Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0860-2013

for

NXP J3D081_M59_DF and J3D081_M61_DF Secure Smart Card Controller Revision 2 of JCOP V2.4.2 R2

from

NXP Semiconductors Germany GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0860-2013

Smart Cards and similar devices: Operation Systems and Applications

NXP J3D081_M59_DF and J3D081_M61_DF Secure Smart Card Controller Revision 2 of JCOP V2.4.2 R2

from	NXP Semiconductors Germany GmbH
PP Conformance:	Java Card System - Open Configuration Protection Profile, Version 2.6, 19 April 2010, ANSSI-CC-PP-2010/03
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_DVS.2, ASE_TSS.2, 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, 31 July 2013

For the Federal Office for Information Security

SOGIS IT SECURITY CERTIFIED

Joachim Weber
Head of Division

L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

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....7
1 Specifications of the Certification Procedure....7
2 Recognition Agreements....7
3 Performance of Evaluation and Certification....8
4 Validity of the Certification Result....8
5 Publication....9
B Certification Results....11
1 Executive Summary....12
2 Identification of the TOE....13
3 Security Policy....15
4 Assumptions and Clarification of Scope....15
5 Architectural Information....15
6 Documentation....16
7 IT Product Testing....16
8 Evaluated Configuration....19
9 Results of the Evaluation....19
10 Obligations and Notes for the Usage of the TOE....22
11 Security Target....23
12 Definitions....23
13 Bibliography....26
C Excerpts from the Criteria....29
CC Part 1:....29
CC Part 3:....30
D Annexes....39

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

---

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

As of September 2011 the new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Details on recognition and the history of the agreement can be found at https://www.bsi.bund.de/zertifizierung.

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

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 September 2011 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 website: 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 by the nations listed above.

This evaluation contains the components ALC_DVS.2, ASE_TSS.2 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 J3D081_M59_DF and J3D081_M61_DF Secure Smart Card Controller Revision 2 of JCOP V2.4.2 R2 has undergone the certification procedure at BSI.

The evaluation of the product NXP J3D081_M59_DF and J3D081_M61_DF Secure Smart Card Controller Revision 2 of JCOP V2.4.2 R2 was conducted by Brightsight BV. Brightsight BV is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the 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

[6] Information Technology Security Evaluation Facility

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, as 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 J3D081_M59_DF and J3D081_M61_DF Secure Smart Card Controller Revision 2 of JCOP V2.4.2 R2 has been included in the BSI list of 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.

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

This page is intentionally left blank.

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 a Java Card product. The TOE consists of the Java Card Operating System, the NXP Crypto Library for SmartMX v2.7 (certified under BSI-DSZ-CC-0864-2011) and the hardware platform P5CD081V1D or P5CC081V1D (certified under BSI-DSZ-CC-0707-2011).

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Java Card System - Open Configuration Protection Profile, Version 2.6, 19 April 2010, ANSSI-CC-PP-2010/03 [7][8].

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 4 augmented by ALC_DVS.2, ASE_TSS.2, AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [8], chapter 6. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Functions	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.LoadIntegrity	Package integrity check
SF.Transaction	Transaction management
SF.Hardware	TSF of the underlying IC
SF.CryptoLib	TSF of the certified crypto library
SF.DFEmulation	TSF of the MIFARE DESFire Emulation in the underlying IC

Table 1: TOE Security Functionalities

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 Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [8], chapter 3.

[8] NXP had decided to use the certified PP version 2.6 and not the latest version 3.0 of the PP certified by ANSSI

This certification covers the following configurations of the TOE: NXP J3D081_M59_DF and J3D081_M61_DF both on top of the NXP P5CD081V1D or P5CC081V1D hardware chip. For details refer to chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms 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 J3D081_M59_DF and J3D081_M61_DF Secure Smart Card Controller Revision 2 of JCOP V2.4.2 R2

The following table outlines the TOE deliverables:

