Certification Report

MaskTech eSign Applet on Secora™ ID S v1.1

Sponsor and developer: ***MaskTech International GmbH***
Nordostpark 45
90411 Nuremberg
Germany

Evaluation facility: ***SGS Brightsight B.V.***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-0299278-CR**

Report version: **1**

Project number: **0299278**

Author(s): **Kjartan Jæger Kvassnes**

Date: **18 October 2022**

Number of pages: **12**

Number of appendices: **0**

Head Office:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Recognition of the Certificate

The presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the MaskTech eSign Applet on Secora™ ID S v1.1. The developer of the MaskTech eSign Applet on Secora™ ID S v1.1 is MaskTech International GmbH located in Nuremberg, Germany and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE securely create or import, use and manage, signature creation data (SCD). The SSCD protects the SCD during its whole life cycle beginning with import as to be used in a signature creation process solely by its signatory. The TOE comprises all IT security functionality necessary to ensure the secrecy of the SCD and the security of the electronic signature. The TOE stores signatory reference authentication data (RAD) to authenticate a user as its signatory. The RAD is a password e.g. PIN, a biometric template or a combination of these. The TOE protects the confidentiality and integrity of the RAD.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 18 October 2022 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the MaskTech eSign Applet on Secora™ ID S v1.1, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the MaskTech eSign Applet on Secora™ ID S v1.1 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL5 augmented (EAL5+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) and AVA_VAN.5 (Advanced methodical vulnerability analysis).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the MaskTech eSign Applet on Secora™ ID S v1.1 from MaskTech International GmbH located in Nuremberg, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier		Version
Hardware	Smart Card IC		IFX_CCI_000005
Software	Java Card Operating System Secora ID S		v1.1
	MaskTech eSign Applet Identified by Applet ID 0x0013	Helper Applet	v1.0
		eSign Applet	v1.0
		PACE Applet	v1.0
		TLV-Library	v1.0

To ensure secure usage a set of guidance documents is provided, together with the MaskTech eSign Applet on Secora™ ID S v1.1. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

The TOE is a combination of hardware and software configured to securely create or import, use and manage signature creation data (SCD). The SSCD protects the SCD during its whole life cycle beginning with import as to be used in a signature creation process solely by its signatory. The TOE comprises all IT security functionality necessary to ensure the secrecy of the SCD and the security of the electronic signature.

The TOE provides the following functions:

- generate SCD and the correspondent signature verification data (SVD),
- import SCD and, optionally, the corresponding SVD through a trusted channel
- export the SVD for certification through a trusted channel to the CGA,
- prove the identity as SSCD to external entities,
- optionally, receive and store certificate info,
- switch the TOE from a non-operational state to an operational state, and
- if in an operational state, create digital signatures for data with the following steps:
  - select a set of SCD,
  - authenticate the signatory and determine its intent to sign,
  - receive data to be signed or a unique representation there of (DTBS/R) through a trusted channel from SCA,
  - apply an appropriate cryptographic signature creation function using the selected SCD to the DTBS/R.

2.3 Assumptions and Clarification of Scope

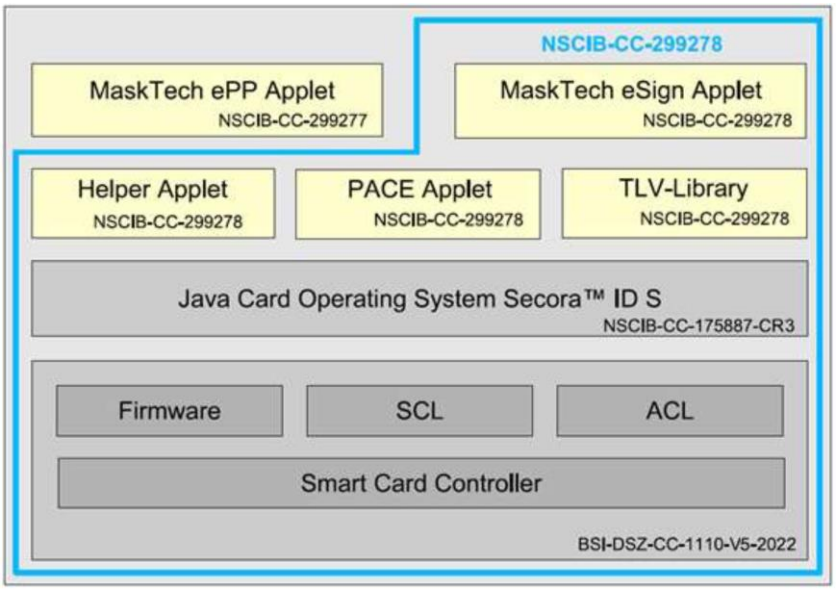
2.3.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 6.2 of *[ST-lite]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information



The light yellow blocks represent the applets provided by the developer that together yield the MaskTech eSign Applet on Secora™ ID S v1.1. Only the components surrounded by the blue outline are part of TOE.

