Certification Report

NXP J3E081_M64_DF, J3E081_M66_DF, J3E041_M66_DF,J3E016_M66_DF, J3E041_M64_DF and J3E016_M64_DF Secure Smart Card Controller Revision 3

Sponsor and developer: ***NXP Semiconductors Germany GmbH,***
Business Unit Identification
Stresemannallee 101
D-22529 Hamburg
Germany

Evaluation facility: ***Brightsight***
Delftechpark 1
2628 XJ Delft
The Netherlands

Report number: **NSCIB-CC-13-37762-CR**

Report version: **1**

Project number: **NSCIB-CC-13-37762**

Authors(s): **Wouter Slegers**

Date: **October 16th, 2013**

Number of pages: **16**

Number of appendices: **0**

Head office Apeldoorn:
Boogschutterstraat 11A
P.O. Box 541
7300 AM Apeldoorn
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

Location Apeldoorn:
Vissenstraat 6
P.O. Box 541
7300 AM Apeldoorn
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

Location Enschede:
Josink Esweg 10
P.O. Box 337
7500 AH Enschede
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 859

TÜV Rheinland Nederland B.V. is a registered company with the Amsterdam Chamber of Commerce under number 27288788
info@nl.tuv.com
www.tuv.com/nl

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 4 (ISO/IEC 15408)
Certificate number	**C13-37762**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer	**NXP Semiconductors Germany GmbH, Business Unit Identification** **Stresemannallee 101, D-22529 Hamburg, Germany**
Product and assurance level	**NXP J3E081_M64_DF, J3E081_M66_DF, J3E041_M66_DF, J3E016_M66_DF, J3E041_M64_DF and J3E016_M64_DF Secure Smart Card Controller Revision 3,** Assurance Package: ▪ EAL4 augmented with ALC_DVS.2, AVA_VAN.5, and ASE_TSS.2 Protection Profile Conformance: ▪ Java Card System - Open Configuration Protection Profile, Version 2.6, Certified by ANSSI, the French Certification Body April, 19th 2010
Project number	**NSCIB-CC-13-37762-CR**
Evaluation facility	**Brightsight BV located in Delft, the Netherlands** Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 4 (ISO/IEC 18045)

Common Criteria Recognition Arrangement for components up to EAL4

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 4 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 4. 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 issue : **16-10-2013**

Certificate expiry : **16-10-2018**

Registration number

PRODUCTS
RvA C078
Accredited by the Dutch Council for Accreditation

TÜV Rheinland Nederland B.V.
P.O. Box 541
7300 AM Apeldoorn
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.

A part of the procedure is the technical examination (evaluation) of the product 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 complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, 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 satisfies the security requirements.

Recognition of the certificate

The Common Criteria Recognition Arrangement and SOG-IS logos are printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

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.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the NXP J3E081_M64_DF, J3E081_M66_DF, J3E041_M66_DF, J3E016_M66_DF, J3E041_M64_DF, J3E016_M64_DF Secure Smart Card Controller Revision 3. The developer is NXP Semiconductors Germany GmbH, Business Unit Identification 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 Target of Evaluation (TOE) is a set of JCOP 2.4.2 R3 products. In total there are currently 19 certified JCOP 2.4.2 R3 products and their certification is divided over 3 certification IDs (NSCIB 13-37760, 13-37761, and 13-37762). All JCOP 2.4.2 R3 products are composed of a P5 secure smart card controller, a Version 2.7/2.9 Cryptographic Library and the Java Card functionality.

The TOE in this Certification Report (i.e., the NXP J3E081_M64_DF, J3E081_M66_DF, J3E041_M66_DF, J3E016_M66_DF, J3E041_M64_DF, J3E016_M64_DF Secure Smart Card Controller Revision 3) is delivered as one of six JCOP 2.4.2 R3 products based on the P5Cx081V1D hardware.

The evaluation of the TOE was conducted as a composite evaluation and uses the results of the CC evaluation of the NXP Secure Smart Card Controllers P5CD016V1D/ P5CD021V1D/ P5CD041V1D/ P5CD081V1D with DESFire EV1, certified under the German CC Scheme on August 13, 2012 (BSI-DSZ-CC-0707-2012 *[HW CERT]*) and the Crypto Library V2.7/V2.9 on SmartMX P5CX081/CD041/CD021/CD016 V1D, certified under the German CC Scheme on 19 December 2012 (BSI-DSZ-CC-0864 *[CL-CERT]*).

