Certification Report

Sm@rtCafé® Expert 8.0 C1

Sponsor:	***Veridos Gmbh*** **Truderinger Straße 15** **81677 Munich** **Germany**
Developer:	***Giesecke+Devrient Mobile Security GmbH*** **Prinzregentenstraße 159** **81677 Munich** **Germany**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-0289060-CR**
Report version:	**1**
Project number:	**0289060**
Author(s):	**Jordi Mujal**
Date:	**01 September 2022**
Number of pages:	**13**
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 Sm@rtCafé® Expert 8.0 C1. The developer of the Sm@rtCafé® Expert 8.0 C1 is Giesecke+Devrient Mobile Security GmbH located in Munich, Germany and Veridos GmbH was 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 described in the *[ST]* is a dual-interface, contact based or a pure contactless smart card with a Javacard operating system (OS). The TOE is a multi-purpose Java card where applets of different kinds can be installed. Since a post-issuance installation of applets is possible, the TOE corresponds to an *open configuration*, as defined in *[PP]*.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 01 September 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 Sm@rtCafé® Expert 8.0 C1, 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 Sm@rtCafé® Expert 8.0 C1 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 EAL6 augmented (EAL6+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.1 (Basic Flaw Remediation).

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 Sm@rtCafé® Expert 8.0 C1 from Giesecke+Devrient Mobile Security GmbH located in Munich, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	IFX SLC37GDA512 (BSI-DSZ-CC-1107-V3-2022) IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh	T11 (design step)
Firmware (of certified IC)	BOS & POWS	80.306.16.0 & 80.306.16.1
	Flash Loader	09.12.0005
Software (of the certified IC)	UMSLC	v01.30.0564
Software (embedded)	Sm@rtCafé® Expert 8.0	C1

To ensure secure usage a set of guidance documents is provided, together with the Sm@rtCafé® Expert 8.0 C1. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST-lite]*, Chapter 2.4.

2.2 Security Policy

The TOE has the following main features:

- The hardware platform [HW_CERT] with the following configurations according to [HW_ST]:
  - FLASH: up to 512 kBytes
  - ROM: only used by IFX
  - RAM for the user: up to 16 kByte
  - SCP (Symmetric Crypto Co-processor for DES and AES Standards): accessible
  - Crypto2304T (Crypto Co-processor for asymmetric algorithms like RSA and EC): accessible
  - Interfaces: ISO/IEC 7816 and/or ISO/IEC 14443
- Java Card Runtime Environment (JCRE)
- Java Card Virtual Machine (JCVM)
- Java Card API
- On-card Installer
- Applet Deletion Manager
- Card Manager
- Logical Channels
- Object Deletion
- Transaction and atomicity concept according to [JCRE301]
- firewall access control
- Cryptographic services implemented in the G&D crypto library:
  - RSA-CRT and RSA key generation,
  - ECC over GF(p) key generation
  - RSA and RSA-RCT signature generation, RSA signature verification, RSA and RSA-CRT decryption and RSA Encryption.

- 3DES for en-/decryption (CBC and ECB) and MAC generation and verification (2-key3DES, 3-key 3DES, Retail-MAC, CMAC and CBC-MAC).
- AES (Advanced Encryption Standard) for en-/decryption (GCM, CBC and ECB) and MAC generation and verification (CMAC, CBC-MAC).
- ECC over GF(p) for signature generation and verification (ECDSA).
- Random number generation according to class DRG.4
- ECC over GF(p) Diffie Hellman and Generic Mapping key exchange
- SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512

- Integrity check of checksum-protected data
- Secure state of information
- Non-observability of operations on sensitive information
- Unavailability of previous information content
- Secure installation of post-issuance applications on the card
- Secure post-issuance deletion of previously installed applets

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

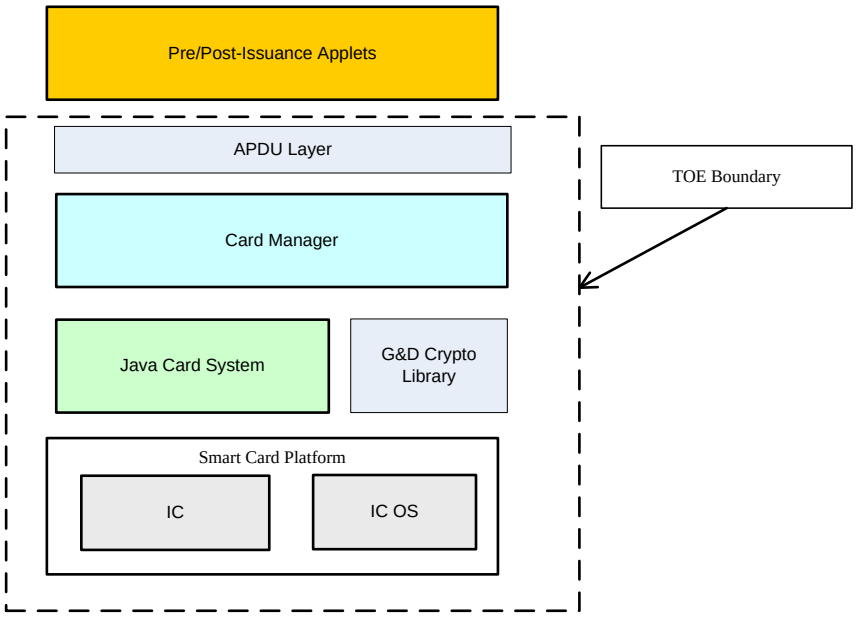
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 6.2 of the *[ST-lite]*.

