Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0861-2014

for

MICARDO V4.0 R1.0 eHC v1.2

from

Morpho Cards GmbH

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

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0861-2014

eHealth: Smart Cards

MICARDO V4.0 R1.0 eHC v1.2

from	Morpho Cards GmbH
PP Conformance:	Protection Profile for electronic Health Card (eHC) - elektronische Gesundheitskarte (eGK), Version 2.9, 19 April 2011, BSI-CC-PP-0020-V3-2010-MA-01
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by AVA_VAN.5

Common Criteria Recognition Arrangement for components up to EAL 4

Common Criteria

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

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 15 May 2014
For the Federal Office for Information Security

Bernd Kowalski
Head of Department

L.S.

SOGIS Recognition Agreement

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

This page is intentionally left blank.

Preliminary Remarks

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

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

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

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

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

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

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

Contents

A Certification

1 Specifications of the Certification Procedure

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

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

2 Recognition Agreements

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

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

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

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic). In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

---

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

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

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

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

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

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

2.2 International Recognition of CC – Certificates (CCRA)

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

As of September 2011 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

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

This evaluation contains the component AVA_VAN.5 that is 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 MICARDO V4.0 R1.0 eHC, v1.2 has undergone the certification procedure at BSI.

The evaluation of the product MICARDO V4.0 R1.0 eHC, v1.2 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 30 April 2014. SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Morpho Cards GmbH.

The product was developed by: Morpho Cards GmbH.

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

4 Validity of the Certification Result

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

[6] Information Technology Security Evaluation Facility

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

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

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

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

5 Publication

The product MICARDO V4.0 R1.0 eHC, v1.2 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

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

[7] Morpho Cards GmbH
An der Talle 89
33102 Paderborn

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 the product MICARDO V4.0 R1.0 eHC v1.2 provided by Morpho Cards GmbH. It is an electronic Health Card (eHC) representing a smart card with contacts programmed according to ISO 7816-1 to 3 containing Electronic Health Card Applications with the related user data and associated guidance documentation.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile for electronic Health Card (eHC) - elektronische Gesundheitskarte (eGK), Version 2.9, 19 April 2011, BSI-CC-PP-0020-V3-2010-MA-01 [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 AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [8], chapter 6.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functions of the Smartcard Embedded Software:

TOE Security Functionality	Addressed issue
F.ACS_SFP	Security Attribute Based Access Control
F.IA_AKEY	Key Based User / TOE Authentication Based on Asymmetric Cryptography
F.IA_SKEY	Key Based User / TOE Authentication Based on Symmetric Cryptography
F.IA_PWD	Password Based User Authentication
F.DATA_INT	Stored Data Integrity Monitoring and Action
F.EX_CONF	Confidentiality of Data Exchange
F.EX_INT	Integrity and Authenticity of Data Exchange
F.RIP	Residual Information Protection
F.FAIL_PROT	Hardware and Software Failure Protection
F.SIDE_CHAN	Side Channel Analysis Control
F.SELFTEST	Self-Test
F.CRYPTO	Cryptographic Support
F.GEN_DIGSIG	RSA Generation of Digital Signatures
F.VER_DIGSIG	RSA Verification of Digital Signatures
F.RSA_ENC	RSA Encryption
F.RSA_DEC	RSA Decryption

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] and [8], chapter 7.1.2.

The assets to be protected by the TOE are defined in the Security Target [6] and [8], chapter 3.1.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [8], chapter 3.2, 3.3 and 3.4.

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

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

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

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

MICARDO V4.0 R1.0 eHC, v1.2

There are two different delivery configurations for the TOE.

a) If delivered after phase 4 in the life-cycle model, the product is delivered to an external initialiser as un-initialised smartcard or module. Dedicated initialisation files, the product data sheet, and the guidance for the initialiser and the personaliser are included.

b) If delivered after phase 5 of the life-cycle model, the product is delivered to an external personaliser as initialised smartcard or module. The product data sheet and the guidance for the personaliser are included.

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery	a)	b)
1	HW/SW	NXP SmartMX2 P60C080[8] Secure Smart Card Controller (incl. its IC Dedicated Software, covering in particular the NXP SmartMX2 P60C080PVC(y) Crypto Library)	V1.0	Delivery of un-initialised / initialised modules or smartcards	yes	yes
2	SW	Smartcard Embedded Software / Part Basic Software (implemented in ROM/EEPROM of the microcontroller)	V4.0	Delivery of initialisation files in electronic form (if applicable)	yes	yes
3	SW	Smartcard Embedded Software / Part Application Software (containing the eHC Application implemented in the EEPROM of the microcontroller)	R10	Delivery of initialisation files in electronic form (if applicable)	yes	yes
4	DOC	User guidance for the User of the MICARDO Operating System platform [12]	X1.005	Document in paper form / electronic file	yes	yes
5	DOC	User guidance for the Initialiser of the eHC Card [11]	X1.004	Document in paper form / electronic file	yes	no
6	DOC	User guidance for the Personaliser of the eHC Card (in particular the eHC Application) [10]	X1.002	Document in paper form / electronic file	yes	yes