Product	Component	Version/ID	Form of delivery[9]
J3D081_M59_DF	P5CD081V1D hardware platform Crypto library ROM Code (Mask ID) Mask name Patch Code (Patch ID)	V1D V2.7 59 NX212A 05	Wafer, modules and packages (dice include identification T046D)
J3D081_M61_DF	P5CD081V1D hardware platform Crypto library ROM Code (Mask ID) Mask name Patch Code (Patch ID)	V1D V2.7 61 NX212B 05	Wafer, modules and packages (dice include identification T046D)
Guidance Documentation (for all products)	Administrator Manual (AGD_PRE) [11] User Manual (AGD_OPE) for the applet developer [12] Secure Box User Manual [13] Product hardware data sheet [14]	3.1 (15.01.2013) 3.3 (27.02.2013) 3.3 (28.02.2013) 3.0 (17.10.2011)	encrypted files (restricted distribution)

Table 2: Deliverables of the TOE

In chapter 2 of [11] the user is instructed to use the IDENTIFY command to verify the identity of the product. According to [12] Chapter 7, the identify command returns identification data. The data items that are relevant for the unique identification of the TOE are as follows:

[9] According to the Security Target of the certified hardware

Name	Expected
FabKey ID	xx (check OEF)
Patch ID	*x3 (3 = Patch ID 3)* *x4 (4 = Patch ID 4)* **x5 (5 = Patch ID 5) ← this is the TOE**
Target ID	01
Mask ID	3B = Mask 59 3D = Mask 61
Custom Mask ID	00 00 00 00 = Default mask
Mask Name	NX212A = Mask 59 NX212B = Mask 61
Fused State	00 = Not fused 01 = Fused
ROM Info Length	03
ROM Info	e.g. 065BFE = JxD145_M59
FIPS	00 = FIPS disabled

Table 3: EEPROM data for TOE identification (xxx for FABKEY ID)

The actual TOE identification is the combination FabKey ID, Mask ID.

- The FabKey is the area in EEPROM with user dependent content. The FabKey ID refers to a so called “Order Entry Form” (OEF) that specifies the user configuration data[10] and also identifies the hardware platform for the customer product and his FabKey ID.
- The size of the FabKey ID is 3 nibbles, which allows for 2^{12} FabKey identifications per Mask ID.
- The ROM Info gives a checksum value calculated over the entire ROM mask. This value will differ depending on the Mask ID and the hardware platform.
- In addition also customer applets and native library in the Secure Box can be installed in ROM. These may lead to additional customer mask IDs and further differences in the ROM Info checksum.

The TOE is delivered by NXP either as wafer in phase 3 (IC production) or in packaged form in phase 4 (packaging) of the smart card life cycle as defined in the Smart Card IC Protection Profile.

Applets and native libraries in the Secure Box can be loaded in ROM or EEPROM. Loading in ROM is possible in Phase 3. Loading of the native library (in the Secure Box) software in EEPROM is only possible by NXP in Phase 4. Loading of applets in EEPROM

[10] The user configuration data are the configuration settings that partly determine the behaviour of the TOE. Examples are the protocol communication parameters such as e.g. waiting time extension, selection of SCP protocol etc.

is possible in Phases 3, 4, 5 (composite product manufacturer, applet loading) or 6 (applet personalisation). Applets and native libraries in the Secure Box are outside the scope of the TOE. In the guidance [11] as part of the delivery procedure it is explained that when the TOE is powered for the first time it is in the “prepersonalization” state. In this state a so called “Root Applet” is available to configure OS parameters. For a detailed description of the delivery procedure of the native library to the developer is referred to chapter 9 of [13].

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues: It provides a protected environment on the card where multiple applications, within dedicated memory areas, can be hosted by using Java Card Technology.

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.APPLET: No applet loaded post-issuance shall contain native methods.
- 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. See #.VERIFICATION ([8] p.34) for details.
- 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.PROCESS_SEC_IC Protection during composite product manufacturing Security procedures shall be used after TOE Delivery up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use). This means that Phases after TOE Delivery up to the end of Phase 6 (refer to Section 1.3.3) must be protected appropriately.

