Certification Dossier Code:	2021-5
Certification Report Creation Date:	19th February 2024
Certification Report Code:	2021-5-REP-69 (internal) 2021-5-REP-84 (public)
NASK RWA code:	OSiC.8711.10.2021

Certification Report

[2021-5] Certification Report on biocertiX EAL2

COMMON CRITERIA

CERTIFICATE

Certification Identification: **2021-5** | Type of Product: **Products for Digital Signatures**

Product Name and Version: **biocertiX – handwritten biometric signatures on PDF documents, version 1.1**

Target of Evaluation:

biocertiX – handwritten biometric signatures on PDF documents, version 1.1

Certificate holder/Manufacturer: **Asseco Data Systems S.A., Jana z Kolna 11, 80-864 Gdańsk, Poland**
Assurance Package: **EAL 2**

TOE developers:

Asseco Data Systems S.A., Jana z Kolna 11, 80-864 Gdańsk, Poland
Xtension Sp. z o.o., Opacka 12, 80-338 Gdańsk, Poland
Samsung Electronics Polska Sp. z o.o., Postępu 14, 02-676 Warsaw, Poland

Name of Certification Body:

NASK National Research Institute, Standardisation and Certification Centre, 12 Kolska, Warsaw, 01-045, Poland

Certification Report Identifier: **2021-5-REP-69**

The IT Product identified in this certificate has been evaluated at an Evaluation Facility accredited and approved under the rules of the Polish IT Security Evaluation and Certification Scheme (PC1) using the Common Methodology for IT Security Evaluation, April 2017 Revision 5, for conformance to the Common Criteria for IT Security Evaluation, April 2017 Revision 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and conjunction with the complete Certification Report. The evaluation has been conducted following the provisions of the IT Security Evaluation and Certification Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT Product by the NASK National Research Institute or any other organisation that recognises or gives effect to this certificate. No warranty of the IT Product by NASK National Research Institute or any other organisation that recognises or gives effect to this certificate is expressed or implied. The validity of the certificate may change over time. For information regarding the current status of the certificate, please contact NASK National Research Institute (Certification Body) or look at the NASK's website.

NASK

PCA Polskie Centrum Akredytacji – Certyfikacja Wyrobów

AC 223

Certificate Identifier: 1/PC1/AC223/2024

Certificate decision date: 29.02.2024

Certificate expiry date: 28.02.2029

Paweł Krzysztof Kostkiewicz 2024.04.30 12:21:09 +02'00'

NASK National Research Institute
Certification Body Manager

NASK

Table of content

1. **Introduction** **3**
2. **Certification overview** **3**

Recognition of the certificate 4

European Recognition of CC Certificates (SOGIS-MRA) 4

International Recognition of CC Certificates (CCRA) 4

Executive Summary 4

Documentation available for users 5

Security Target 5

3. **TOE Summary** **6**

TOE Overview 6

Security Assurance Requirements 7

Security Functional Requirements 8

Security Policy 9

4. **Assumptions and Clarification of Scope** **9**

Usage Assumptions 9

Environmental Assumptions 10

Clarification of Scope 11

Threats 11

OSPs 12

5. **Architectural Information** **12**

Physical scope 12

Logical scope 14

6. **Product Documentation** **15**

Security Target 15

7. **IT security evaluation** **16**

Evaluated Configuration 16

Functional testing 18

Developer testing 18

Evaluator testing 19

Penetration testing 19

Evaluation verdicts 20

Evaluator Comments/Recommendations 21

8. **Certifier Recommendations** **22**
9. **Acronyms** **22**
10. **Bibliography** **23**

References 24

List of related documents 25

1. Introduction

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been tested at an approved Laboratory (IT Security Evaluation Facility) – on the basis of the IT Security Evaluation and Certification Scheme – using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5. This certification report, and its associated certificate, applies only to the identified version and release of the product in its tested and evaluated configuration. The evaluation has been conducted in accordance with the provisions of the IT Security Evaluation and Certification Scheme - PC1, and the conclusions of the Laboratory in the technical evaluation report are consistent with the evidence. This report, and its associated certificate, are not an endorsement of the IT product by the NASK National Research Institute, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the NASK National Research Institute, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied. This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration.

