Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0750-V2-2014

for

Crypto Library V2.7/2.9 on SmartMX P5Cx128/P5Cx145 V0v/ V0B(s)

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-0750-V2-2014

Smart Cards and similar devices: IC, Cryptolib

Crypto Library V2.7/2.9 on SmartMX P5Cx128/P5Cx145 V0v/ V0B(s)

from	NXP Semiconductors Germany GmbH
PP Conformance:	Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007
Functionality:	PP conformant plus product specific extensions 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

TThe 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, 16 July 2014

For the Federal Office for Information Security

INFORMATION TECHNOLOGY SECURITY
SOGIS
IT SECURITY CERTIFIED
MUTUAL RECOGNITION AGREEMENT

Bernd Kowalski
Head of Department

L.S.

SOGIS Recognition
Agreement

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....9
5 Publication....9

B Certification Results....11

1 Executive Summary....12
2 Identification of the TOE....13
3 Security Policy....16
4 Assumptions and Clarification of Scope....16
5 Architectural Information....17
6 Documentation....17
7 IT Product Testing....17
8 Evaluated Configuration....18
9 Results of the Evaluation....18
10 Obligations and Notes for the Usage of the TOE....22
11 Security Target....22
12 Definitions....22
13 Bibliography....25

C Excerpts from the Criteria....27

CC Part 1:....27
CC Part 3:....28

D Annexes....37

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 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 Crypto Library V2.7/2.9 on SmartMX P5Cx128/P5Cx145 V0v/ V0B(s) has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0750-2011-MA-02. Specific results from the evaluation process BSI-DSZ-CC-0750-2011-MA-02 were re-used.

The evaluation of the product Crypto Library V2.7/2.9 on SmartMX P5Cx128/P5Cx145 V0v/ V0B(s) was conducted by Brightsight BV. The evaluation was completed on 2 July 2014. Brightsight BV 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.

[6] Information Technology Security Evaluation Facility

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, 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 Crypto Library V2.7/2.9 on SmartMX P5Cx128/P5Cx145 V0v/ V0B(s) 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 evaluated TOE is “Crypto Library V2.7/V2.9 on SmartMX P5Cx128/P5Cx145 V0v/ V0B(s)”. This TOE is a composite TOE, consisting of:

- The hardware “NXP SmartMX P5Cx128/P5Cx145 V0v/ V0B(s) Secure Smart Card Controller”, which is used as evaluated platform, and all its Major Configurations
- The “Crypto Library V2.7/V2.9 on SmartMX P5Cx128/P5Cx145 V0v/ V0B(s) ”, which is built upon this platform.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007 [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 4.1. 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 Functionality:

TOE Security Functionality	Addressed issue
SS.RNG	Hardware Random Number Generator
SS.HW_AES	Hardware AES Co-processor
SS.HW_DES	Hardware Triple-DES Co-processor
SF.OPC	Control of Operating Conditions
SF.PHY	Protection against Physical Manipulation
SF.LOG	Logical Protection
SF.COMP	Protection of Mode Control
SF.MEM_ACC	Memory Access Control
SF.SFR_ACC	Special Function Register Access Control
F.AES	AES encryption and decryption
F.DES	DES encryption and decryption
F.RSA_encrypt	RSA encryption
F.RSA_sign	RSA signature generation and verification
F.RSA_public	computation of an RSA public key
F.ECC_GF_p_ECDSA	ECC Signature Generation and Verification
F.ECC_GF_p_DH_KeyExch	Diffie-Hellman Key Exchange
F.RSA_KeyGen	generate RSA key pairs
F.ECC_GF_p_KeyGen	ECC Key Generation
F.SHA	compute Secure Hash Algorithms

TOE Security Functionality	Addressed issue
F.RNG_Access	software RNG
F.Object_Reuse	clearing memory areas
F.LOG	Extended Logical Protection

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] and [8], chapter 5.1.

The assets to be protected by the TOE are defined in the Security Target [6] and [8], chapter 2.1. 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], chapters 2.2, 2.3 and, 2.4.

