Certification Report

SXF1800HN/V102B

Sponsor and developer: ***NXP Semiconductors Germany GmbH***
Troplowitzstrasse 20
22529 Hamburg
Germany

Evaluation facility: ***Riscure***
Delftechpark 49
2628 XJ Delft
The Netherlands

Report number:	**NSCIB-CC-235750-CR**
Report version:	**1**
Project number:	**235750**
Author(s):	**Andy Brown**
Date:	**24 December 2019**
Number of pages:	**13**
Number of appendices:	**0**

Headoffice:
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 Dutch Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 5 (ISO/IEC 15408)
Certificate number	**CC-19-235750**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer	**NXP Semiconductors Germany GmbH** **Troplowitzstrasse 20, 22529 Hamburg, Germany**
Product and assurance level	**SXF1800HN/V102B** Assurance Package: ▪ EAL4 augmented with ALC_DVS.2, ALC_FLR.1, AVA_VAN.5 Protection Profile Conformance (if appropriate): ▪ CAR 2 CAR Communication Consortium – Working Group Security (WG SEC), C2C Protection Profile V2X HSM, version 1.4.0, 2 September 2019.
Project number	**235750**
Evaluation facility	**Riscure BV located in Delft, the Netherlands** Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5 (ISO/IEC 18045)

Common Criteria Recognition Arrangement for components up to EAL2

SOGIS Mutual Recognition Agreement for components up to EAL7

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 5 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Validity	Date of 1st issue : **24-12-2019** Certificate expiry : **24-12-2024**

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

R. de Jonge, Managing director
TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220, NL-6802 CE Arnhem
The Netherlands

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

CONTENTS:

TÜVRheinland®
Precisely Right.

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 license 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, in order 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.

TÜVRheinland®
Precisely Right.

Recognition of the certificate

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations.

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting 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. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.eIDAS-Regulation

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the SXF1800HN/V102B. The developer of the SXF1800HN/V102B is NXP Semiconductors Germany GmbH located in Hamburg, 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 implements a V2X Hardware Security Module (HSM) to be part of an Intelligent Transport System (ITS) composed of stations (e.g. vehicles, roadside modules) periodically broadcasting information as their position or particular events in their vicinity.

Such communications need to be protected to prevent the spreading of wrong information which could cause issues ranging from minor, such as traffic disorganization, to dramatic, such as accidents leading to people's physical integrity.

Also, the privacy of messages preventing the tracking of vehicles/drivers by unauthorized entity is required in several countries' regulations.

The whole solution is based on two modules:

- V2X VCS, in charge of messages building and certificate management;
- V2X HSM (SXF1800), in charge of message signatures and private keys protection.

The two components are physically separated and communicate through a secure channel to protect messages exchanged between them.

The current TOE is limited to the V2X HSM module, which in this solution is a smart card implementing the services to be invoked by the V2X VCS.

The TOE has been evaluated by Riscure B.V. located in Delft, The Netherlands. The evaluation was completed on 24/12/2019 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 SXF1800HN/V102B, 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 SXF1800HN/V102B 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 provides 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.1 (Basic Flaw Remediation) 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]*.

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. It should be noted that the certification results only apply 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 releasable for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the SXF1800HN/V102B from NXP Semiconductors Germany GmbH located in Hamburg, Germany.

The TOE is comprised of the following main components:

Type	Name	Release
Hardware	NCJ38A0 High-performance secure microcontroller for Automotive (short name NCJ38A0) (as per base certification)	B0.207
Software	NCJ38AC High-performance secure microcontroller with Crypto Library for Automotive (short name NCJ38AC) (as per base certification)	B0.2CB
	JCOP SE 4.4 R12.1 RC2	J5S2M0024BB70800
	V2X HSM	v2.12.3
	GS applet (non-TSF part of the TOE)	v2.12.1

To ensure secure usage a set of guidance documents is provided together with the SXF1800HN/V102B. Details can be found in section ”Documentation” of this report.

The main version of the TOE is delivered from regular production. A delta version is also available through an update to JCOP SE 4.4 R10.3 (J5S2M001E0800800) in the field.

For a detailed and precise description of the TOE lifecycle refer to the *[ST]*, chapter 2.2.

2.2 Security Policy

The TOE implements the following services:

- Device management
- Connection to the TOE and reset;
- Application selection, deselection, logical channel management.
- Export of non-sensitive TOE information (e.g. components configuration);
- JCOP firmware including SCP03 implementation;
- TOE security parameters configuration;
- TOE monitoring and attack counter management.