2. Certification overview

The NASK's "IT Security Evaluation and Certification Scheme" provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by an approved Laboratory under the oversight of the Certification Body, which is managed by the NASK National Research Institute. Laboratory is a commercial facility that has been approved by the Certification Body to perform Common Criteria based cybersecurity evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025:2018- The General Requirements for the Competence of Testing and Calibration Laboratories. By awarding a Common Criteria certificate, the Certification Body asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. **The consumer of certified IT products should review the Security Target, in addition to this Certification Report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the Laboratory**. The Certification Report, Product Certificate and Security Target are posted to the Certified Products List for the IT Security Evaluation and Certification Scheme published by NASK National Research Institute.

NASK

Recognition of the certificate

European Recognition of CC Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA, version 3) became effective in April 2010. It defines the recognition of certificates for IT-Products up to EAL4. A higher recognition levels are provided for IT-Products related to certain SOGIS Technical Domains only.
The current list of signatory nations and approved certification schemes can be found on https://www.sogis.eu/.
The SOGIS-MRA logo printed on the certificate indicates that it is recognized under the terms of this agreement by signatory nations. This certificate is recognized under SOGIS-MRA for all assurance components selected.

International Recognition of CC Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the Common Criteria (Common Criteria Recognition Arrangement, CCRA) became effective in September 2014. It covers Common Criteria certificates based on: collaborative Protection Profiles, assurance components up to EAL2 augmented by ALC_FLR and certificates for PP and cPP.
The current list of signatory nations and of collaborative Protection Profiles can be found on https://www.commoncriteriaportal.org .
The CCRA logo printed on the certificate indicates that it is recognized under the terms of this agreement by signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition. This certificate is recognized under CCRA for all assurance components selected.

Executive Summary

This document constitutes the Certification Report for the certification file of the product:
biocertiX - handwritten biometric signatures on PDF documents

TOE Version:	1.1
Developer:	Asseco Data Systems S.A. Xtension Sp. z o.o. Samsung Electronics Polska Sp. z o.o.
Sponsor:	Asseco Data Systems S.A.
Security Target:	SECURITY TARGET FOR biocertiX, version 2.3-lite, date of issue 2023-09-25
Protection Profile:	None
Laboratory/ITSEF:	Information Technology Security Evaluation Facility of National Institute of Telecommunications - ITSEF NIT
Evaluation Level:	Common Criteria version 3.1 release 5, Evaluation Assurance Level EAL 2
Evaluation end date:	October 2023 (Final ETR ver.1.2, issue date 09.02.2024)
Expiration Date:	28/02/2029

All the assurance components required by the evaluation level EAL 2 of Common Criteria standard have been assigned a "PASS" verdict. Consequently, the laboratory ITSEF NIT assigned the "PASS" VERDICT to the whole evaluation due all the Evaluator actions are satisfied for the EAL 2, as defined by the Common Criteria v3.1 Revision 5 and the CEM v3.1 Revision 5. Considering the obtained evidences during the process of the certification of the biocertiX - handwritten biometric signatures on PDF documents , a positive resolution by Certification Body is proposed.

Documentation available for users

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version:

[EXT-1159] [EVD-ST-V2.3]	**Security Target for biocertiX - handwritten biometric signatures on PDF documents version 1.1, v.2.3, issue date 25.09.2023 (confidential document – LITE version available)**
[EXT-1111] [EVD-AGD_PRE-V0.97]	**AGD_ PRE EAL2 for biocertix, version 0.97, issue date 25.09.2023 (confidential document)**
[EXT-1140] [EVD-AGD_OPE-V1.0]	**AGD_OPE EAL2 for biocertiX, v.1.0, issue date 25.09.2023 (confidential document)**

Security Target

Along with this certification report, the complete Security Target of the evaluation is stored and protected in the Certification Body premises. This document is identified as:

SECURITY TARGET FOR biocertiX, version 2.3, date of issue 2023-09-25.

The public version of this document is the same as complete Security Target described above and it is published along with this certification report on the Certification Body website.

3. TOE Summary

TOE Overview

The Target of Evaluation (TOE) is the biocertiX that 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 Software and biocertiX App accordingly) for signing PDF documents.

The 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.

Usage of the biocertiX, which is the Target of Evaluation (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) Binding of seal and time-stamp with PDF document with embedded encrypted biometric data (the actual seal and time-stamp is prepared in Simply Sign outside of the TOE),
5) A biometrically signed document is securely made available for download by the ES.

The TOE consists of the following elements (see Table 1 section 1.5.1. in [EVD-ST-V2.3]):

- ***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, [EVD-ST-V2.3].

- ***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).

