



Certification Report

BSI-DSZ-CC-0620-2010

for

NXP MIFARE Plus MF1SPLUSx0y1

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



Deutsches IT-Sicherheitszertifikat

erteilt vom



Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0620-2010

Secure Smart Card Controller

NXP MIFARE Plus MF1SPLUSx0y1

from NXP Semiconductors Germany GmbH

PP Conformance: Security IC Platform Protection Profile, Version 1.0,
BSI-CC-PP-0035-2007

Functionality: PP conformant plus product specific extensions,
Common Criteria Part 2 extended

Assurance: Common Criteria Part 3 conformant,
EAL 4 augmented by
ALC_DVS.2, AVA_VAN.5, ASE_TSS.2



Common Criteria
Recognition
Arrangement
for components up to
EAL 4



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 4 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, 17 February 2010

For the Federal Office for Information Security



SOGIS - MRA

Bernd Kowalski
Head of Department

L.S.

This page is intentionally left blank.

Preliminary Remarks

Under the BSIG¹ 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
2.1 European Recognition of ITSEC/CC - Certificates.....	7
2.2 International Recognition of CC - Certificates.....	8
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.....	16
5 Architectural Information.....	16
6 Documentation.....	16
7 IT Product Testing.....	17
8 Evaluated Configuration.....	17
9 Results of the Evaluation.....	18
9.1 CC specific results.....	18
9.2 Results of cryptographic assessment.....	19
10 Obligations and Notes for the Usage of the TOE.....	19
11 Security Target.....	19
12 Definitions.....	19
12.1 Acronyms.....	19
12.2 Glossary.....	20
13 Bibliography.....	21
C Excerpts from the Criteria.....	23
D Annexes.....	33

A Certification

1 Specifications of the Certification Procedure

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

- BSIG²
- BSI Certification Ordinance³
- BSI Schedule of Costs⁴
- 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 3.1⁵ [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

The SOGIS-Mutual Recognition Agreement (MRA) for certificates based on ITSEC became initially effective in March 1998.

This agreement on the mutual recognition of IT security certificates was extended in April 1999 to include certificates based on the Common Criteria for the Evaluation Assurance Levels (EAL 1 – EAL 7). This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and United Kingdom, and from The Netherlands since January 2009 within the terms of this 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 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

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

2.2 International Recognition of CC - Certificates

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

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

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

This evaluation contains the components ALC_DVS.2, AVA_VAN.5, ASE_TSS.2 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 MIFARE Plus MF1SPLUSx0y1 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0586-2009. Specific results from the evaluation process BSI-DSZ-CC-0586-2009 were re-used.

The evaluation of the product NXP MIFARE Plus MF1SPLUSx0y1 was conducted by T-Systems GEI GmbH. The evaluation was completed on 29. January 2010. The T-Systems GEI GmbH is an evaluation facility (ITSEF)⁶ recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: NXP Semiconductors Germany GmbH.

The product was developed by: NXP Semiconductors Germany GmbH.

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

4 Validity of the Certification Result

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

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

⁶ Information Technology Security Evaluation Facility

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 may evolve over time, the resistance of the certified version of the product against new attack methods can be re-assessed if required and the sponsor applies for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme. It is recommended to perform a re-assessment on a regular 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 MIFARE Plus MF1SPLUSx0y1 has been included in the BSI list of the certified products, which is published regularly (see also Internet: [https:// www.bsi.bund.de](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 developer⁷ of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

⁷ NXP Semiconductors Germany GmbH
Business Line Identification
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 called NXP MIFARE Plus MF1SPLUSx0y1 (x and y are wild-card characters which define the size of the EEPROM and the format of the UID). The NXP MIFARE Plus MF1SPLUSx0y1 (short “MF1SPLUSx0y1”) is designed for secure contact-less transport applications and related loyalty programs as well as access management systems.

The TOE is a Smartcard comprising a hardware platform and a fixed software package (Security IC Embedded Software and IC Dedicated Software). The software package provides an operating system with a set of functions used to manage the data stored in the non-volatile EEPROM memory. The TOE includes IC Dedicated Test Software for test purposes after production. The Smart Card Controller hardware comprises an 8-bit processing unit, volatile and non-volatile memories, a cryptographic AES co-processor, security components and a contact-less communication interface. The TOE includes a functional specification and a guidance document. This documentation contains a description of the hardware and software interface, the secure configuration and usage of the product by the terminal designer.

