**TÜV Rheinland Nederland B.V.**

Version 2016-2

# Certification Report

## JCOP 3 EMV P60

| | |
|---|---|
| Sponsor and developer: | ***NXP Semiconductors GmbH***<br>**Business Unit Security and Connectivity**<br>**Stresemannallee 101**<br>**D-22529 Hamburg**<br>**Germany** |
| Evaluation facility: | ***Brightsight***<br>**Delftechpark 1**<br>**2628 XJ Delft**<br>**The Netherlands** |
| Report number: | **NSCIB-CC-15-67351-CR** |
| Report version: | **1** |
| Project number: | **NSCIB-CC-15-67351** |
| Authors(s): | **Claire Loiseaux & Wouter Slegers** |
| Date: | **22 September 2016** |
| Number of pages: | **14** |
| Number of appendices: | **0** |

*Reproduction of this report is authorized provided the report is reproduced in its entirety.*

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

Headoffice:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek

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 with the
Amsterdam 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 4 (ISO/IEC 15408)

Certificate number
**CC-16-67351**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer
**NXP Semiconductors Germany GmbH, Business Unit Security and Connectivity**

**Stresemannallee 101, D-22529 Hamburg, Germany**

Product and assurance level
**JCOP 3 EMV P60**

Assurance Package:

- EAL5 augmented with AVA_VAN.5, ALC_DVS.2, ASE_TSS.2 and ALC_FLR.1

Protection Profile Conformance:

- Java Card Protection Profile – Open Configuration, Version 3.0, May 2012, published by Oracle, Inc.

Project number
**NSCIB-CC-15-67351**

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 EAL2

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.

SOGIS Mutual Recognition Agreement for components up to EAL7

Validity
Date of issue : **23-09-2016**
Certificate expiry : **23-09-2021**

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

TÜV Rheinland Nederland B.V.
P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

# CONTENTS:

**Foreword** 4

**Recognition of the certificate** 5

International recognition 5
European recognition 5

**1 Executive Summary** 6

**2 Certification Results** 7

2.1 Identification of Target of Evaluation 7
2.2 Security Policy 7
2.3 Assumptions and Clarification of Scope 8
2.4 Architectural Information 8
2.5 Documentation 9
2.6 IT Product Testing 9
2.7 Evaluated Configuration 11
2.8 Re-used evaluation results 11
2.9 Results of the Evaluation 11
2.10 Comments/Recommendations 12

**3 Security Target** 13

**4 Definitions** 13

**5 Bibliography** 14

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

# 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 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 satisfies the security requirements stated in the security target.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

## Recognition of the certificate

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate would indicate 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 nation

### International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting 8 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.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

# 1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the JCOP 3 EMV P60. The developer of the JCOP 3 EMV P60 is NXP Semiconductors 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.

This TOE is a composite TOE, consisting of a Java Card smart card operating system, a library which provides cryptographic functions, and an underlying platform, which is a secure micro controller. The TOE provides Java Card 3.0.4 functionality with post-issuance applet loading, card content management and secure channel features as specified in Global Platform 2.2.1 including SCP03. Cryptographic functionality includes AES, AES-CMAC, DES, Triple-DES (3DES), RSA, RSA-CRT and SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 hash algorithms and includes MAC and various modes of operation (e.g. ECB, CBC). Furthermore, the TOE provides random number generation according to class DRG.3 of AIS 20. Finally, it provides three communication protocols, i.e. ISO/IEC 7816 T=1, T=0 and ISO/IEC 14443 T=CL (contactless) over two physical interfaces (i.e. ISO/IEC 7816 and ISO/IEC 14443).

It includes a Configuration Applet for TOE configuration purposes and patch loading (Bulk Update feature) available at pre-personalisation. This Configuration Applet shall be removed at end of personalisation phase (phase 6). The TOE allows post-issuance downloading of Java Card applications (applets), provided these applets have been verified by an off-card trusted component. A Java Card application developer may develop applications (applets) that are loaded post-issuance to execute on the Java Card JCOP operating system. The Java Card applications are stored in persistent memory of the NXP hardware and are not part of the TOE.

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 Controller P6021J VB, certified under the German CC Scheme on 17 March 2016 (BSI-DSZ-CC-0955-2016 *[HW-CERT]*) and the Crypto Library V3.1.1 on P6021y VB, certified under Netherlands CC Scheme on 10 June 2016 (CC-16-66030-CR *[CL-CERT]*).