Security Assurance Requirements

The product was evaluated with all the evidence required to fulfil the evaluation level EAL 2, according to Common Criteria v3.1 Revision 5.

Assurance Class	Assurance Component
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims

Assurance Class	Assurance Component
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

Security Functional Requirements

Functional requirement	Description
FAU: Security audit	FAU_GEN.1 Audit data generation
FCS: Cryptographic support	FCS_COP.1 Cryptographic operation
	FCS_CKM.1Cryptographic key generation
	FCS_CKM.2 Cryptographic key distribution
	FCS_CKM.4 Cryptographic key destruction
	FCS_RNG.1 Random number generation
FDP: User Data Protection	FDP_ACC.1 Subset access control
	FDP_ACF.1 Security attribute based access control
FIA: Identification and authentication	FIA_ATD.1 User attribute definition
	FIA_UAU.2 User authentication before any action
	FIA_UAU.5 Multiple authentication mechanisms
	FIA_UID.2 User identification before any action
	FIA_USB.1 User-subject binding
FMT: Security management	FMT_SMF.1 Specification of Management Functions
	FMT_MSA.1 Management of security attributes
	FMT_MSA.3 Static attribute initialisation
	FMT_SMR.2 Restrictions on security roles
FPT: Protection of the TSF	FPT_ITT.1 Basic internal TSF data transfer protection
	FPT_STM.1 Reliable time stamps
	FPT_TST.1 TSF testing
FTA: TOE access	FTA_SSL.3 TSF-initiated termination
FTP: Trusted path/channels	FTP_ITC.1 Inter-TSF trusted channel

Identification

Product:	biocertiX - handwritten biometric signatures on PDF documents, version 1.1
Security Target:	SECURITY TARGET FOR biocertiX, version 2.3, issue date 2023-09-25

Security Policy

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 (S.User, S.Privileged_Users) shall be held accountable for security-relevant actions within the system.

OSP.CRYPTOGRAPHY

Approved cryptographic functions shall be used to perform cryptographic operations (e.g. meeting the FIPS or SOGIS requirements when appropriate).

4. Assumptions and Clarification of Scope

The assumptions are constraints to the conditions used to assure the security properties and functionalities introduced by the Security Target. All assumptions are to be taken into consideration when calculating the attack potential and affect the vulnerability of the product (mostly in terms of reduction). In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its usage and operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE. These assumptions have been applied during the evaluation to determine if the identified vulnerabilities can be exploited.

Usage Assumptions

The Security Target [EVD-ST-V2.3] contains five assumptions related to the usage of the TOE.

A.PRIVILEGED_USER: It is assumed that all personnel administering the TOE (S.Privileged_Users) 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 S.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 S.User and S.BioSigner to interact with TOE is under the S.User control for the signature operation, e.g. protected against malicious code, protected against physical interception by unauthorized entities. It is assumed that the process of initialization and management of keys and certificates (public key involved in encrypting the biometric data in biocertiX App and certificates for TLS) used by biocertiX App are secure (Knox). It is assumed that the TLS keys (in volatile memory) are secured and protected against any unauthorised access,

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

Environmental Assumptions

The assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the Security Target. These assumptions have been applied during the evaluation to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

The Security Target [EVD-ST-V2.3] makes five assumptions on the operational environment of the TOE:

A.ACCESS_PROTECTED: It is assumed that the signaturiX Core part of the TOE operates in a protected environment. Only S.Privileged_Users have access to TOE. The TOE software and hardware environment is installed, configured and managed by S.Privileged_Users in a secure state that mitigates against the specific risks applicable to the deployment environment. It is assumed that the TLS keys (in volatile memory of biocertiX server) are secured and protected against any unauthorised access,

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

A.EXTERNAL_SYSTEM: It is assumed that each S.User has to be authenticated in S.ES before using the biocertiX system and it is assumed that the S.ES provides TLS 1.3 for communication with the TOE.

A.TRUSTED_PKI: It is assumed that TTP (Certum SimplySign) service providers that exchange data with the TOE are trusted. It is assumed that Certum SimplySign supports and enforces at least one the following TLS cipher suites for all communication with the TOE:

TLS 1.3 suites:	TLS_AES_128_GCM_SHA256,
	TLS_AES_256_GCM_SHA384TLS_CHACHA20_POLY1305_SHA256.
TLS 1.2 suites:	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384.