Chapter 1 of the Security Target [6] and [8] gives a detailed TOE description, including its hardware and software description, documentation, life cycle and delivery of the TOE, the TOE intended usage, interfaces of the TOE, and general IT features of the TOE. It also contains a detailed list of all evaluated package types (in chapter 1.4.1.1 and in table 2 of the Security Target [6] and [8]).

Note that since the TOE comprises the complete IC Dedicated Software and the Security IC Embedded Software stored in the ROM there is no possibility to download further Security IC Embedded Software.

A number of package types are supported for the TOE. Each package type has a different commercial type name. For details please read chapter 2 of this report and the Security Target [6] and [8], chapter 1.4.1.1.

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

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 in the PP claimed in the Security Target. Thus the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality (“Security Services” SS and “Security Features” SF):

TOE Security Functionality	Addressed issue
SS.AUTH	Authentication
SS.ACC_CTRL	Access Control
SS.MAC	Message Authentication Code
SS.NO_TRACE	Preventing Traceability
SF.OPC	Control of Operating Conditions
SF.PHY	Protection against Physical Manipulation
SF.LOG	Logical Protection
SF.COMP	Protection of Mode Control

Table 1: TOE Security Functionality

For more details please refer to the Security Target [6] and [8], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [6] and [8], chapter 3.1. Based on these assets the TOE Security Environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [8], chapter 3.

This certification covers different configurations and package formats of the TOE as listed in chapter 2 of this report. See also the Security Target [6] and [8], chapter 1.4.1.1.

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 4, Para. 3, 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 MIFARE Plus MF1SPLUSx0y1

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	NXP MIFARE Plus MF1SPLUSx0y1 Master	t507B, i.e. Release t507B.gds2 (11.02.2009)	Wafer or modules (dice include reference t507B)

No	Type	Identifier	Release	Form of Delivery
2	HW / SW	Mask NXP MIFARE Plus MF1SPLUSx0y1 Via It comprises the following three items (Test ROM, Boot ROM, and MF1SPLUSx0y1 Embedded Software)	Release 002 romt0byf002.eco (08.05.2009)	As part of wafer or modules (dice include reference 002 on via)
2a	SW	Test ROM Software (the IC Dedicated Test Software)	Version 1.13, March 24th, 2009 (DF8_TestOS_YAM1_P ROD.hex)	on the chip as part of item 2
2b	SW	Boot ROM Software (the IC Dedicated Support Software)	Version 1.13, March 24th, 2009 (included in Test ROM)	on the chip as part of item 2
2c	SW	MF1SPLUSx0y1 Embedded Software (the Security IC Embedded Software)	Version 1.20, May 6th, 2009 (MFP_PROD.hex)	on the chip as part of item 2
3	DOC	Data Sheet, MF1SPLUSx0y1, Mainstream contactless smart card IC for fast and easy solution development, NXP Semiconductors [11]	Rev. 3.1, 23 July 2009, Document Number: 171231	electronic document
4	DOC	Guidance, Delivery and Operation Manual, MF1SPLUSx0y1, NXP Semiconductors [12]	Rev. 1.2, 03 December 2009, Document Number 173412	electronic document

Table 2: Deliverables of the TOE

The TOE is manufactured in the IC fabrication SSMC in Singapore indicated by the nameplate (on-chip identifier) t507B. For information about all production and development sites that are related to the evaluated configuration of the TOE please read Annex B of this report.

When the TOE is received from NXP the Historical Bytes of the ATS include "0xC1, 0x05, 0x2F, 0x2F, 0x00, 0x35, 0xC7" there the "0x00, 0x35, 0xC7" at the end of this term are specific for the MF1SPLUSx0y1 as listed in the Guidance, Delivery and Operation Manual, [12], chapter 2.1. The ATS can be changed afterwards during the personalisation of the TOE.

The commercial type name can be used by the customer of NXP to order the TOE with the package type and configuration coded in the name. In consequence this means that a full commercial product name that fits in the variable forms described in table 3 determines that the smart card product is an evaluated product. In addition the hardware and software version can be identified by the nameplate on the surface of the die as described in Chapter 2 of the Guidance, Delivery and Operation Manual, MF1SPLUSx0y1 [12].

