Version 2021-04

Certification Report

JCOP 3 P60

Sponsor and developer:	***NXP Semiconductors GmbH*** **Business Unit Security & Connectivity** **Troplowitzstrasse 20** **22529 Hamburg** **Germany**
Evaluation facility:	***Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-98209-CR5**
Report version:	**5**
Project number:	**98209**
Author(s):	**Kjartan Jæger Kvassnes**
Date:	**23 July 2021**
Number of pages:	**14**
Number of appendices:	**0**

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

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

Head Office:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS

® 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 licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

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

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

Recognition of the Certificate

The presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

® 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 P60. The developer of the JCOP 3 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.

The TOE is a composite TOE, consisting of a Java Card operating system, a library which provides cryptographic functions, and an underlying platform, which is a secure microcontroller. The TOE provides Java Card 3.04 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. It includes a configuration service for TOE configuration and patch loading purposes. The Secure Box feature allows providing native functions to applets through a Secure Box Native Library. 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).

Please note that a Secure Box Native Library is not part of the TOE, the Secure Box feature however is a part of the TOE.

The TOE was evaluated initially by Brightsight B.V located in Delft, The Netherlands and was certified on 02-08-2017. The TOE was recertified on 15 January 2018 and maintained on 19 May 2018, followed by recertification on 29 November 2018 and maintenance on 29 July 2019, and a further recertification that was completed on 14 January 2020. This re-evaluation of the TOE has also been conducted by Brightsight B.V and was completed on 20 July 2021 with the approval of the ETR. The re-certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

This fifth issue of the Certification Report is a result of a “recertification with major changes”.

As in the previous re-certification, the major changes are the recertification of the hardware platform with changes. To the guidance, the recertification of the cryptographic library, and associated change to the TOE´s guidance and ST.

For clarity to composite evaluations and certifications, this certification report has been updated to explicitly state that the additional minor hardware configurations were removed for the underlying hardware recertification [HW-CERT].

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

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the JCOP 3 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 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 the TOE meets the EAL5 augmented (EAL5+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ASE_TSS.2 (TOE Summary Specification), ALC_FLR.1 (Flaw Remediation), ALC_DVS.2 (Sufficiency of security measures) and AVA_VAN.5 (Advanced methodical vulnerability analysis).

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

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

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

® 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 P60 from NXP Semiconductors GmbH located in Hamburg, Germany.

The TOE is comprised of the following main components:

Component type	Name	Version	Form of delivery
Hardware (platform)	NXP Secure Smart Card Controller P6022y VB	P6022J VB (y = J) Nameplate "9072B" 18 January 2016	wafer, module, inlay, package
IC dedicated Software	Test ROM software	10.1D 25-04-2015	On-Chip-software
	Boot ROM software	10.1D 25-04-2015	On-Chip-software
	Firmware Operating System (FOS)	0C.60, 04-2016 0C.70, 04-2016	On-Chip-software
	Test ROM software	10.1D, 25-04-2015	On-Chip-software
	Crypto Library V3.1.x on P6022y VB" (NSCIB-CC-15-67206-CR3)	V3.1.2	On-Chip-software
Software TOE	OSB RC9;		On-Chip Software
	Rom Code (Platform ID): svn6521	JxHyyy0019790400	
	Patch Code (Patch ID): ○ 03 00 00 00 00 00 00 00 (PL3) ○ 04 00 00 00 00 00 00 00 (PL4)		
	OSC RC9.		On-Chip Software
	ROM Code (Platform ID) : svn7702	JxHyyy0077020400	
	Patch code (platform ID): ○ 01 00 00 00 00 00 00 00 (PL1)		

To ensure secure usage a set of guidance documents is provided, together with the JCOP 3 P60. For details, see section 2.5 "Documentation" of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 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 functions 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

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

various modes of operation (e.g. ECB, CBC). Furthermore, the TOE provides random number generation according to class DRG.3 of AIS 20. It includes a configuration service for TOE configuration and patch loading purposes. 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. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 5.2 of the *[ST]*.