The TOE relies on the following security features of the Java Card platform Secora™ ID S v1.1:

- Cryptographic ciphers (AES, TDES)
- Signature algorithms (ECDSA, RSA)
- Key agreement algorithms (ECDH, PACE)
- Key pair generation (EC, RSA)
- Message digest algorithms (SHA-1, SHA-2 family)
- Random number generation (PTG.3 according to *[AIS31]*)
- Secure channel SCP03 from *[GP_SCP03]*
- Content management provided by *[GP]*
- LDS-API according to *[ICAO_9303]*
- PACE API, a proprietary API for the PACE cryptographic protocol which is especially
- hardened against side channel attacks.

The MaskTech eSign Applet on Secora™ ID S v1.1 supports PACE for:

- the identification and authentication of the user as the legitimate card holder
- the establishment of a trusted channel between the terminal and the card
- the protection against tracking and eavesdropping

The MaskTech eSign Applet on Secora™ ID S v1.1 supports Chip Authentication version 1 for:

- proof the authenticity of the chip to the terminal
- establish a trusted channel between the terminal and the card.

The MaskTech eSign Applet on Secora™ ID S v1.1 supports Terminal Authentication version 1 to restrict the service provisions to authorized SCAs and CGAs.

2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	**Version**
MaskTech eSign Applet on SECORA™ ID S v1.1, User Manual, dated 08 September 2022	version 1.08

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer performed extensive testing on functional specification, subsystem and SFR-enforcing module level. All parameter choices were addressed at least once. All boundary cases identified were tested explicitly, and additionally the near-boundary conditions were covered probabilistically. The testing was largely automated using industry standard and proprietary test suites. A proprietary test suite was used to ensure the correctness of the personalization and the functional compliance of the TOE security policy.

The underlying hardware and crypto-library test results are extendable to composite evaluations, because the underlying platform is operated according to its guidance and the composite evaluation requirements are met.

For the testing performed by the evaluators, the developer provided samples and a test environment. The evaluators repeated a selection of the developer tests were chosen based on representative selection of different test suites and different test configurations.

2.6.2 Independent penetration testing

The methodical analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considered whether potential vulnerabilities can already be identified due to the TOE type and/or specified behaviour in such an early stage of the evaluation.
- For ADV_IMP a thorough implementation representation review was performed on the TOE. During this attack oriented analysis the protection of the TOE was analysed using the knowledge gained from all previous evaluation classes. This resulted in the identification of (additional) potential vulnerabilities. This analysis was performed according to the attack methods in *[JIL-AP]* and included consideration of the technical report *[HW-ETRfC]* and *[Plat-ERTfC]* of the underlying platform.
- All potential vulnerabilities were analysed using the knowledge gained from all evaluation classes and information from the public domain, including latest guidance issued on the secure use of platform components. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. The potential vulnerabilities were addressed by penetration testing, an update of platform and/or TOE usage guidance or in other ways that were deemed appropriate.

The total test effort expended by the evaluators was 2 weeks. During that test campaign, 100% of the total time was spent on Perturbation attacks.

2.6.3 Test configuration

The TOE was tested in the following configurations:

- The test samples were identified as: SECORA™ ID S v1.1 platform combined with applet ID 0x0025, which corresponds to the ePP product. The combined test plan for ePP product and eSign TOE generated assurance for perturbation attack resistance of both applet ID 0x0025 (ePP product) and applet ID 0x0013 (this TOE, eSign applet) that share the essential internal mechanisms against perturbation attacks.

2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

2.7 Reused Evaluation Results

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by the use of three Site Technical Audit Reports. Sites involved in the development and production of the hardware platform were reused by composition.

No sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number MaskTech eSign Applet on Secora™ ID S v1.1.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the MaskTech eSign Applet on Secora™ ID S v1.1, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5 augmented with AVA_VAN.5 and ALC_DVS.2**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims 'strict' conformance to the Protection Profile *[EN419211-2], [EN419211-3], [EN419211-4], [EN419211-5]* and *[EN419211-6]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: none.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength to satisfy the AVA_VAN.5 "high attack potential". To be protected against attackers with a "high attack potential", appropriate cryptographic algorithms with sufficiently large cryptographic key sizes shall be used (references can be found in national and international documents and standards).

3 Security Target

The Security Target – MaskTech eSign Applet on Secora™ ID S v1.1, version 0.10, Dated 09 September 2022 *[ST]* is included here by reference.