Commercial Type Name	Description
MF1SPLUS6021DUD/02	2K EEPROM, 4 byte UID; UID0=xF according to ISO 14443-3, 120µm sawn wafer, L1 card, SW-Version 2
MF1SPLUS6011DUD/02	2K EEPROM, 4 byte UID, 120µm sawn wafer, L1 card, SW-Version 2

Commercial Type Name	Description
MF1SPLUS6001DUD/02	2K EEPROM, 7 byte UID, 120µm sawn wafer, L1 card, SW-Version 2
MF1SPLUS6021DA4/02	2K EEPROM, 4 byte UID; UID0=xF according to ISO 14443-3, MOA4 module on reel, L1 card, SW-Version 2
MF1SPLUS6011DA4/02	2K EEPROM, 4 byte UID, MOA4 module on reel, L1 card, SW-Version 2
MF1SPLUS6001DA4/02	2K EEPROM, 7 byte UID, MOA4 module on reel, L1 card, SW-Version 2
MF1SPLUS8021DUD/02	4K EEPROM, 4 byte UID; UID0=xF according to ISO 14443-3, 120µm sawn wafer, L1 card, SW-Version 2
MF1SPLUS8011DUD/02	4K EEPROM, 4 byte UID, 120µm sawn wafer, L1 card, SW-Version 2
MF1SPLUS8001DUD/02	4K EEPROM, 7 byte UID, 120µm sawn wafer, L1 card, SW-Version 2
MF1SPLUS8021DA4/02	4K EEPROM, 4 byte UID; UID0=xF according to ISO 14443-3, MOA4 module on reel, L1 card, SW-Version 2
MF1SPLUS8011DA4/02	4K EEPROM, 4 byte UID, MOA4 module on reel, L1 card, SW-Version 2
MF1SPLUS8001DA4/02	4K EEPROM, 7 byte UID, MOA4 module on reel, L1 card, SW-Version 2

Table 3: Supported package types and memory configurations of the TOE

The following examples clarify the naming conventions: the commercial type name “MF1SPLUS6011DUD/02” denotes a MIFARE Plus SLIM supplied in wafer form, with 2 K EEPROM, 4 byte UID, manufactured in SSMC and supporting security levels 0, 1 and 3, SW-Version 2. The commercial type name “MF1SPLUS8001DA4/02” denotes a MIFARE Plus SLIM supplied in modules on a reel, with 4K EEPROM, 7 byte UID, manufactured in SSMC and supporting security levels 0,1 and 3, SW-Version 2.

All configurations support the same set of commands. The package type does not influence the security functions 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 Functionality to be used to support the overall security of a smart card system. Therefore, the TOE implements an algorithm to ensure the integrity of data by message authentication and to support secure authentication protocols. The TOE also implements a physical random number generator.

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 and the correct operation of Security Functionality (security mechanisms and associated functions) 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 composite product manufacturing, Generation of secure values, Terminal support to ensure integrity and confidentiality. Details can be found in the Security Target [6] and [8], chapter 4.2.

5 Architectural Information

The TOE is an integrated circuit (smart card controller) with Security IC Embedded Software. There is no possibility to download further Security IC Embedded Software.

The integrated circuit (hardware platform) comprising the components 8-bit CPU, DES co-processor (not enabled in the evaluated configuration), AES co-processor, Random Number Generator (RNG), Contactless Interface, Power Module, Security Sensors and Filters as well as memory blocks. The IC Dedicated Software as well as the Security IC Embedded Software are completely stored in the ROM. The EEPROM is used for data only.

The Security IC Embedded Software provides the main functionality of the TOE in the usage phase. The MF1SPLUSx0y1 is primarily designed for secure contact-less transport applications and related loyalty programs as well as access management systems. Its functionality consists of:

- A data storage system that contains blocks grouped in sectors.
- Authentication on sector level with fine-grained access conditions blocks.
- Message authentication to support replay attack protection.
- Unique serial number for each device (UID) with optional random ID.

The TOE must be personalised according to the security concept and the access control policies of the associated service provider before it can be used in the field. This is a sensitive process that is determining the security of the product and the access rights to the files stored on the TOE.

A comprehensive description of the hardware and software is given in section 2.1 of the Security Target [6] and [8]. The description of the functional interface of the NXP MF1SPLUSx0y1 can be found in the "Data Sheet MF1SPLUSx0y1", [11] and "Guidance, Delivery and Operation Manual, MF1SPLUSx0y1" [12].