This certification covers the configurations of the TOE as outlined in chapter 8.

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:

Crypto Library V2.7/2.9 on SmartMX P5Cx128/P5Cx145 V0v/ V0B(s)

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
Components TOE variation P5Cx128/P5Cx145 V0A with MIFARE MSO				
1	HW	NXP Secure Smart Card Controllers P5Cx128/P5Cx145 V0A	V0A	wafer, module, inlay, package (dice have nameplate T051A)
2	SW	Test-Rom Software for MIFARE MSO	97	Test-ROM on the chip acc. to: tmfos_97_collected.ms3
3	SW	Boot-ROM Software for MIFARE MSO	97	Test-ROM on the chip acc. to: tmfos_97_collected.ms3
4	SW	MIFARE Operating System MSO	97	Test-ROM on the chip acc. to: tmfos_97_collected.ms3
5	DOC	Data Sheet P5Cx128/P5Cx145 family, Secure dual interface and contact PKI smart card controller		Electronic document

No	Type	Identifier	Release	Form of Delivery
6	DOC	Instruction Set, SmartMX-Family, Secure and PKI Smart Card Controller	1.1	Electronic document
7	DOC	Guidance, Delivery and Operation Manual NXP Secure Smartcard Controllers P5Cx128/P5Cx145V0v, NXP Semiconductors, Business Unit Identification		Electronic document
8	SW	Crypto Library	2.7	Electronic File
9	SW	Crypto Library	2.9	Electronic File
10	DOC	Guidance documents [12]		Electronic document
Components TOE variation P5Cx128/P5Cx145 V0A with MIFARE FleX™				
11	HW	NXP Secure Smart Card Controllers P5Cx128/P5Cx145 V0A	V0A	wafer, module, inlay, package (dice have nameplate T051A)
12	SW	Test-ROM Software for MIFARE FleX™	102	Test-ROM on the chip acc. to: tmfos_102_collected.hex
13	SW	Boot-ROM Software for MIFARE FleX™	102	Test-ROM on the chip acc. to: tmfos_102_collected.hex
14	SW	MIFARE FleX™ Operating System	102	Test-ROM on the chip acc. to: tmfos_102_collected.hex
15	DOC	Data Sheet P5Cx128/P5Cx145 family, Secure dual interface and contact PKI smart card controller		Electronic document
16	DOC	Instruction Set, SmartMX-Family, Secure and PKI Smart Card Controller	1.1	Electronic document
17	DOC	Guidance, Delivery and Operation Manual NXP Secure Smartcard Controllers P5Cx128/P5Cx145V0v, NXP Semiconductors, Business Unit Identification		Electronic document
18	SW	Crypto Library	2.7	Electronic File
19	SW	Crypto Library	2.9	Electronic File
20	DOC	Guidance documents [12]		Electronic document
Components TOE variation P5Cx128/ P5Cx145 V0B with MIFARE FleX™				
21	HW	NXP Secure Smart Card Controllers P5Cx128/P5Cx145 V0B	V0B	wafer, module, inlay, package (dice have nameplate T051B)