Application note: *In SOGIS-ACM [9], algorithms such as CHACHA20 and POLY1305 have not been defined as either recommended or legacy. However, following the recommendation in section 9.1 Mandatory-to-Implement Cipher Suites of RCF8446 [10] the cipher suite TLS_CHACHA20_POLY1305_SHA256 has been implemented as part of the TLS 1.3 support.*

Clarification of Scope

Threats

The Security Target [EVD-ST-V2.3] defines eight threats which have been taken into consideration during the evaluation process.

T.BIOSIGNER_IMPERSONATION: S.Attacker impersonates a S.BioSigner and binds R.EmbeddedBioSignature created by the S.BioSigner with R.Document unaccepted by S.BioSigner. The assets R.Document and R.EmbeddedBioSignature are threatened.

This threat covers the following attacks:

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

T. USER_IMPERSONATION:

A S.Attacker impersonates S.User. As examples, it could be:

- by transferring wrong R.Reference_User_Authentication_Data to TOE from S.ES.

The assets R.Reference_User_Authentication_Data are threatened

T.EXCESS_AUTHORITY: A S.Attacker may be able to exercise S.Privileged_User authorities to inappropriately manage the TOE. The assets R.Privileged_User, R.Reference_Privileged_User_Authentication_Data and R.TSF_Data are threatened.

T.TSF_COMPROMISE: S.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: A S.Attacker may gain access to R.TSF_Data and/or user data for which they are not authorized. All the assets are threatened.

T.UNDETECTED_ACTIONS: A S.Attacker may gain unauthorised access to an unattended S.Privileged_User session, or is positioned on a communication channel or elsewhere in the network infrastructure, causing altered communication between the application software and other endpoints to compromise it. All the assets are threatened.

T.AUDIT: A S.Attacker may be able to cause the lost, destruction of R.Audit or may be able to tamper R.Audit or eavesdrop on R.Audit. The asset R.Audit is threatened.

T.CRYPTO: A S.Attacker can exploit weakness of crypto considering parameters values and known cryptanalysis attacks, thus compromise the cryptographic mechanisms and the data protected by those mechanism. All the assets requiring integrity and/or confidentiality and/or authenticity protection are threatened.

OSPs

Additionally, The Security Target contains two Organisational Security Policies (OSPs),

OSP.ACCOUNTABILITY

The users of the TOE (S.User, S.Privileged_Users) shall be held accountable for security-relevant actions within the system.

OSP.CRYPTOGRAPHY

Approved cryptographic functions shall be used to perform cryptographic operations (e.g. meeting the FIPS or SOGIS requirements when appropriate).

5. Architectural Information

Physical scope

The TOE consists of the following elements (see Table 1 section 1.5.1. in [EVD-ST-V2.3]):

- 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, [EVD-ST-V2.3].

- 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

biocertiX Software elements	**Version**
signaturiX Core	2.5.2
Document database	2.1
Database (licenses and configuration)	12.10
signaturiX Admin	2.5.2
biocertiX Application	**Version**
biocertiX App	1.008
Guidance documentation	**Version**
AGD_PRE	0.97
AGD_OPE	1.0

- The biocertiX Software is delivered in a tamper-protected file. Specifically, the biocertiX Software along with the guidance documentation and non-TOE elements defined in section 1.5.1.1. are placed in a zip-archive protected by SHA512 digest/hash. Link to this archive 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.

Logical scope

The logical scheme of the biocertiX is presented in Figure 1.

