Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0425-2009

for

Electronic Health Card and SSCD
Version 2.10

from

Gemalto

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-0425-2009

Electronic Health Card and SSCD
Version 2.10

from	Gemalto
PP Conformance:	Common Criteria Protection Profile electronic Health Card (eHC) – elektronische Gesundheitskarte (eGK), BSI-PP-0020-V2-2007-MA02
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, 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, 07 October 2009
For the Federal Office for Information Security

IT Security Certified
SOGIS - MRA

Bernd Kowalski
Head of Department

L.S.

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

This page is intentionally left blank.

Preliminary Remarks

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

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

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

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

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

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

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

Contents

A Certification

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 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

2.1 European Recognition of ITSEC/CC - Certificates

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

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

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

2.2 International Recognition of CC - Certificates

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

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

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

This evaluation contains the components ADV_IMP.2, AVA_MSU.3 and AVA_VLA.4 that are not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4 components of these assurance families are relevant.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product Electronic Health Card and SSCD Version 2.10 has undergone the certification procedure at BSI.

The evaluation of the product Electronic Health Card and SSCD Version 2.10 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 2 October 2009. The TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Gemalto

The product was developed by: Gemalto

[6] Information Technology Security Evaluation Facility

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

4 Validity of the certification result

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

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

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods may evolve over time, the resistance of the certified version of the product against new attack methods can be re-assessed if required and the sponsor applies for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme. It is recommended to perform a re-assessment on a regular basis.

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

5 Publication

The product Electronic Health Card and SSCD Version 2.10 has been included in the BSI list of the 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] Gemalto
Adalperostrasse 45
85737 Ismaning

This page is intentionally left blank.

B Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1 Executive Summary

The Target of Evaluation (TOE) is a Smart Card Integrated Circuit (IC) with a Gemalto Embedded Software (ES) and Applicative Data Structures (APP) including a health application and a Digital Signature application. The TOE is intended to be used as an Electronic Health Card and SSCD and is conformant to the specification documents ”The specification of the German Electronic Health Card eHC” [18 and 19]. The TOE is also aimed to be compliant to the requirement specified for products for electronic signatures in the German Digital Signature Act (SigG -§17(1)) [24], Ordinance (SigV - §15(1,4)), Appendix 1 [25] and the Directive [23] Annex 3.

The evaluation of the TOE was conducted as a composite evaluation making use of the platform evaluation results of the CC evaluation of the underlying Smart Card Integrated circuit Infineon SLE66CX680PE / m1534-a14. The IC is certified at the level EAL5+ and is registered under the Certification-ID BSI-DSZ-CC-0437-2008-MA-02, see [15] The evaluation of the IC is based on the Protection Profile “Smartcard IC Platform Protection Profile” [12]. Within the composite evaluation process, the evaluation of the Electronic Health Card and SSCD is built on the results of the evaluation of the IC.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile “Electronic Health Card (eHC)” BSI-PP-0020-V2-2007-MA02 [10] which defines the security objectives and requirements for the electronic Health Card (German: “elektronische Gesundheitskarte”) based on the regulations for the German health care system. It addresses the security services provided by this card. Furthermore, the Security Target is based on but not conformant to the certified Protection Profile Secure Signature-Creation Device Type 3, EAL 4+, BSI-PP-0006-2002 [11].

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

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [9], chapter 5.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The Security Functional Requirements (SFR) relevant for the IT-Environment of the TOE are outlined in the Security Target [6] and [9], chapter 5.3.

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

TOE Security Function	Addressed issue
SF1- Operating state checking (supplied by the IC and utilized by the ES)	Operating State checking
SF6- TSF self test (supplied by the IC and utilized by the ES)	TSF self test
SF7- Notification of physical attack (supplied by the IC and utilized by the ES)	Notification of physical attack
SF_TSF_PROTECTION	Protection of the TSF
SF_CRYPTO	Cryptographic computation

TOE Security Function	Addressed issue
SF_AUTHENTICATION	Authentication management
SF_ACCESS	Access control
SF_CARD_INIT	Card Initialization and Personalization

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 8.3 is confirmed. The rating of the Strength of Functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, 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.