No	Type	Identifier	Release	Form of Delivery
22	SW	Test-ROM Software for MIFARE FleX™	102	Test-ROM on the chip acc. to: tmfos_102_collected.hex
23	SW	Boot-ROM Software for MIFARE FleX™	102	Test-ROM on the chip acc. to: tmfos_102_collected.hex
24	SW	MIFARE FleX™ Operating System	102	Test-ROM on the chip acc. to: tmfos_102_collected.hex
25	DOC	Data Sheet P5Cx128/P5Cx145 family, Secure dual interface and contact PKI smart card controller		Electronic document
26	DOC	Instruction Set, SmartMX-Family, Secure and PKI Smart Card Controller	1.1	Electronic document
27	DOC	Guidance, Delivery and Operation Manual NXP Secure Smartcard Controllers P5Cx128/P5Cx145V0v, NXP Semiconductors, Business Unit Identification		Electronic document
28	SW	Crypto Library	2.7	Electronic File
29	SW	Crypto Library	2.9	Electronic File
30	DOC	Guidance documents [12]		Electronic document
Components TOE variation P5Cx128/ P5Cx145 V0B with MIFARE FleX™				
31	HW	NXP Secure Smart Card Controllers P5Cx128/P5Cx145 V0B(s)	V0B(s)	wafer, module, inlay, package (dice have nameplate s051B)
32	SW	Test-ROM Software for MIFARE FleX™	102	Test-ROM on the chip acc. to: tmfos_102_collected.hex
33	SW	Boot-ROM Software for MIFARE FleX™	102	Test-ROM on the chip acc. to: tmfos_102_collected.hex
34	SW	MIFARE FleX™ Operating System	102	Test-ROM on the chip acc. to: tmfos_102_collected.hex
35	DOC	Data Sheet P5Cx128/P5Cx145 family, Secure dual interface and contact PKI smart card controller		Electronic document
36	DOC	Instruction Set, SmartMX-Family, Secure and PKI Smart Card Controller	1.1	Electronic document

No	Type	Identifier	Release	Form of Delivery
37	DOC	Guidance, Delivery and Operation Manual NXP Secure Smartcard Controllers P5Cx128/P5Cx145V0v, NXP Semiconductors, Business Unit Identification		Electronic document
38	SW	Crypto Library	2.7	Electronic File
39	SW	Crypto Library	2.9	Electronic File
40	DOC	Guidance documents [12]		Electronic document

Table 2: Deliverables of the TOE

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: The security policy of the TOE is to provide basic Security Functions to be used by the smart card operating system and the smart card application thus providing an overall smart card system security. Therefore, the TOE will implement algorithms to ensure the confidentiality of plain text data by encryption and to support secure authentication protocols and it will provide a random number generator.

The TOE is a hardware security platform, the security policy of the TOE is also to provide protection against leakage of information (e.g. to ensure the confidentiality of cryptographic keys during cryptographic functions performed by the TOE), against physical probing, against malfunctions, against physical manipulations and against abuse of functionality. Hence the TOE shall

- maintain the integrity and the confidentiality of data stored in the memory of the TOE and
- maintain the integrity, the correct operation and the confidentiality of Security Features provided by the 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:

- Protection during Packaging, Finishing and Personalization
- Usage of Hardware Platform
- Treatment of User Data
- Check of initialisation data by the Smartcard Embedded Software
- Usage of Key-dependent Functions
- Operational Environment for RSA Key Generation function

Details can be found in the Security Target [6] and [8], chapter 2.2.

5 Architectural Information

The evaluated TOE is “Crypto Library V2.7/V2.9 on SmartMX P5Cx128/P5Cx145 V0v/ V0B(s)”. This TOE is a composite TOE, consisting of:

- The hardware “NXP SmartMX P5Cx128/P5Cx145 V0v/ V0B(s) Secure Smart Card Controller”, which is used as evaluated platform, and all its Major Configurations
    - P5CD145V0A
    - P5CC145V0A
    - P5CN145V0A
    - P5CD128V0A
    - P5CC128V0A
    - P5CD145V0B
    - P5CC145V0B
    - P5CN145V0B
    - P5CD128V0B
    - P5CC128V0B
    - P5CD145V0B(s)
    - P5CC145V0B(s)
    - P5CN145V0B(s)
    - P5CD128V0B(s)
    - P5CC128V0B(s)
- The “Crypto Library V2.7/V2.9 on SmartMX P5Cx128/P5Cx145 V0v/ V0B(s) ”, which is built upon this platform.

The TOE provides AES, DES, Triple-DES (TDES), RSA, RSA key generation, RSA public key computation, ECC over GF(p), ECC over GF(p) key generation, ECC Diffie-Hellman key-exchange, SHA-1, SHA-224 and SHA-256 algorithms.

In addition, the Crypto Library implements a software (pseudo) random number generator, which is initialised (seeded) by the hardware random number generator of the SmartMX.