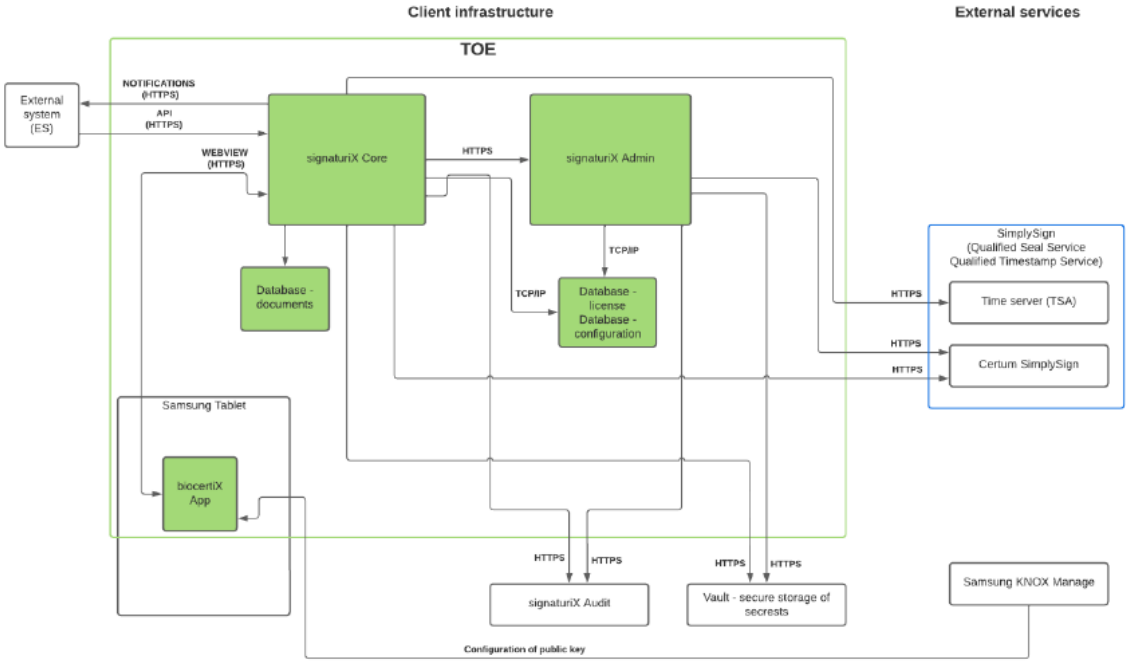

Figure 1: biocertiX – Secure Biosignature System

The biocertiX is a combination of web and mobile applications (biocertiX Software and biocertiX App accordingly) for signing PDF documents (Figure 1). The 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 [5, 6, 7]

with hardware enhanced entropy provided by Samsung technology that complies with the statistical random number generator tests specified in NIST SP 800-90A [8]. 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].

6. Product Documentation

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version:

1. [EXT-1159] [EVD-ST-V2.3]	Security Target for biocertiX - handwritten biometric signatures on PDF documents version 1.1, v.2.3, issue date 25.09.2023 (confidential document - LITE version available)
2. [EXT-1111] [EVD-AGD_PRE-V0.97]	AGD_ PRE EAL2 for biocertix, version 0.97, issue date 25.09.2023 (confidential document)
3. [EXT-1140] [EVD-AGD_OPE-V1.0]	AGD_OPE EAL2 for biocertiX, v.1.0, issue date 25.09.2023 (confidential document)

Security Target

Along with this Certification Report, the complete Security Target of the evaluation is stored and protected in the Certification Body premises. This document is identified as: **SECURITY TARGET FOR biocertiX, version 2.3, date of issue 2023-09-25.**

The public version of this document is a sanitized[2] subversion of complete Security Target described above and it is published along with this Certification Report on the Certification Body website.

[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] To protect the vendor's proprietary information.

7. IT security evaluation

The Evaluation Assurance Level EAL 2 requires the independent testing provided by Evaluator.

The Evaluator has performed an installation and configuration of the TOEs and their operational environment following the steps included in the installation and operation manual. The TOE configuration used to execute the independent tests is consistent with the evaluated configuration according to Security Target.

The main objective of the tests performed by the Evaluator was to check that the security functional requirements are implemented as expected and that the TSFIs definitions are consistent with the TOE. The Evaluator's independent test plan was SFR oriented, and the functionality of each SFR included at the Security Target has been considered. The independent tests plan covered the whole TOE functionality: all the SFRs have been tested through their TSFIs.

Evaluated Configuration

The test environment consists of following components:

a) Physical test server (IBM x3550 M4) with Debian 10 OS running on it, VirtualBox 6.1 hypervisor for server virtualization and tools required for communication: bind9 (DNS server for resolving domain names in local network) and smtp4dev (SMTP Server for development environment). Virtualized servers including the following vm instances: TOE (signaturiX Core and signaturiX Admin), External System running on Debian 10, signaturiX Audit running on Debian 10. All vm instances are running Debian 10 under control of the VirtualBox 6.1 hypervisor as indicated above,

b) Tablet Samsung Galaxy Tab Active 3 with installed biocertiX App,

c) Test workstation (Dell Latitude running Windows10 Pro 64bit) with installed tools required for the repeated and independent test, specifically including:

- Postman v10.14.6,
- Soap UI v5.7.0, and
- Wireshark v4.0.5.

