Certification Report

BSI-DSZ-CC-0712-2011

For

NXP MIFARE DESFire EV1 MF3ICD81

from

NXP Semiconductors Germany GmbH

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0712-2011

Secure Smart Card Controller with Smartcard Embedded Software

NXP MIFARE DESFire EV1 MF3ICD81

from	NXP Semiconductors Germany GmbH
PP Conformance:	Smartcard IC Platform Protection Profile, Version 1.0, July 2001, BSI-PP-0002-2001
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4

Common Criteria
Recognition
Arrangement
for components up to
EAL 4

Common Criteria

The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 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 2.3 (ISO/IEC 15408:2005).

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, 12 July 2011
For the Federal Office for Information Security

SOGIS
IT SECURITY CERTIFIED

Bernd Kowalski   L.S.
Head of Department

This page is intentionally left blank.

Preliminary Remarks

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

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

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

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

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

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

---

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

Contents

A   Certification

1   Specifications of the Certification Procedure

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

- BSIG[2]

- BSI Certification Ordinance[3]

- BSI Schedule of Costs[4]

- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)

- DIN EN 45011 standard

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

- Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)[5] [1]

- Common Methodology for IT Security Evaluation, Version 2.3 [2]

- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

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).

---

[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

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

---

[7]   NXP Semiconductors Germany GmbH
       Stresemannallee 101
       22529 Hamburg

B   Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,

- the relevant evaluation results from the evaluation facility, and

- complementary notes and stipulations of the certification body.

TOE Security Function	Addressed issue
F.AUTH	Authentication
F.ACC_CTRL	Access Control
F.CONFID	Confidentiality and Integrity
F.TRANS	Transaction Control
F.NO_TRACE	Preventing traceability
F.OPC	Control of Operating Conditions
F.PHY	Protection against Physical Manipulation
F.LOG	Logical Protection
F.COMP	Protection of Mode Control

Table 1: TOE Security Functions

For more details please refer to the Security Target [6] and [9], chapter 6.1.

The claimed TOE's Strength of Functions 'high' (SOF-high) for specific functions as indicated in the Security Target [6] and [9], chapter 1.3 is confirmed. The rating of the Strength of Functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2). For details see chapter 9 of this report.

The assets to be protected by the TOE are defined in the Security Target [6] and [9], 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 [9], chapter 3.2, 3.3 and 3.4.

This certification covers different configurations of the TOE. The TOE will be available in four different packages and four different memory configurations. Additionally, there are two different hardware versions, t504C (related to commercial type name MF3ICD81) and t507C (related to commercial type name MF3ICDH81) which implement either 17pF or 70pF input capacitance. The operating system is the same for all different configurations. The individual commercial type name is formed according to the detailed information and naming conventions as displayed in tables 4 and 5 of the Security Target [6] and [9], chapter 2.2. There, you will find all necessary information on the evaluated and certified configurations of the TOE.

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 DESFire EV1 MF3ICD81

The following table outlines the TOE deliverables:

No	Type	Detailed Information	Form of Delivery
1	HW / SW	Hardware platform "t504C": The hardware platform "t504C" provides a resonance capacitor with 17pF. The hardware is named MF3xDyyz/05 with x defining the form, yy defining the EEPROM memory size and z defining the package (see Security Target [6] and [9], chapter 2.2). The hardware platform includes the ROM-layer "romt0cdf005.eco". The ROM-layer comprises: ● IC Dedicated Test Software, t504C005,23.06.2010, DF8_TestOS.hex ● IC Dedicated Support Software, t504C005,23.06.2010, DF8_TestOS.hex ● Smartcard Embedded Software (DESFire EV1) t504C005,15.07.2010, DesFire8.hex The customer can identify the product based on the response of the command "GetVersion": First frame 0x04 0x01 0x01 0x01 0x00 0x"SZ" 0x05 Second frame 0x04 0x01 0x01 0x01 0x04 0x"SZ" 0x05 Hardware platform "t507C": The hardware platform "t507C" provides a resonance capacitor with 70pF. The hardware is named MF3xDHyyz/05 with x defining the form, yy defining the EEPROM memory size and z defining the package (see Security Target [6] and [9], chapter 2.2). The hardware platform includes the ROM-layer "romt0cyf003.eco". The ROM-layer comprises: ● IC Dedicated Test Software, t507C003, 30.06.2010, DF8_TestOS.hex ● IC Dedicated Support Software, t507C003, 30.06.2010, DF8_TestOS.hex ● Smartcard Embedded Software (DESFire EV1) t507C003, 15.07.2010, DesFire8.hex The customer can identify the product based on the response of the command "GetVersion": First frame 0x04 0x01 0x02 0x01 0x00 0x"SZ" 0x05 Second frame 0x04 0x01 0x01 0x01 0x04 0x"SZ" 0x05 Note: "SZ" is the size of the EEPROM as defined in [12] and can have one of the following values: 0x1A, 0x18, 0x16, 0x12.	Wafer or Module
2	DOC	MF3ICD81 MIFARE DESFire EV1 Product Data Sheet, NXP Semiconductors, Doc.No. 134036, Rev. 3.6, 09 February 2011 [11]	electronic document
3	DOC	Guidance, Delivery and Operation Manual, MF3ICD81, Doc.No. 146939, NXP Semiconductors, Rev. 3.9, 26 May 2011 [12]	electronic document

Table 2: Deliverables of the TOE

Both hardware platforms are available with four different EEPROM configurations. The EEPROM size and the hardware version are also part of the response of the command "GetVersion" as described in the table above. Each configuration can be delivered either as die or as module. In case of dice the customer can chose between 120µm and 75µm thick wafers. In case of modules the customer can chose between MOA4 and MOA8 packages.

The commercial type name can be derived from the table 4 and table 5 of the Security Target [6] and [9]. For example the commercial type name MF3ICD4101DUD/05 denotes a NXP MIFARE DESFire EV1 MF3ICD81 with 17pF resonance capacitor supplied in wafer form, with 4 kByte EEPROM and 120µm thick dice. The commercial type name "MF3MODH8101DA4/05" denotes a NXP MIFARE DESFire EV1 MF3ICD81 with 70pF resonance capacitor supplied in modules on a reel, with 8 kByte EEPROM.

The commercial type name is the identification used to order the TOE in the respective package, form and memory configuration. In consequence this means that a full commercial product name that fits in the variable forms described in table 4 and table 5 of the Security Target [6] and [9] determines the certified version of the TOE.

The requirements for the delivery of these package types are described in section 2 of the Guidance [12].

For each delivery form NXP offers two ways of delivery of the TOE:

● The customer collects the product himself at the NXP site.

● The product is sent to the customer by NXP with special protective measures.

These methods are described in the Guidance [12], chapter 2, as part of the requirements for delivery.

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 to ensure an overall smart card system security. Therefore, the TOE implements an algorithm to ensure the confidentiality of plain text data by encryption and to support secure authentication protocols using an internal 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, the correct operation and the confidentiality of Security Functions (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 TOE Development and Production; Protection during Packaging, Finishing and Personalisation; Generation of secure values; Terminal support to ensure integrity and confidentiality. Details can be found in the Security Target [6] and [9] chapter 4.2.

5   Architectural Information

The NXP MIFARE DESFire EV1 MF3ICD81 smart card product is an integrated circuit (smart card controller) with Smartcard Embedded Software. There is no possibility to download further Smartcard Embedded Software.

The Smartcard Embedded Software comprises the complete operating system including the applications. The operating system including the applications supports a command set that comprises proprietary as well as standardised commands. The command set allows different authentication methods between terminal and the TOE and provides various commands to generate, modify and delete different types of files. These files are assigned to applications. The Smartcard Embedded Software allows to setup 28 applications. Each application can store up to 32 files. The possibility to access applications and files depends on the configuration of the Administrator and the Application Manager.

Each of the two different integrated circuits (i.e. hardware platforms) comprise the components 8-bit CPU, Triple- DES coprocessor and AES coprocessors, Random Number Generator (RNG), contact-less Communication Interface, Power Control, Security Sensors and Filters as well as memory blocks. The IC Dedicated Software as well as the Smartcard Embedded Software is completely stored in the ROM. The IC Dedicated Support Software and the Smartcard Embedded Software are identical for both hardware platforms. The EEPROM is used for data only.

