Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0730-2011

for

NXP J3A040 & J2A040 Secure Smart Card Controller Revision 3

from

NXP Semiconductors Germany GmbH

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0730-2011

Smart Card with Java Card Platform

NXP J3A040 & J2A040 Secure Smart Card Controller Revision 3

from	NXP Semiconductors Germany GmbH
PP Conformance:	None
Functionality:	Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5

Common Criteria
Recognition
Arrangement
for components up to
EAL 4

Common Criteria

The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

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 certification scheme of the German Federal Office for Information Security (BSI) 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 the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 25 May 2011
For the Federal Office for Information Security

INFORMATION TECHNOLOGY SECURITY
SOGIS
IT SECURITY CERTIFIED
MUTUAL RECOGNITION AGREEMENT

Bernd Kowalski
Head of Department

L.S.

This page is intentionally left blank.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

Contents

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1 European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and in addition at higher recognition levels for IT-Products related to certain technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic).

The new agreement was initially signed by the national bodies of Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom.

[2] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

[3] Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

[4] Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

[5] Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

Within the terms of this agreement the German Federal Office for Information Security (BSI) recognises

- for the basic recognition level certificates issued as of April 2010 by the national certification bodies of France, The Netherlands, Spain and the United Kingdom.
- for the higher recognition level in the technical domain Smart card and similar Devices certificates issued as of April 2010 by the national certification bodies of France, The Netherlands and the United Kingdom.

In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement.

Historically, the first SOGIS-Mutual Recognition Agreement Version 1 (ITSEC only) became initially effective in March 1998. It was extended in 1999 to include certificates based on the Common Criteria (MRA Version 2). Recognition of certificates previously issued under these older versions of the SOGIS-Mutual Recognition Agreement is being continued.

2.2 International Recognition of CC – Certificates (CCRA)

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of January 2009 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the web site: http://www.commoncriteriaportal.org

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement.

This evaluation contains the components ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2, ATE_DPT.3 and AVA_VAN.5 that are not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4 components of these assurance families are relevant.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product NXP J3A040 & J2A040 Secure Smart Card Controller Revision 3 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0674-2011. Specific results from the evaluation process BSI-DSZ-CC-0674-2011 were re-used.

The evaluation of the product NXP J3A040 & J2A040 Secure Smart Card Controller Revision 3 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 19 May 2011. The TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is:

NXP Semiconductors Germany GmbH.

The product was developed by:

NXP Semiconductors Germany GmbH.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

4 Validity of the Certification Result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report and in the Security Target.

For the meaning of the assurance levels please refer to the excerpts from the criteria at the end of the Certification Report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

5 Publication

The product NXP J3A040 & J2A040 Secure Smart Card Controller Revision 3 has been included in the BSI list of the certified products, which is published regularly (see also Internet: https://www.bsi.bund.de/ and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

[6] Information Technology Security Evaluation Facility

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] NXP Semiconductors Germany GmbH
Stresemannallee 101
22529 Hamburg

B Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1 Executive Summary

The Target of Evaluation (TOE) is the product NXP J3A040 and J2A040 Secure Smart Card Controller Revision 3, also referred to shortly as JCOP v2.4.1 R3. The product type is identified as Java Card on the hardware P5CD040V0B and P5CC040V0B (BSI-DSZ-CC-0404-2007 [18]) including a crypto library (BSI-DSZ-CC-0710-2010 [15]). The TOE consists of the following components:

- Smart card platform (SCP) (parts of the hardware platform and hardware abstraction layer) and
- Embedded software (Java Card Virtual Machine, Runtime Environment, Java Card API, Card Manager).

The J3A040 Secure Smart Card Controller Revision 3 also includes the

- Native MIFARE application (physically present but logically disabled in minor configuration “MIFARE Emulation = A” and logically enabled in the minor configurations “MIFARE Emulation = B1” and “MIFARE Emulation = B4” (see section 2.2.4 of the hardware Security Target [19])).

The TOE is based on Java Card 2.2.2 and GlobalPlatform 2.1.1 industry standards. It does not include any software on the application layer (Java Card applets) whereby the TOE does not include some parts of the certified hardware platform [18]. For details refer to the Security Target [6] and [8].