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on September 16, 2016 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 JCOP 3 EMV P60, 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 3 EMV P60 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 EAL5 augmented (EAL5+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) and AVA_VAN.5 (Advanced methodical vulnerability analysis), ASE_TSS.2 (TOE summary specification with architectural design summary) and ALC_FLR.1 (Basic flaw remediation).

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 JCOP 3 EMV P60. 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.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

# 2 Certification Results

## 2.1 *Identification of Target of Evaluation*

The Target of Evaluation (TOE) for this evaluation is the JCOP 3 EMV P60 from NXP Semiconductors GmbH located in Hamburg, Germany.

The TOE is comprised of the following main components:

| Type | Name | Version | Date | Form of delivery |
|---|---|---|---|---|
| Hardware | NXP Secure Smart Card Controller P6021y VB | P6021J VB (y = J)<br>Nameplate “9071C” | - | Based on [HW-ST] Section 1.4.1.3: waver, module, inlay, package |
| | Security IC Dedicated Software | | | |
| | Test ROM software | 10.1D | 25-04-2015 | |
| | Boot ROM software | 10.1D | 25-04-2015 | |
| | Firmware Operating System (FOS) | 0C.21,<br>0C.22 | 06-2015<br>01-2016 | |
| | Security IC Embedded Software | | | |
| | ROM Code (Platform ID) | JxHyyy00E4D80300 | - | |
| | Patch Code (Patch ID) | E4D8000000000004 | - | - |
| | Config Applet | 1.2 | - | - |

The Crypto Library V3.1.x (x=1) is part of the ROM Code and is used in its evaluated form. It is part of the Security IC Embedded Software and identified by the Platform Identifier.

To ensure secure usage, a set of guidance documents is provided together with the JCOP 3 EMV P60. 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. Applets can be loaded in ROM or EEPROM. Loading in ROM is possible in Phase 3. Loading of applets in EEPROM is possible in Phases 3, 4, 5 or 6. Applets are outside the scope of the TOE.

For a detailed and precise description of the TOE lifecycle refer to the *[ST]*, chapter 1.3.2.

## 2.2 *Security Policy*

The TOE provides Java Card 3.0.4 functionality with post-issuance applet loading, card content management and secure channel features as specified in Global Platform 2.2.1 including SCP03. Cryptographic functionality includes AES, AES-CMAC, DES, Triple-DES (3DES), RSA, RSA-CRT and SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 hash algorithms and includes MAC and various modes of operation (e.g. ECB, CBC). Furthermore, the TOE provides random number generation according to class DRG.3 of AIS 20. Finally, it provides three communication protocols, i.e. ISO/IEC 7816 T=1, T=0 and ISO/IEC 14443 T=CL (contactless) over two physical interfaces (i.e. ISO/IEC 7816 and ISO/IEC 14443).

The TOE includes a Configuration Applet for TOE configuration purposes and patch loading (Bulk Update feature) available at pre-personalisation. This Configuration Applet is removed at end of personalisation phase (phase 6).

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

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

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 provides access to random numbers generated by a software (pseudo) random number generator as part of the Java Card API. The TOE performs a test of the hardware (true) random number generator at initialisation and power-up.

The TOE implements Java Card 3.0.4 garbage collection and extended APDUs, Global Platform 2.2.1 CVM Management (Global PIN), Secure Channel Protocol (SCP01, SCP02, and SCP03), Card Manager that allows post-issuance installation and deletion of applets, packages and objects, DAP and Delegated Management. It complies to mapping guidelines and ID configuration.

The TOE additionally implements JCOP proprietary services: MIFARE functionality available from the hardware and via Java Card APIs, proprietary Java Card API (JCOPX API extension) for algorithms and utility functions.

## *2.3 Assumptions and Clarification of Scope*

### 2.3.1 Assumptions

Detailed information on the assumption and threats can be found in the *[ST]* sections 4.4 and 4.2 respectively. Detailed information on the security objectives that must be fulfilled by the TOE environment can be found in section 5.2 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.

Note that the scope of the evaluation did not include any applets besides the config applet. The config applet shall be deleted at the end of Phase 6 "Personalisation" before delivery according to the ST and the guidance.

Note also that the TOE includes other functionality such as a bulk update mechanism that is not evaluated for security functionality. These features have been examined to not impact the claimed security functionality.