Each JCOP v2.4.2 R3 product from NXP is based on Java Card 3.0.1 and Global Platform 2.2.1 industry standards, and allows post-issuance downloading of applications that have been previously verified by an off-card trusted IT component. It implements high security mechanisms and supports various protocols, cryptographic algorithms, and the SecureBox to allow secure integration with a customer's native library.

The JCOP v2.4.2 R3 provides Triple-DES (3DES) including en-/decryption and MAC generation and verification, AES including en-/decryption and MAC generation and verification, RSA and RSA CRT en-/decryption and signature generation and verification, RSA and RSA CRT key generation, RSA public key computation, SHA-1, SHA-224, SHA-256 and hash algorithms, ECC over GF(p) algorithm that can be used for signature generation and verification (ECDSA), ECC key generation, ECC point addition, and ECDH. In addition, the Crypto Library implements a software (pseudo) random number generator, which is initialised (seeded) by the hardware random number generator. For more details refer to the *[ST]*, chapter 1.3.2.

The JCOP v2.4.2 R3 provides Java Card 3.0.1 functionality, including garbage collection and support for extended length APDUs. The JCOP v2.4.2. R3 provides Global Platform 2.2.1 functionality including the CVM Management (Global PIN), Secure Channel Protocol (SCP01, SCP02, and SCP03 (only in Mask 64)), Card Manager and Delegated Management. The JCOP v2.4.2 R3 also provides secure messaging acceleration (for the use in for example LDS applets used in the electronic passport as defined by ICAO), a pre-personalisation mechanism and a MIFARE DESFire application accessible via contactless interface and via Java Card API (availability depends on configuration and hardware)

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands and was completed on September 27th, 2013 with the final delivery 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 certification was completed on October 16th, 2013 with the preparation of this Certification Report.

The scope of the evaluation is defined by the Security Target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the JCOP v2.4.2 R3, 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 JCOP v2.4.2 R3 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 it 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), AVA_VAN.5 (Advanced methodical vulnerability analysis), and ASE_TSS.2 (TOE summary specification with architectural design summary).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4 *[CEM]*, for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 4 *[CC]*.

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the NXP J3E081_M64_DF, J3E081_M66_DF, J3E041_M66_DF, J3E016_M66_DF, J3E041_M64_DF, J3E016_M64_DF Secure Smart Card Controller Revision 3 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 NXP J3E081_M64_DF, J3E081_M66_DF, J3E041_M66_DF, J3E016_M66_DF, J3E041_M64_DF, J3E016_M64_DF Secure Smart Card Controller Revision 3 from NXP Semiconductors Germany GmbH, Business Unit Identification located in Hamburg, Germany.

This report pertains to the TOE which is comprised of the following main components:

Type	Component	Version/ID	Form of delivery
Product	NXP J3E081_M64_DF, J3E081_M66_DF, J3E041_M66_DF, J3E016_M66_DF, J3E041_M64_DF, J3E016_M64_DF Secure Smart Card Controller Revision 3	See next table	Wafer, modules and packages (dice include identification T046D)

The product version information differs per product and is in the combination of Mask ID, Mask Name and Patch ID:

Product	Mask ID	Mask Name	Patch ID
J3E081_M64_DF J3E041_M64_DF J3E016_M64_DF	64	NX250B	01
J3E081_M66_DF J3E041_M66_DF J3E016_M66_DF	66	NX250C	01

To ensure secure usage a set of guidance documents is provided together with the JCOP v2.4.2 R3. Details can be found in section 2.5 of this report.

The TOE is delivered following the procedures of the hardware part of the TOE, i.e. as a wafer in phase 3 or in packaged form in phase 4 of the smart card life cycle as defined in the Smart Card IC Protection Profile *[BSI-PP-0035]*. Applets and native libraries in the SecureBox can be loaded in ROM or EEPROM. Loading in ROM is possible in Phase 3. Loading of the native library (in the SecureBox) software in EEPROM is only possible by NXP in Phase 4. Loading of applets in EEPROM is possible in Phases 3, 4, 5 or 6. Applets and native libraries in the SecureBox are outside the scope of the TOE.

2.2 Security Policy

The TOE provides the Java Card/Global Platform security services of the cryptographic algorithms 3DES, AES, RSA, RSA key generation, SHA-1, SHA-224, and SHA-256, ECDSA, ECC key generation, ECDH, and ECC point addition, and random number generation (seeded with the hardware random number generator), in addition to the functionality described in the Hardware Security Target *[ST-HW]* for the hardware platform. The cryptographic algorithms (except SHA) are resistant against Side Channel Attacks, including Simple Power Analysis (SPA), Differential Power Analysis (DPA), Differential Fault Analysis (DFA) and timing attacks. SHA has only limited resistance for a limited amount of operations against Side Channel Attacks (see the ETR for composition for details *[ETRfC]*). Details on the resistance claims are provided in the Security Target *[ST],* relevant details are provided in the user guidance documents.