The Security Target [6] is the basis for this certification. It does not claim conformance to any Protection Profile (PP) but it is based on the CC 2.1 certified Java Card PP [7].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [8], chapter 6.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionalities:

TOE Security Functionality	**Addressed issue**
SF.AccessControl	Enforces the access control
SF.Audit	Audit functionality
SF.CryptoKey	Cryptographic key management
SF.CryptoOperation	Cryptographic operation
SF.I&A	Identification and authentication
SF.SecureManagement	Secure management of TOE resources
SF.PIN	PIN management
SF.Transaction	Transaction management
SF.Hardware	TSF of the underlying IC
SF.CryptoLib	TSF of the certified crypto library

Table 1: TOE Security Funktionalities

For more details please refer to the Security Target [6] and [8], chapter 7.1.

The assets to be protected by the TOE are defined in the Security Target [6] and [8], chapter 3.2. Based on these assets the TOE Security Environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [8], chapter 3.3, 3.4 and 3.5.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

NXP J3A040 & J2A040 Secure Smart Card Controller Revision 3

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW/SW	NXP J3A040 and J2A040 Secure Smart Card Controller Revision 3 including ROM mask and EEPROM patch	Mask ID: 33h (51) Mask name: NX011C Patch ID: x1h ("x" is different) Target ID: 00h (SmartMX)	Sawn Wafer or embedded into specific module package
2	DOC	User Manual [12]	Revision 3.1 12.05.2011	Electronic PDF document, encrypted and signed
3	DOC	Administrator Manual [13]	Revision 3.0 08.03.2011	Electronic PDF document, encrypted and signed
4	DOC	HW Data Sheet [14]	Revision 3.0 04.03.2011	Electronic PDF document, encrypted and signed

Table 2: Deliverables of the TOE

The delivery process from NXP to their customers guarantees, that the customer is aware of the exact versions of the different parts of the TOE as outlined above.

To ensure that the customer receives the evaluated version of the chip, the TOE is sent by NXP to the customer protected by special ordering, secured transport and tracking measures. Additionally, a Transport Key has to be used to support the secure delivery and the identification of the TOE.

When packed sometimes it is not possible to identify the TOE (NXP J3A040 and J2A040 Secure Smart Card Controller Revision 3) by sending commands to the TOE since there are no physical contacts available due to the production step. In that case the identification is done by the commercial name of the product as described in the Administrator Manual [13], chapter 2.1 and 7.1.

3 Security Policy

The TOE is the composition of an IC, IC Dedicated Software and Smart Card Embedded Software and is intended to be used as a Java Card platform and to be equipped with Java applets conformant to the Java Card standard.

The Java Card Virtual Machine (JCVM) is responsible for ensuring language-level security. The basic runtime security feature imposed by the Java Card Runtime Environment (JCRE) enforces isolation of applets using an applet firewall. It prevents objects created by one applet from being used by another applet without explicit sharing. This prevents unauthorized access to the fields and methods of class instances, as well as the length and contents of arrays.

The applet firewall is considered as the most important security feature. It enables complete isolation between applets or controlled communication through additional mechanisms that allow them to share objects when needed. The JCVM should ensure that the only way for applets to access any resources are either through the JCRE or through the Java Card API (or other vendor-specific APIs).

The Card Manager is responsible for the management of applets in the card. No post-issuance loading and deletion of applets is allowed for the present TOE.

4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and organisational Security Policies 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:

- OE.USE_DIAG: Secure TOE communication protocols shall be supported and used by the environment.
- OE.USE_KEYS: During the TOE usage, the terminal or system in interaction with the TOE, shall ensure the protection (integrity and confidentiality) of their own keys by operational means and/or procedures.
- OE.NATIVE: Those parts of the APIs written in native code as well as any pre-issuance native application on the card shall be conformant with the TOE so as to ensure that security policies and objectives described herein are not violated.
- OE.NO-DELETION: No installed applets (or packages) shall be deleted from the card.
- OE.NO-INSTALL: There is no post-issuance installation of applets. Installation of applets is secure and shall occur only in a controlled environment in the pre-issuance phase.
- OE.VERIFICATION: All the bytecodes shall be verified at least once, before the loading, before the installation or before the execution, depending on the card capabilities, in order to ensure that each bytecode is valid at execution time.