Details can be found in the Security Target [8], chapter 3 and 4.2.

5 Architectural Information

The target of evaluation (TOE) is the **NXP J3D081_M59_DF and J3D081_M61_DF Secure Smart Card Controller Revision 2 of JCOP V2.4.2 R2**. It consists of:

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

- Native MIFARE DESFire application (physically always present but logical availability depends on configuration)

Logical Architecture:

The JCOP v2.4.2 R2 TOE from NXP is a Java Card (version. 3.0.1) and Global Platform (version 2.2.1) allowing post-issuance loading and installation of applets. Furthermore, the TOE supports the deletion of Applets and objects and implements a SecureBox. The SecureBox feature of the TOE allows the execution of a (unknown) native library in a from JCOP separated mode, using the (certified) MMU of the underlying hardware platform. This native library is loaded preissuance by the card manufacturer in ROM or EEPROM and is only accessible through the JCOPX API. The TOE supports a variety of crypto algorithms, supported through the Java Card API and the JCOPX API.

The TOE does not include any software on the application layer (Java Card applets). This is shown schematically in [8], Figure 1 in Chapter 1.3.1.

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 TOE test configuration

The developer provided the evaluator with test samples in a DIL package in prepersonalised state.

7.2 Developer testing

The Developer used a variety of test tools from which the TOE was tested both in its final configuration and in an emulator tool. The following test tools were used by the developer:

- GlobalPlatform test suite (The GlobalPlatform test suite is an industrial standard test suite used to test if the TOE complies with the GlobalPlatform standard[11])
- Visa GlobalPlatform test suite (The Visa GlobalPlatform test suite is the Visa addition to the GlobalPlatform test suite.)
- Unit test (The unit test test suite is developed along with the TOE development to test the developed functionalities of the TOE.)
- JCTCK (Java Card Technology compatibility Kit – JCTCK – The JCTCK test bench is the official test bench of Oracle and tests all compliance aspects of Java Card.)
- NXPTCK (The NXPTCK test bench is using the Oracle JT Harness environment that is also used by Oracle in JCTCK. The environment is used to implement tests for the JCOPX API.)

[11] This testset is for an earlier version than the GlobalPlatform version implemented in the TOE. During ATE testing it is determined that the used version is sufficient to test the implemented GlobalPlatform functionality that complies to version 2.2.1

- Add1 test (The Add1 test bench is proprietary to NXP)
- Add2 test (The Add2 test bench is proprietary to NXP)
- Adv test (The Adv test bench is based on JUnit and provides more flexible test creation.)

Typically some tests can only be performed in an emulator test environment. Testing these security mechanisms is done using the Unit test tool and a specially build TOE with additional test software. This allows changing TOE data and interrupting TOE execution, in order to test the checksums and attack counter mechanism.

7.3 Evaluator independent developer testing

The evaluators sampled test scripts and test applets per test suite. Next the tests were performed and the respective test logs were compared with the expected test results.

The evaluator independent developer tests have been conducted on products with the M59 and M61 software masks on the P5Cx145 hardware and the P5CD081V1D hardware respectively. Because the evaluator independent testing concerns logical testing the P5Cx145 hardware will show the same logical behaviour for the M59 mask as the P5CD081V1D hardware controller. Therefore, samples of each test suite for each test tool has been conducted for the TOE.

7.4 Evaluator independent testing

The evaluator has judged the developer's tests to be so extensive that testing specific interfaces would lead to tests that are only superficially different from the developer's testing. The evaluator therefore judges that tests, supplementing the developer's tests, should be defined based on how well the TOE security functions are implemented, rather than on how well the different standards are met.