The TOE implements a software (pseudo) random number generator, which is initialised (seeded) by the hardware random number generator.

The TOE implements Java Card 3.0.1 garbage collection and extended APDUs, Global Platform 2.2.1 CVM Management (Global PIN), Secure Channel Protocol (SCP01, SCP02, and SCP03 (only in Mask 64)), Card Manager that allowing post-issuance installation and deletion of applets, packages and objects, and Delegated Management.

The TOE additionally implements JCOP proprietary services for secure messaging acceleration, pre-personalization, SecureBox for constrained execution of the user's native libraries, MIFARE DESFire implementation and an EDC protected array.

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. The following topics are of relevance:

- Ø Applets loaded post-issuance do not contain native methods.
- Ø All the bytecodes are verified at least once before the loading on the TOE.
- Ø The operational environment supports and uses the secure communication protocols offered by TOE.
- Ø Keys which are stored outside the TOE and which are used for secure communication and authentication between Smart Card and terminals, are protected for confidentiality and integrity in their own storage environment.
- Ø It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the endconsumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use),
- Ø For the DESFire functionality, it is assumed that only confidential and secure keys shall be used to set up the authentication and access rights for the MIFARE DESFire Emulation. These values are generated outside the TOE. They must be protected during generation, management outside the TOE and downloaded to the TOE.
- Ø For the DESFire functionality, it is assumed that the terminal verifies information sent by the TOE in order to ensure integrity and confidentiality of the communication.

Details can be found in the Security Target *[ST]* section 3.5.

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

This chapter provides a high-level description of the IT product and its major components based on the evaluation evidence described in the Common Criteria assurance family entitled "TOE design (ADV_TDS)". The intent of this chapter is to characterise the degree of architectural separation of the major components and to show dependencies between the TOE and products using the TOE in a composition (e.g. dependencies between HW and SW).

The target of evaluation (TOE) is the JCOP 2.4.2 R3. It consists of:

- Smart card platform (SCP) (parts of the hardware platform and hardware abstraction layer)
- Embedded software (Java Card Virtual Machine, Runtime Environment, Java Card API, Card Manager), and
- Native MIFARE application (physically always present but logical availability depends on configuration)

The TOE does not include any software on the application layer (Java Card applets) nor the optional native libraries in the SecureBox. See *[ST]* section 1.3 for details.

2.5 Documentation

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

Type	Component	Version/ID
Document	User Manual (AGD_OPE) for the applet developer	Rev. 0.6
Document	Administrator Manual (AGD_PRE)	Rev. 0.5
Document	HW Data Sheet	Rev. 0.2
Document	SecureBox User Manual*)	Rev. 3.4
Document	HW Guidance Manual*)	Rev. 3.0

*) It is noted that only a native library developer will also receive the SecureBox User Manual and the HW Guidance document of the underlying hardware platform.

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 FSP, subsystem and 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 hardware test results are extendable to composite evaluations on this hardware TOE, as the hardware is operated according to its guidance and the composite evaluation requirements are met.

For the testing performed by the evaluators, the developer has provided a testing environment. The evaluators have 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 evaluator independent penetration tests were devised after performing an Evaluator Vulnerability Analysis. This was done in the following steps.

1. Inventory of required resistance
   This step used the JIL attack list [JIL-AM] as a reference for completeness and studied the ST claims to decide which attacks in the JIL attack list applied for the JCOP R3.
2. Validation of security functionalities
   This step identified the implemented security functionalities and performed evaluator independent tests to verify implementation and to validate proper functioning of the security functions.
3. Vulnerability analysis
   In this step the design and the implementation of the security functionalities was studied and an analysis was performed to determine whether the implementation potentially could be vulnerable against the attacks of step 1. Based on this analysis the evaluators determined whether the design and implementation provide sufficient assurance or whether penetration testing is needed to provide sufficient assurance.
4. Penetration testing
   This step performed the penetration tests identified in step 4.

5. Conclusions on resistance
   This step performed a *[JIL]* compliant rating on the results of the penetration tests in relation with the assurance already gained by the design analysis. Based on the ratings the evaluators made conclusions on the resistance of the TOE against attackers possessing a high attack potential.

2.6.3 Test Configuration

The developer provided the evaluator with the TOE in a DIL package in pre-personalised state. For penetration tests, TOEs with certain countermeasures disabled were used. See the *[ETR]* for details.

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.