Details can be found in the Security Target [6] and [8], chapter 4.2.

5 Architectural Information

The TOE does not include any software on the Application Layer (Java Card applets) and does not include some parts of the Hardware Platform. This is shown schematically in the following figure:

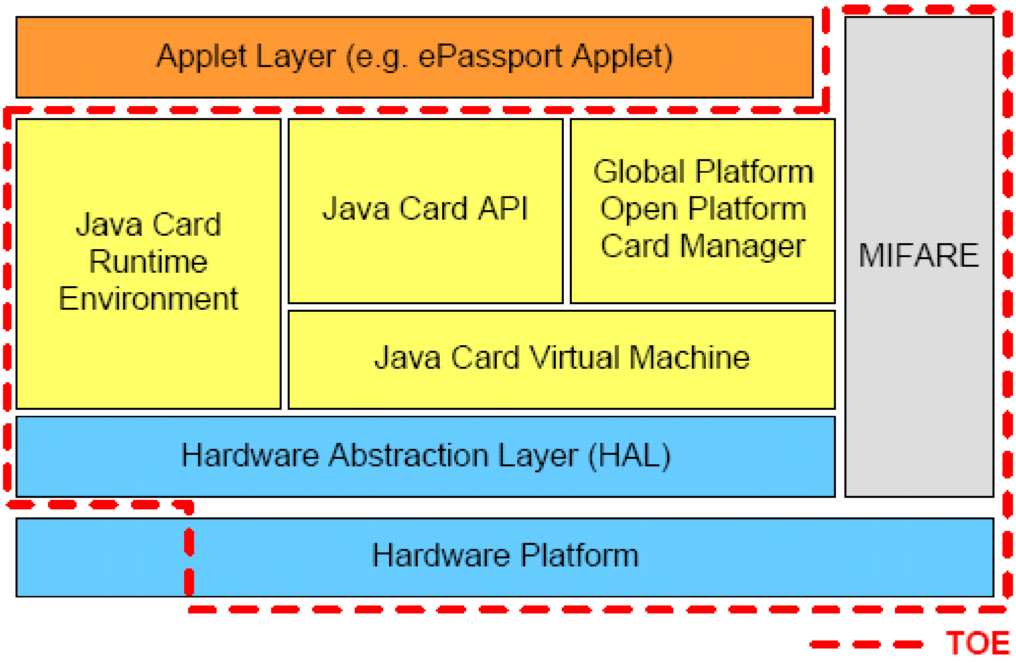
Applet Layer (e.g. ePassport Applet)
Java Card Runtime Environment
Java Card API
Global Platform Open Platform Card Manager
MIFARE
Java Card Virtual Machine
Hardware Abstraction Layer (HAL)
Hardware Platform
TOE

Figure 1: JCOP Architecture

The Smart Card Platform (SCP) consists of the Hardware Abstraction Layer (HAL) and the Hardware Platform. The cryptographic library (Crypto Library) is part of the HAL. Not all functionality of the Crypto Library is used, but this unused functionality is not linked with the code and is therefore not part of the HAL. Instead this functionality is implemented in JCOP embedded software. All functions in the HAL are used by the TOE. Not all functionality of the Hardware Platform is used for the TOE functionality and exposed at external interfaces. Therefore, some parts of the Hardware Platform are not part of the TOE.

The following functionality of the Smart Card Platform is not used for the composite TOE and not exposed at external interfaces:

- Hardware Special Function Register Access Control,
- AES functionality of the Crypto Library (implemented by JCOP embedded SW instead),
- RSA functionality of the Crypto Library (implemented by JCOP embedded SW instead),
- Random Number Generator of the Crypto Library (implemented by JCOP embedded SW instead) and
- Copy functionality of the Crypto Library (implemented by JCOP embedded SW instead).

The Java Card System is intended to transform a Smart Card into a Platform Capable of executing applications written in a subset of the Java programming language. The intended use of a Java Card Platform is to provide a framework for implementing IC independent applications conceived to safely coexist and interact with other applications into a single Smart Card.

Applications installed on a Java Card Platform can be selected for execution when the card is inserted into a card reader. In some configurations of the TOE, the card reader may also be used to enlarge or restrict the set of applications that can be executed on the Java Card Platform according to a well-defined card management policy.