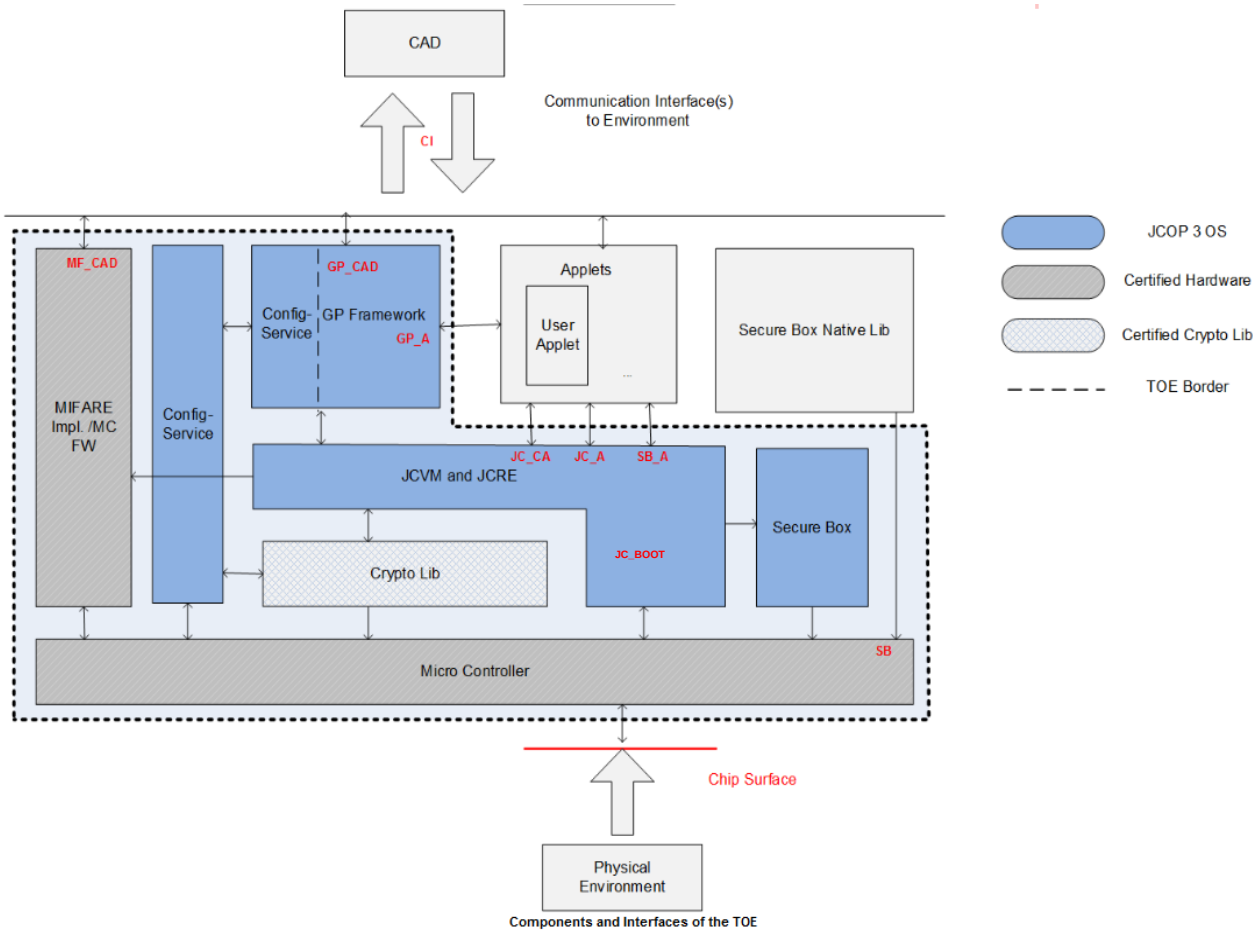
2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

Note that a Secure Box Native Library is not part of the TOE, the Secure Box feature however is a part of the TOE.