Therefore the evaluator selected the following to be tested:
a) Integrity/error testing on the emulator:

- Test to show that the TOE terminates upon detection of EEPROM write Error
- Test to show that the TOE halts when an integrity error of a KEY/PIN object is detected
- Test to show that the TOE halts upon detecting FabKey integrity error
- Test to show that the TOE terminates itself upon detecting applet life cycle inconsistency
- Test to show that the memory is indeed cleared after the garbage collector removes the unreferenced objects

b) Testing of Unsupported APIs, this means verification that the VM will throw an Exception in case unused or switched off (as a result of a build flag) functionality is invoked.

c) Testing for obvious logical mistakes using the Brightsight Java Card Test Suite. The Brightsight Java Card Test Suite consists of more than 500 test cases, where each test case is performed by executing a script (and different test applets that are loaded as part of the test). The test suite interprets the test verdicts in pass, mild fail, and fail verdicts. Any inconclusive test results are analysed by the evaluator using knowledge of the implementation.

The integrity/error testing (at item 1.) has been performed on an Ashling EPKSCSmartMX emulator for the M59 mask using a specially developed test applet. The tested behavior is equal in the M61 mask.

The testing of Unsupported APIs (at item 2.) has been conducted on card products with the help of a specially developed test applet. The Brightsight Java Card testing (at item 3.) has also been conducted on card products. The testing of Unsupported APIs and the Brightsight Java Card testing have been conducted on the J3D081_M59 TOE product (which is part of BSI-DSZ-CC-0784 certification) for the M59 mask, on the J3D120_M60 which is part of the BSI-DSZ-CC-0783 certification and the J3D081_M61_DF product (which is part of this certification).

Because the testing concerns logical testing the test results for the J3D081_M61_DF product are considered also applicable for the TOE product with mask M59.

The testing results show that the TOE exhibits the expected behaviour. No deviations were found.

7.5 Penetration testing

The penetration tests were devised after performing the Evaluator Vulnerability Analysis. This was done in the following steps.

a) Inventory of required resistance
   This step uses the JIL attack list as a reference for completeness and studies the ST claims to decide which attacks in the JIL attack list apply for the JCOP 2.4.2 R2.

b) Validation of security functionalities
   This step identifies the implemented security functionalities and performs evaluator independent tests to verify implementation and to validate proper functioning of the security functions (ATE).

c) Vulnerability analysis
   In this step the design of the implemented security functionalities is studied and an analysis is performed to determine whether the design possibly contains vulnerabilities against the respective attacks of step 1. This step also analyses the design from the attack perspective as defined in 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. The evaluators have also considered the results of the AVA kick-off meeting (AVA).

d) Penetration testing
   This step performs the penetration tests identified in step 3. (AVA)

e) Conclusions on resistance
   This step performs a 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 TOE against attackers possessing a high attack potential.

The evaluator performed a wide variety of penetration tests on the concluded potential vulnerabilities comprising of side-channel tests, light-manipulation perturbation tests and Java Card testing. The overall conclusion is that the two JCOP 2.4.2 R2 products J3D081_M59_DF and J3D081_M61_DF are protected against attackers possessing a high attack potential, provided the user guidance is followed.

8 Evaluated Configuration

The JCOP 2.4.2 R2 contains 12 single products based on different combinations of hardware controller and mask used and EEPROM data setting. All of them have a P5 secure smart card controller, a Version 2.7 Cryptographic Library and JCOP 2.4.2 R2 functionality.

The TOE incudes the following 2 products: NXP J3D081_M59_DF and J3D081_M61_DF. Both products are composite TOEs each consisting of:

- P5CD081V1D secure smart card controller;
- Version 2.7 Cryptographic Library;
- Native MIFARE application (depending on the hardware configuration);
- Embedded JCOP 2.4.2 R2 software consisting of Java Card Virtual Machine, Runtime Environment, Java Card API and Card Manager.

Table 2 above outlines the specific hardware platform, Crypto library version, ROM Code (Mask ID), Mask name and Patch Code (Patch ID).

The difference between Mask 59 and Mask 61 is that in Mask 61 the FIPS Selftest API is not implemented, and no SCP03 implementations are available (not included in the TOE). Both configurations support the same set of SFRs.

The Mask Name identifies the version of the Mask ID which is among other based on the date of TOE generation.