6 Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7 IT Product Testing

7.1 Developer's Test according to ATE_FUN

The test of the TOE NXP J3A040 and J2A040 Secure Smart Card Controller Revision 3 is divided into several distinct phases:

- Unit testing,
- Integration testing and
- Acceptance testing.

The overall goal of the tests is to show that the TOE implements the TSF as described by the Security Target and the Functional Specification. Since SF.Hardware is covered by the HW certification, the testing approach has been to verify that the recommendations from HW to the SW granted by the HW guidance are fulfilled by the embedded software instead of doing functional testing of the HW security functions again. Therefore most of the tests for HW functions are done via code inspections, unit tests or acceptance tests. Furthermore, the TOE requires compliancy to three core specifications:

- Java Card 2.2.2,
- GlobalPlatform 2.1.1 and
- Visa GlobalPlatform 2.1.1 CIR.

The tests to be executed refer to the test plans of these specifications in conjunction with two supported interfaces:

- Contact based - ISO7816, EMV 4.1
- Contactless - ISO14443, ISO10373

Additionally NXP Semiconductors created tests to cover special areas of interest:

- Unit Tests
- Amendatory Java Card Tests

All TSF, which are related to the core specifications, are tested with the main test suites used during acceptance testing. The test suites are:

- JC-TCK 2.2.2,
- GP 2.1.1 - Official GP test suites and
- VGP 2.1.1 - Test suite used by VISA test labs.

The acceptance tests are mainly done with externally developed test suites for testing compliance to the Java Card specifications. The product is a Java Card providing a platform for Java applets. Therefore the TOE is implemented according to well known specifications. The definition of TSF in [6] and [8] is based on the Java Card functionality defined in the specifications. Therefore the overall testing strategy is to prove for compliance to the specifications and there with to give proof for the correct implementation of the TSF.

All the different configurations of the TOE (No MIFARE or MIFARE A, B1, B4; all with mask ID 51 and patch ID 1) have been tested successfully.

7.2 Evaluator's Test according to ATE_IND

The evaluator’s testing effort is described as follows, outlining the testing approach, configuration, depth and results.

The samples used for testing have been the composite product, which means the JCOP SW part on the platform provided as SO28 samples. All samples have been provided with the following parameters: FABKEY ID: 0x04, PATCH ID: 0x31, TARGET ID: 0x00 (null), MASK ID: 0x33 (51), CUSTOM MASK: 00000000, MASK NAME: NX011C, FUSE STATE: not fused, ROM INFO: 39F873, COMBO NAME: null-m33.04.31-NX011C. The configuration has been different in COMBO NAME to the 3 major configurations A, B1 and B4 and J2A040 as stated in the Security Target [6] and [8].

The APDU and API interfaces are most significant for the TOE. Therefore they are most often used during testing and the test samples are provided as composite TOE consisting of a SO28 sample which can only be connected via adapter to a terminal using contact or contact less interface.

The choice of the subset of interfaces used for testing has been done according to the following approach:

- Augmentation of developer testing for interfaces and supplementation of developer testing strategy for interfaces are both used for setting up test cases.
- The number of interfaces from which to draw upon for the test subset leads to focus on contact and contactless interface including MIFARE interface; Test Applets are used to perform functional testing (API interfaces are tested as well).
- Related to the complexity of interfaces the evaluator included repeating of all unit tests, JC-TCK tests and Global Platform tests each for one TOE configuration covering all interfaces.
- Repetition of the unit tests, JC-TCK tests and Global Platform tests using the external visible interfaces the independent testing covers all interfaces also the internal ones implicitly.
- Other types of interfaces are either covered by the hardware certificate [18] (e. g. electrical interfaces) or are not available (e. g. USB) or are implicitly included (e. g. contact less and ISO7816 APDU interface used to implicitly test the programming interfaces by test applets).

- One stressed feature (BAC functionality) is completely covered by unit tests and additionally tested by the evaluator.

During the evaluator’s independent testing the TOE operated as specified. The evaluator found that all TSFI have been suitably tested, and all interfaces are properly implemented.