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

For the Crypto Library, the developer has defined an extensive test set. The test set covers all TOE interfaces, and all modes of operation of the implemented algorithms, as well as all available parameters. Since the TOE is not an end-user product it is not possible to perform testing without first embedding it in a testable configuration. To this end, the developer has created a proprietary test operating system. The main purpose of the test OS is to provide access to the crypto library's functionality. The test OS, and its documentation was provided to the evaluators, and was used in all the testing.

The penetration tests are devised after performing the Evaluator Vulnerability Analysis. This analysis has followed the following steps: The reference for attack techniques against which smart card-based devices controllers such as the Crypto Library on SmartMX must be protected against is the document "Attack methods for smart cards". Additional guidance for testing was provided by the certification body in the form of a number of questions regarding the TOE. The vulnerability of the Crypto Library for these attacks has been analysed in a white box investigation conforming to AVA_VAN.5.

8 Evaluated Configuration

The evaluated TOE is "Crypto Library V2.7/V2.9 on SmartMX P5Cx128/P5Cx145 V0v/ V0B(s)". There are no additional version or other identification and configuration characteristics.

The environment of the TOE is characterised by the general environment descriptions in the Eurosmart Smartcard IC Platform Protection Profile:

- OE.Plat-Appl Usage of Hardware Platform
- OE.Resp-Appl Treatment of User Data
- OE.Process-Sec-IC Protection during composite product manufacturing

Additional refinements in the Hardware Security Target are also valid. The TOE assumes that the Smartcard Embedded Software abides by the provisions detailed in section 4.3 "Security Objectives for the Operational Environment", and the following additional security objective for the Smart Card Embedded Software:

- OE.Check-Init Check of initialization data by the Smart Card Embedded Software.

The TOE imposes one additional requirement on the environment:

- OE.RSA-Key-Gen In case that resistance of the fast, but insecure mode of the RSA Key Generation against side channel attacks is needed, the operational environment shall ensure that side-channel attacks cannot be performed.

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) *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 have been applied in the TOE evaluation.*

(see [4]4], AIS 20, AIS 25, AIS 26, AIS 37).

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.

The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

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-0750-2011-MA-02, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on vulnerability analysis, penetration testing and changes to the Security Target.

The evaluation has confirmed:

● PP Conformance:	Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007 [7]
● for the Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
● for the Assurance:	Common Criteria Part 3 conformant EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5

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 strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But Cryptographic Functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these 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).

Any Cryptographic Functionality that is marked in column '*Security Level above 100 Bits*' of the following table with '*no*' achieves a security level of lower than 100 Bits (in general context).

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
1	Cryptographic Primitive	DES	FIPS 46-3 (DES)	56	no
2		DES in ECB, CBC, CBC-MAC mode	FIPS 46-3 (DES), SP 800-38A (ECB), SP 800-38A (CBC), ISO 9797-1, Alg. 1 (CBC-MAC)	56	no
3		TDES	FIPS 46-3 (DES)	112	no
4		TDES	FIPS 46-3 (DES)	168	yes
5		TDES in ECB mode	FIPS 46-3 (DES),, SP 800-38A (ECB)	112, 168	no
6		TDES in CBC, CBC-MAC mode	FIPS 46-3 (DES), SP 800-38A (CBC), ISO 9797-1, Alg. 1 (CBC-MAC)	112	no
7		TDES in CBC, CBC-MAC mode	FIPS 46-3 (DES), SP 800-38A (CBC), ISO 9797-1, Alg. 1 (CBC-MAC)	168	yes
8		AES	FIPS 197 (AES)	128, 192, 256	yes
9		AES in ECB mode	FIPS197 (AES), SP 800-38A (ECB	128, 192, 256	no
10		AES in CBC, CBC-MAC mode	FIPS197 (AES), SP 800-38A (CBC), ISO 9797-1, Alg. 1 (CBC-MAC)	128, 192, 256	yes
11		SHA-1	FIPS 180-2 (SHA)	None	no
12		SHA-{224,256}	FIPS 180-2 (SHA)	None	yes
13		RSA signature generation and verification (RSASSA-PSS)	PKCS#1 v2.1 (RSA)	modulus length = 256-1975	no
14		RSA signature generation and verification (RSASSA-PSS)	PKCS#1 v2.1 (RSA)	modulus length = 1976-5024	yes
15		RSA signature generation and verification without EMSA-PSS (RSASP1, RSAVP1)	PKCS#1 v2.1 (RSA)	modulus length = 256-1975	no
16		RSA signature generation and	PKCS#1 v2.1 (RSA)	modulus length = 1976-5024	yes

