Certification Report

SLS37CSAEU 01.03.4091

Sponsor and developer:	***Infineon Technologies AG*** **Am Campeon 1-15** **85579 Neubiberg** **Germany**
Evaluation facility:	***TÜV Informationstechnik GmbH*** **Langemarckstr. 2** **45141 Essen** **Germany**
Report number:	**NSCIB-CC-0238862-CR**
Report version:	**1**
Project number:	**0238862**
Author(s):	**Jordi Mujal**
Date:	**04 August 2021**
Number of pages:	**11**
Number of appendices:	**0**

Reproduction of this report is authorised only if the report is reproduced in its entirety.

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 3

Recognition of the Certificate 4

International recognition 4
European recognition 4

1 Executive Summary 5

2 Certification Results 6

2.1 Identification of Target of Evaluation 6
2.2 Security Policy 6
2.3 Assumptions and Clarification of Scope 6
2.3.1 Assumptions 6
2.3.2 Clarification of scope 7
2.4 Architectural Information 7
2.5 Documentation 7
2.6 IT Product Testing 7
2.6.1 Testing approach and depth 7
2.6.2 Independent penetration testing 8
2.6.3 Test configuration 8
2.6.4 Test results 8
2.7 Reused Evaluation Results 8
2.8 Evaluated Configuration 8
2.9 Evaluation Results 8
2.10 Comments/Recommendations 8

3 Security Target 10

4 Definitions 10

5 Bibliography 11

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.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

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 SLS37CSAEU 01.03.4091. The developer of the SLS37CSAEU 01.03.4091 is Infineon Technologies AG located in Neubiberg, 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 is a V2X HSM (Vehicle-to-anything Hardware Security Module) which is used for secure cryptographic operations and key management according to the V2X HSM Protection Profile [PP]. The TOE serves a communication device (VCS) in Cooperative Intelligent Transport System (C-ITS). The TOE is intended to be used in vehicle or in stationary deployments and has an interface towards the VCS.

The TOE has been evaluated by TÜV Informationstechnik GmbH located in Essen, Germany. The evaluation was completed on 04 August 2021 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 SLS37CSAEU 01.03.4091, 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 SLS37CSAEU 01.03.4091 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_FLR.1 (Basic Flaw Remediation) and AVA_VAN.4 (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 SLS37CSAEU 01.03.4091 from Infineon Technologies AG located in Neubiberg, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware Platform		
Hardware	IFX_CCI_00003Dh with embedded software	G11
Firmware	Boot-OS (BOS)	80.203.00.3
	Flash Loader	8.06.001
Software	ACL	v3.03.003
	SCL	v2.13.001
	HCL	v1.13.001
	RCL	v1.10.006
	HSL	v2.01.6198
Composite TOE		
Software	V2X application	01.03.4091
	VFUL application	01.03.3526

To ensure secure usage a set of guidance documents is provided, together with the SLS37CSAEU 01.03.4091. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 1.4.3.

2.2 Security Policy

The TOE is a discreet chip security controller and realises an external V2X HSM according to the V2X HSM Protection Profile [PP]. The TOE encompasses the following main features:

- Global Platform SCP03 protected communication
- Random number generation
- Digital signature generation
- User data ECIES encryption/decryption
- Protection of user data during transport and storages
- Supporting functions for Butterfly key derivation and implicit certificates
- Role based private key access control
- Private key import
- V2X Key Management
- Genuiness proof
- In field software update

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

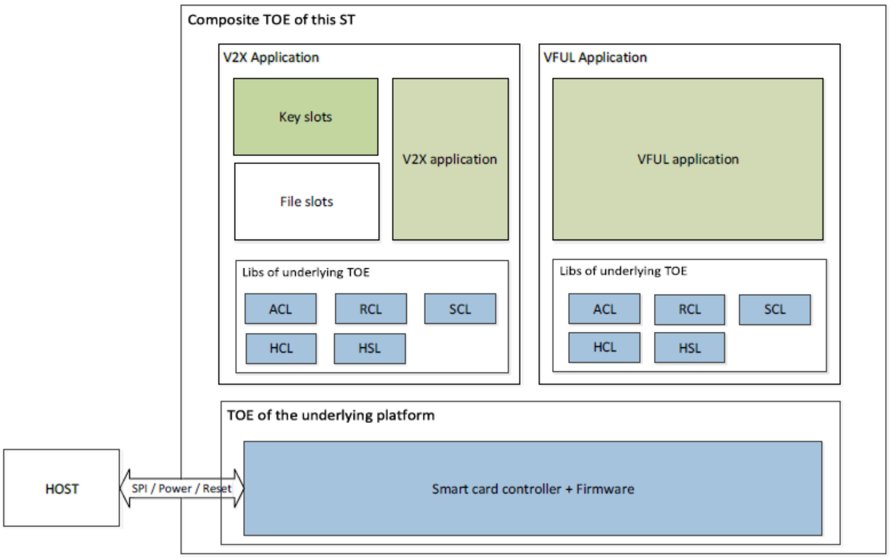
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.3 of the *[ST]*.