7.3 Penetration Testing according to AVA_VAN

The penetration testing approach was based on the developer's vulnerability analysis and based on the independent vulnerability assessment of the evaluator. The evaluator's approach was to systematically search for potential vulnerabilities and for known attacks in public domain sources and the use of actual information from international working groups. Analysis why vulnerabilities are not exploitable in the intended environment of the TOE were performed assuming high attack potential. To support and to verify the analysis specific penetration attacks were performed in the course of this evaluation.

During the evaluator's penetration testing the TOE operated as specified. During the tests using high attack potential it has not been possible to succesfully penetrate the TOE and the usage of the certified secure HW could be verified. In the intended environment of use the TOE does not feature any exploitable vulnerabilities in the meaning of the Security Targets [6] and [8] for typical attackers possessing a high attack potential, if all the measures required are taken into consideration.

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential „high“ was successful in the TOE’s operational environment as defined in the ST [6] and [8] provided that all measures required by the developer are applied.

8 Evaluated Configuration

The TOE was evaluated in the configuration as outlined in table 2. In case of the J3A040 Secure Smart Card Controller Revision 3 the underlying hardware allows for three minor configurations, named MIFARE Emulation = A, B1 and B4. All of these configurations have been evaluated in the hardware evaluation of the P5CD040V0B (see [18]). These configurations need to be specified when ordering the hardware at NXP, where the configuration process is performed during the testing phase. There is no way to switch from one configuration to a different one after the manufacturing process is finished.

The difference between these minor configurations is the presence and memory size of the MIFARE emulation.

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [9] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used for those components up to EAL4 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the technology was used:

- The Application of CC to Integrated Circuits,
- Application of Attack Potential to Smartcards and
- Public Version of Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies

(see [4], AIS 25, AIS 26, AIS 35).

For RNG assessment the scheme interpretations AIS 20 was used (see [4]).

To support composite evaluations according to AIS 36 the document ETR for composite evaluation [10] was provided and approved. This document provides details of this platform evaluation that have to be considered in the course of a composite evaluation on top.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 5 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_DVS.2 and AVA_VAN.5 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0674-2011, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the change of the underlying hardware platform from P5Cx080V0B to P5Cx040V0B including its corresponding cryptographic library.

The evaluation has confirmed:

● for the Functionality:	Common Criteria Part 2 extended
● for the Assurance:	Common Criteria Part 3 conformant EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2 Results of cryptographic assessment

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2). This holds for the TOE Security functionality SF.CryptoOperation.

The following cryptographic algorithms are used by the TOE to enforce its security policy:

Algorithm	Bit Length	Application	Portion of the TSF	Standard of Implementation	Standard of Application[8]	Validity Period[9]
AES in ECB/CBC Mode	128 / 224 / 256	data encryption / decryption	SF.CryptoOperation	FIPS 197	-	-
EC over GF(p)	224 to 320	Diffie-Hellman key agreement	SF.CryptoOperation	ISO 11770-3	-	-
EC over GF(p)	224 to 320	Secure point addition	SF.CryptoOperation	ISO14888-3	-	-
EC with SHA-1, SHA-224, and SHA-256	224 to 320	digital signature generation and verification	SF.CryptoOperation	ISO14888-3	-	-
Retail MAC	112	secure messaging message authentication code	SF.CryptoOperation	ISO 9797-1	-	-
RSA (and PKCS#1 padding)	1976 to 2048	data encryption / decryption	SF.CryptoOperation	PKCS#1	-	-
RSA with SHA-1	1976 to 2048	digital signature generation and verification	SF.CryptoOperation	ISO 9796-2	-	-
RSA with SHA-1	1976 to 2048	digital signature generation and verification	SF.CryptoOperation	PKCS#1	-	-
SHA-1	none	secure hash computation	SF.CryptoOperation	FIPS 180-1	-	-
SHA-224	none	secure hash computation	SF.CryptoOperation	FIPS 180-1	-	-
SHA-256	none	secure hash computation	SF.CryptoOperation	FIPS 180-1	-	-
Triple DES in ECB/CBC Mode	112 / 168	data encryption / decryption	SF.CryptoOperation	FIPS 46-3	-	-
Triple-DES in CBC mode	112	secure messaging encryption and decryption	SF.CryptoOperation	FIPS 46-3	-	-
Triple-DES in outer CBC Mode	112 / 168	8 byte MAC generation and verification	SF.CryptoOperation	ISO 9797-1	-	-

Table 3: TOE cryptographic functionality

[8] Due to the character of the TOE, which provides platform functionality, no Application Standard is applicable.