The test workstation has installed WSL with the Ubuntu 20.04 LTS operating system and following tools required to execute tests:

- sslscan (2.0.16-static), tool for testing enabled services to discover supported cipher suites (accessible at: https://github.com/rbsec/sslscan)
- curl (curl 7.68.0), a command-line tool for retrieving or sending data using URL syntax.

d) network infrastructure encompassing: wireless router (for connecting tablet and test workstation to local network) and the lab switch connected to the lab network infrastructure.

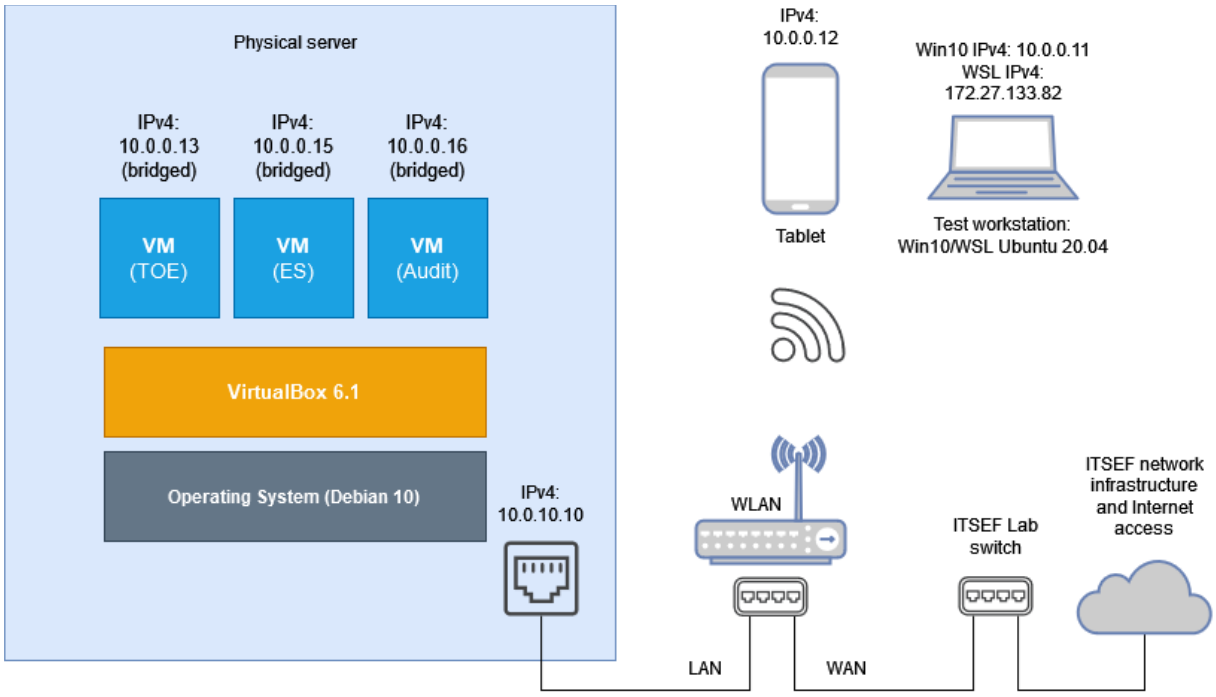

Figure 2. Test environment

The TOE (encompassing virtual machine with the signaturiX Core instance and the biocertiX App on the tablet) is run the local network as shown in the Figure 2. In the same local network are run non-TOE components encompassing instances of External System (ES) and signaturiX Audit. The test workstation is also connected to the same local network.

Network interfaces of: vm-s, server, tablet and test workstation have assigned addresses from the same subnetwork 10.0.0.0/16. Domain name resolution in the local network is performed using the bind9 service running on the test server.

Machines in test environment have assigned following IP addresses:

a. Router (network interface for LAN side): 10.0.0.1
b. Physical server (the host machine for vm-s): 10.0.0.10
c. Test workstation (physical network interface): 10.0.0.11
    - WSL Ubuntu Linux machine running on the test workstation has virtual network adapter with assigned IP address: 172.27.133.82
d. Tablet (biocertiX App): 10.0.0.12
e. Virtual network interface of the TOE vm: 10.0.0.13
f. Virtual network interface of the ES vm: 10.0.0.15
g. Virtual network interface of the Audit vm: 10.0.0.16

The biocertiX Software components installed on the vm-s are also reachable from inside the local network based on the domain names. Domain names are resolved by the bind9 server installed on the physical server. Domain names assigned to IPv4 addresses are as follows:

a. TOE (signaturiX Core): https://internal.adress:
b. TOE (signaturiX Admin): https://internal.adress;

c. External System (Client system): https://internal.adress;
d. signaturiX Audit: https://internal.adress;