2.7 Re-used evaluation results

This security evaluation (the JCOP 2.4.2 R3) is a full composite evaluation under NSCIB. It cannot be seen a delta since the JCOP 2.4.2 R2 has been certified under BSI, not NSCIB. It was performed in conjuncture with NSCIB-CC-13-37761 and NSCIB-CC-13-37762 (JCOP 2.4.2R3 on slightly different hardware platforms).

Nevertheless in agreement with NSCIB, the evaluator has reused parts of the work that has been done in JCOP 2.4.2 R2 evaluations (BSI-DSZ-CC-784, BSI-DSZ-CC-783, BSI-DSZ-CC-860). Some of the characteristics of the R3 evaluations are:

- Together with the TOE other R3 products have been evaluated whereby testing is reused from other R3 products;
- Testing is reused from previous evaluations on R2 products;
- Alternative Evaluator Reporting according to *[NSP#6]* has been used for the CEM work items in the form of formal presentations to the scheme.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number NXP J3E081_M64_DF, J3E081_M66_DF, J3E041_M66_DF, J3E016_M66_DF, J3E041_M64_DF, J3E016_M64_DF Secure Smart Card Controller Revision 3.

In chapter 2 of administrative guidance the user is instructed to use the IDENTIFY command to verify the identity of the product. The hardware part of the TOE can be verified by reading out the FabKey ID, which should match the specific Order Entry Form (OEF) and its hardware identifier. The software part of the TOE can be verified by checking the Mask ID and Patch ID against the ST, and the specific settings again via the FabKey ID to the settings in the Order Entry Form. Note that deviations of the Order Entry Form defaults might bring the TOE outside the evaluated configuration.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[2] which references several Intermediate Reports and other evaluator documents. To support composite evaluations according to *[CCDB-2007-09-01]* a derived document *[ETRfC]* was provided and approved. This document provides details of the TOE evaluation that have to be considered when this TOE is used as platform in a composite evaluation.

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

The verdict of each claimed assurance requirement is given in the following tables:

Development		Pass
Security architecture	ADV_ARC.1	Pass
Functional specification	ADV_FSP.4	Pass
Implementation representation	ADV_IMP.1	Pass
TOE design	ADV_TDS.3	Pass

Guidance documents		Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass

Life-cycle support		Pass
Configuration Management capabilities	ALC_CMC.4	Pass
Configuration Management scope	ALC_CMS.4	Pass
Delivery	ALC_DEL.1	Pass
Development security	ALC_DVS.2	Pass
Life-cycle definition	ALC_LCD.1	Pass
Tools and techniques	ALC_TAT.1	Pass

Security Target		Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives	ASE_OBJ.2	Pass
Security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.2	Pass

Tests		Pass
Coverage	ATE_COV.2	Pass
Depth	ATE_DPT.1	Pass
Functional tests	ATE_FUN.1	Pass
Independent testing	ATE_IND.2	Pass

Vulnerability assessment		Pass
Vulnerability analysis	AVA_VAN.5	Pass

Based on the above evaluation results the evaluation lab concluded the NXP J3E081_M64_DF, J3E081_M66_DF, J3E041_M66_DF, J3E016_M66_DF, J3E041_M64_DF, J3E016_M64_DF Secure Smart Card Controller Revision 3 to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of EAL4 augmented with ALC_DVS.2, AVA_VAN.5, and ASE_TSS.2. This implies that the product satisfies the security technical requirements specified in Security Target "NXP J3E081_M64_DF, J3E081_M66_DF, J3E041_M66_DF,J3E016_M66_DF, J3E041_M64_DF and J3E016_M64_DF Secure Smart Card Controller Revision 3 Security Target, Rev. 01.02 — 13th August 2013, NSCIB-CC-13-37762".

The Security Target claims 'demonstrable conformance' to the Java Card System - Open Configuration Protection Profile, Version 2.6, certified by ANSSI, the French Certification Body April, 19th 2010 *[JAVACARD]*.

2.10 Comments/Recommendations

The user guidance (as outlined in section 2.5 of this report) 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 (for both the applet and the native library developer) and the hardware (in the case of the native library developer) 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, including a limited resistance of the SHA implementation and limitations on the DES CMAC.
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 implemented cryptographic algorithms was not rated in the course of this evaluation. To fend off attackers with high attack potential appropriate cryptographic algorithms with adequate key lengths must be used (references can be found in national and international documents and standards).

The developer of the native library must implement the advices of the hardware user guidance.

3 Security Target

The Security Target "NXP J3E081_M64_DF, J3E081_M66_DF, J3E041_M66_DF,J3E016_M66_DF, J3E041_M64_DF and J3E016_M64_DF Secure Smart Card Controller Revision 3 Security Target, Rev. 01.02 — 13th August 2013, NSCIB-CC-13-37762" is included here by reference.