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

The tests performed by the developer can be divided into the following categories:

1. Tests of the hardware platform comprising:
 - tests which are performed in a simulation environment with different tools for the analogue circuitries and for the digital parts of the TOE.
 - functional tests which are performed with special software.
 - characterisation and verification tests to release the hardware platform for production including tests with different operating conditions as well as special verification tests for Security Functionality of the hardware.
 - functional tests at the end of the production process using IC Dedicated Test Software.
2. Test of the smart card product comprising:
 - tests of the Security IC Embedded Software in a simulation environment to check the security measures and integrity checks that cannot be tested by external stimulation.
 - regression tests including checks of error conditions.
 - functional tests, of the Security IC Embedded Software including all commands supported.

The developer tests cover all Security Functionality and all security mechanisms as identified in the functional specification as well as in the high and low level designs.

The ITSEF repeated the tests of the developer using the protocol of the tests provided by the developer. The tests of the developer were repeated by sampling. In addition the ITSEF performed additional independent tests to supplement, augment and to verify the tests performed by the developer. The tests of the ITSEF include special tests and examination of the hardware platform using special samples as well as tests of the smart card product using all authentication methods and command sequences supported by the evaluated configuration.

The evaluation provides evidence that the TOE provides the Security Functions as specified by the developer. The test results confirm the correct implementation of the TOE Security Functions.

For penetration testing the ITSEF took all Security Functionality into consideration. Penetration testing was performed to test the security mechanisms used to provide the Security Functionality and considered both physical tampering of the hardware platform and attacks which do not modify the hardware platform physically. The test of the smart card product included attacks that must be averted by the combination of the hardware platform and the software as well as attacks against the software. In addition logical attacks that were based on the command interface of the Security IC Embedded Software were performed.

8 Evaluated Configuration

This certification covers the configurations of the TOE that are listed in table 3 of this report.

For information about the supported EEPROM sizes and different package formats please read chapter 2 of this report which also gives details about the identification of the TOE.

The TOE comprises the complete IC Dedicated Software and Security IC Embedded Software stored in the ROM. There is no possibility to download further Security IC Embedded Software.

9 Results of the Evaluation

9.1 CC specific results

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

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

The following guidance specific for the technology was used:

- The Application of CC to Integrated Circuits
- Application of Attack Potential to Smart Cards
- Functionality classes and evaluation methodology of physical random number generators

(see [4], AIS 25, AIS 26, AIS 31, AIS 34, AIS 35, AIS 37 were used.)

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

- All components of the class ASE
- All components of the EAL 4+ package as defined in the CC (see also part C of this report)
- The components ALC_DVS.2, AVA_VAN.5, and ASE_TSS.2, 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-0586-2009, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was a modified configuration of the product that supports a subset of the security functional requirements certified under BSI-DSZ-CC-0586-2009.

The evaluation has confirmed:

- PP Conformance: Security IC Platform Protection Profile, Version 1.0, BSI-CC-PP-0035-2007 [1]
- for the Functionality: PP conformant plus product specific extensions, Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant, EAL 4 augmented by ALC_DVS.2, AVA_VAN.5, ASE_TSS.2

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 4, Para. 3, Clause 2). This holds for the TOE Security Functionality SS.AUTH: Authentication (AES 128 bit key) and SS.MAC: Message Authentication Code (AES 128 bit key).

10 Obligations and Notes for the Usage of the TOE

The operational documents as outlined in table 2 and the Security Target [6] and [8] contain necessary information about the usage of the TOE and all security hints therein have to be considered.

Since the TOE comprises the complete IC Dedicated Software and Security IC Embedded Software stored in the ROM, there is no possibility to download further Security IC Embedded Software.

Principally, the user has to follow the instructions in the user guidance documents and has to ensure the fulfilment of the assumptions about the environment in the Security Target [6] and [8].