[9] The Validity Period refers to the Application Standard and is therefore not applicable for this TOE.

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 4, Para. 3, Clause 2). But Cryptographic Functionalities with a security level of 80 bits or lower can no longer be regarded as secure against attacks with high attack potential without considering the application context. Therefore for this functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

The cryptographic function 2-key Triple DES (2TDES) provided by the TOE achieves a security level of maximum 80 Bits (in general context).

10 Obligations and Notes for the Usage of the TOE

The operational documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. 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.

11 Security Target

For the purpose of publishing, the Security Target [8] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12 Definitions

12.1 Acronyms

AES	Advanced Encryption Standard
AID	Application identifier, an ISO-7816 data format used for unique identification of Java Card applications
API	Application Programming Interface
APDU	Application Protocol Data Unit, an ISO 7816-4 defined communication format between the card and the off-card applications.
BCV	Byte Code Verifier (here: Off-card verifier)
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CC	Common Criteria for IT Security Evaluation
CM	Card Manger
CVM	C (programming language) Virtual Machine

DES	Data Encryption Standard
DPA	Differential Power Analysis
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptograpy
EEPROM	Electrically Erasable Programmable ROM
ES	Embedded Software
HAL	Hardware Abstraction Layer
HW	Hardware
IC	Integrated Circuit
IT	Information Technology
JCOP	Java Card Open Platform
JCRE	Java Card Runtime Environment
JCVM	Java Card Virtual Machine
NOS	Native Operating System
PP	Protection Profile
RAM	Random Access Memory
ROM	Read Only Memory
RSA	algorithm for public-key cryptography
RTE	Runtime Environment
SCP	Smart Card Platform
SFP	Security Function Policy
SPA	Simple Power Analysis
ST	Security Target
SW	Software
TCK	Test Compatibility Kit
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
VM	Virtual Machine

12.2 Glossary

Applet The name is given to a Java Card technology-based user application

Augmentation - The addition of one or more requirement(s) to a package.

Extension - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - An passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Protection Profile - An implementation-independent statement of security needs for a TOE type.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - A set of software, firmware and/or hardware possibly accompanied by guidance.

TOE Security Functionality - combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 3, July 2009
Part 2: Security functional components, Revision 3, July 2009
Part 3: Security assurance components, Revision 3, July 2009

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 3, July 2009

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[10].

[5] German IT Security Certificates (BSI 7148), periodically updated list published also in the BSI Website

[6] Security Target BSI-DSZ-CC-0730-2011, Version 1.02, 07.12.2010, NXP J3A040 and J2A040 Secure Smart Card Controller Revision 3 – Security Target, NXP Semiconductors (confidential document)

[7] Java Card System - Minimal Configuration Protection Profile, Version 1.1, May 2006, part of: Java Card Protection Profile Collection, Version 1.1, May 2006

[8] Security Target BSI-DSZ-CC-0730-2011, Version 1.03, 13.05.2011, NXP J3A040 and J2A040 Secure Smart Card Controller Revision 3 – Security Target lite, NXP Semiconductors (sanitised public document)

[9] Evaluation Technical Report, Version 3, 18.05.2011, Evaluation Technical Report for NXP J3A040 and J2A040 Secure Smart Card Controller Rev. 3, TÜV Informationstechnik GmbH (confidential document)

[10] ETR for composition according to AIS 36 for the Product NXP J3A040 and J2A040 Secure Smart Card Controller Revision 3, BSI-DSZ-CC-0730-2011, Version 3, 18.05.2011, TÜV Informationstechnik GmbH (confidential document)

[10] specifically

- AIS 20, Version 1, 2. December 1999, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 6, 7 September 2009, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 7, 3 August 2010, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 32, Version 6, 3 August 2010, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, 3 September 2009, Evaluation Methodology for CC Assurance Classes for EAL5+ (CCv2.3 & CCv3.1) and EAL6 (CCv3.1)
- AIS 35, Version 2.0, 12 November 2007, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 3, 19 October 2010, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