To ensure the separation between the different applications the TOE must be personalised according to the security concept and the access control policies of the associated service provider before it is used in the field. This is a sensitive process that is determining the security of the product and the integrity and confidentiality of the files stored in the different applications.

For more information about the architectural information about the TOE see also the Security Target [6] and [9] chapter 2.1.

6   Documentation

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

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

7   IT Product Testing

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

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 Functions of the hardware,

- functional tests at the end of the production process using IC Dedicated Test Software.

Test of the smart card product comprising:

- tests of the Smartcard 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 Smartcard Embedded Software including all commands supported.

The developer tests cover all Security Functions 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 on both hardware platforms using special samples as well as tests of the smart card products using all authentication methods and command sequences supported by the evaluated configurations. The same set of evaluator tests was performed for both hardware platforms.

The evaluation gives 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 Functions into consideration. Extensive penetration testing was performed to test the security mechanisms used to provide the Security Functions. The tests for both hardware platforms comprise the use of bespoke equipment and expert knowledge. The penetration tests considered both the physical tampering of the hardware platforms and attacks which do not modify the hardware platform physically. The tests of the smart card products comprise 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 are performed based on the logical interface using various command sequences. These logical tests include tests with data values and protocol parameters outside the specified ranges, command sequences that must generate errors and random sequences of commands.

8   Evaluated Configuration

A combination of different package types and configurations of the TOE are included in the certification. Each variant has a different commercial type name. The TOE will be available in four different packages and four different memory configurations. Additionally, there are two different hardware versions, t504C (relating to MF3ICD81) and t507C (relating to MF3ICDH81) which implement either 17pF or 70pF input capacitance.

For information about the different commercial type names in relation to the two hardware platforms, the EEPROM variations, and the different package formats please read chapter 2 of this report and chapter 2.2 of the Security Target [6] and [9] .

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [7] 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:

(i) *The Application of CC to Integrated Circuits*

(ii) *Application of Attack Potential to Smart Cards*

(iii) *Functionality classes and evaluation methodology of physical random number generators*

(see [9], AIS 25, AIS 26, AIS 31, AIS 34, AIS 35, AIS 37 were used.)

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 class ASE

● All components of the EAL 4 package as defined in the CC (see also part C of this report)

● The components ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4 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-0487-2009, re-use of specific evaluation tasks was possible. The initial hardware platform t504C was not changed. The re-evaluation includes an additional hardware platform t507C with another resonance capacity to support different antennas. The security functionality of both hardware platforms is the same. The operating system of the initial evaluation assessed in BSI-DSZ-CC-0487-2009 has not been changed. The same operating system is implemented on both hardware platforms. Thus the security functions and the interfaces are the same, however the response of the command "GetVersion" was updated to support the distinction of the different versions of the TOE. The IC Dedicated Support Software was updated to improve the stability of the boot phase and enable an additional security feature. The IC Dedicated Support Software is only active during the boot phase of the chip. In addition the IC Dedicated Test Software was updated to increase the resistance against misuse. Furthermore new delivery types were introduced and an additional configured EEPROM size is supported.

The evaluation has confirmed:

● PP Conformance: Smartcard IC Platform Protection Profile, Version 1.0, July 2001, BSI-PP-0002-2001 [10]

- 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
                          ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4

- The following TOE Security Functions fulfil the claimed Strength of Function high:
  F.AUTH, F.LOG.
  In order to assess the Strength of Function the scheme interpretations AIS 25, AIS 26 and AIS 31(see [4]) were used.

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 rating of the Strength of Functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2). This holds for the TOE Security Function F.AUTH (two-key and three-key Triple-DES and AES 128 bit key) and F.CONFID (supporting the AES algorithm).

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

– hash functions:

– algorithms for the encryption and decryption:

   - 2-key Triple-DES, 3-key Triple-DES, 112 or 168 bit, according to FIPS PUB 46-3;

   - 128-bit AES according to FIPS PUB 197.

