

Polish IT Security Evaluation and Certification Scheme (PC1)

Maintenance Report

[2025-1] Maintenance Report on **biocertiX - handwritten biometric signatures on PDF documents, version 1.2**

Certification Maintenance Dossier Code: **2025-1**

Certification Dossier Code: **2021-5**

Certification Maintenance Report Creation Date: 12th November 2025

Maintenance Report Code: **2025-1-REP-100**

Certification Authority: NASK National Research Institute (**POLAND**)



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., Opaska 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



AC 223

**Certificate Identifier:
1/PC1/AC223/2024**

Certificate decision date: 29.02.2024

Certificate expiry date: 28.02.2029

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

NASK National Research Institute
Certification Body Manager

Certification NASK

Table of content

Assurance Continuity Maintenance Report 4

1. Certification Dossier Index 4

2. Change description 5

3. Assessment of Changes 7

4. Conclusion 7

5. References 8

Assurance Continuity Maintenance Report

1. Certification Dossier Index

Maintenance Report Issue Date:	12th November 2025
Maintenance Report Identifier:	2025-1-REP-100
Maintenance Dossier:	2025-1
Impact Analysis Report: Current TOE version: Current Security Target: Evaluation Technical Report: Certificate Identifier: Certified TOE version: Security Target: TOE Developer: Certificate decision date: Certificate expiry date: Certification Dossier: Certification Report Identifier:	IMPACT ANALYSIS REPORT for biocertiX, issue date 14.10.2025, v0.92 v1.2 v2.4 P-0004-ETR-01 1/PC1/AC223/2024 v1.1 v2.3 Asseco Data Systems S.A. 29.02.2024 28.02.2029 2021-5 2021-5-REP-69
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
Assurance Package:	EAL 2
Certificate holder/Manufacturer:	Asseco Data Systems S.A. Jana z Kolna 11 Str., 80-864 Gdańsk, Poland
Name of Certification Body:	NASK National Research Institute Standardisation and Certification Centre, 12 Kolska, Warsaw, 01-045, Poland

2. Change description

Change description:

New Features:

- Redirecting users from another mobile application to the biocertiX mobile application using an additional authentication method;
- The system lock's cause is being checked;
- Extension of REST and SOAP APIs with methods for confirming receipt of document packages;
- Extension of REST and SOAP APIs with methods for deleting document packages;
- Extension of the REST and SOAP APIs with additional parameters to display related documents;
- Extension of REST and SOAP APIs with new methods enabling theme definition;
- Collect additional biometric attributes;
- Checking the version of the signaturix Core application;
- Consent to the processing of biometric signature data;
- Extension of REST and SOAP APIs with an additional parameter "biometricDataConsentHasBeenGiven" and "privacyPolicyConsentHasBeenGiven";
- Extension of REST and SOAP APIs with an additional parameter "allowStamp";
- Extension of REST and SOAP APIs with an additional parameter "removePlaceholderIfPossible";
- Extension of REST and SOAP APIs with an additional parameter "RequirementCondition";
- Extension of REST and SOAP APIs with an additional parameter "allowedNotifications";
- Extension of REST and SOAP APIs with additional parameters that enable PDF forms to be filled in with read-only data;
- Configuration change notification;
- Change of audit certificates;
- Preventing configuration changes in signatureX Admin GUI when signaturix Audit is not available;
- Device validation based on the biocertiX mobile app;
- Removal of 'CalculationMethod' functionality.

Improvements:

- Clearing cookies when loading the signaturix Core page;
- The Android SDK has been updated to a new version;
- Secure access to integration documentation;
- signaturix Core and signaturix Admin can operate behind a proxy that requires authentication;
- Stop sending new documents when the SignatureX Core instance is overloaded;
- DOCUMENT_EXPIRED notifications;

- Change in time server configuration;
- Time verification with an NTP server;
- Information about the blocking or unblocking of systems;
- Changes of the administrator's TOTP secret;
- Authentication using AC codes in multi-instance environments;
- Support for screen synchronization in multi-instance environments;
- API error code reorganization;
- Distinguishing between uppercase and lowercase letters in API;
- Information about the user and the date of creation in the databases;
- Changes to the user list approved in signaturix Admin GUI;
- Configuration of seals in signaturix Admin GUI;
- Collecting additional statistics on the use of TOE functionalities;
- Removal of validation of the timestamps field in the audit module;
- Extension the ST.

Fixed bugs:

- Fixed an error in authentication using QR code;
- Fixed an error in handling client certificate requests.

Affected Evaluation Evidence

The affected evaluation evidence is:

- the ST - new version identifier;
- the TOE itself - new version;
- Operational Guidance document is updated due to changes;
- Preparative Guidance document is updated due to changes;
- Other evidence affected by changes - ADV_FSP, ADV_ARC, ALC_CMC, ALC_CMS, ALC_DEL.

The CB has verified that the updated TOE is marked with the new version identifier, and the developer has provided evidence of regression testing.

Version of the Product after changes: 1.2

3. Assessment of Changes

Assessment of Changes:

The ICT product identified in this report was assessed according to the document Assurance Continuity [1], procedure P33 – Product certification [2].

The baseline for this assessment was the Certification Report [5], the Security Target [4] and the developer's Impact Analysis Report (IAR) [3].

The IAR is intended to satisfy the requirements outlined in the document Assurance Continuity [1].

In accordance with those requirements, the IAR describes:

- the changes made to the certified TOE;
- the evidence updated as a result of the changes;
- the security impact of the changes.

4. Conclusion

Conclusion:

CB reviewed the description of the changes and the analysis of their impact upon security and found it to be satisfactory.

As all the changes to the maintained TOE have been classified as minor, it is the conclusion of the CB that the maintained TOE is appropriate for assurance maintenance and re-evaluation is not required.

The assurance statement as outlined in the Certification Report on biocertiX, 2021-5-REP-84 (public), issue date 19.02.2024 **remains valid**, considering the changes as described in this report.

This report is **an addendum** to the Certification Report on biocertiX, **2021-5-REP-84 (public)**, issue date 19.02.2024.

5. References

- [1] Common Criteria supporting document "Assurance Continuity" as adopted by SOG-IS: Joint Interpretation Library, Version 1.2, March 2024 and CCRA: maintained by CCDB, Unique Identifier: 015, Version: 3.1, Issue Date: 2024-02-29, Approved by: CCMC.
- [2] Procedure P33 – Product certification, v3.4(1), from PC1 – IT Security Evaluation and Certification Scheme.
- [3] Impact Analysis Report for biocertiX, v0.92, issue date 14.10.2025 (confidential document).
- [4] Security Target for biocertiX - ver. 2.4, issue date 24.09.2025 (confidential document – LITE version available).
- [5] Certification Report on biocertiX, 2021-5-REP-84 (public), issue date 19.02.2024.
- [6] Evaluation Technical Report for biocertiX - ver. 1.2, P-0004-ETR-01, issue date 09.02.2024 (confidential document).
- [7] Instruction I29 – Certificate scope verification, v2.3, from PC1 - IT Security Evaluation and Certification Scheme.