC.1.1/ Signing: The TSF shall enforce the ***Signing SFP***[46] on:

Subjects: Device

Objects: R.Document, R.EmbeddedBioSignature
R.Reference_Device_Authentication_Data

Operations: Signing:

The Device on demand the TOE to perform a signature operation containing the following steps:

The TOE verifies R. Reference_Device_Authentication_Data

The TOE gets the biometrics binaries resulting in, R.EmbeddedBioSignature

The User accepts or rejects R.EmbeddedBioSignature

The TOE deactivates the Device when the signature operation is completed[47].

FDP_ACF.1/Signing - Security attribute based access control

FDP_ACF.1.1/ Signing: The TSF shall enforce the ***Signing SFP***[48] to objects based on the following:

1) ***Whether the subject is a User authorized to create a signature***[49].

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

1) ***The R.EmbeddedBioSignature are verified that they are bound to the R.Document.***
2) ***None***[50].

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

1) ***The User shall be the owner of the Device used to generate the signature***[51].

[43] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
[44] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]
[45] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]
[46] [assignment: access control SFP]
[47] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]
[48] [assignment: access control SFP]
[49] [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]
[50] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
[51] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

FDP_ACF.1.4/ Signing: The TSF shall explicitly deny access of subjects to objects based on the following additional rule:

1) ***None***[52].

6.3.4. Identification and Authentication (FIA)

FIA_ATD.1 User attribute definition

FIA_ATD.1.1: The TSF shall maintain the following list of security attributes belonging to individual users:

a) ***user ID or name,***
b) ***security roles,***
c) ***None***[53].

FIA_ATD.1/1 User attribute definition

FIA_ATD.1.1/1: The TSF shall maintain the following list of security attributes belonging to individual users: ***the security attribute as defined in FIA_USB.1***[54].

FIA_USB.1 User-subject binding

FIA_USB.1.1: The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:

1) ***R.Reference_User_Authentication_Data***

2) ***user ID or name***
3) ***Subject identity***
4) ***Security roles***

5) ***R.User]***[55]

to User

1) ***R.Reference_Priviliged_User_Authentication_Data***

2) ***None***][56]

to Privileged User.

FIA_USB.1.2: The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:

a) The subject identity is specified as follows:
   1. the username imported into the signaturiX Core in the login list form;
b) The security roles associated with the subject shall be the roles that meet:
   1. the basic role conditions: user and group membership to roles;
   2. date and time role conditions;
   3. context TOE.

c) :*None*[57].

FIA_USB.1.3: The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users:

1) ***Whether the subject is a Privileged User authorized to modify an User object.***

2) ***None***[58].

[52] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]
[53] [assignment: list of security attributes]
[54] [assignment: list of security attributes]
[55] [assignment: list of user security attributes]
[56] [assignment: list of user security attributes]
[57] [assignment: rules for the initial association of attributes [assignment: rules for the initial association of attributes]]
[58] [assignment: rules for the changing of attributes [assignment: rules for the changing of attributes]]

6.3.5. Security Management (FMT)

FMT_SMR.2 Restrictions on security roles

FMT_SMR.2.1: The TSF shall maintain the roles ***User and Privileged User***[59].

FMT_SMR.2.2: The TSF shall be able to associate users with roles.

FMT_SMR.2.3: The TSF shall ensure that the conditions ***User can’t be a Privileged User***[60] are satisfied.

6.3.6. TSF physical protection (FPT)

FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from **disclosure**[61] when it is transmitted between separate parts of the TOE.

Application Note 19

It is necessary to satisfy this objective because it ensures that TSF data is protected when it is transmitted between components of the TOE. The communication between the App on the tablet and the Core on the server is encrypted to prevent the disclosure of information. This data would include the biometric data as it leaves the capture device, or as it is transmitted between other parts of the TOE.

FPT_ITT.1/1 Basic internal TSF data transfer protection

FPT_ITT.1.1/1 The TSF shall protect TSF data from **modification**[62] when it is transmitted between separate parts of the TOE.

Application Note 20

TOE ensures the integrity of the TSF data when it is transmitted between various parts of the TOE. Ensuring the integrity of the TSF data is crucial in order to ensure the TSF can enforce its security policies.

FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

Application Note 21

It is ensured by operating system on the server that it synchronizes its system clock with trusted NTP server. The TOE trusts the hosts system time, but also compares the system time with trusted NTP server (in configured regular intervals) to check it. This time stamp source is required for audit purposes.

6.3.7. TOE Access (FTA)

FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after a time configured by the **R.Privileged_User** in system parameters[63].

Application Note 22

The TOE should provide an ability to terminate a session of a specified user after defined period .

6.3.8. Trusted Paths/Channels (FTP)

FTP_ITC.1 - Inter-TSF trusted channel

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

[59] [assignment: authorized identified roles]

[60] [assignment: conditions for the different roles]

[61] [selection: *disclosure, modification*]

[62] [selection: *disclosure, modification*]

[63] [assignment: time interval of user inactivity]

FTP_ITC.1.2: The TSF shall permit the **another trusted IT product**[64], to initiate communication via the trusted channel.

FTP_ITC.1.3: The TSF shall initiate communication via the trusted channel for ***communication with trusted service providers (Certum Simplysign)*** [65].

6.4. Security Assurance Requirements

The security assurance requirement level is EAL2. The assurance components are identified in the table below.

Assurance Class	Assurance Components
Development (ADV)	Security architecture description (ADV_ARC.1)
	Security-enforcing functional specification (ADV_FSP.2)
	Basic design (ADV_TDS.1)
Guidance documents (AGD)	Operational user guidance (AGD_OPE.1)
	Preparative procedures (AGD_PRE.1)
Life-cycle support (ALC)	Use of a CM system (ALC_CMC.2)
	Parts of the TOE CM coverage (ALC_CMS.2)
	Delivery procedures (ALC_DEL.1)
Security Target evaluation (ASE)	Conformance claims (ASE_CCL.1)
	Extended components definition (ASE_ECD.1)
	ST introduction (ASE_INT.1)
	Security objectives (ASE_OBJ.2)
	Derived security requirements (ASE_REQ.2)
	Security problem definition (ASE_SPD.1)
	TOE summary specification (ASE_TSS.1)
Tests (ATE)	Analysis of coverage (ATE_COV.2)
	Functional testing (ATE_FUN.1)
	Independent testing - sample (ATE_IND.2)
Vulnerability assessment (AVA)	Vulnerability analysis (AVA_VAN.2)

Table 6.11. Security Assurance Requirements

[64] [selection: the TSF, another trusted IT product]

[65] [assignment: list of functions for which a trusted channel is required]

7. Rationale

7.1. Security Requirements Rationale - Coverage

The following table is used to demonstrate that every SFR is used to cover an objective and that every objective is covered by an SFR

	OT. USER_MANAGEMENT	OT. BIOSIGNATURE_INTEGRITY_CONFIDENTIALITY	OT.SELF_PROTECTION	OT.ROBUST_TOE_ACCESS	OT.IDENTIFICATION_AUTHENTICATION	OT.SECURE_CHANNEL	OT.INTEGRITY	OT.CRYPTOGRAPHIC_FUNCTIONS	OT.MANAGE	OT.AUDIT
Security Audit										
FAU_GEN.1							X			X
FAU_GEN.2										X
Cryptographic Support										
FCS_CKM.1						X				
FCS_CKM.1/1								X		
FCS_CKM.2						X				
FCS_CKM.2/1								X		
FCS_CKM.4								X		
FCS_COP.1		X						X		
FCS_COP.1/1						X	X	X		
FCS_COP.1/2							X	X		
FCS_COP.1/3						X	X	X		
FCS_RNG.1								X		
User Data Protection										
FDP_ACC.1/ User Maintenance	X									
FDP_ACF.1/ User Maintenance	X									
FDP_ACC.1/ Signing		X								
FDP_ACF.1/ Signing		X								
Identification & Authentication										
FIA_ATD.1				X						
FIA_ATD.1/1					X					
FIA_USB.1					X					
Security Management										

FMT_SMR.2									X	X
Protection of the TSF										
FPT_ITT.1			X							
FPT_ITT.1/1							X			
FPT_STM.1										X
TOE access										
FTA_SSL.3				X						
Trusted Path/Channels										
FTP_ITC.1						X				

Table 7.1. Security requirement coverage

7.1.1. Rationale

OT.USER_MANAGEMENT is handled by the requirements for access control in FDP_ACC.1/ User Maintenance and FDP_ACF.1/ User Maintenance.