Software management:

- OS update firmware.
  GlobalPlatform 2.2.1 applet management services.

V2X applets content management:

- Generation/Derivation of ECDSA key pairs;
- Import of ECDSA key pairs;
- Export of ECDSA public keys.
- Secure storage of generated/derived/imported private keys.
- Deletion of ECDSA key pair.

V2X end-usage security services:

- Access control to services;
- Import of message to be signed;
- Generation of ECDSA signature;
- ECIES encryption and decryption;

- Random number generation.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

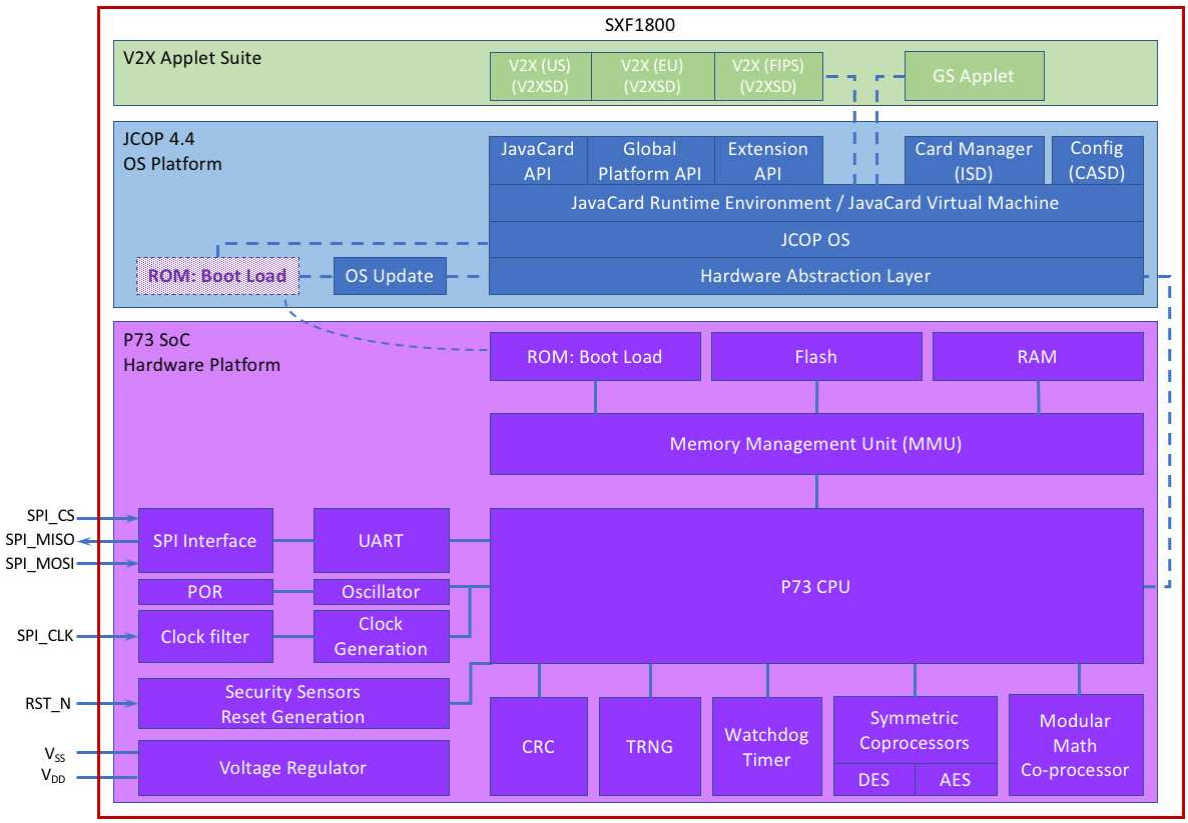
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 5 of the *[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 figure below depicts the current TOE physical and logical scope:



The TOE physical scope is the full integrated circuit hardware.

Physical interfaces are then all included modules, in particular the memories (ROM, RAM and Flash), CPU, internal buses, external buses (SPI) and cryptographic co-processors.

The TOE logical scope is the JCOP platform and the application layer made of two applet packages (V2X and GS).

GlobalPlatform applet loading functionalities remains invokable and related APDUs are therefore TOE external interface; however, their access is restricted to the NXP administrators; JavaCard APIs and bytecodes are not invokable by any customer and are therefore not considered as external interfaces of the TOE.

Logical interfaces are then restricted to APDUs handled by the platform and the V2X applets.

