Certification Report

itsme Second Factor Attestation Engine, version 1.0.0

Sponsor and developer: ***Belgian Mobile ID NV***
Markiesstraat 1
1000 Brussel
Belgium

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

Report number:	**NSCIB-CC-2400154-01-CR**
Report version:	**1.1**
Project number:	**NSCIB-2400154-01**
Author(s):	**Andy Brown/Wim Ton**
Date:	**15 January 2026**
Number of pages:	**11**
Number of appendices:	**0**

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, TrustCB 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 TrustCB 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 TrustCB 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, TrustCB 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

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 itsme Second Factor Attestation Engine, version 1.0.0. The developer of the itsme Second Factor Attestation Engine, version 1.0.0 is Belgian Mobile ID NV located in Brussels, Belgium 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 is a software library, allowing a user to generate an attestation that their second factor was verified. The second factor attestation uniquely ties together the user's subject public key(s), the data to be signed and the fact that their second factor has been verified at a given time. The TOE also allows the user to securely update their second factors and/or subject public keys

The TOE has been evaluated by SGS Brightsight B.V located in Delft. The evaluation was completed on 15 January 2026 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 itsme Second Factor Attestation Engine, version 1.0.0, 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 itsme Second Factor Attestation Engine, version 1.0.0 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 EAL3 augmented (EAL3+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ADV_FSP.4 (Complete functional specification), ADV_IMP.1 (Implementation representation of the TSF), ADV_TDS.3 (Basic modular design), ALC_FLR.1 (Basic flaw remediation) and ALC_TAT.1 (Well-defined development tools).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, CEM:2022 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, CC:2022 *[CC]*.

TrustCB 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.

This document was initially issued on 15 January 2026 as version 1 and re-issued on 15 January 2026 as version 1.1 to correct a typo in the section 1 date of ETR approval.

[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 itsme Second Factor Attestation Engine, version 1.0.0 from Belgian Mobile ID NV located in Brussels, Belgium.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	itsme Second Factor Attestation Engine client subsystem software package	1.0.0
	itsme Second Factor Attestation Engine server subsystem software package	1.0.0

To ensure secure usage a set of guidance documents is provided, together with the itsme Second Factor Attestation Engine, version 1.0.0. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

The TOE is intended to be used as a component of the itsme mobile user authentication technology, to conduct the following high-level functions:

- Generating a key pair and signature from a user’s PIN (client subsystem);
- Creating an authenticated set of messages (client subsystem);
- Verifying an authenticated set of messages (server subsystem);
- Creating second factor attestations (server subsystem); and
- Generating audit records (server subsystem).

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 4.2 of the *[ST]*.

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

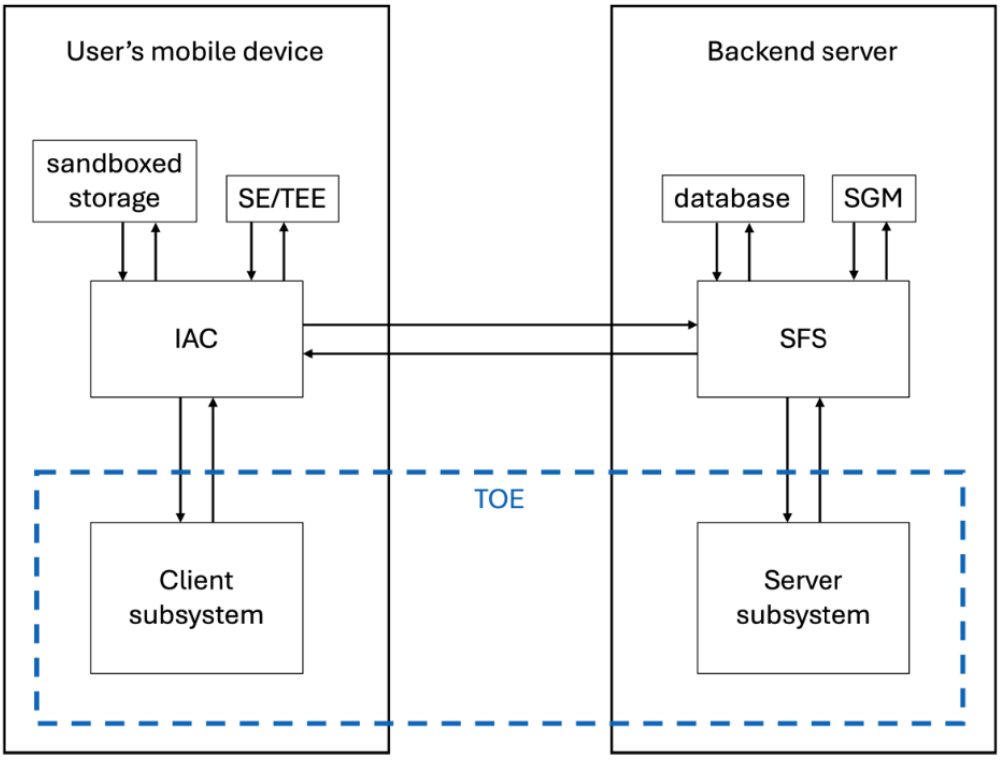
The TOE is a software library, allowing a user to generate an attestation that their second factor was verified. The second factor attestation uniquely ties together the user’s subject public key(s), the data to be signed and the fact that their second factor has been verified at a given time. The TOE also allows the user to securely update their second factors and/or subject public keys.