Please note that, to satisfy the need for publication, a public version *[ST-lite]* has been created and verified according to *[ST-SAN]*.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

AES	Advanced Encryption Standard
CA	Chip Authentication
CGA	Certificate Generation Application
DES	Data Encryption Standard
DTBS/R	Data To Be Signed or its unique Representation
EAC	Extended Access Control
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
IC	Integrated Circuit
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
LDS	Logical Data Structure
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PACE	Password Authenticated Connection Establishment
PP	Protection Profile
QSCD	Qualified Signature/Seal Creation Device
PACE	Password Authenticated Connection Establishment
PTRNG	Physical True Random Number Generator
RAD	Reference authentication data
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman Algorithm
SCA	Signature Creation Application
SCD	Signature Creation Data
SHA	Secure Hash Algorithm
SM	Secure Messaging
SSCD	Secure Signature/Seal Creation Device
SVD	Signature Verification Data
TA	Terminal Authentication
TDES	Triple DES
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[AIS31] Functionality classes and evaluation methodology for deterministic/physical random number generators, version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik

[CC] Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017

[CEM] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017

[COMP] Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018

[EN419211-2] EN 419211-2:2013 Protection profiles for Secure signature creation device – Part2: Device with key generation, Information Society Standardization System CEN/ISSS, registered under the reference BSI-CC-PP-0059-2009-MA-02, 30 June 2016

[EN419211-3] EN 419211-3:2013 Protection profiles for Secure signature creation device – Part 3: Device with key import, Information Society Standardization System CEN/ISSS, registered under the reference BSI-CC-PP-0075-2012-MA-01E, 30 June 2016

[EN419211-4] EN 419211-4:2013 Protection profiles for Secure signature creation device – Part4: Extension for device with key generation and trusted communication with certificate generation application, Information Society Standardization System CEN/ISSS, registered under the reference BSI-CC-PP-0071-2012-MA-01, 30 June 2016

[EN419211-5] EN 419211-5:2013 Protection profiles for Secure signature creation device– Part5: Extension for device with key generation and trusted communication with signature creation application, Information Society Standardization System CEN/ISSS, registered under the reference BSI-CC-PP-0072-2012-MA-01, 30 June 2016

[EN419211-6] EN 419211-6:2014 Protection profiles for Secure signature creation device – Part 6: Extension for device with key import and trusted communication with signature creation application, Information Society Standardization System CEN/ISSS, registered under the reference BSI-CC-PP-0076-2013-MA-01, 30 June 2016

[ETR] Evaluation Technical Report MaskTech eSign Applet on Secora™ ID S v1.1, 22-RPT-324, Version 9.0, 29 September 2022

[EU-REG] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[GP] GPC_SPE_034, GlobalPlatform Card - Card specification Version 2.3.1, GlobalPlatform, March 2018

[GP_SCP03] GPC_SPE_014, GlobalPlatform Technology - Secure Channel Protocol ’03’ - Card Specification v2.3 - Amendment D - Version 1.2, April 2020

[HW-CERT]	BSI-DSZ-CC-1110-V5-2022 for Infineon Security Controller IFX_CCI_000003h,000005h, 000008h, 00000Ch, 000013h, 000014h,000015h, 00001Ch, 00001Dh, 000021h, 000022h in the design step H13 and including optional software libraries and dedicated firmware in several versions from Infineon Technologies AG, v1.0, Dated 29 April 2022
[HW-ETRfC]	ETR for composite evaluation according to AIS 36 for the Product BSI-DSZ-CC- 1110-V5-2022, ETR for Composite evaluation (EFC), TÜV Informationstechnik GmbH (confidential document)
[HW-ST]	Public Security Target BSI-DSZ-CC-1110-V5-2022, Version 2.0, 2022-03-28, “Public Security Target IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h design step H13”, Infineon Technologies AG
[ICAO_9303]	ICAO Doc 9303, Machine Readable Travel Documents, Eighth Edition, 2021
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.1, June 2020
[JIL-AM]	Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution)
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[Plat-CERT]	NSCIB-CC-21-175887-CR3, SECORA™ ID S v1.1 (SLJ52GxxyyyzS), EAL6 augmented with ALC_FLR.1, Version 1.0, Dated 30 August 2022
[Plat-ETRfC]	Evaluation Technical Report for Composition “SECORA™ ID S v1.1 (SLJ52GxxyyyzS)” – EAL6+, 19-RPT-630, version 10.0, 29 August 2022
[Plat-ST]	SECORA™ ID S v1.1 (SLJ52GxxyyyzS) Security Target, Rev 2.1, 03 August 2022
[ST]	Security Target – MaskTech eSign Applet on Secora™ ID S v1.1, version 0.10, Dated 09 September 2022
[ST-lite]	Security Target – MaskTech eSign Applet on Secora™ ID S v1.1, version 1.2, Dated 09 September 2022 – Public Version
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)