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 EAL5 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:

(i) The Application of CC to Integrated Circuits

(ii) Application of Attack Potential to Smartcards

(iii) Guidance, Smartcard Evaluation

(iv) Composite product evaluation for Smart Cards and similar devices (see AIS 36). According to this concept the relevant guidance documents of the underlying platform and the documents ETR for Composition from the platform evaluations (i.e. on hardware [15], [17] and crypto library [16] and [18]) have been applied in the TOE evaluation.

(see [4], AIS 25, AIS 26, AIS 37).

For RNG assessment the scheme interpretations AIS 20 and 31 were used (see [4]).

A document ETR for composite evaluation according to AIS 36 has not been provided in the course of this certification procedure. It could be provided by the ITSEF and submitted to the certification body for approval subsequently.

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

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_DVS.2, ASE_TSS.2, AVA_VAN.5 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Java Card System - Open Configuration Protection Profile, Version 2.6, 19 April 2010, ANSSI-CC-PP-2010/03 [7]
- for the Functionality: PP conformant
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by ALC_DVS.2, ASE_TSS.2, 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 functionalities:

Algorithm	Bit length	Purpose	Implementation standard
AES in one of the following modes of operation: ECB, CBC with padding method 1 or method 2 or without padding	128, 192, 256 bits	encryption and decryption	FIPS Publication 197, Advanced Encryption Standard (AES), NIST Special Publication 800-38A, 2001 (ECB and CBC mode) and ISO 9797-1, padding method 1 or method 2 (CBC mode)
Triple-DES in one of the following modes of operation: ECB, CBC, with padding method 1 or method 2 or without padding	double-length (112 bit) or triple-length (168 bit)	encryption and decryption	ANSI X9.52-1998 (ECB and CBC mode) and ISO 9797-1, padding method 1 and method 2 (CBC mode) FIPS 46-3 (TDES)
Triple-DES in CBC-MAC mode MAC algorithm 1 without padding algorithm 3 with padding method 1 or method 2	double-length (112 bit) or triple-length (168 bit)	signature generation and verification	ISO 9797-1, Algorithm 1 without padding and Algorithm 2 with padding method 1 and method 2 (CBC-MAC mode) FIPS 46-3 (TDES)

Algorithm	Bit length	Purpose	Implementation standard
AES CBC-MAC mode MAC algorithm 1 without padding	128, 192, 256 bits	MAC generation and verification	ISO 9797-1, Algorithm 1 without padding (CBC-MAC mode) FIPS Publication 197, Advanced Encryption Standard (AES)
Triple-DES CMAC mode	double-length (112 bit) or triple-length (168 bit)	MAC generation and verification	NIST special publication 800-38B, section 5 and 6 FIPS 46-3 (TDES)
AES CMAC mode	128, 192, 256 bits	MAC generation and verification	NIST special publication 800-38B, section 5 and 6 FIPS Publication 197, Advanced Encryption Standard (AES)
RSA without or with EME-PKCS1-v1_5 encoding method	1976 bits to 2048 bits	encryption and decryption	PKCS #1, v2.1 (RSAEP, RSADP, RSAES-PKCS1-V1_5-ENCRYPT, RSAESPKCS1-V1_5-DECRYPT)
RSA with EMSA-PSS encoding method	1976 bits to 2048 bits	signature generation and verification	PKCS #1, v2.1 (RSASSA-PSS)
RSA with EMSA-PKCS1-v1_5 encoding method	1976 bits to 2048 bits	signature generation and verification	PKCS #1, v2.1 (RSASSA-PKSCS1-v1.5)
RSA	1976 bits to 2048 bits (Straight Forward) or 1976 to 2048 bits (CRT)	signature generation and verification	ISO 9796-2:2002
ECDSA over GF(p)	160, 192, 224, 256, 320 bits	signature generation and verification	ISO 14888-3
ECC over GF(p)	160, 192, 224, 256, 320 bits	secure point addition	ISO 14888-3
ECDH over GF(p)	160, 192, 224, 256, 320 bits	Diffie-Hellman Key Exchange	ISO 11770-3
Diffie-Hellman key exchange (RSA exponentiation)	1976 bits to 2048 bits	Diffie-Hellman Key Exchange	PKCS#3
SHA-224 and SHA-256	none	cryptographic checksum generation	FIPS 180-3 section 6

Table 4: Cryptographic functions

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 functionalites 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 Functionalities 2-key Triple DES (2TDES), Triple-DES in ECB-Mode, AES in ECB-Mode, ECC 160 provided by the TOE achieves a security level of maximum 80 Bits only (in general context).