[8] For details on the eHC's chip and the IC Dedicated Software see certification report BSI-DSZ-CC-0837-2013

No	Type	Identifier	Release	Form of Delivery	a)	b)
7	DOC	Data Sheet with information on the actual identification data and configuration of the eHC Card delivered to the customer	n.a.	Document in paper form / electronic file	yes	yes
8	DOC	File containing data needed for the initialisation process	5161	Document in paper form / electronic file	yes	no
9	KEY	Public part of the authentication key pair relevant for the authenticity of the eHC Card Note: The card's authentication key pair is generated by Morpho Cards GmbH and depends on the TOE's configuration delivered to the customer. Furthermore, the key pair may be chosen customer specifically.	n.a.	Document in paper form / electronic file	yes	yes
10	KEY	Personalisation key relevant for the personalisation of the eHC Card Note: The card's personalisation key pair is generated by Morpho Cards GmbH and depends on the TOE's configuration delivered to the customer. Furthermore, the key may be chosen customer specifically.	n.a.	Document in paper form / electronic file	yes	yes

Table 2: Deliverables of the TOE

The IC embedded software consists of the operating system MICARDO V4.0 R1.0 eHC v1.2. The initialisation and personalisation agent can use the 'Get Data' command to read out the chip information and identify the chip and its embedded software. The format of the data returned is as follows:

Byte #	Data type
1-2	offset bytes
3-4	ICC serial number
5	chip manufacturer
6	chip and mask identification
7-8	time stamp
9-13	batch number
14	wafer number
15	X-coordinate on wafer
16	Y-coordinate on wafer

Table 3: Retun data if 'Get Data'

The identification data must comply with the data given in Annex D of [10] in order for the TOE to be verified as certified version.

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. The TOE is the composition of an IC with Smartcard Embedded Software, including the eHC Application and will be used as electronic Health Card (eHC).

The security policy of the TOE is to provide basic Security Functions to ensure an overall smartcard system security. Therefore, the TOE will implement an algorithm to ensure the confidentiality of plain text data by encryption and to support secure authentication protocols. 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 security objectives related to the environment of the TOE's dedicated eHC Application can be found in the protection profile [7] in chapter 4.2 and 4.3. See also the Security Target [6] and [8] chapter 4.2 and 4.3.

5 Architectural Information

The TOE is a composite product. It is composed from an Integrated Circuit, IC Embedded Software and IC Application Software containing the eHC Applications. The IC Embedded software contains the operating system MICARDO V4.0 R1.0 eHC v1.2. For details concerning the CC evaluation of the NXP IC see the evaluation documentation under the certification ID BSI-DSZ-CC-0837-2013 and for details concerning the CC evaluation of the NXP cryptographic library see the evaluation documentation under the certification ID NSCIB-CC-12-36243.

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 developer tested all TOE Security Functions either on real cards or with emulator tests. For all commands and functionality tests, test cases are specified in order to demonstrate its expected behavior including error cases. Hereby a representative sample including all boundary values of the parameter set, e.g. all command APDUs with valid and invalid inputs were tested and all functions were tested with valid and invalid inputs. Repetition of developer tests were performed during the independent evaluator tests.

The developer tests include a full coverage of all security functionality. Furthermore penetration tests were chosen by the evaluators for those Security Functions where internal secrets of the card might be modified or observed during testing. During their independent testing, the evaluators covered

- testing APDU commands related to Access Control,
- testing APDU commands related to Identification and Authentication,
- testing APDU commands related to the Secure Messaging Channel,
- testing APDU commands related to the Creation of Digital Signatures,
- penetration testing related to verify the Reliability of the TOE,
- source code analysis performed by the evaluators,
- side channel analysis for SHA and RSA,
- fault injection attacks (laser attacks),
- fault injection attacks (alpha radiation attacks),
- statistical testing of the output of the deterministic random number generator,
- testing APDU commands for the initialization, personalization and usage phase,
- testing APDU commands for the commands using cryptographic mechanisms.

The evaluators have tested the TOE systematically against high attack potential during their penetration testing. The achieved test results correspond to the expected test results.