OT. BIOSIGNATURE_INTEGRITY_CONFIDENTIALITY is handled by FCS_COP.1, which describes requirements on the algorithms. The FDP_ACC.1/Signing and FDP_ACF.1/Signing ensures access control for the BioSignature operation.

OT.SELF_PROTECTION is handled by FPT_ITT.1 which ensure that the TSF data that is transmitted between components of the TOE is encrypted.

OT.ROBUST_TOE_ACCESS is handled by FIA_ATD.1 which ensures that users are authenticated, including administrative if appropriate. The FTA_SSL.3 is limited to the exposure of an administrative session that is inactive for whatever reason.

OT.IDENTIFICATION_AUTHENTICATION is handled by FIA_ATD.1/1 and FIA_USB.1 which ensure that only identified and authenticated users gain access to protected resources.

OT.SECURE_CHANNEL is handled by FTP_ITC.1and FCS_COP.1/1, which ensure that the TOE provides trusted channels via the TLS protocol. The FCS_COP.1/3 provides a trusted channel for REST and SOAP. The FCS_CKM.1 and FCS_CKM.2 defines the generation of cryptographic keys and how this keys and digital certificates are exchanged between the separated TOE components.

OT.INTEGRITY is handled by FPT_ITT.1/1, FCS_COP.1/1, FCS_COP.1/2, FCS_COP.1/3 which ensure the integrity of TOE. The TOE must implement mechanisms to ensure the integrity of software, plug-ins and extensions, and to ensure that they come from legitimate sources. The FAU.GEN.1 requires to save the all modifications to the audit configuration that occur while the audit collection functions are operating.

OT.CRYPTOGRAPHY_FUNCTION is handled by FCS_COP.1, FCS_COP.1/1, FCS_COP.1/2 and FCS_COP.1/3 provide cryptographic functionality that is used by the TOE. The core functionality to be supported is encryption/decryption using a symmetric algorithm, and digital signature generation and verification using asymmetric algorithms. Since these operations involve cryptographic keys, how the keys are generated and/or otherwise obtained have to also be specified. The FCS_CKM.1/1 and FCS_CKM.2/1 requires that the TSF validate all keys generated to assure that meet relevant standards. The FCS_CKM.4 require that the TSF zeroises keys to be destroyed. The FCS_RNG.1 requires that any random number generation is compliant with NIST SP 800-90A ..

OT.MANAGE is handled by FMT_SMR.2, which describes access control rules for managing TSF dat~~a~~.

OT.AUDIT is handled by the requirements for audit record generation FAU_GEN.1 and FAU_GEN.2 using reliable time stamps in FPT_STM.1 & FMT_SMR.2. It describes the users roles and associate users with roles.

7.2. SFR Dependencies

7.2.1. General

The dependencies between SFRs are addressed as shown in Table 7.2.

Requirement	Dependencies	Fulfilled by	Unfulfilled by
FAU_GEN.1	FPT_STM.1	FPT_STM.1	
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1	FIA_UID.1: User is identified outside the TOE.
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_CKM.2 FCS_CKM.4	
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1	
FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1	
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1 FCS_CKM.4	
FCS_RNG.1	None		
FDP_ACC.1/User Maintenance	FDP_ACF.1	FDP_ACF.1/User Maintenance	
FDP_ACC.1/Signing	FDP_ACF.1	FDP_ACF.1/Signing	
FDP_ACF.1/User Maintenance	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/User Maintenance	FMT_MSA.3 The TOE only checks that the user is in the login list and cannot change it. Any change requires a reinitialisation of the TOE
FDP_ACF.1/Signing	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Signing	FMT_MSA.3 The TOE only checks that the user is in the login list and cannot change it. Any change requires a reinitialisation of the TOE
FIA_ATD.1	None		
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	
FMT_SMR.2	FIA_UID.1		FIA_UID.1 User is identified outside the TOE.
FPT_ITT.1	None		

Requirement	Dependencies	Fulfilled by	Unfulfilled by
FPT_ITC.1	None		

Table 7.2. Dependencies`

7.3. Rationales for SARs

EAL2 permits a developer to gain assurance from positive security engineering based on good commercial development practises which, through rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL2 is the level at which it is likely to be economically feasible to retrofit to an existing product line.