Moreover, the selected biocertiX Software components installed on the vm-s expose human interfaces (via browser) for administrator, user and auditor. Therefore, following addresses are accessible for browser running on the PC that is connected to the local network:

a. TOE (signaturiX Admin): https://internal.adress;
b. External System (Client system): https://internal.adress;
c. signaturiX Audit: https:// internal.adress;

Physical IBM server hardware:

a. 8-core Intel Xeon E5-2660 processor
b. 260GB RAM
c. 180 GB HDD

Functional testing

The Evaluation Assurance Level EAL 2 requires the Developer to deliver design information and test results, consistent with good commercial practise.

The Evaluator's task is divided int two activities. The Evaluators shall confirm the Developer's tests results using the sampling strategy described in details by the Common Criteria methodology. Additionally, the Evaluator's task is to devise and perform their own subset of tests which are intended to be the supplementary for the tests prepared by the Developer.

Developer testing

The Developer's testing verifies the functionality of their corresponding TSFI either directly or indirectly (using the interface to test other functionality). The correspondence between the test documentation and TSFIs described in the functional specification is accurate,

The Developer prepared tests which are divided into three groups: 8 unit tests covering the basic requirements, 17 unit tests covering the Audit Generation and 4 unit tests are connected with the User Data Protection.

All the 29 test cases have obtained a PASS verdict.

Evaluator testing

The decided to repeat all functional tests delivered by the Developer. The positive results of the Developer's tests were confirmed by the Evaluators.

Additionally, the Evaluators independently devised and conducted 4 test cases.

The Evaluator has decided to focus on the testing of those interfaces that have not been covered by the developer tests but are underrepresented in SFRs. Moreover, the Evaluator puts emphasis on testing those interfaces that are exposed to the user, rather than the internal TOE interfaces.

The final verdict takes into account the results of the developer's tests that were repeated by the Evaluator and the results of the tests devised by the Evaluator. The final result of Evaluator testing is PASS as all the test cases are assigned a PASS verdict.

All the 33 test cases have obtained a PASS verdict.

Penetration testing

The attack potential used for this evaluation is consistent with AVA_VAN.2: Basic attack potential. The developed test plan was based on vulnerability survey of the evaluation evidence as well as the information available in the public domain is performed by the Evaluator to ascertain potential vulnerabilities that may be easily found by an attacker. TOE configuration used to execute the penetration test plan was consistent with the evaluated configuration according to the Security Target. The intention of the vulnerability analysis is to determinate if there are faults or weaknesses of the TOE that can be exploited in the operational environment.

The evaluation of documentation analysis and tests resulted in the 16 vulnerability notes, which represented a potential vulnerability. Analysis of the assumptions for the environment showed that only 4 of 16 vulnerability notes were classified as applicable and therefore considered exploitable vulnerabilities. At the end, 4 vulnerabilities had an attack potential at the EAL level corresponding to the TOE evaluation and these vulnerabilities were used for the 4 penetration tests.

All penetration tests resulted with FAIL verdict, which is the proof for the resilience of the product and fulfilment of the assumptions of the Security Problem Definition.

After providing all planned tests the Evaluator concluded that there were not exploitable vulnerabilities in the TOE operational environment according to the scope of this evaluation.

Evaluation verdicts

The Evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation and concluded that the TOE meets the security objectives stated in the Security Target for an attack potential Basic.

The Certifier reviewed the work of the Evaluator and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The verdicts for the assurance classes and components are summarised in the following table:

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

Assurance Class	Assurance Component	Laboratory Verdict	Certification Body Validation
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis	PASS	CONFORMANT

Evaluator Comments/Recommendations

Recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and shall to be considered when using the product.