Please note that for the need of publication a public version (*[ST-Lite]* NXP J3E081_M64_DF, J3E081_M66_DF, J3E041_M66_DF,J3E016_M66_DF, J3E041_M64_DF and J3E016_M64_DF Secure Smart Card Controller Revision 3, Security Target Lite Rev. 00.03, 13 August 2013) 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:

BSI	Bundesamt für Sicherheit in der Informationstechnik
CBC	Cipher Block Chaining (a block cipher mode of operation)
CBC-MAC	Cipher Block Chaining Message Authentication Code
DES	Data Encryption Standard
DFA	Differential Fault Analysis
ECB	Electronic Code Book (a block cipher mode of operation)
IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
NSCIB	Nederlands Schema voor Certificatie op het gebied van IT-Beveiliging
PP	Protection Profile
PRNG	Pseudo Random Number Generator
RMI	Remote Method Invocation
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
SPA/DPA	Simple/Differential Power Analysis
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

[BSI-PP-0035]	"Security IC Platform Protection Profile", Version 1.0, June 2007.
[CC]	Common Criteria for Information Technology Security Evaluation, Parts I version 3.1 revision 1, and Part II and III, version 3.1 revision 4.
[CEM]	Common Methodology for Information Technology Security Evaluation, version 3.1, Revision 4.
[CL-CERT]	Certification Report, Crypto Library V2.7 on NXP Smart Card Controller P5CD081V1D and its major configurations, 19 December 2012, BSI-DSZ-CC-0864-2012 (including MA-01 Crypto Library V2.7/V2.9 on SmartMX P5Cx081/CD041/CD021/CD016 V1D dated 4 July 2013).
[ETR]	Brightsight, Evaluation Technical Report NXP J3E081_M64_DF, J3E081_M66_DF, J3E041_M66_DF, J3E016_M66_DF, J3E041_M64_DF, J3E016_M64_DF Secure Smart Card Controller Revision 3 EAL4+, reference 13-RPT-257 v2.0, dated 27 September 2013.
[ETRfC]	Brightsight, ETR for Composite Evaluation NXP J3E081_M64_DF, J3E081_M66_DF, J3E041_M66_DF,J3E016_M66_DF, J3E041_M64_DF and J3E016_M64_DF Secure Smart Card Controller Revision 3 EAL4+, reference 13-RPT-262 v2.0, dated 27 September 2013
[ETR-CL]	Brightsight, ETR for composition NXP Crypto Library V2.7 on SmartMX P5Cx081/CD041/CD021/CD016V1D according to AIS36, Brightsight, Revision 3.0, 12 December 2012.
[ETR-HW]	T-Systems, ETR for composition according to AIS36 as summary of the Evaluation Technical Report Version 1.2 Date June 8th, 2012, NXP Secure Smart Card Controllers P5CD081V1D, BSI-DSZ-CC-0707
[HW CERT]	Certification Report. NXP Secure PKI Smart Card Controllers P5CD016V1D/P5CD021V1D/P5CD041V1D/ P5CD081V1D with DESFire EV1, 13 August 2012, BSI-DSZ-CC-0707-2012.
[JAVACARD]	Java Card System - Open Configuration Protection Profile, Version 2.6, Certified by ANSSI, the French Certification Body April, 19th 2010
[JIL]	Attack methods for Smart cards and similar devices, JIL, version 2.2, January 2013.
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.1, August 1st, 2011.
[NSP#6]	NSCIB Scheme Procedure #6 Alternative Evaluator Reporting, draft version 1.1.
[ST]	NXP J3E081_M64_DF, J3E081_M66_DF, J3E041_M66_DF,J3E016_M66_DF, J3E041_M64_DF and J3E016_M64_DF Secure Smart Card Controller Revision 3 Security Target, Rev. 01.02 — 13th August 2013, NSCIB-CC-13-37762
[ST-Lite]	NXP J3E081_M64_DF, J3E081_M66_DF, J3E041_M66_DF,J3E016_M66_DF, J3E041_M64_DF and J3E016_M64_DF Secure Smart Card Controller Revision 3 Security Target Lite, Rev. 00.03 — 13 August 2013, NSCIB-CC-13-37762
[ST-HW]	NXP Secure Smart Card Controllers P5CD016V1D / P5CD021V1D / P5CD041V1D / P5Cx081V1D with DESFire EV1 Security Target Lite, Rev 1.1, 24 October 2011, BSI-DSZ-CC-0707
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report).