Certification Report

NXP JCOP 3 SECID P60 (OSA)

Sponsor and developer: ***NXP Semiconductors GmbH***
Business Unit Security & Connectivity
Stresemannallee 101
22505 Hamburg, Germany

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

Reportnumber:	**NSCIB-CC-16-99111-CR**
Report version:	**1**
Projectnumber:	**NSCIB-CC-16-99111**
Authors(s):	**Wouter Slegers**
Date:	**10 August 2016**
Number of pages:	**13**
Number of appendices:	**0**

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 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 4 (ISO/IEC 15408)
Certificate number	**CC-16-99111-CR**

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	**NXP JCOP 3 SECID P60 (OSA),** Assurance Package: ▪ EAL5 augmented with AVA_VAN.5, ALC_DVS.2, ASE_TSS.2 and ALC_FLR.1 Protection Profile Conformance: ▪ ANSSI-PP-2010/03-M01: Java Card Protection Profile – Open Configuration, Version 3.0, May 2012
Project number	**NSCIB-CC-16-99111-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 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 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	: **10-08-2016**
	Certificate expiry	: **10-08-2021**

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

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 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.

TÜVRheinland®
Precisely Right.

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.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the NXP JCOP 3 SECID P60 (OSA). The developer of the NXP JCOP 3 SECID P60 (OSA) 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.

The 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, DES, Triple-DES (3DES), RSA, RSA-CRT, RSA key-generation, ECC over GF(p), ECC over GF(P) key generation, ECC over GF(p) secure point addition, and SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 hash algorithms and includes MAC, CMAC 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).

Note that Match-on-Card (MoC) libraries are included in the TOE, but as there are no security claims on these, the biometric functionality has not been assessed, only the self-protection of the TSF.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on August 8th 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 NXP JCOP 3 SECID P60 (OSA), 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 NXP JCOP 3 SECID P60 (OSA) 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 EAL5augmented (EAL5(+)) assurance requirements for the evaluated security functionality. This assurance level is augmented with ASE_TSS.2 (ST TOE Summary Specification), ALC_FLR.1 (Flaw remediation), ALC_DVS.2 (Sufficiency of security measures) 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 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 JCOP 3 SECID P60 (OSA) 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 JCOP 3 SECID P60 (OSA) 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 P6022y VB	P6022J VB Nameplate “9072B”	18 January 2016	Based on [HW-ST] Section 1.4.1.3: TOE Components
	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.22, 0C.32	01-2016 01-2016	
	Security IC Embedded Software			
	ROM Code (Platform ID)	JxHyyy0005860400 (SVN 0x0586=1414)	-	
	Patch Code (Patch ID)	02 00 00 00 00 00 00 00 (Patch 02)	-	

To ensure secure usage a set of guidance documents is provided together with the NXP JCOP 3 SECID P60 (OSA). Details can be found in section 2.5 of this report.

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

2.2 Security Policy

The 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, DES, Triple-DES (3DES), RSA, RSA-CRT, RSA key-generation, ECC over GF(p), ECC over GF(P) key generation, ECC over GF(p) secure point addition, and SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 hash algorithms and includes MAC, CMAC 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).

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.

Details can be found in the Security Target *[ST]* section 4.8.

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 MoC libraries are included in the TOE, but as there are no security claims on these, the biometric functionality has not been assessed, only the self-protection of the TSF.

2.4 Architectural Information

The logical architecture of the TOE can be depicted as follows (based on *[ST]*):

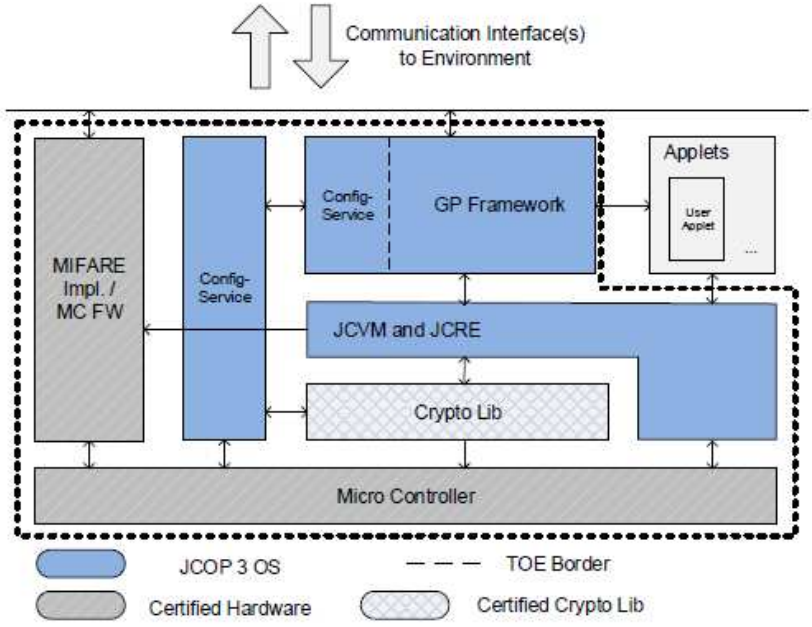

Fig. 1.1: Components of the TOE

The TOE is a composite TOE consisting of the following components:

- Hardware “NXP Secure Smart Card Controller P6022y VB including IC Dedicated Software” used as evaluated platform *[HW-CERT];*
- Cryptographic Library: “Crypto Library V3.1.x on P6022y VB” built upon this hardware platform (NSCIB-CC-15-67206) *[CL-CERT];*
- JCOP OS “svn1414” which is built upon this hardware platform and using the Crypto Library;
- Patch code “0200000000000000”.