8. TOE Summary Specification

The TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. **Table 8.1 Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	Security Audit	**Cryptographic Support**	**User Data Protection**	**Identification & Authenticatio**	**Security Management**	**Protection of the TSF**	**TOE Access**	**Trusted Path/Channels**
FAU_GEN.1	X							
FAU_GEN.2	X							
FCS_CKM.1		X						
FCS_CKM.4		X						
FCS_CKM.2		X						
FCS_COP.1		X						
FCS_RNG.1		X						
FDP_ACC.1/ User Maintenance			X					
FDP_ACF.1/ User Maintenance			X					
FDP_ACC.1/ Signing			X					
FDP_ACF.1/ Signing			X					
FIA_ATD.1				X				
FIA_USB.1				X				
FMT_SMR.2					X			
FPT_ITT.1						X		
FPT_STM.1						X		
FTA_SSL.3							X	
FTP_ITC.1								X

Table 8.1 Security Functions vs. Requirements Mapping

8.1. TOE Security Functions

8.1.1. Security Audit (FAU)

The TOE logs all security events. The Security relevant events are all changes to the system that may impact the overall system security and include all operations invoked through the Privileged User and User.

Each log entry contains the date and time of the event (using a reliable timestamp), the type of event, the identity of the entity that initiated the event. Log entries are associated with the user (R.Privileged_User or R.User) that caused the event and the outcome (success or failure) of the event.

The resulting audit records are securely stored in an external database and are protected from modification.

The security functionality described above meets the requirements:

- FAU_GEN.1 & FAU_GEN.2

8.1.2. Cryptographic Support (FCS)

The used cryptographic mechanism ensure the quality of the generated and distributed keys, which are invoked by the TOE with appropriate parameters such as key type and size.

- the generation of encryption keys (AES-256) are used for:
  - ➢ biometric data encryption in signaturiX App and signaturiX Core and ,
  - ➢ client and server encryption keys and client and server MAC keys for the TLS protocol (derived from the master secret).
- the distribution of encryption keys are used for:
  - ➢ transport protocol from signaturiX App to signaturiX Core and wrapping of AES-256 biometrics decryption key;
  - ➢ establish of session keys and exchange of client and server X.509 v3 certificates in the TLS protocol.
- When the cryptographic keys are no longer used, they are destroyed by the zeroising.

The security functionality described above meets the requirements:

- FCS_CKM.1 & FCS_CKM.2 & FCS_CKM.4

Several validated versions of the hash and encoding functions are available for:

- the generation of biometric data encryption and data encryption keys wrapping in signaturiX App and signaturiX Core, and,
- the generation of digital signatures and verification used by the TLS protocol
- digital signatures and verification of API requests

The security functionality described above meets the requirements:

- ▪ FCS_COP.1

Additionally, the TOE is extended with RNG/PRNG (random Number Generation/ pseudorandom number generation) seeded by one or more independent software-based entropy sources.

The security functionality described above meets the requirements:

- ▪ FCS_RNG.1

8.1.3. User Data Protection (FDP)

8.1.3.1. Access Control

a) User Maintenance

The User maintenance is handled by the Privileged User. The Privileged User before it handles any task related to the User's maintenance (e.g., the task of modifying the security attributes of the R. User according to R. Reference_User_Authentication_Data) must first be authenticated.

The security functionality described above meets the requirements:

- ▪ FDP_ACC.1/User Maintenance & FDP_ACF.1/User Maintenance

b) BioSigning

In order to BioSign the document(s), the BioSigning operation must be authorized. Authorisation is handled by the TOE after the BioSigner scans the QR code or input AC code via the Tablet keyboard. Then credentials present in QR/ACcode is used to display the document /Documents to Biosigner on the Tablet. The BioSigner uses S Pen to place a handwritten signature, thus creating 'primary biometric data' in a format appropriate for the biometric sampling device used.