This holds for the following security functions:

   - F.AUTH, authentication of subjects is performed by a cryptographic challenge-response;

   - F.CONFID supporting the AES algorithm.

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

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

10   Obligations and Notes for the Usage of the TOE

The operational documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

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

Principally, the user has to follow the instructions in the user guidance document [12] and has to ensure the fulfilment of the assumptions about the environment in the Security Target [6] and [9].

11   Security Target

For the purpose of publishing, the Security Target [9] 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
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
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
OS	Operating System
PP	Protection Profile
RSA	Rivest Shamir Adleman Algorithmus
SF	Security Function
SFP	Security Function Policy

SOF   Strength of Function

ST   Security Target

TOE   Target of Evaluation

TSC   TSF Scope of Control

TSF   TOE Security Functions

TSP   TOE Security Policy

12.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance 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 entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

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

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

13   Bibliography

[1]   Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

[2]   Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2.3, August 2005

[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, BSI 7149), periodically updated list published also on the BSI Website

[6]   Security Target, MIFARE DESFire EV1 MF3ICD81 Secure Smart Card Controller, NXP Semiconductors, Rev. 2.1, 10 May 2011 (confidential document)

[7]   Evaluation Technical Report, NXP MIFARE DESFire EV1 MF3ICD81, BSI-DSZ-CC-0712 Version 1.5, 24 June 2011, T-Systems GEI GmbH (confidential document)

[8]   MIFARE DESFire EV1 MF3ICD81 Configuration List, NXP Semiconductors, Rev. 1.6, 10. May 2011; MIFARE DESFire EV1 MF3ICDH81 Configuration List, NXP Semiconductors, Rev. 1.6, 10. May 2011 (confidential documents)

[9]   Security Target Lite, MIFARE DESFire EV 1 MF3ICD81, NXP Semiconductors, Rev. 1.5, 10 May 2011 (sanitised public document)

[10]   Smartcard IC Platform Protection Profile, Version 1.0, July 2001, BSI-PP-0002-2001

[11]   MF3ICD81 MIFARE DESFire EV1 Product Data Sheet, NXP Semiconductors, Doc.No. 134036, Rev. 3.6, 09 February 2011

[12]   Guidance, Delivery and Operation Manual, MF3ICD81, Doc.No. 146939, NXP Semiconductors, Rev. 3.9, 26 May 2011

---

[8]   specifically

- AIS 25, Version 6, 7 September 2009, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document

- AIS 26, Version 7, 3 August 2010, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document

- AIS 31, Version 1, 25 September 2001 Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren

- AIS 32, Version 6, 3 August 2010, CC-Interpretationen im deutschen Zertifizierungsschema

- AIS 34, Version 3, 3 September 2009, Evaluation Methodology for CC Assurance Classes for EAL5+ (CCv2.3 & CCv3.1) and EAL6 (CCv3.1)

- AIS 35, Version 2.0, 12 November 2007, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies

- AIS 36, Version 3, 19 October 2010, Kompositionsevaluierung including JIL Document and CC Supporting Document

- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

This page is intentionally left blank.

C　　Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

"The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to CC Part 2 (functional requirements), CC Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

–　**CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.

–　**CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

–　**CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.

–　**CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

–　**Package name Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.

–　**Package name Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

–　**PP Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result."

CC Part 3:

Protection Profile criteria overview (chapter 8.2)

"The goal of a PP evaluation is to demonstrate that the PP is complete, consistent, technically sound, and hence suitable for use as a statement of requirements for one or more evaluatable TOEs. Such a PP may be eligible for inclusion within a PP registry.

Assurance Class	Assurance Family
Class APE: Protection Profile evaluation	TOE description (APE_DES)
	Security environment (APE_ENV)
	PP introduction (APE_INT)
	Security objectives (APE_OBJ)
	IT security requirements (APE_REQ)
	Explicitly stated IT security requirements (APE_SRE)

Table 3 - Protection Profile families - CC extended requirements"

Security Target criteria overview (Chapter 8.3)

"The goal of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.