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
ATS	Answer to Select
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Errichtungsgesetz
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CPU	Central Processing Unit
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read Only Memory
IC	Integrated Circuit

IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
OS	Operating System
PP	Protection Profile
RNG	Random Number Generator
ROM	Read Only Memory
SAR	Security Assurance Requirement
SF	Security Feature
SFP	Security Function Policy
SS	Security Service
SSMC	Systems on Silicon Manufacturing Company
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functionality
TSP	TOE Security Policy

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 - A set consisting of all hardware, software, and firmware of the 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 1, September 2006
Part 2: Security functional components, Revision 2, September 2007
Part 3: Security assurance components, Revision 2, September 2007
- [2] Common Methodology for Information Technology Security Evaluation (CEM),
Evaluation Methodology, Version 3.1, Rev. 2, September 2007
- [3] BSI certification: Procedural Description (BSI 7125)
- [4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE⁸
- [5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list
published also in the BSI Website
- [6] Security Target BSI-DSZ-CC-0620, MIFARE Plus MF1SPLUSx0y1, NXP
Semiconductors, Rev. 1.1, 2 June 2009 (confidential document)
- [7] Security IC Platform Protection Profile, Version 1.0, 15.06.2007, registered and
certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the
reference BSI-CC-PP-0035-2007
- [8] ST-lite BSI-DSZ-CC-0620, MIFARE Plus MF1SPLUSx0y1, NXP Semiconductors,
Rev. 1.1, 23rd July 2009 (sanitised public document)
- [9] Evaluation Technical Report BSI-DSZ-CC-0620, Version 1.2, 14-12-2009, NXP
MIFARE Plus MF1SPLUSx0y1, T-Systems GEI GmbH (confidential document)
- [10] MF1PLUSx0y1 and MF1SPLUS0y1 Configuration List, NXP Semiconductors, Rev.
1.5, 24 July 2009 (confidential document)
- [11] Data Sheet, MF1SPLUSx0y1, Mainstream contactless smart card IC for fast and
easy solution development, NXP Semiconductors, Rev. 3.1, 23 July 2009,
Document Number: 171231
- [12] Guidance, Delivery and Operation Manual, MF1SPLUSx0y1, NXP Semiconductors,
Rev. 1.2, 03 December 2009, Document Number 173412

⁸specifically

- AIS 25, Version 6, 07.09.2009, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 6, 07.05.2009, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 1, 25 Sept. 2001 Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 1, 2 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.
- AIS 34, Version 2, 24.10.2008, Evaluation Methodology for CC Assurance Classes for EAL5+
- AIS 35, Version 2.0, 12 November 2007, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 37, Version 2.0, 12 November 2007, Terminologie und Vorbereitung von Smartcard-Evaluierungen

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance Claim (chapter 9.4)

„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 A.

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-

Assurance Class	Assurance Components
	level design presentation
AGD:	AGD_OPE.1 Operational user guidance
Guidance documents	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_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
ATE: Tests	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	2	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-0620-2010

Evaluation results regarding development and production environment



The IT product NXP MIFARE Plus MF1SPLUSx0y1 (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 4 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 17 February 2010, 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) Development, Documentation: NXP Semiconductors GmbH; Business Line Identification; Mikron-Weg 1; A-8101 Gratkorn, Austria
- b) Development: NXP Semiconductors GmbH Business Line Identification Georg-Heyken-Str. 1 D-21147 Hamburg, Germany
- c) Development support: NXP Caen Campus EfficScience, esplanade Anton Philips 2, Colombelles, BP 2000, 14906 Caen cedex 9, France
- d) Semiconductor Factory: Systems on Silicon Manufacturing Co. Pte. Ltd. (SSMC); 70 Pasir Ris Drive 1; Singapore 519527; Singapore
- e) Mask Shop: Toppan Photomasks Korea Ltd.; 345-1, Sooha-Ri ShinDoon-Myon; 467-840 Ichon, South Korea
- f) Wafer Bumping: Chipbond Technology Corporation; No. 3, Li-Hsin Rd. V; Science Based Industrial Park; Hsin-Chu City; Taiwan R.O.C.
- g) Test Center, documentation: NXP Semiconductors GmbH; IC Manufacturing Operations - Test Center Hamburg (IMO TeCH); Stresemannallee 101; D-22529 Hamburg, Germany
- h) Test Center, Module Assembly: NXP Semiconductors (Thailand); Assembly Plant Bangkok, Thailand (APB); 303 Moo 3 Chaengwattana Rd.; Laksi, Bangkok 10210, Thailand

The TOE is manufactured in the IC fabrication SSMC in Singapore indicated by the nameplate (on-chip identifier) t507B.

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.