10 Obligations and Notes for the Usage of the TOE

The 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 OSPs 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 limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process.

Some security measures are partly implemented in the hardware and require additional configuration or control or measures to be implemented by the application software on top. For this reason the TOE includes guidance documentation (see table 2) which contains guidelines for the developer of the application software on how to securely use the TOE and which measures have to be implemented in the software in order to fulfil the security requirements of the Security Target of the TOE.

In the course of the evaluation of the composite product or system on top it must be examined if the required measures have been correctly and effectively implemented by the application software.

The user of the TOE – the applet developer - must implement the advices of the user guidance [12]. Important to mention are:

- All applets have to verified with a byte code verifier at least once.
- None of the applets may use `APDU.Sendbyteslong` method with a data length of more than 1456 byte.
- Applets using the method `SACAccelerator.unwrapAPDU` need to implement an additional MAC verification while processing the received APDU.
- The length of RSA keys generated using the method `KeyPair.genKeyPair` has to be checked after key generation for the proper length.
- For security critical random data checks should be implemented for `RandomData` API parameters (i.e. length). Also it should be checked that the requested number of random data bytes have been generated and stored in the destination array.
- Adequate integrity protection mechanisms to detect changes in critical data caused by perturbation attacks should be implemented. This applies to persistent data which is not protected by the operating system, e.g. data in simple byte arrays. Note that Java Card key objects and `OwnerPIN` are protected by the operating system.

Depending on the application of the TOE and usage of the AES algorithm, the composite evaluator must determine whether confidentiality of input data of the AES algorithm is claimed and if this is the case, the composite evaluator must consider testing to provide assurance.

As explained in section 2 it is possible in the “prepersonalization” state to change the behaviour of the TOE with a number of configuration settings using the ROOT applet. However, if one of the following settings is changed it will result in a non-certified product configuration:

- The TOE does not allow the use of multiple logical channels.
- The TOE does not allow changes in the setting for the attack counter, or modifying the behaviour upon detection of a potential attack using FEATURE_MODE3.
- The TOE does also not allow the use of the FIPS mode. In the certified configuration this should be disabled.
- The power configuration (clock settings and HIGHSEC) are fixed.
- Configuration for security domains (e.g. Supplementary Security Domains) which relates to the Mandated DAP option is always enabled on the TOE.
- The Patch identification
- The developer default settings for MIFARE FLEX and DESFire must not be changed.
- The developer is responsible for making sure that the appropriate addresses are initialised for the PHEAP end address, transaction buffer size and extended patch.

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

AIS Application Notes and Interpretations of the Scheme

API Application Programming Interface

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

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation

CEM Common Methodology for Information Technology Security Evaluation

DES Data Encryption Standard

DIL	Dual In-Line
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Read Only Memory
ES	Embedded Software
ETR	Evaluation Technical Report
HAL	Hardware Abstraction Layer
HW	Hardware
IC	Integrated Circuit
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
LDS	Logical Data Structure
OEF	Order Entry Form
PP	Protection Profile
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

12.2 Glossary

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[12].