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 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	Date
Preparative Procedures Sm@rtCafé® Expert 8.0 C1	2.2	15-06-2022
Operational User Guidance Sm@rtCafé® Expert 8.0 C1	2.3	31-08-2022

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. 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.

2.6.2 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 (additional) potential vulnerabilities. This analysis used the attack methods in *[JIL-AM]* 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 16 weeks. During that test campaign, 13% of the total time was spent on Perturbation attacks, 79% on side-channel testing, and 8% 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]* and in some specific cases, an earlier revision of the TOE was also used. The assurance gained from testing on an earlier revision has been assessed to be valid for the final TOE version, because the changes introduced were minimal and did not have an impact on the TSF.

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.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength for satisfying the AVA_VAN.5 “high attack potential”. The TOE supports a wider range of key sizes (see *[ST]*), including those with sufficient algorithmic security level to exceed 100 bits 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. For composite evaluations, please consult the *[ETRfC]* for details.

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 4 Site Technical Audit Reports.

All assurance components that are needed for the sites are considered during the evaluation. In determining whether the TOE meets the EAL6+ ALC requirements, STARs were used to re-use site audit results of sites involved in the TOE life-cycle. For several production sites, these STARs were the results of audits at EAL5+. Nonetheless, the evaluator has established that the TOE meets all EAL6+ requirements, independent of which production site is used.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Sm@rtCafé® Expert 8.0 C1.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents. To support composite evaluations according to *[COMP]* a derived document *[ETRfC]* was provided and approved. This document provides details of the TOE evaluation that must be considered when this TOE is used as platform in a composite evaluation.

The verdict of each claimed assurance requirement is “**Pass**”.

Based on the above evaluation results the evaluation lab concluded the Sm@rtCafé® Expert 8.0 C1, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 6 augmented with ALC_FLR.1**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims ‘demonstrable’ conformance to the Protection Profile *[PP]*.

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 Veridos/ Giesecke + Devrient MS Security Target Sm@rtCafé® Expert 8.0 C1 Version 3.1/Status 31 August 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
CBC	Cipher Block Chaining (a block cipher mode of operation)
CBC-MAC	Cipher Block Chaining Message Authentication Code
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
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDH	Elliptic Curve Diffie Hellman
EDC	Error Detection Code
EdDSA	Elliptic Curve Edwards-curve Digital Signature Algorithm
GCM	Galois/Counter Mode
GF	Galois Field
GP	Global Platform
GCM	Galois/Counter Mode
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MAC	Message Authentication Code
NSCIB	Netherlands Scheme for Certification in the area of IT security
PP	Protection Profile
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
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 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
[ETR]	Evaluation Technical Report “Sm@rtcafe Expert 8.0 C1” – EAL6+, 21-RPT-1111, version 5.0, 01 September 2022
[ETRfC]	ETR for Composition Sm@rtCafé® Expert 8.0 C1, 22-RPT-658, version 4.0, 01 September 2022
[HW-CERT]	BSI-DSZ-CC-1107-V3-2022 for IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah,IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h,IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h,IFX_CCI_00004Ah, IFX_CCI_00004Bh,IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Ehdesign step T11 with firmware 80.306.16.0 & 80.306.16.1,optional NRG™ SW 05.03.4097, optional HSLv3.52.9708, UMSLC lib v01.30.0564, optional SCLv2.15.000 and v2.11.003, optional ACL v3.33.003 andv3.02.000, optional RCL v1.10.007, optional HCLv1.13.002 and user guidance, 16 May 2022
[HW-ETRfC]	EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION (ETR COMP) Common Criteria CC 3.1, (EAL6 augmented with ALC_FLR.1), Project / Certification ID: 8120103228 / BSI-DSZ-CC-1107-V3, Version 5, 11 May 2022.
[HW-ST]	IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh T11, Security Target Lite, v 4.3.1, 05 May 2022.
[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
[PP0099]	Java Card Protection Profile - Open Configuration, version 3.1, April 2020 (BSI-CC-PP-0099-V2-2020)
[ST]	Veridos/ Giesecke + Devrient MS Security Target Sm@rtCafé® Expert 8.0 C1 Version 3.1/Status 31 August 2022
[ST-lite]	Veridos/ Giesecke + Devrient MS Security Target Lite Sm@rtCafé® Expert 8.0 C1 Version 3.1/Status 31 August 2022

[ST-SAN] ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)