Where the all biosignature operations are verified and accepted by the TOE (see 1.4) the user approves the signed document(s) on the Tablet and logged out of the TOE.

The security functionality described above meets the requirements:

- FDP_ACC.1/signing & FDP_ACF.1/ Signing

8.1.4. Identification and authentication (FIA)

8.1.4.1. User security attribute

The TOE maintains User security attributes. The User security attributes are associated with the following objects (R.Reference_User_Authentication_Data and User).

The Environmant maintains Privileged User security attributes associated with the following objects (R.Reference_Priviliged_User_Authentication_Data and R. Priviled User).

The TOE requires Privileged User to be the only user can modifying the User security attributes and if necessary its attributes.

The security functionality described above meets the requirements:

- FIA_ATD.1 & FIA_USB.1

8.1.5. Security Management (FMT)

8.1.5.4. Management, specification and restrictions on security data

Any request to manage Users, etc. can only be executed by an authorised User and is logged by audit.

The security functionality described above meets the requirements:

- FMT_SMR.2

8.1.6. TSF Physical Protection (FPT)

8.1.6.1 Basic internal TSF data transfer protection

The data transmitted between separate parts of the TOE is protected from modification and disclosure. The communication between the App on the tablet and the signaturiX Core on the server is encrypted. This data would include the biometric data as it leaves the capture device, or as it is transmitted between other parts of the TOE. This would also include any configuration data "TSF DATA" that is sent from an administrative application to the TOE. It occurs only during initialization of TOE.

The security functionality described above meets the requirements:

- FPT_ITT.1

8.1.6.2. Reliable time stamps

The TOE is synchronized with a reliable timestamp (the time synchronisation is based on the server internal clock and NTP protocol). If the TOE detects a time deviation, it automatically notifies the System Administrator or logs the event and suspends its operations.

The security functionality described above meets the requirements:

- FPT_STM.1

8.1.7. TOE ACCESS (FTA)

8.1.7.1. TSF-initiated termination

TOE limit the exposure of an administrative session that is inactive for whatever reason. If an administrative session becomes inactive for a System Administrator defined period, the session is terminated. This requirement applies both to remote and direct connections to the TOE.

The security functionality described above meets the requirements:

- FTA_SSL.3

8.1.8. Trusted Paths/Channels (FTP)

8.1.8.1. Inter-TSF trusted channel

The TOE provides trusted communication channel between itself and another trusted IT product, which is logically separated from other communication channels and provides authentication of its endpoints and protection of the transmitted data from modification or disclosure. The TOE permit another trusted IT product to initiate communication via the trusted channel for communication with application clients and external LDAP servers (qualified timestamp and qualified seal).

The security functionality described above meets the requirements:

- FTP_ITC.1

Bibliography

1. ETSI EN 319 142-1 V1.1.1 Electronic Signatures and Infrastructures (ESI), PAdES digital signatures, Part 1: Building blocks and PAdES baseline signatures
2. https:// developer.android.com/reference/java/security/SecureRandom
3. https:// csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3900
4. https:// csrc.nist.gov/publications/detail/fips/140/2/final
5. SP 800-90A Rev. 1: Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015
6. ISO/IEC 19794-7:2014 Information technology — Biometric data interchange formats — Part 7: Signature/sign time series data
7. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017
8. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
9. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017
10. FIPS197 - Specification for the ADVANCED ENCRYPTION STANDARD (AES). http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, 2001
11. E. Rescorla: The Transport Layer Security (TLS) Protocol Version 1.3. - RFC8446, http://www.ietf.org/rfc/rfc8446.txt, 2018
12. D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC5280, http://www.ietf.org/rfc/rfc5280.txt, 2008
13. K. Moriarty B. Kaliski,. J. Jonsson, A. Rusch: Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.2. RFC8017, http://www.ietf.org/rfc/rfc8017.txt, 2016
14. SP800-38A - Recommendation for Block Cipher Modes of Operation: Methods and Techniques. Version NIST Special Publication 800-38A 2001 Edition, http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf
15. Common Methodology for Information Technology Security Evaluation, Evaluation methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017

Andrzej Ruciński
2025.10.07
14:08:10 +02'00'