2.4 Architectural Information

The architecture of the TOE is as follows:



Components and Interfaces of the TOE

The TOE is a composite TOE, consisting of:

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

- **Hardware** “NXP Secure Smart Card Controller P6022y VB including IC dedicated software” used as evaluated platform [HW-CERT], where only the P6022J VB (y=J) configuration os allowed for this TOE.
- **Cryptographic Library** “Crypto Library V3.1.x on P6022y VB” built upon this hardware platform [CL-CERT], where only the V3.1.2 version is allowed for this TOE.
- **Operating System** “JCOP OS” built upon this hardware platform and using the crypto library as follows:
  - “svn6521”, or
  - “svn7702”
- **Patch code** as follows:
  - For “svn6521”: “03 00 00 00 00 00 00 00 (PL3)” or “04 00 00 00 00 00 00 00 (PL4)”
  - For “svn7702”: “01 00 00 00 00 00 00 00 (PL1)”

The TOE is a Jaca Card (version 3.0.4) smart card allowing post-issuance of applications using the Global Platform (version 2.2.1) framework. It includes a configuration service for TOE configuration and patch loading purposes. Please note that HMAC is not supported. The Secure Box feature allows providing native functions to applets through a Secure Box Native Library. Please note that a secure box Native Library is not part of the TOE, the Secure Box feature is however part of the TOE. The MIFARE and FIDO U2F related functionality is not part of the evaluation.

2.5 Documentation

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

For EMV and Secure ID Use Cases:

Type	Name	Version	Date
Electronic Document	User Guidance and Administrator Manual	3.6	26-05-2021
Electronic Document	ES_JCOP 3 SECID P60 CS (OSB) Errata Sheet	2.6	26-05-2021
Product Data Sheet	SmartMX2 family P6022y VB Secure high-performance smart card controller	3.6	22-08-2019
Electronic Document	HW Wafer and delivery specification	3.3	12-07-2019

For Fingerprint and Token Use Cases:

Type	Name	Version	Date
Electronic Document	User Guidance and Administrator Manual	1.8	05-02-2021
Electronic Document	ES_JCOP3 SECID P60 Errata Sheet	1.1	25-05-2021
Product Data Sheet	SmartMX2 family P6022y VB Secure high-performance smart card controller	3.6	22-08-2019
Electronic Document	HW Wafer and delivery specification	3.3	12-07-2019

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

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

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

For the testing performed by the evaluators, the developer provided samples and a test environment. The evaluators 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 testing was conducted according to the following testing approach:

- When evaluating the evidence in the classes ASE, ADV and AGD, the evaluator considers whether potential vulnerabilities can already be identified due to the TOE type and/or specified behaviour in such an early stage of the evaluation.
- For ADV_IMP a thorough implementation representation review is performed on the TOE. During this attack oriented analysis, the protection of the TOE is analysed using the knowledge gained from all previous evaluation classes. This results in the identification of (additional) potential vulnerabilities. For this step, analysis will be performed according to the attack methods in [JIL-AM]. An important source for assurance in this step is the technical report [ETRfC-HW] and [ETRfC-CL] of the underlying platform.
- All potential vulnerabilities are analysed using the knowledge gained from all evaluation classes and information from the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. The potential vulnerabilities are addressed by penetration testing, a guidance update or in other ways that are deemed appropriate.
- During the re-certification, the vulnerability analysis was re-assessed. This showed that part of the test results was outdated. To address this, a number of representative tests have been performed to provide assurance and validate outdated tests

The total test effort expended by the evaluators was 10 weeks. During that test campaign, 25% of the total time was spent on Perturbation attacks, 50% on side-channel testing, and 25% on logical tests.