8 Evaluated Configuration

The evaluated TOE configuration is defined by the notation: “MICARDO V4.0 R1.0 eHC v1.2” and configured as described in the Guidance document [11] provided with the TOE. The initialisation and personalisation agent can use the ‘GetData’ command to read out the chip information and identify the chip. The following table (cf. Table 3) describes the evaluated configuration:

Byte #	Data type	Data of evaluated TOE
1-2	offset bytes	'0000'
3-4	ICC serial number	'12A4'
5	chip manufacturer	'04'
6	chip and mask identification	'0A'

Byte #	Data type	Data of evaluated TOE
7-8	time stamp	'1A45'
9-13	batch number	'91 65 53 00 00'
14	wafer number	'10'
15	X-coordinate on wafer	'07'
16	Y-coordinate on wafer	'3C'

Table 4: Evaluated Configuration

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] and guidance specific for the technology of the product [4] (AIS 34) was used.

The following guidance specific for the technology was used:

- Application of CC to Integrated Circuits (AIS 25)
- Application of Attack Potential to Smart Cards (AIS 26)
- Functionality classes and evaluation methodology of physical random number generators (AIS 31)
- Composite product evaluation for Smart Cards and similar devices (AIS 36)

According to this concept the relevant guidance documents of the underlying platform and the documents ETR for Composition from the platform evaluations (i.e. [14], [15], [16], [17], [18]) have been applied in the TOE evaluation.

(see [4], AIS 20, AIS 25, AIS 31, AIS 36).

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

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

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

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

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

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0673-2010, re-use of specific evaluation tasks was possible. The primary objective of the re-certification was the porting of the HAL from P5CC080V0B to P60C080P_VC(y) including integration of P60 Crypto-Library and MICARDO V3.5 patches into the MICARDO V4.0 ROM mask. Secondary objective was a review of the security architecture and evolution of the development environment.

The evaluation has confirmed:

- PP Conformance: Protection Profile for electronic Health Card (eHC) - elektronische Gesundheitskarte (eGK), Version 2.9, 19 April 2011, BSI-CC-PP-0020-V3-2010-MA-01 [7]
- 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 AVA_VAN.5

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

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

9.2 Results of cryptographic assessment

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

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
Authenticity	RSA Signature Generation with padding variantRSA_ISO 9796_2_DS1_SIGN	PKCS#1 ISO 9796-2	Moduluslength= 2048	[19] [20]	RSA Generation of Digital Signatures (FCS_COP.1/CCA_SIGN)
	RSA Signature Generation with padding variant RSASSA-PSS-SIGN	PKCS#1	Moduluslength= 2048	[19] [20]	RSA Generation of Digital Signatures (FCS_COP.1/CSA)
	RSA Signature Verification with padding variant RSA_ISO9796_2_DS1_VERIFY	PKCS#1 ISO 9796-2	Moduluslength= 2048	[19] [20]	RSA Verification of Digital Signatures (FCS_COP.1/CCA_VERIF)

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
Authentication	Authentication scheme based on 3TDES in CBC-Mode and Retail-MAC	ANSI X9.52, NIST 800-38B, ANSI X9.19, [21]	|k|=168	[19] [20]	Key Based User / TOE Authentication Based on Symmetric Cryptography (FCS_COP.1/SM)
Key Agreement	SHA-256	FIPS 180-4	n.a.	[19] [20]	Hash for key derivation Cryptographic Support (FCS_COP.1/Hash, FCS_CKM.1/SM)
Confidentiality	3TDES in CBC-Mode	ANSI X9.52 NIST 800-38B	|k|=168	[19] [20]	Secure Messaging Confidentiality of Data Exchange Cryptographic Support (FCS_COP.1/Sym)
	RSA Decryption RSAESPKCS1-V1_5 RSA-OAEP	PKCS#1	Moduluslength= 2048	[19] [20]	RSA Decryption (FCS_COP.1/Asym_DEC)
Integrity	Retail-MAC with 3TDES	ANSI X9.52, ANSI X9.19	|k|=168	[19] [20]	Cryptographic Support (FCS_COP.1/MAC)
Cryptographic Primitive	DRG.3	AIS20 [4] Custom solution based on ANSI X9.17 / ANSI X9.31	n.a.	[20]	Cryptographic Support (FCS_RND.1)

Table 5: TOE cryptographic functionality

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2).

According to the mentioned standards of implementation the algorithms are suitable for the purpose of their usage. An explicit validity period is not given.

10 Obligations and Notes for the Usage of the TOE

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

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and

techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

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

11 Security Target

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

12 Definitions

12.1 Acronyms

AIS	Application Notes and Interpretations of the Scheme
APDU	Application Protocol Data Unit
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
eHC	Electronic Health Card
ETR	Evaluation Technical Report
IC	Integrated Circuit
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
HAL	Hardware Abstraction Layer
PP	Protection Profile
RSA	Rivest-Shamir-Adleman Algorithm
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

12.2 Glossary

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

13 Bibliography

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

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

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

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[9].