The TOE consists of a client and server subsystem:

- The TOE client subsystem securely handles the user’s PIN and biometrics. Biometrics are handled indirectly through the environment with the support of the mobile device’s *[SE]/[TEE]*.

- The TOE client subsystem allows to register additional keys (called 'subject' keys) linked to the user with the server. Note that the generation, maintenance and actual usage of these keys is out of scope for the TOE.
- The TOE server subsystem allows for the secure enrolment, verification and updates of the user's second factor (PIN or biometrics) and subject keys.
- The TOE server subsystem produces an attestation (including a reference to all registered subject keys for that user) and audit records of the correct usage of the second factor.

The logical architecture, originating from the Security Target *[ST]* of the TOE can be depicted as follows:



2.5 Documentation

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

Identifier	Version
itsme Second Factor Attestation Engine Operation Guide,	1.2.5

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 which was divided into four areas: TOE client subsystem tests, TOE Server subsystem tests, cryptography tests and internal tests. Testing was performed on different phone operating systems to be able to check TOE's functionality in the mobile phone environment. The evaluators checked and confirmed that the developer test environment was

functionally equivalent to the operational environment with respect to the SFR's. All results from the developer tests were as expected.

The evaluator repeated all of the developer tests and all results were also as expected. For the evaluator-defined tests, a number of test cases were designed and executed by the evaluator.

2.6.2 Independent penetration testing

The evaluator defined independent tests to perform based on the vulnerability analysis. Possible vulnerabilities were identified first from which potential vulnerabilities were derived. Possible vulnerabilities were discovered through the design assessment, using applicable attack lists and a public domain vulnerability search.

The penetration test plan that was generated was based around software attacks.

The total test effort expended by the evaluators was 3 weeks. During that test campaign, 100% of the total time was spent on logical tests.

2.6.3 Test configuration

The configuration of the sample used for independent evaluator testing and penetration testing was the same as described in the *[ST]*.

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.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

2.7 Reused Evaluation Results

There is no reuse of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number itsme Second Factor Attestation Engine, version 1.0.0.

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 itsme Second Factor Attestation Engine, version 1.0.0, to be **CC Part 2 extended, CC Part 3 conformant** and to meet the requirements of **EAL 3 augmented with ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_FLR.1, and ALC_TAT.1**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" contains necessary information about the usage of the TOE.

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

3 Security Target

The itsme Second Factor Attestation Engine Security Target, Version 1.4.8, 24 October 2025 *[ST]* is included here by reference.

4 Definitions

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

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
SE	Secure Enclave
TEE	Trusted Execution Environment
TOE	Target of Evaluation

5 Bibliography

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

[CC]	Common Criteria for Information Technology Security Evaluation, Parts 1 to 5, CC:2022 Revision 1, November 2022
[CEM]	Common Methodology for Information Technology Security Evaluation, CEM:2022 Revision 1, November 2022
[ETR]	Evaluation Technical Report itsme Second Factor Attestation Engine – EAL3+, 25-RPT-796, Version 5.0, 14 January 2026
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[ST]	itsme Second Factor Attestation Engine Security Target, Version 1.4.8, 24 October 2025

(This is the end of this report.)