Certification Report

SXF1800HN/V102B

Sponsor and developer:	***NXP Semiconductors Germany GmbH*** **Beiersdorfstraße 12** **22529 Hamburg** **Germany**
Evaluation facility:	***Riscure B.V.*** **Delftechpark 49** **2628 XJ Delft** **The Netherlands**
Report number:	**NSCIB-CC-2300149-01-CR**
Report version:	**1**
Project number:	NSCIB-2300149-01
Author(s):	**Andy Brown**
Date:	**2023-12-18**
Number of pages:	**13**
Number of appendices:	**0**

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

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.

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

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 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 (i.e. vehicles or road infrastructure components) 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 from minor issues, as traffic disorganization, to dramatic events, as accident involving people 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 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 was previously evaluated by Riscure B.V. located in Delft, The Netherlands and was certified under the accreditation of TÜV Rheinland Nederland on 24-12-2019 (CC-19-235750). The current evaluation of the TOE has also been conducted by Riscure B.V. and was completed on 18 December 2023 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]*.

Add the boxed text if appropriate:

The major changes from previous evaluations are:

The scope of certification of underlying IC and crypto library has changed from those used for the previous certification of this TOE. The design and implementation of underlying IC and crypto library remain the same.

The certification took into account that the security evaluation reused the evaluation results of previously performed evaluations. A full, up-to-date vulnerability analysis has been made, as well as renewed testing.

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 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.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]* (Parts I, II and III).

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

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.

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:

Delivery item type	Identifier	Version
Hardware	NCJ38AC High-performance secure microcontroller with Crypto Library for Automotive (short name NCJ38AC)	B0.2CB
Software	JCOP SE 4.4 J5S2M0024BB70800	R12.1 RC2
Application	V2X Applet	v2.12.3
	GS Applet (Generic Storage)	v2.12.1

To ensure secure usage a set of guidance documents is provided, together with the SXF1800HN/V102B. For details, see section 2.5 “Documentation” of this report.

Optional Statement about the lifecycle to be used, where applicable (in all cases, for smartcards). For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 2.2.

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.

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

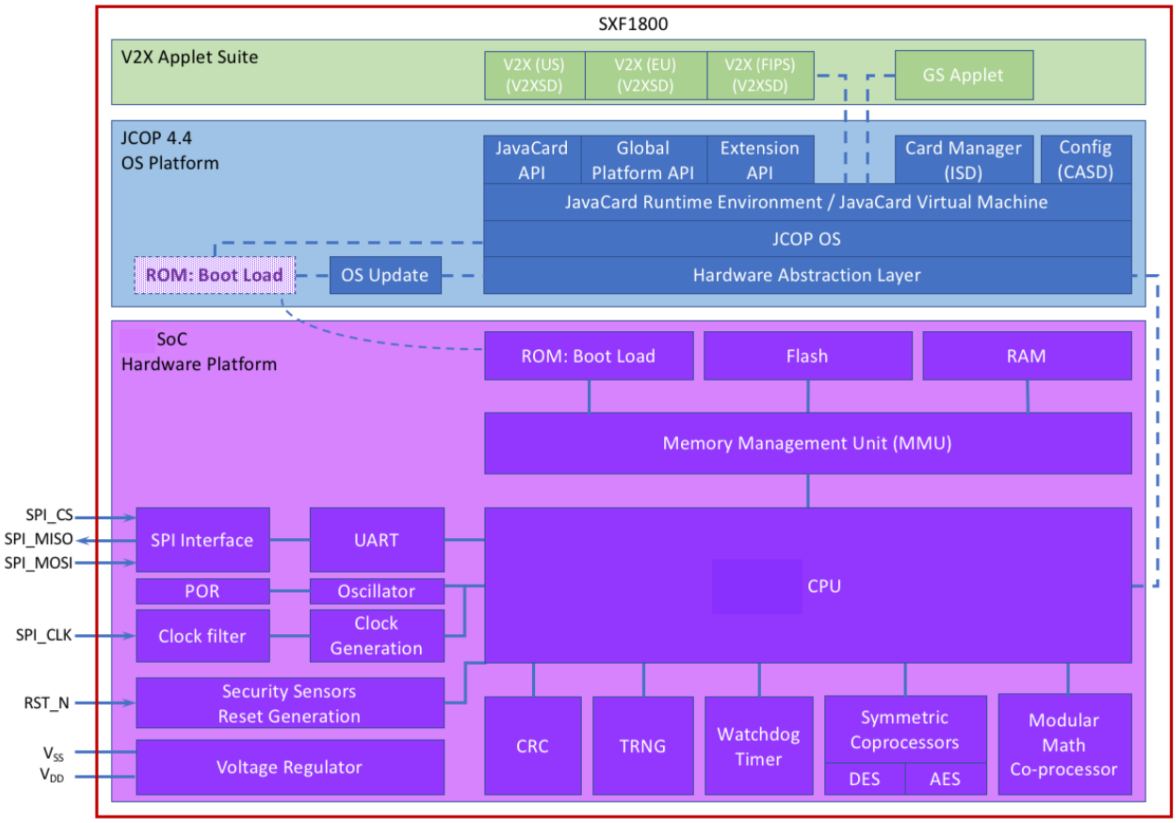
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 5 of the *[ST]*.

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 and the guidance documents.

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:

Identifier	Version
JCOP 4.4 Automotive - User Guidance Manual	1.2
JCOP 4.4 Automotive - Customer User Guidance Manual	1.1
JCOP 4.4 Automotive – User Guidance Manual Addendum V2X	1.1
SXF1800HN/V102 - UGM for preparation phase	1.1
SXF1800HN/V102 - UGM for operational phase	1.2
SXF1800 Secure Element for V2X communication - Product Data Sheet	2.1
SXF1800 Errata sheet	2.1

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.

For the intial TOE, 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 using the configuration of TOE with underlying platform and crypto library.

The analysis of the subsequent update to the underlying platform and crypto library showed that additional testing was required The total test effort expended by the evaluators was 3.5 weeks. During that test campaign,55% of the total time was spent on Perturbation attacks and 45% on side-channel testing.

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

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of 21 Site Technical Audit Reports.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number SXF1800HN/V102B.

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 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]*.

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 SXF1800HN/V102B Security Target, Rev. 2.3, 30 October 2023 *[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:

C-ITS	Cooperative Intelligent Transport Systems and Services
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
V2X	Vehicle to anything
VCS	Vehicle C-ITS Station

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, 20190451-D1, Version 2.1, 11 December 2023

[HW-CERT-BASE] Rapport de certification ANSSI-CC-2019/62 P73N2M0B0.2C2/2C6 Version B0.2, 24 December 2019.

[HW-CERT-MNT] Rapport de maintenance ANSSI-CC-2019/62-M01 P73N2M0B0.2C2/2C6, 10 February 2023

[JIL-AAPS] JIL Application of Attack Potential to Smartcards, Version 3.2, November 2022

[JIL-AMS] 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 2.6, 02 August 2022

[PP] CAR 2 CAR Communication Consortium, Protection Profile V2X Hardware Security Module, version 1.0.1, release 1.6.0, 30 November 2021, registered under the reference BSI-CC-PP-0114-2021.

[ST] SXF1800HN/V102B Security Target, Rev. 2.3, 30 October 2023

[ST-lite] SXF1800HN/V102B Security Target Lite, Rev. 2.3, 30 October 2023

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

(This is the end of this report.)