## *2.4 Architectural Information*

The target of evaluation (TOE) is the JCOP 3 EMV P60. It consists of:

- Micro controller Hardware "NXP Secure Smart Card Controller P6021y VB" used as evaluated platform (BSI-DSZ-CC-0955) including IC Dedicated Software: Micro Controller Firmware and Native MIFARE application (physically always present but logical availability depends on configuration)
- Cryptographic Library V3.1.x on P6021y VB built upon this hardware platform (NSCIB-CC-16-66030) – minor version V3.1.1
- Embedded software (Java Card Virtual Machine, Runtime Environment, JCOP OS "svn58584" (Java Card API, Card Manager, GlobalPlatform framework) which is built upon this hardware platform and using the Crypto Library
- Patch code"E4D8000000000004"
- Config Applet v1.2

The TOE is a Java Card (version 3.0.4) smart card allowing post-issuance loading of applications using the Global Platform (version 2.2.1) framework. It includes a Config Applet for TOE configuration and patch loading (Bulk Update) purposes. The Config Applet can be used pre-issuance according to the *[ST]* and guidance and shall be deleted prior issuance in the operational phase.

The TOE does not include any software on the application layer (Java Card applets). See *[ST]* section 1.2 and 1.3 for details.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

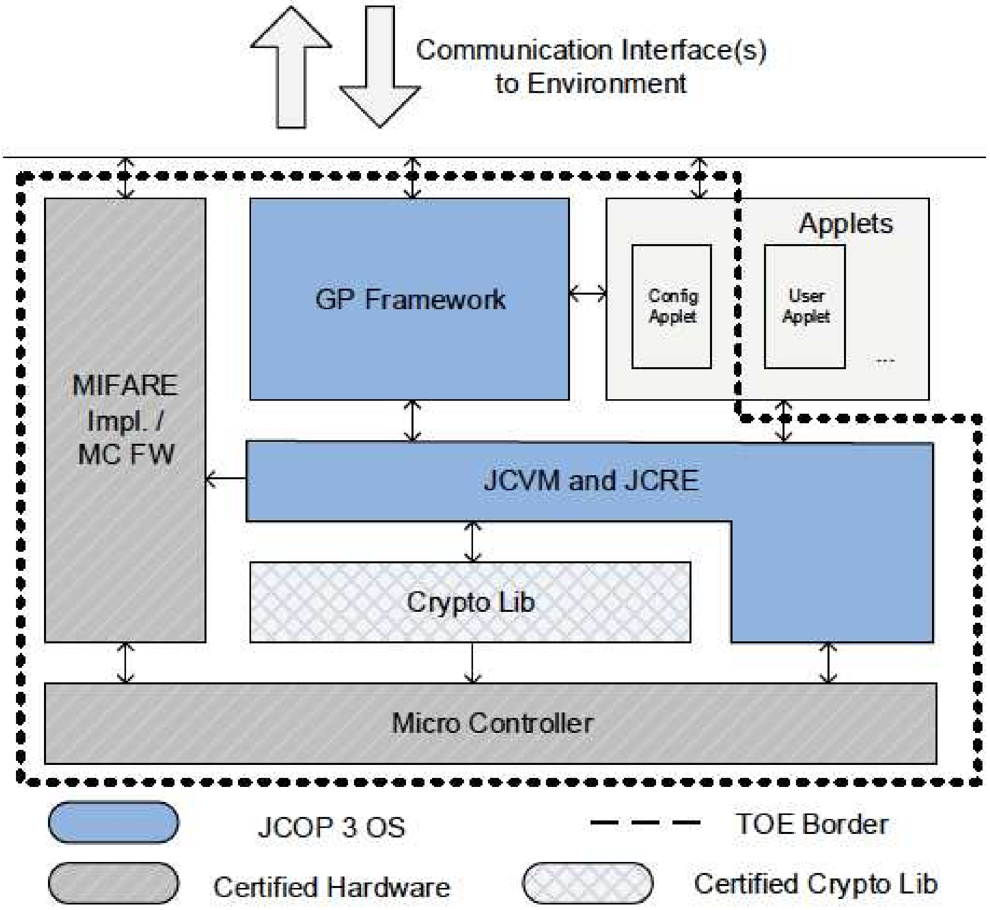

**Fig. 1.1:** Components of the TOE

## *2.5 Documentation*

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

| Identifier | Version | Issue Date |
|---|---|---|
| JCOP 3 EMV P60, User Guidance and Administrator Manual | 3.1 | 2015-12-04 |
| Objective Data Sheet: SmartMX2 family P6021y VB Secure high-performance smart card controller | 3.1 | 2016-01-15 |

## *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, module and module interface level. The developer used a set of test suites (industry standard and proprietary ones) and tools, which

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

were used to test the TOE in its final configuration as well as in an emulator, PC and FPGA tool as some tests can only be performed on such environment. The list is provided in *[ETR]* in Table 8. The test tools and scripts are extensively used to verify that the tests return expected values.