This certification covers the fully configured, initialized and personalised TOE with generated keys and completed QES, being in life cycle phase 8 (Usage Phase), according to the life cycle model in the Security Target [6] and [9], chapter 2.4.

The Card Manufacturer is responsible for the initialization of the TOE and its testing, and he is also responsible for the personalization of the card, see Security Target [6] and [9], chapter 2.4.

Note: The application of the QES is always present in the card; only for the SCD/SVD key pair it is possible to generate it during pre-personalisation in phase 6 (see chapter 2.4 of the Security Target [6] and [9]) or in the usage phase (phase 8). Both generations (phase 6b or phase 8) are done in the card and loading of keys from outside is not possible. The "QES-Nachladung" is not part of the certification.

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:

Electronic Health Card and SSCD Version 2.10

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1a	HW	Infineon SLE66CX680PE	Mask Identifier: SLE66CX680PE / m1534-a14	Smart Card modules, ROM mask of the TOE already mounted into an ID-1 Smart Card.

No	Type	Identifier	Release	Form of Delivery
1b	SW	Card Operating System GeGKOS	Version 2.10	Software on the Smart Card
1c	SW	EEPROM image of Electronic Health Card and SSCD	Integrated in TOE	Image on the Smart Card
2	DOC	User guidance Electronic Health Card and SSCD [16]	Version 1.41/2009-10-01	Document in paper / electronic form
3	DOC	Administrator guidance Electronic Health Card and SSCD [17]	Version 1.41/2009-10-01	Document in paper / electronic form

Table 2: Deliverables of the TOE

The TOE is Electronic Health Card and SSCD version 2.10. The customer can identify the TOE as the certified product with the help of the GET DATA command, sent with tag ‘DF71’ (for the platform identification) or ‘DF75’ (for the image identification) in the data fields P1 and P2,. The command with these parameters retrieves card production statistic data from a GeGKOS card. The returning data objects identify the OS and the EEPROM image data, identifying the TOE (for details see [16, Annex 1]).

According to [16, Annex 1], following responses identify the TOE:

For the ROM Mask: 05 11 10 65 47 4B 61 33

For the EEPROM Image: A3 10 FF 02 00 17 08 09

To ensure the confidentiality the corresponding guidance documentation must be provided in a secure way e.g. as encrypted mail or in paper form only by registered mail.

3 Security Policy

The TOE is the composition of an IC with Smart Card Embedded Software, including the Electronic Health Card and SSCD applications and will be used as electronic Health Card (eHC) within the German Health Care System. The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE.

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 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. Details can be found in the Security Target [6] and [9] chapter 4.

5 Architectural Information

The TOE is a composite TOE. The underlying hardware is an Infineon SLE66CX680PE / m1534-a14 integrated circuit (Cert-ID: BSI-DSZ-CC-0437-2008-MA-02). The embedded software stored in the ROM is the operating system (OS) named GeGKOS, which provides all required OS commands. In the EEPROM the application of the electronic health card and the application of the digital signature (data structures and their content) are stored.

A structural overview of the TOE and an overview of the architecture including a figure of the global architecture of the TOE is given in chapter 2.1 of the Security Target [6] and [9].

A top level block diagram of the hardware IC including an overview of subsystems can be found in chapter 2.1 of the Security Target of the chip [14].

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 TSF in order to assure complete coverage. The overall approach was to test all commands stated in the Functional Specification and their methods of use. Test procedures were implemented in accordance with Functional Specification and High Level Design of the TOE in order to verify the TOE’s compliance with its expected behaviour. All test cases in each test scenario were executed successfully. The developer tested the TSFs of the TOE with a test suite in an automatically performed batch run. The developer tested the TOE systematically at the level of TSF functionalities. All tests of individual test cases were passed, i.e. all TSF were successfully tested against the Functional Specification and High Level Design of the TOE. The developer’s testing results demonstrate that the TSF perform as specified in the Functional Specification and High Level Design of the TOE.