Assurance Class	Assurance Family
Class ASE: Security Target evaluation	TOE description (ASE_DES)
	Security environment (ASE_ENV)
	ST introduction (ASE_INT)
	Security objectives (ASE_OBJ)
	PP claims (ASE_PPC)
	IT security requirements (ASE_REQ)
	Explicitly stated IT security requirements (ASE_SRE)
	TOE summary specification (ASE_TSS)

Table 5 - Security Target families - CC extended requirements "

Assurance categorisation (chapter 7.5)

"The assurance classes, families, and the abbreviation for each family are shown in Table 1.

Assurance Class	Assurance Family
ACM: Configuration management	CM automation (ACM_AUT)
	CM capabilities (ACM_CAP)
	CM scope (ACM_SCP)
ADO: Delivery and operation	Delivery (ADO_DEL)
	Installation, generation and start-up (ADO_IGS)
ADV: Development	Functional specification (ADV_FSP)
	High-level design (ADV_HLD)
	Implementation representation (ADV_IMP)
	TSF internals (ADV_INT)
	Low-level design (ADV_LLD)
	Representation correspondence (ADV_RCR)
	Security policy modeling (ADV_SPM)
AGD: Guidance documents	Administrator guidance (AGD_ADM)
	User guidance (AGD_USR)
ALC: Life cycle support	Development security (ALC_DVS)
	Flaw remediation (ALC_FLR)
	Life cycle definition (ALC_LCD)
	Tools and techniques (ALC_TAT)
ATE: Tests	Coverage (ATE_COV)
	Depth (ATE_DPT)
	Functional tests (ATE_FUN)
	Independent testing (ATE_IND)
AVA: Vulnerability assessment	Covert channel analysis (AVA_CCA)
	Misuse (AVA_MSU)
	Strength of TOE security functions (AVA_SOF)
	Vulnerability analysis (AVA_VLA)

Table 1: Assurance family breakdown and mapping"

Evaluation assurance levels (chapter 11)

"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 11.1)

"Table 6 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 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 extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 6: Evaluation assurance level summary"

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 11.3)

"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 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, and that it provides useful protection against identified threats."

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 11.4)

"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 practice. 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 11.5)

"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 practices.

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 11.6)

"Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices 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 11.7)

"Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices 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 11.8)

"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 11.9)

"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."

Strength of TOE security functions (AVA_SOF) (chapter 19.3)

"Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim."

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users."

"Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis."

"Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential."

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-0712-2011

Evaluation results regarding development and production environment

The IT product NXP MIFARE DESFire EV1 MF3ICD81 (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 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 2.3 (ISO/IEC 15408:2005).

As a result of the TOE certification, dated 12 July 2011, the following results regarding the development and production environment apply. The Common Criteria Security Assurance Requirements

- ACM – Configuration management (i.e. ACM_AUT.1, ACM_CAP.4, ACM_SCP.2),

- ADO – Delivery and operation (i.e. ADO_DEL.2, ADO_IGS.1) and

- ALC – Life cycle support (i.e. 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 Unit Identification; Mikron-Weg 1; A-8101 Gratkorn

   b) Semiconductor Factory: Systems on Silicon Manufacturing Co. Pte. Ltd. (SSMC); 70 Pasir Ris Drive 1; Singapore 519527; Singapore

   c) Mask Shop: Photronics Singapore Pte. Ltd.; 6 Loyang Way 2; Loyang Industrial Park; Singapore 507099; Singapore

   d) Mask Shop: Photronics Semiconductors Mask Corp. (PSMC); 1F, No.2, Li-Hsin Rd.; Science-Based Industrial Park; Hsin-Chu City Taiwan R.O.C.

   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) Development, Documentation, Test Center: NXP Semiconductors GmbH; Hamburg (IMO TeCH); Stresemannallee 101; D-22529 Hamburg

   h) Module Assembly, Test Center: NXP Semiconductors (Thailand); Assembly Plant Bangkok, Thailand (APB); 303 Moo 3 Chaengwattana Rd.; Laksi, Bangkok 10210 Thailand

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 [9]) are fulfilled by the procedures of these sites.

This page is intentionally left blank.