All parameter choices, also for the module interface level, have been addressed at least once; all the cryptographic operations with keys of all key sizes have been tested at least once. All boundary cases identified have been tested explicitly, and additionally the near-boundary conditions have been covered probabilistically.

The evaluator used an acceptable alternative approach (as described in the application notes, Section 14.2.2 in *[CEM]*) and used analysis of the implementation representation (i.e. inspection of source code) on few occasions. See the *[ETR]* for details.

The cryptographic algorithms have been validated as part of the Crypto Library evaluation (as stated in Section 5.4 of *[CL_ETRfC]*).

The protection against side channel analysis and perturbation attacks has been verified by performing code inspection on the countermeasures in the implementation representation of the JCOP OS, on key handling by the operating system and operations not provided by the hardware or Crypto Library.

### 2.6.2 Independent Penetration Testing

The penetration tests are devised after performing the Evaluator Vulnerability Analysis. The reference for attack techniques against which smart card-based devices controllers such as the TOE must be protected against is the document named "Attack methods for smart cards" and referenced as *[JIL-AM]*. The susceptibility of the TOE for these attacks has been analysed in a white box investigation conforming to AVA_VAN.5. This analysis has followed the following steps:

1. *Inventory of required resistance*
   This step uses the JIL attack list as described in *[JIL-AM]* as a reference for completeness and studies the ST claims to decide which attacks in the JIL attack list apply for the TOE.
2. *Validation of security functionalities*
   This step identifies the implemented security functionalities and performs tests to verify implementation and to validate proper functioning (ATE).
3. *Vulnerability analysis*
   This step first gives an overview against which attacks the implemented security functionalities are meant to provide protection. Secondly in this step the design of the implemented security functionalities is studied. Thirdly, an analysis is performed to determine whether the design contains vulnerabilities against the respective attacks of step1 (AVA).
4. *Analysis of input from other evaluation activities*
   This step first analyses the input from other CC-evaluation classes expressed as possible vulnerabilities. Secondly, the evaluators made an analysis of the TOE in its intended environment to check whether the developer vulnerability analysis provides sufficient assurance or whether penetration testing is needed to provide sufficient assurance (AVA).
5. *Design assurance evaluation*
   This step analyses the results from an attack perspective as defined in step 1. Based on this design analysis the evaluators determine whether the design provides sufficient assurance or whether penetration testing is needed to provide sufficient assurance (AVA).
6. *Penetration testing*
   This step performs the penetration tests identified in step 4 and step 5 (AVA).
7. *Conclusions on resistance*
   This step performs a *[JIL-AM]* 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 draw conclusions on the resistance of the TOE against attackers possessing a high attack potential.

Side channel attack resistance is mostly provided by the underlying crypto library and assessed in that certification, so one side channel analysis attack on the key handling was performed. Perturbation attack resistance was tested with 6 light and 2 EMFI attacks. No exploitable vulnerabilities were found.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

### 2.6.3 Test Configuration

The developer provided the evaluator with the TOE in a DIL and CLCC68 package in pre-personalised state. For penetration tests, TOEs with certain countermeasures disabled and specific patch code was 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.

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.

The strength of the implementation of the cryptographic functionality has been assessed in the evaluation, as part of the AVA_VAN activities. These activities revealed that for some cryptographic functionality the security level could be reduced. As the remaining security level still exceeds 80 bits, this is considered sufficient. So no exploitable vulnerabilities were found with the independent penetration tests.

For composite evaluations, please consult the *[ETRfC]* for details.

## *2.7 Evaluated Configuration*

The TOE is defined uniquely by its name and version number JCOP 3 EMV P60.

## *2.8 Re-used evaluation results*

This is a new certification.