2.5 Documentation

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

Name	Version	Form of Delivery
NXP administrators User Guidance Manual	1.2	Electronic Document
Customer administrators User Guidance Manual	1.1	Electronic Document
Preparation User Guidance Manual	1.1	Electronic Document
End-user User Guidance Manual	1.2	Electronic Document
SXF1800 Datasheet	1.5	Electronic Document
SXF1800 Errata Sheet	1.2	Electronic Document

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 has performed extensive testing on functional specification, subsystem and SFR-enforcing module level.

All parameter choices have been addressed at least once. All boundary cases identified have been tested explicitly, and additionally the near-boundary conditions have been covered probabilistically. The testing was largely automated using industry standard and proprietary test suites. Test scripts were extensively used to verify that the functions return the expected values.

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

Amount of developer testing performed:

The tests are performed on security mechanisms, subsystem and module level with a total amount of several thousand test scenarios.

As demonstrated by ATE_COV.2 the developer has tested all security mechanisms and TSFIs.

As demonstrated by ATE_DPT.1 the developer has tested all the TSF subsystems against the TOE design and against the security architecture description.

For the testing performed by the evaluators, the developer has provided samples and a test environment. The evaluators have verified the execution of a selection of the developer tests and conducted a number of test cases designed by the evaluator.

2.6.2 Independent Penetration Testing

The evaluator independent penetration tests were conducted according to the following vulnerability analysis approach:

- Consideration of Riscure attack repository, which is an internal repository of potential attacks maintained on the basis of the expert knowledge amassed within Riscure.

- Analysis of the TOE design and implementation for resistance against the JIL attacks.
- Analysis of the TOE in its intended environment to check whether the developer vulnerability analysis in ARC has assessed all information.

The evaluators concluded that a small number of areas could be potentially vulnerable for attackers possessing a high attack potential. Consequently, practical penetration testing was performed.

2.6.3 Test Configuration

Testing was performed on slightly different versions of the TOE OS and V2X applet identified in chapter 2.1.

The differences between these component versions and the certified TOE have been analysed. They have no impact on the test results, hence the test results apply to the TOE.

2.6.4 Testing 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 Re-used evaluation results

This is a composite certification. Evaluation results of the underlying hardware has been re-used.

There has been extensive re-use of the ALC aspects for the sites involved in the software component of the TOE (NXP Hamburg, NXP Mougins, NXP Eindhoven, NXP Caen, NXP Gratkom, NXP Glasgow 2, NXP San Jose, SII Gdansk 2, NXP Bangalore, NXP Leuven, Company GlobalLogic)

Sites involved in the development and production of the hardware platform were re-used 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 SXF1800HN/V102B. The configuration is further detailed in *[ST]* chapter 1.2.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[2] and which references a 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 SXF1800HN/V102B, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with ALC_DVS.2, ALC_FLR.1, 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 *[PP]* with the following packages: Communication Link Extended Protections, Private Key Import (online), Software Update, Key Derivation.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 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 with respect to 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 need to 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. In order for the evolution of attack methods and techniques to be covered, he 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 SXF 1800HN/V102B Security Target, Rev. 1.2, Dated 06/12/2019 *[ST]* is included here by reference.

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

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

VCS	Vehicle C-ITS Station
C-ITS	Cooperative Intelligent Transport Systems and Services
V2X	Vehicle to anything
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
ST	Security Target
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.
[ETR]	Evaluation Technical Report for SXF1800HN/V102B, 2018545, Version 1.6, 24 December 2019
[HW-CERT1]	Rapport de certification ANSSI-CC-2018/60 NCJ38A0 B0.207, 09 January 2019
[FW-CERT1]	Rapport de certification ANSSI-CC-2019/23 NCJ38AC(B0.2C8 ou B0.2CB), 04 July 2019.
[ETRfC-IC]	Serma Safety & Security ITSEF, ETR Lite - PHANTOM project (NCJ38A0), V1.0, 23/11/2018 .
[ETRfC-IC-CL]	Serma Safety & Security ITSEF, ETR Lite for Composition PHANTOM-CL Project (NCJ38AC), V1.1, 17/05/2019.
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.
[PP]	CAR 2 CAR Communication Consortium, C2C Protection Profile V2X HSM, version 1.4.0, 13 September 2019.
[ST]	SXF 1800HN/V102B Security Target, Rev. 1.2, Dated 06/12/2019.
[ST-Lite]	SXF 1800HN/V102B Security Target Lite, Rev. 1.2, Dated 06/12/2019
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.

(This is the end of this report).