Certification Report

MobileID on Dakota IoT, version 09AF41

Sponsor and developer:	***IDEMIA*** **2 pl Samuel Champlain,** **92400 Courbevoie,** **France**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-2500032-01-CR**
Report version:	**1**
Project number:	NSCIB-**2500032-01**
Author(s):	**Jordi Mujal**
Date:	**17 November 2025**
Number of pages:	**12**
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 MobileID on Dakota IoT, version 09AF41 . The developer of the MobileID on Dakota IoT, version 09AF41 is IDEMIA located in Courbevoie, France 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 comprises of the IDEMIA MobileID signature application installed on top of the eUICC IDEMIA Dakota IoT Global Platform Java Card and Telecom operating system based on the IDEMIA SC31 security controller.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 17 November 2025 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 MobileID on Dakota IoT, version 09AF41 , 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 MobileID on Dakota IoT, version 09AF41 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 EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) ALC_FLR.3 (Systematic Flaw Remediation) and AVA_VAN.5 (Advanced methodical vulnerability analysis).

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.

The TOE is stated as a Qualified Signature Creation Device for the purposes of electronic identification and trust services as detailed by the [EU-REG]. The evaluation by SGS Brightsight included an examination of the TOE according to the eIDAS Dutch Conformity Assessment Process Version 6 0.

TrustCB B.V., as the Dutch eIDAS-Designated Body responsible in The Netherlands for the assessment of the conformity of qualified electronic signature and/or qualified electronic seal creation devices declares that the evaluation meets the conditions for eIDAS certification for listing on the EU eIDAS compiled list of Qualified Signature/Seal Creation Devices.

[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 MobileID on Dakota IoT, version 09AF41 from IDEMIA located in Courbevoie, France.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	SCE900U	A
Software	DAKOTA IoT v1.1 Phase 2 on SCE900U	09A792
	MobileID on Dakota IoT	09AF41

To ensure secure usage a set of guidance documents is provided, together with the MobileID on Dakota IoT, version 09AF41 . For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 5.

2.2 Security Policy

The TOE relies on an eUICC JavaCard Open Platform software consisting of

- Java Card virtual machine, ensuring language-level security;
- Java Card runtime environment, providing additional security features for Java card technology enabled devices;
- Java card API, providing access to card’s resources for the Applet;
- Global Platform Card Manager, responsible for management of Applets on the card;
- GSMA framework: an eUICC Operating System with telecom framework and profile management.

The applet part contains components to securely create, use and manage signature-creation data (SCD) with key generation and import:

- SSCD Part 2: that performs the generation of signature keys in the device [EN419211-2],
- SSCD Part 3: that performs the import of the signature keys generated in a trusted manner outside the device [EN419211-3]

In addition, trusted channel of TOE for the data to be signed import is supported.

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 8.2 of the *[ST]*.

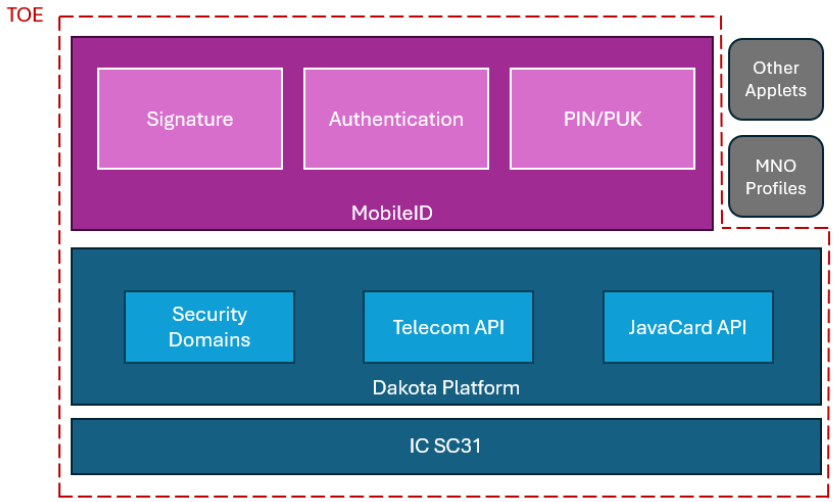
2.3.2 Clarification of scope

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

Note that the TOE is composed on the top of an eUICC JavaCard Open Platform software. Details on the scope for that part are provided in *[PL-ST]* and *[PL-CERT]*.

2.4 Architectural Information

The architecture of the TOE according to the [ST]:



2.5 Documentation

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

Identifier	Version
Mobile Id Applet V1.0 Operational User Guidance (AGD_OPE), FQR 110 A432	Ed 1.2
Mobile Id Applet Perso Guide, FQR 110 A435	Ed 2.3
Dakota IoT - Applet Security Recommendations, FQR 110 A2FB	Ed 3
Dakota IoT v1.1 Phase 2 on SCE900U AGD_OPE, FQR 110 A3E0	Ed 5
Dakota IoT v1.1 Phase 2 on SCE900U – Perso Guide, FQR 110 A3C6	Ed 4
Dakota IoT - Application Loading Protection Guidance, FQR 110 A2FD	Ed 2
Dakota IoT - JCVM Patch Loading Protection Guidance, FQR 110 A30B	Ed 1
Public Security Target DAKOTA IOT V1.1 Phase 2 on SCE900U, FQR 110 A41B,	Ed 3

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.

testing was largely automated using industry standard and proprietary test suites. Test scripts were used extensively to verify that the functions return the expected values.