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

[6] Security Target BSI-DSZ-CC-0860-2013, Revision 01.15, 18 March 2013, NXP J3D081_M59_DF, and J3D081_M61_DF Secure Smart Card Controller Revision 2 Security Target, NXP Semiconductors Germany GmbH (confidential document)

[7] Java Card System - Open Configuration Protection Profile, Version 2.6, 19 April 2010, ANSSI-CC-PP-2010/03

[8] Security Target lite BSI-DSZ-CC-0860-2013, Revision 01.15, 18 March 2013, NXP J3D081_M59_DF, and J3D081_M61_DF Secure Smart Card Controller Revision 2 Security Target, NXP (sanitised public document)

[9] Evaluation Technical Report, Version 2.1, Evaluation Technical Report NXP J3D081_M59_DF, J3D081_M61_DF Secure Smart Card Controller, Brightsight (confidential document)

[10] Configuration list for the TOE, Version 1.3, NXP J3D145 J2D145 J3D145 J2D145 J3D145DF Secure Smart Card Controller Revision 2 (confidential document)

[11] Administrator manual JCOP V2.4.2 Revision 2 secure smart card controller, Rev. 3.1, 15 January 2013, Doc.No. 209431, NXP Semiconductors Germany GmbH (confidential document)

[12] User manual JCOP V2.4.2 Revision 2 secure smart card controller, Rev. 3.3, 27 February 2013, Doc.No. 209233, NXP Semiconductors Germany GmbH (confidential document)

---

[12] specifically

- AIS 25, Version 7, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 8,E valuationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL5+ (CCv2.3 & CCv3.1) and EAL6 (CCv3.1)
- AIS 35, Version 2.0, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 3, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2.9, Reuse of evaluation results

[13] UM Secure Box JCOP V2.4.2, Rev. 3.3, 28 February 2013, Doc.No. 221133[13], NXP Semiconductors Germany GmbH (confidential document)

[14] Product hardware data sheet JCOP V2.4.2 Revision 2 J3D081_DF secure smart card controller, Rev. 3.0, 17 October 2011, Doc.No. 219530, NXP Semiconductors Germany GmbH (confidential document)

[15] Certification Report, BSI-DSZ-CC-0707-2012 for NXP Secure Smart Card Controllers P5CD016V1D/P5CD021V1D/P5CD041V1D/P5Cx081V1D with DESFire EV1 from NXP Semiconductors Germany GmbH, Version 1.0, 13 August 2012, BSI

[16] Certification Report, BSI-DSZ-CC-0864-2012 for Crypto Library V2.7 NXP Smart Card Controller P5CD081V1D and its major configurations from NXP Semiconductors Germany GmbH, Version 1.0, 19 December 2012, BSI

[17] ETR for composition, BSI-DSZ-CC-0707 for NXP Secure Smart Card Controllers P5CD016V1D/P5CD021V1D/P5CD041V1D/P5Cx081V1D with DESFire EV1 Version 1.2, 8 June 2012, T-Tystems GmbH (confidential document)

[18] ETR for composition, BSI-DSZ-CC-0864, NXP Crypto library V2.7 on SmartMX P5CX081/CD041/CD021/CD016V1D according to AIS36, v3.0, 12 December 2012, Brightsight (confidential document)

[13] Please note that [6] and [8] contain incorrect references to older versions of the document

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part 1:

Conformance Claim (Release 3 = 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

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development and production environment

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0860-2013

Evaluation results regarding development and production environment

The IT product NXP J3D081_M59_DF and J3D081_M61_DF Secure Smart Card Controller Revision 2 of JCOP V2.4.2 R2, (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 31 July 2013, 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.4, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.1)

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

a) NXP Semiconductors Hamburg (software development and TOE integration)
NXP Semiconductors GmbH, Business Unit Identification, Development Center, Stresemannallee 101, 22529 Hamburg

b) NXP Semiconductors Gratkorn (software development and document control)
NXP Semiconductors GmbH, Business Unit Identification, Document Control Office, Mikron-Weg 1, A-8101 Gratkorn

c) NXP Semiconductors Leuven (software (crypto) development)
NXP Semiconductors, Interleuvenlaan 80, B-3001 Leuven, Belgium

d) NXP Bangalore (tool development)
NXP Semiconductors India Private Limited, Information Technology Park, Nagawara Village, Kasaba Hobli,Bangalore 560 045 India

e) For the list of sites used as part of the platform development and production see annex B of [15] and [16]

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.