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

[6] Security Target BSI-DSZ-CC-0861-2014, Version X1.00.19, 10 April 2014, Security Target – MICARDO V4.0 R1.0 V1.2, Morpho Cards GmbH (confidential document)

[7] Protection Profile for electronic Health Card (eHC) - elektronische Gesundheitskarte (eGK), Version 2.9, 19 April 2011, BSI-CC-PP-0020-V3-2010-MA-01, Bundesamt für Sicherheit in der Informationstechnik (public document)

[8] Security Target Lite BSI-DSZ-CC-0861-2014, Version V1.00, 17 April 2014, Security Target – MICARDO V4.0 R1.0 V1.2, Morpho Cards GmbH (public document)

[9] Evaluation Technical Report BSI-DSZ-CC-0861, Version 1.8, 25 April 2014, SRC Security Research & Consulting GmbH (confidential document)

[10] Preparative Procedures for the Personaliser for MICARDO V4.0 R1.0 V1.2, Version X1.002, 17 January 2013, Morpho Cards GmbH (confidential document)

[11] Preparative Procedures for the Initialiser for MICARDO V4.0 R1.0 V1.2, Version X1.004, 02 December 2013, Morpho Cards GmbH ()

[12] Operational User Guidance for MICARDO V4.0 R1.0 V1.2, Version X1.005, 04 July 2013, Morpho Cards GmbH ()c

[13] Configuration list for the TOE, Configuration List: Micardo v4.0 Release 1 (Software Release Sheet – SRS), Version X1.0010, 10 April 2014, Morpho Cards GmbH (confidential document)

[9] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 7, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 8, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 35, Version 1, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 4, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2, Reuse of evaluation results

[14] Certification Report BSI-DSZ-CC-0837-2013 for NXP Smart Card Controller P60D080PVC and its major configurations P60D052PVC, P60D040PVC, P60C080PVC, P60C052PVC and P60C040PVC from NXP Semiconductors Germany GmbH, 24 June 2013, Bundesamt für Sicherheit in der Informationstechnik

[15] Assurance Continuity Maintenance Report BSI-DSZ-CC-0837-2013-MA-01, 04 February 2014, Bundesamt für Sicherheit in der Informationstechnik

[16] ETR for composition according to AIS36, NXP Secure Smart Card Controller P60x040/052/080 VC, BSI-DSZ-CC-0837, Version 5.0, 23 April 2013, TÜV Informationstechnik GmbH

[17] ETR for composition according to AIS36, Crypto Library V1.0 on P60x080/052/040 PVC, NSCIB-CC-36243, Version 5.0, 24 July 2013, brightsight b.v.

[18] Assurance Continuity Maintenance Report, NSCIB-CC-12-36243-MA1, 09 April 2014, NLNCSA

[19] Spezifikation der elektronischen Gesundheitskarte, Teil 1: Spezifikation der elektrischen Schnittstelle, as specified in the Base Roll-Out Release 0.5.3 eGK V1.0.0 (including SRQ supplements), 11 April 2011, gematik mbH

[20] Technische Richtlinie BSI TR-03116-1, Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 1: Telematikinfrastruktur, Version 3.18, 30 January 2014, Bundesamt für Sicherheit in der Informationstechnik

[21] DIN EN 14890-1:2008, Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic services

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part 1:

Conformance Claim (chapter 10.4)

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

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

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

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

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

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

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

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

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

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

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

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

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

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

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

The following table shows the assurance class decomposition.

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

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

Assurance class decomposition

Evaluation assurance levels (chapter 8)

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

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

Evaluation assurance level (EAL) overview (chapter 8.1)

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

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

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

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

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

Table 1: Evaluation assurance level summary”

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

“Objectives

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

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

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

Class AVA: Vulnerability assessment (chapter 16)

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

Vulnerability analysis (AVA_VAN) (chapter 16.1)

“Objectives

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

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

This page is intentionally left blank

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development and production environment

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0861-2014

Evaluation results regarding development and production environment

The IT product MICARDO V4.0 R1.0 eHC, v1.2 (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 15 May 2014, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.1, ALC_LCD.1, ALC_TAT.1)

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

No.	Site	Task within the evaluation
1	Morpho Cards GmbH e-Documents Division Riemekestraße 160 33106 Paderborn Germany	Development
2	Morpho Cards GmbH Konrad-Zuse-Ring 1 24220 Flintbek Germany	Production, initialisation and card production site
3	Multiple sites	Inlay manufacturing The inlay of the TOE is assembled at the sites covered by the hardware evaluation BSI-DSZ-CC-0837-2013, see Annex B of [14]

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]) are fulfilled by the procedures of these sites.

This page is intentionally left blank.