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 reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.

2.6.1 Independent penetration testing

The independent vulnerability 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 could 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 evaluation classes. This resulted in the identification of potential vulnerabilities. This analysis used the attack methods in *[JIL-AMS]* and *[JIL-AAPS]*.
- All potential vulnerabilities were analysed using the knowledge gained from all evaluation classes and information from the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. The potential vulnerabilities were addressed by penetration testing, a guidance update or in other ways that are deemed appropriate.

The total test effort expended by the evaluators was 2 weeks. During that test campaign, 0% of the total time was spent on physical attacks, 0% overcoming sensors and filters, 50% perturbation attacks, 0% retrieving keys with FA, 50% side-channel attacks, 0% exploitation of test features, 0% attacks on RNG, 0% ill-formed Java Card application, 0% software attacks, and 0% application isolation penetration tests.

2.6.2 Test configuration

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

2.6.3 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.

The algorithmic security level exceeds 100 bits for all evaluated cryptographic functionality as required for high attack potential (AVA_VAN.5).

The strength of the implementation of the cryptographic functionality has been assessed in the evaluation, as part of the AVA_VAN activities.

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 use of multiple site certificates and Site Technical Audit Reports.

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 MobileID on Dakota IoT, version 09AF41 .

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 MobileID on Dakota IoT, version 09AF41 , to be **CC Part 2 extended, CC Part 3 conformant** and to meet the requirements of **EAL 4 ALC_DVS.2, ALC_FLR.3 and AVA_VAN.5**. 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]* and *[EN419211-3]*.

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.

3 Security Target

The MobileID on Dakota IoT – Security Target, FQR 110 A40B, Version 10, 03 November 2025 *[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
CBC	Cipher Block Chaining (a block cipher mode of operation)
CBC-MAC	Cipher Block Chaining Message Authentication Code
CFB	Cipher Feedback
CTR	Counter
DES	Data Encryption Standard
CPLC	Card Production Life Cycle
CRT	Chinese Remainder Theorem
DES	Data Encryption Standard
DRG	Deterministic Random Generator
ECB	Electronic Code Book (a block cipher mode of operation)
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie Hellman
EDC	Error Detection Code
EdDSA	Elliptic Curve Edwards-curve Digital Signature Algorithm
eUICC	embedded Universal Integrated Circuit Card
GCM	Galois/Counter Mode
GF	Galois Field
GP	Global Platform
GCM	Galois/Counter Mode
GSMA	Groupe Speciale Mobile Association
HMAC	Hashed MAC
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MAC	Message Authentication Code
MNO	Mobile Network Operators
NSCIB	Netherlands Scheme for Certification in the area of IT security
PP	Protection Profile
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm

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
[COMP]	Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.6, April 2024
[eIDAS-REP]	Assessment Reporting Sheet eIDAS IDEMIA MobileID on Dakota IoT, 25-RPT-1197, version 2.0, 17 November 2025
[EN419211-2]	EN 419 211-2:2013, Protection profiles for secure signature creation device - Part 2: Device with key generation, V2.0.1, registered under the reference BSI-CC-PP-0059-2009-MA-02
[EN419211-3]	EN 419 211-3:2013, Protection profiles for secure signature creation device - Part 3: Device with key import, V1.0.2, registered under the reference BSI-CC-PP-0075-2012-MA-01
[ETR]	Evaluation Technical Report “MobileID on Dakota IoT” – EAL4+, 25-RPT-841, version 6.0, 05 November 2025
[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
[PL-CERT]	Certification Report DAKOTA IoT v1.1 Phase 2 on SCE900U, version 09A792, NSCIB-CC-2500034-01-CR, version 1, 18 July 2025.
[PL-ETRfC]	Evaluation Technical Report for Composition “Dakota IoT Phase 2 on SCE900U” – EAL4+, 25-RPT-843, version 3.0, 10 July 2025
[PL-ST]	Public Security Target DAKOTA IOT V1.1 Phase 2 on SCE900U, version Ed3, 07 July 2025
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.2.1, February 2024
[JIL-AMS]	Attack Methods for Smartcards and Similar Devices, Version 2.5, May 2022 (sensitive with controlled distribution)
[JIL_QSCD]	Security Evaluation and Certification of Qualified, Electronic Signature/Seal Creation Devices, JIL Interpretations for Security Certification according to eIDAS Regulation 910/2014, Version 1.0, July 2022
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[ST]	MobileID on Dakota IoT – Security Target, FQR 110 A40B, Version 10, 03 November 2025
[ST-lite]	MobileID on Dakota IoT – Public Security Target, 041467_01, Version 9, 03 November 2025
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)