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 following figure describes the main TOE architecture. The Host is not part of the TOE.



2.5 Documentation

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

Identifier	Version	Date
SLS37CSAEU V2X Databook	1.3	2021-06-23
SLS37CSAEU V2X Errata and Update	1.2	2021-06-16

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, all TSFs and related security mechanisms, subsystems and modules were tested in order to assure complete coverage of all SFRs. The developer tests were consistent with the definition of each TSFI given in the functional specification, the modules of the TOE design and the security mechanisms described in the security architecture.

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 supported the test environment preparation. The evaluator did not repeat developer tests but used them as input to specify independent functional test cases. The evaluators proposed functional tests for each APDU.

2.6.2 Independent penetration testing

The independent vulnerability analysis has been performed according to *[CC]*, *[JIL-AAPS]*, and *[JIL-AM]*. The ratings have been calculated according to *[JIL-AAPS]*.

The total test effort expended by the evaluators was 7 weeks. During that test campaign, 48% of the total time was spent on Perturbation attacks, 29% on side-channel testing, and 23% 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]*.

In some specific functional and penetration tests, an earlier revision of the TOE or the HW platform was used. The assurance gained from testing on an earlier revision or the HW platform was 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.

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 9 site certificates and 28 Site Technical Audit Reuse report approaches.

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 SLS37CSAEU 01.03.4091.

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 SLS37CSAEU 01.03.4091, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with ALC_FLR.1 and AVA_VAN.4**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims 'strict' conformance to the Protection Profile *[PP]*. Note that the Protection profile used was not certified and ASE activities were carried out as specified in *[CEM]*..

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 SLS37CSAEU V2X HSM Security Target, Version 1.2, 20 July 2021 *[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:

APDU	Application Protocol Data Unit
C-ITS	Cooperative Intelligent Transport System
HSM	Hardware Security Module
IC	Integrated Circuit
ITS	Intelligent Transport System
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
TOE	Target of Evaluation
V2X	Vehicle to anything
VCS	Vehicle C-ITS Station
VFUL	V2X Field Upgrade Loader

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

[ETR] EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY), NSCIB-CC-02238862, version 4, 30 July 2021

[HW-CERT] Certification Report IFX_CCI_00003Fh,IFX_CCI_000059h,IFX_CCI_00005Bh, IFX_CCI_00003Ch, IFX_CCI_00003Dh, IFX_CCI_00005Ah, design step G11 with optional HSL v2.01.6198, optional SCL v2.13.001, optional ACL v3.03.003, optional HCL v1.13.001, optional RCL v1.10.006 and with specific IC-dedicated firmware identifier 80.203.00.3, Version 1, 22 April 2021.

[HW-ST] Public Security Target IFX_CCI_00003Fh IFX_CCI_000059h IFX_CCI_00005Bh IFX_CCI_00003Ch IFX_CCI_00003Dh IFX_CCI_00005Ah G11 including optional software libraries: Flash Loader according Package1 and Package2, HCL, RCL, HSL, ACL and SCL, v1.5, 14 April 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

[PP] CAR 2 CAR Communication Consortium, Protection Profile V2X Hardware Security Module, version 1.4.1, SHA2-512 hash:

346efc021fb47fedf770d705e93be16effa6812fb6a95b009bf2d46ac64c52cb90
af6524c6a5252b946e0202a999edf87eaaf930b3a764319adc3d8aa06bbbf0

[ST] SLS37CSAEU V2X HSM Security Target, Version 1.2, 20 July 2021

(This is the end of this report.)