The respective identifiers for the hardware and the Crypto Library (platform) are as follows:

- **Hardware:** “NXP Secure Smart Card Controller P6022y VB including IC Dedicated Software” where only the P6022J VB configuration is allowed for this TOE;
- **Cryptographic Library:** “Crypto Library V3.1.x on P6022y VB” where only the V3.1.2 version is allowed for this TOE.

2.5 Documentation

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

Type	Name	Version	Date	Form of delivery
Document	User Guidance and Administrator Manual	1.5	26-07-2016	Electronic document
	ES_JCOP 3 SECID P60 (OSA) Errata Sheet,	1.2	26-07-2016	Electronic document
	ES_JCOP 3 SECID P60 (OSA) Errata Sheet for Morpho,	1.1	26-07-2016	Electronic document
	Objective Data Sheet SmartMX2 family P6022y VB Secure high-performance smart card controller	2.0	15-01-2016	Electronic document
	HW Wafer and delivery specification	2.2	08-03-2016	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 FSP, subsystem, module and module interface level. The tests are performed by NXP through execution of the test scripts using an automated and distributed system. 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 developer tests are extensive and as such evaluator testing would lead to tests that are only superficially different from testing performed by the developer. As a result, the evaluator judged that tests should be defined that are supplementing the developer's tests and should be based on how adequate the TOE security functions are implemented rather than on how well the various industry standards are met. Further focus of the defined tests was on proprietary functionality and behaviour of disabled functionality (since some Java Card functions are disabled on this TOE).

2.6.2 Independent Penetration Testing

The penetration tests are devised after performing the Evaluator Vulnerability Analysis. The reference for attack techniques against smart card-based devices 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 to 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 attacks of step 1 (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.

A number of penetration tests were performed on an earlier TOE version. For this evaluation an analysis was performed that allowed full use of the penetration test results. For a summary of VA results (AVA_VAN.5-5), see *[ETR]*.

The TOE is a composite with the hardware IC and Crypto Library. As a result a high degree of assurance originates from these two composite parts and they provide assurance for protection against attacks.

2.6.3 Test Configuration

Testing was performed on the following TOE test configurations:

Component	Versions
Hardware IC	P6022y VB where y = J (P6022J VB) in DIL24 and CLCC68 packaging
Crypto Library	“Crypto Library V3.1.x on P6022y VB” with minor version (x = 2) resulting in V3.1.2
JCOP OS	“JxHyyy0005860400 (SVN 1414)”
Patch code	“E1 00 00 00 00 00 00 00 (Patch 01 + attack counter patch)” or “E2 00 00 00 00 00 00 00 (Patch 02 + attack counter patch)”

Table 1. Test configuration

Testing was performed by employing test applets using TSFIs: JC_A and GP_CAD over the IEO/IEC 7816 T=0 interface.

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 algorithmic security level exceeds 100 bits for all evaluated cryptographic functionality as required for high attack potential (AVA_VAN.5).

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 NXP JCOP 3 SECID P60 (OSA).

2.8 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[2] which references the ASE Intermediate Report 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.

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

Based on the above evaluation results the evaluation lab concluded the NXP JCOP 3 SECID P60 (OSA) to be **CC Part 2 extended**, **CC Part 3 conformant**, 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 Security Target *[ST]*.

Security Target claims demonstrable conformance to the Java Card Protection Profile - Open Configuration, Version 3.0, Certified by ANSSI, the French Certification Body May, 2012. This TOE does not support the optional Java Card RMI.

2.9 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 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).

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

3 Security Target

The JCOP 3 SECID P60 (OSA) Security Target, revision 1.4, dated 2016-08-08 *[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
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
MAC	Message Authentication Code
NSCIB	Nederlands Schema voor Certificatie op het gebied van IT-Beveiliging
PP	Protection Profile
RMI	Remote Method Invocation
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
TOE	Target of Evaluation

TÜVRheinland®
Precisely Right.

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.
[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 P6022y VB, document reference NSCIB-CC-15-67206-CR, dated July 28th, 2016.
[CL-ETRfC]	ETR for Composite Evaluation Crypto Library V3.1.x on P6022y VB EAL6+/5+, Document reference 16-RPT-208, version 2.0, dated 2016-07-04.
[CL-ST]	Crypto Library V3.1.x on P6022y VB Security Target, Rev. 1.5, June 27, 2016.
[ETR]	Evaluation Technical Report NXP JCOP 3 SECID P60 (OSA) EAL5+, document reference 16-RPT-287 version 2.0, dated 8 August 2016.
[ETRfC]	ETR for Composition Evaluation NXP JCOP 3 SECID P60 (OSA) EAL5+, document reference 16-RPT-288 version 6.0, dated 8 August 2016.
[HW-CERT]	Certification report NXP Secure Smart Card Controller P6022y VB including IC Dedicated Software, BSI-DSZ-CC-0973-2016, 17 June 2016.
[HW-ETRfC]	ETR for Composite Evaluation - P6022y VB, version 2, 14 June 2016.
[HW-ST]	NXP Secure Smart Card Controller P6022y VB, Security Target, Rev. 1.11, 14 June 2016.
[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.
[ST]	JCOP 3 SECID P60 (OSA) Security Target, revision 1.4, dated 2016-08-08.
[ST-lite]	JCOP 3 SECID P60 (OSA) Security Target Lite, revision 1.2, dated 2016-08-08.
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.

(This is the end of this report).