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
		verification without EMSA-PSS (RSASP1, RSAVP1)			
17		RSA public key computation (RSAEP, RSAVP1)	PKCS#1 v2.1 (RSA)	modulus length = 256-1975	no
18		RSA public key computation (RSAEP, RSAVP1)	PKCS#1 v2.1 (RSA)	modulus length = 1976-2048 (Straight Forward) or 1976-4096 (CRT)	yes
19		ECDSA signature generation and verification	[ISO 14888-3] (ECDSA)	Key sizes corresponding to the used elliptic curves secp{192}r1 (SEC2) and brainpoolP{192}r1 (RFC 5639)	No
20		ECDSA signature generation and verification	[ISO 14888-3] (ECDSA)	Key sizes corresponding to the used elliptic curves secp{224,256,384, 521}r1 (SEC2) and brainpoolP{224,256, 320,384,512}r1 (RFC 5639)	Yes
21		ECDH	[ISO 11770-3]	Key sizes corresponding to the used elliptic curves secp{192}r1 (SEC2) and brainpoolP{192}r1 (RFC 5639)	No
22		ECDH	[ISO 11770-3]	Key sizes corresponding to the used elliptic curves secp{224,256,384, 521}r1 (SEC2) and brainpoolP{224,256, 320,384,512}r1 (RFC 5639)	Yes
23		RSA encryption and decryption without EME-OAEP (RSAEP, RSADP)	PKCS#1 v2.1 (RSA)	modulus length = 256-1975	no
24		RSA encryption and decryption without EME-OAEP (RSAEP, RSADP)	PKCS#1 v2.1 (RSA)	modulus length = 1976-5024	yes

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
25	Confidentiality	RSA encryption and decryption (RSAES-OAEP)	PKCS#1 v2.1 (RSA)	modulus length = 256-1975	no
26		RSA encryption and decryption (RSAES-OAEP)	PKCS#1 v2.1 (RSA)	modulus length = 1976-5024	yes

Table 3: TOE cryptographic functionality

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 of the TOE is required and thus requested from the sponsor of the certificate.

Some security measures are partly implemented in the hardware and require additional configuration or control or measures to be implemented by the IC Dedicated Support Software or Embedded Software.

For this reason the TOE includes guidance documentation (see table 2) which contains guidelines for the developer of the IC Dedicated Support Software and Embedded Software on how to securely use the microcontroller chip 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 it must be examined if the required measures have been correctly and effectively implemented by the software. Additionally, the evaluation of the composite product or system must also consider the evaluation results as outlined in the document ETR for composite evaluation [10].

The Security Target, the user guidance and the ETR for Composition have changed between the issuance of the original certificate and this revision of the certificate. The TOE’s software and hardware components have not changed. Earlier users of this TOE, e.g. developers of a software platform or application on top, are advised to examine the renewed Security Target and guidance, and assess the impact on their composite solutions. Users of the old certificate revision should examine the impact on their composition of these additional restrictions by a re-assessment or re-certification making use of the new ETR for Composition Document.

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
AIS	Application Notes and Interpretations of the Scheme
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
CBC	Cipher Block Chaining
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ECB	Electronic Codebook Mode
ECDSA	Elliptic Curve Digital Signature Algorithm
ETR	Evaluation Technical Report
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	Information Technology Security Evaluation Facility
MAC	Message Authentication Code
PP	Protection Profile
RSA	Rivest-Shamir-Adleman
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
ST	Security Target
TDES	Triple-DES
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 - A 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 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012

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

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[8].