2.6.3 Test configuration

The TOE was tested in the following configurations:

- OS: JCOP 3 P60 Platform ID: "JxHyyy0019790400", Patch ID: "03 00 00 00 00 00 00 00"
- OS: JCOP 3 P60 Platform ID: "JxHyyy0077020400", Patch ID: "01 00 00 00 00 00 00 00"

2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

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

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 from an algorithmic security level above 100 bits to a practical remaining security level lower than 100 bits. The remaining security level still exceeds 80 bits, so this is considered sufficient. Therefore, no exploitable vulnerabilities were found with the independent penetration tests.

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

2.7 Reused Evaluation Results

This is a re-certification. Documentary evaluation results of the earlier version of the TOE have been reused, but vulnerability analysis and penetration testing has been renewed.

Sites involved in the development and production of the hardware platform and Crypto library where re-used by composition

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of four STAR reports.

- NXP Semiconductors Hamburg
- NXP Semiconductors Austria GmbH Styria
- NXP Bangalore
- NXP Glasgow 2

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number JCOP 3 P60 as described in the identification part of this report.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an 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 must 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 JCOP 3 P60, to be **CC Part 2 extended, CC Part 3 conformant**, (check ST compliance claim) 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 requirements specified in Security Target *[ST]*.

The Security Target claims ‘strict’ conformance to the Protection Profile *[PP]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 “Documentation” contains necessary information about the usage of the TOE. Certain aspects of the TOE’s security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the

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

customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations:

- MIFARE and FIDO U2F support (as there are no security claims)

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength to satisfy the AVA_VAN.5 “high attack potential”. To be protected against attackers with a "high attack potential", appropriate cryptographic algorithms with sufficiently large cryptographic key sizes shall 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 P60 Security target, Rev. 4.3, 10 June 2021 *[ST]* is included here by reference.

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

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

AES	Advanced Encryption Standard
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)
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
EMA	Electromagnetic Analysis
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
PACE	Password Authenticated Connection Establishment
PKI	Public Key Infrastructure
PP	Protection Profile
RMI	Remote Method Invocation
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
SPA/DPA	Simple/Differential Power Analysis
TRNG	True Random Number Generator

® 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 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[CL-CERT]	NSCIB-CC-67206-CR5 Certification Report Crypto Library V3.1.x on P6022y VB, Version 1.0, 07 July 2021
[CL-ETRfC]	ETR for Composite Evaluation Crypto Library V3.1.x on P6022y VB EAL6+, 18-RPT-116, version 9.0, 06 July 2021.
[CL-ST]	Crypto Library V3.1.x on P6022y VB Security Target, Rev. 2.0, 22 March 2018
[ETR]	Evaluation Technical Report "JCOP 3 P60" – EAL5+, 21-RPT-589, Version 3.0, 16 July 2021
[ETRfC]	Evaluation Technical Report for Composition "JCOP 3 P60" – EAL5+,21-RPT-290, Version 3.0, 16 July 2021
[HW-CERT]	BSI-DSZ-CC-1059-V4-2021 for NXP Secure Smart Card Controller P6022y VB* including IC Dedicated Software from NXP Semiconductors Germany GmbH, 24 June 2021
[HW-ETRfC]	Evaluation Technical for Composite Evaluation (ETR COMP) for the P6022y VB VB, version 2, 2021-05-31
[HW-ST]	Security Target Lite BSI-DSZ-CC-1059-V4-2021, NXP Secure Smart Card Controller P6022y VB – Security Target Lite, Version 2.8, 2021-03-09
[JIL-AM]	Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution)
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[PP]	Java Card Protection Profile – Open Configuration, Version 3.0, May 2012 Published by Oracle, Inc. registered and certified by ANSSI under the reference ANSSI-PP-2010/03-M01
[ST]	JCOP 3 P60 Security target, Rev. 4.3, 10 June 2021
[ST-lite]	JCOP 3 P60 Security Target Lite Rev. 4.3 — 10 June 2021
[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.