No sites have been visited as part of this evaluation. There has been extensive re-use of the ALC aspects for the sites involved in the software component of the TOE. We provide here the list of sites and corresponding certificates:

| Site | Reference | Issuance date |
|---|---|---|
| NXP HTC60 Eindhoven | NSCIB-SS-13-38181-CR2 | 15 June 2016 |
| ATOS Bydgoszcz Poland | NSCIB-SS-13-38175-CR2 | 15 June 2016 |
| NXP Hamburg | BSI-DSZ-CC-0857-V2-2015 | 27 April 2015 |
| NXP Gratkorn | BSI-DSZ-CC-S-0042-2015 | 17 August 2015 |
| NXP Bangalore | BSI-DSZ-CC-858-V2-2015 | 27 April 2015 |

## *2.9 Results of the Evaluation*

The evaluation lab documented their evaluation results in the *[ETR]*[2] which references the ASE Intermediate Report and other NSP#6-compliant evaluator documents. To support composite evaluations according to *[CCDB-2012-04]* 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.

The verdict of each claimed assurance requirement is **"Pass"**.

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

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

Based on the above evaluation results the evaluation lab concluded the JCOP 3 EMV P60,to be **CC Part 2 extended**, **CC Part 3 conformant** and to meet the requirements of **EAL 5 augmented with AVA_VAN.5, ALC_DVS.2, ASE_TSS.2 and ALC_FLR.1**. This implies that the product satisfies the security technical requirements specified in *[ST]*.

The Security Target claims 'demonstrable' conformance to the Java Card Protection Profile – Open Configuration, Version 3.0, 18 May 2012 Published by Oracle, Inc registered and certified by ANSSI under the reference ANSSI-PP-2010/03-M01.

## 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. 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).

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

# 3 Security Target

The JCOP 3 EMV P60, Security Target, Rev. 3.1, dated 2016-05-10 *[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:

| | |
|---|---|
| AES | Advanced Encryption Standard |
| AIS | Anwendungshinweise und Interpretationen zum Schema |
| CBC | Cipher Block Chaining (a block cipher mode of operation) |
| DES | Data Encryption Standard |
| ECB | Electronic Code Book (a block cipher mode of operation) |
| ECC | Elliptic Curve Cryptography |
| IC | Integrated Circuit |
| IT | Information Technology |
| ITSEF | IT Security Evaluation Facility |
| JIL | Joint Interpretation Library |
| MAC | Message Authentication Code |
| NSCIB | Netherlands scheme for certification in the area of IT security |
| PP | Protection Profile |
| RSA | The cryptographic algorithm proposed by Rivest, Shamir and Adleman` |
| SHA | Secure Hash Algorithm |
| TOE | Target of Evaluation |

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

# 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 4, September 2012.

[CCDB-2012-04] Mandatory Supporting Technical Document, Composite product evaluation for Smart Cards and similar devices, April 2012, Version 1.2.

[CEM] Common Methodology for Information Technology Security Evaluation, version 3.1, Revision 4, September 2012.

[CL-CERT] Certification Report Crypto Library V3.1.x on P6021y VB, NSCIB-CC-16-66030-CR, dated June 2nd, 2016.

[CL_ETRfC] ETR for Composite Evaluation Crypto Library V3.1.x on P6021y VB EAL6+/5+, 15-RPT-252, v7.0, April 25, 2016.

[ETR] Evaluation Technical Report NXP JCOP 3 EMV P60 EAL5+, Reference: 16-RPT-207, v5.0, September 15th, 2016.

[ETRfC] Evaluation Technical Report for Composition NXP JCOP 3 EMV P60 EAL5+, Reference: 15-RPT-368 v9.0, September 15th, 2016.

[HW-CERT] Certification report BSI-DSZ-CC-0955-2016 for NXP Secure Smart Card Controller P6021y VB including IC Dedicated Software, dated 17 March 2016.

[HW-ST] NXP Secure Smart Card Controller P6021y VB, Security Target, Rev. 0.93, 2016-01-25.

[JIL-AM] JIL, Attack Methods for Smartcards and Similar Devices (controlled distribution), Version 2.2, January 2013.

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.2, August 10th, 2015.

[SOGIS-2015-02] JIL-Composite-product-evaluation-for-Smart-Cards-and-similar-devices-v1-3 - feb 2015.

[ST] JCOP 3 EMV P60, Security Target, Rev. 3.1, dated 2016-05-10.

[ST-lite] JCOP 3 EMV P60, Security Target Lite, Rev. 3.1, dated 2016-05-10.

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

(This is the end of this report).

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.