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

[6] Security Target BSI-DSZ-CC-0750-V2-2014, Version 1.7, 26 June 2014, Crypto Library V2.7/2.9 on SmartMX P5Cx128/P5Cx145 V0v/ V0B(s), NXP Semiconductors, Business Unit Identification (confidential document)

[7] Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007

[8] Security Target Lite BSI-DSZ-CC-0750-V2-2014, Version 1.7, 26 June 2014, Crypto Library V2.7/2.9 on SmartMX P5Cx128/P5Cx145 V0v/ V0B(s), NXP Semiconductors, Business Unit Identification (sanitised public document)

[9] Evaluation Technical Report, Version 1.0, 26 June 2014, Evaluation Technical Report Crypto Library V2.7/2.9 on SmartMX P5Cx128/P5Cx145 V0v/ V0B(s) EAL5+, Brightsight, (confidential document)

[10] ETR for composite evaluation according to AIS 36, Version 1.0, 26 June 2014, ETR for composition Crypto Library V2.7/V2.9 on SmartMX P5Cx128/P5Cx145 according to AIS36, Brightsight (confidential document)

[11] Configuration list:

- List of Configuration Items for Crypto Library v2.7 on P5Cx128/P5Cx145 V0v/ V0B(s), June 23, 2014

[8] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 8, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 9, Evaluationsmethodologie 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 1, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 4, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2, Reuse of evaluation results

- List of Configuration Items for Crypto Library v2.9 on P5Cx128/P5Cx145 V0v/ V0B(s), June 23, 2014

[12] Guidance documentation for the TOE:

- Secured Crypto Library on the P5Cx128/P5Cx145 family, Revision 1.8, June 6, 2014
- AES Library User Guidance Manual “Secured Crypto Library on the SmartMX”, Rev. 1.2 – 19 August 2010
- Secured Crypto Library on the SmartMX. DES Library, Revision 3.2, May 8, 2013
- ECC over GF(p) User Guidance Manual “Secured Crypto Library on the SmartMX”, Rev. 1.4 – 30 March 2010
- Random Number Generator User Guidance Manual “Secured Crypto Library on the SmartMX”, Rev. 5.0 – 24 August 2007
- RSA Library User Guidance Manual “Secured Crypto Library on the SmartMX”, Rev. 4.5, 15 April 2010
- RSA Key Generation User Guidance Manual “Secured Crypto Library on the SmartMX”, Rev. 4.3 – 30 March 2010
- SHA Library User Guidance Manual “Secured Crypto Library on the SmartMX”, Rev. 4.1 – 12 June 2008
- Utility Library User Guidance Manual “Secured Crypto Library on the SmartMX”, Rev. 1.0 – 24 August 2007

[13] Certification report. NXP Secure Smart Card Controllers P5CD128V0v/ V0B(s), P5CC128V0v/ V0B(s), P5CD145V0v/ V0B(s), P5CC145V0v/ V0B(s), P5CN145V0v/V0B(s), BSI-DSZ-CC-0858-2013, Revision 1.0, June 12, 2013

[14] ETR for composition according to AIS36. NXP Secure Smart Card Controllers P5CD128V0A/B, P5CD128V0B(s), P5CC128V0A/B, P5CC128V0B(s), P5CD145V0A/B, P5CD145V0B(s), P5CC145V0A/B, P5CC145V0B(s), P5CN145V0A/B, P5CN145V0B(s). Revision 1.0, April 22, 2013

C Excerpts from the Criteria

CC Part 1:

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

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-0750-V2-2014

Evaluation results regarding development and production environment

The IT product Crypto Library V2.7/2.9 on SmartMX P5Cx128/P5Cx145 V0v/ V0B(s) (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 16 July 2014, 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:

- BU ID Hamburg
  - Requirements, Functional Specification, High-Level Design, Analysis, Low-Level Design , Coding, Design Review, Testing, Code Review, Delivery, Maintenance, User Guidance, Documentation, Tools, Configuration management
- NXP Gratkorn
  - Providing documentation to customer

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.