[11] Configuration list for the TOE, Version 1.2, 16.05.2011, Configuration List NXP J3A128 J3A095 J3A080 J3A081 J3A040 J3A041 v2.4.1 R3 Secure Smart Card Controller, NXP Semiconductors (confidential document)

[12] Guidance documentation for the TOE, Revision 3.1, 12.05.2011, JCOP V2.4.1 Secure Smart Card Controller Revision 3 - User Manual, NXP Semiconductors

[13] Guidance documentation for the TOE, Revision 3.0, 04.03.2011, JCOP V2.4.1 Secure Smart Card Controller Revision 3 - Administrator Manual, NXP Semiconductors

[14] Guidance documentation for the TOE, Revision 3.0, 04.03.2011, JCOP V2.4.1 Revision 3 JxA080, JxA040, JxA020 and J3A012 secure smart card controller – Product hardware data sheet, Document-ID 201830, NXP Semiconductors

[15] Certification Report BSI-DSZ-CC-0710-2010 for Crypto Library V2.6 on P5CD040V0B / P5CC040V0B / P5CD020V0B / P5CC021V0B / P5CD012V0B from NXP Semiconductors Germany GmbH, 07.01.2011, BSI

[16] Security Target Lite BSI-DSZ-CC-0710-2010, Version 2.4, 14.12.2010, Crypto Library V2.6 on P5CD040V0B / P5CC040V0B / P5CD020V0B / P5CC021V0B / P5CD012V0B, NXP Semiconductors

[17] ETR for composition according to AIS36 for the product Crypto Library Crypto Library V2.6 on P5CD040V0B / P5CC040V0B / P5CD020V0B / P5CC021V0B / P5CD012V0B, BSI-DSZ-CC-0710-2010, Version 1.0, 24.11.2010, Brightsight (confidential document)

[18] Certification Report BSI-DSZ-CC-0404-2007 for NXP Secure Smart Card Controller P5CD040V0B, P5CC040V0B, P5CD020V0B and P5CC021V0B each with specific IC Dedicated Software, NXP Semiconductors Germany GmbH, Business Line Identification, 05.07.2007, BSI

[19] Security Target BSI-DSZ-CC-0404-2007, Version 1.8, 14.07.2010, P5CD040V0B / P5CC040V0B / P5CD020V0B / P5CC021V0B / P5CD012V0B - Security Target Lite, NXP Semiconductors (sanitised public document)

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance Claim (chapter 10.4)

„The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - CC Part 3 extended - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation

Assurance Class	Assurance Components
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next Section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.

Assurance Class	**Assurance Family**	**Assurance Components by Evaluation Assurance Level**						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

“Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 8.4)

“Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 8.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 8.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 8.8)

“Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 8.9)

“Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

"Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

This page is intentionally left blank

D Annexes

List of annexes of this certification report

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0730-2011

Evaluation results regarding development and production environment

The IT product NXP J3A040 & J2A040 Secure Smart Card Controller Revision 3 (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 25 May 2011, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.2)

are fulfilled for the development and production sites of the TOE listed below:

a) NXP Semiconductors GmbH, Business Unit Identification, Development Center, Georg-Heyken-Str. 1, D-21147 Hamburg (Development center, testing and data center with the project database)

b) NXP Semiconductors GmbH, Business Unit Identification, Development Center, Stresemannallee 101, D-22529 Hamburg (Development center, testing and data center with the project database)

c) NXP Semiconductors GmbH, Business Unit Identification, Document Control Office, Mikron-Weg 1, A-8101 Gratkorn (Development Center, Document control and development of documentation)

d) NXP Semiconductors, Interleuvenlaan 80, B-3001 Leuven, Belgium (Debugging, testing and adaptation of source code packages and associated documentation)

For development and production sites regarding the NXP chips P5CD040V0B and P5CC040V0B refer to the certification reports BSI-DSZ-CC-0710-2010 [15] and. BSI-DSZ-CC-0404-2007 [18].

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. The evaluators verified, that the threats, security objectives and requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6] and [8]) are fulfilled by the procedures of these sites.

This page is intentionally left blank.