The TOE usage is recommended given that there are not exploitable vulnerabilities in the operational environment. Nonetheless, the following usage recommendations are given:

- It is mandatory to strictly follow the steps indicated in the installation documentation to install the correct version of the TOE in a proper manner.
- The user guidance must be read and understood to operate the TOE in an adequate manner according to the Security Target.
- The TOE shall be operated in trusted operational environment (as required by OE.SAMPLING_BIOMETRIC_DATA, OE.BIOSIGNER_DEVICE and OE.ENVIRONMENT objectives) and it shall be used and maintained by authorised and trusted personnel (as required by OE.PERSONNEL and OE.RELIABILITY objectives). The customers should pay special attention to enforcing such environment.
- The TOE security functionality heavily utilizes the TLS connections on almost all TSFIs. The customers should pay special care while configuring and maintaining TLS related functionality.
- Since the TOE components (signaturiX Core and signaturiX Admin) are Java applications running on Tomcat server in dockerized environment of the customer internal network, the customer should primarily ensure:
  - implementation of proper firewall rules (to control incoming and outgoing network traffic to/from internal network),
  - regular monitoring: (although no vulnerabilities were found during this assessment, it's essential to maintain continuous monitoring practices including monitoring access logs, system logs, and network traffic),
  - vulnerability management (specifically, scanning the Tomcat server and OpenSSL for vulnerabilities and apply relevant security patches),
  - employee training: as indicated in operational guideline (personnel handling the biocertiX App and biocertiX Software are trained in security practices and remain conscious about emerging threats and security updates – as indicated in operational guidance).

8. Certifier Recommendations

All the assurance components required by the evaluation level EAL2 of Common Criteria standard have been assigned a "PASS" verdict. Consequently, the laboratory assigned the "PASS" VERDICT to the whole evaluation due all the evaluation requirements are satisfied for the EAL2, as defined by the Common Criteria v3.1 Revision 5 and the CEM v3.1 Revision 5.

Considering the obtained and validated evidence during the certification process of the product biocertiX - handwritten biometric signatures on PDF documents - version 1.1, evaluation, **a positive resolution is proposed.**

9. Acronyms

EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ITSEF	Information Technology Security Evaluation Facility
CB	Certification Body
TOE	Target Of Evaluation

10. Bibliography

The following standards and documents have been used for the evaluation of the product:

1. [CC31p1] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and General Model, Version 3.1, Revision 5

2. [CC31p2] Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components, Version 3.1, Revision 5

3. [CC31p3] Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components, Version 3.1, Revision 5

4. [CEM31] Common Criteria for Information Technology Security Evaluation. Evaluation Methodology, Version 3.1 Revision 5

5. Java SecureRandom class
   https://developer.android.com/reference/java/security/SecureRandom

6. Cryptographic Module Validation Program
   https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3900

7. FIPS 140-2 Security Requirements for Cryptographic Modules
   https://csrc.nist.gov/publications/detail/fips/140/2/final

8. SP 800-90A Rev. 1: Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015

9. SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms Version 1.3 February 2023

10. The Transport Layer Security (TLS) Protocol Version 1.3
    https://datatracker.ietf.org/doc/html/rfc8446

References

List of normative documents:

SOG-IS MRA Mutual Recognition Agreement of Information Technology Security Evaluation Certificates v3.0, 8.01.2010

CCRA Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 02.07.2014

ISO/IEC 17025 General requirements for competence of calibration and testing laboratories

ISO/IEC 17065 Conformity assessment - Requirements for bodies certifying products, processes and services

ISO/IEC 18045 Information technology — Security techniques — Methodology for IT security evaluation

PC1 v. 2.4 IT Security Evaluation and Certification Scheme

List of related documents

[EXT-1201] [FIN-ETR-v1.2]	**Final Technical Report for biocertiX, v1.2, issue date 09.02.2024 (ITSEF confidential document)**
[EXT-1159] [EVD-ST-V2.3]	**Security Target for biocertiX - handwritten biometric signatures on PDF documents version 1.1, v.2.3, issue date 25.09.2023 (confidential document)**
[EXT-1249] [EVD-ST-V2.3 LITE]	**Security Target for biocertiX - handwritten biometric signatures on PDF documents version 1.1, v.2.3-lite, issue date 25.09.2023**
[EXT-890] [NOT-V0.1]	**Assecco's request for a new name for the product**
[EXT-1165] [TPR-ATE_LAB-V1.4]	**biocertiX Independent Test Plan and Report, v. 1.4, issue date 10.01.2024 (ITSEF confidential document)**
[EXT-1168] [EVD-PEN_TEST-V1.1]	**AVA Penetration Tests Plan and Report, v. 1.1, issue date 10.01.2024 (ITSEF confidential document)**
[EXT-1169] [EVD-VA-V1.1]	**biocertiX Vulnerability Analysis, v. 1.1, issue date 10.01.2024 (ITSEF confidential document)**

Podpisany elektronicznie przez
NASK - PIB
29.10.2024
12:47:50 +01'00'