The ITSEF repeated a subset of developer tests. During the evaluator’s TSF subset testing the TOE operated as specified.

Independent testing was performed mainly in the ITSEF's premises with the TOE development environment using script based developer test tools with automated comparison of expected and actual test results. Non-automated independent tests e.g. involving an emulator were executed in the test environment of the developer. During independent testing the evaluator tested all TSFs explicitly, with tests including simulator test cases so that all TSF were covered by at least one test case in order to confirm that the TOE operates as specified. Penetration testing was performed in the ITSEF's premises

with the TOE development environment using script based developer test tools with automated comparison of expected and actual test results. The ITSEF has performed penetration testing based on the developer vulnerability analysis and on the independent vulnerability analysis. During the ITSEF's penetration testing the TOE operated as specified. The TOE is resistant to attackers with high attack potential in the intended environment of the TOE.

8 Evaluated Configuration

This certification covers the fully configured, initialized and personalised TOE with generated keys and completed QES, being in life cycle phase 8 (Usage Phase), according to the life cycle model in the Security Target [6] and [9], chapter 2.4.

The Card Manufacturer is responsible for the initialisation of the TOE and its testing, and he is also responsible for the personalisation of the card, see Security Target [6] and [9], chapter 2.4.

The embedding service provider and Personaliser needs to have secure physical environment for the personalisation. The Personaliser is responsible for the Smart Card personalization and final tests.

The application of the QES is always present in the card; only for the SCD/SVD key pair it is possible to generate it during pre-personalisation in phase 6 (see chapter 2.4 of the Security Target [6] and [9]) or in the usage phase (phase 8). Both generations (phase 6b or phase 8) are done in the card and loading of keys from outside is not possible. The "QES-Nachladung" is not part of the certification.

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:

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

see [4], AIS 1, AIS 14, AIS 19, AIS 20, AIS 25, AIS 26, AIS 31, AIS 34, AIS 36, AIS 37.

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, AVA_MSU.3 and AVA_VLA.4 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Common Criteria Protection Profile electronic Health Card (eHC) – elektronische Gesundheitskarte (eGK), BSI-PP-0020-V2-2007-MA02 [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, AVA_MSU.3 and AVA_VLA.4
- The following TOE Security Functions fulfil the claimed Strength of Function : high
  - SF_CRYPTO (Cryptographic computation). There is a probabilistic permutational mechanism for the random number generation (AIS 20).
  - SF_AUTHENTICATION (Authentication management). This SF uses a permutational mechanism for the Authentication of the users.

In order to assess the Strength of Function the scheme interpretations AIS 20, AIS 25 and AIS 26 (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 following cryptographic algorithms are used by the TOE to enforce its security policy:

Hash functions:

- SHA-256 hash value calculation according to FIPS 180-2

Algorithms for the encryption and decryption:

- 3TDES and retail-MAC (Triple-DES with 168 bit) according to [18]
- RSA 2048 bit according to [18]

This holds for the following security functions:

- SF_CRYPTO (RSA, 3TDES, SHA, RNG)

The strength of the cryptographic algorithms was not rated in the course of this evaluation (see BSIG Section 4, Para. 3, Clause 2). According to [21] and [22] the algorithms are suitable for encryption and decryption. The validity period of each algorithm is mentioned in the official catalogues [21] and [22].

10 Obligations and notes for the usage of the TOE

The operational documents as outlined in table 2 and the Security Target [6] and [9] contain necessary information about the usage of the TOE and all security hints therein have to be considered.

For example, the User Guidance [16] gives recommendation concerning the PIN usage, concerning the PUK handling, concerning the Smart Card, concerning the health applications, concerning the Digital Signature Application, concerning the TOE identification, and others, please see chapter 2 of [16].

For example, the Administrator Guidance [17] gives recommendations for administrators concerning security. Administrators must therefore follow the Guidance, especially chapter 2.10 of [17].

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

3TDES	Triple DES
APP	Applicative Data Structures
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
EAL	Evaluation Assurance Level
EEPROM	Electronically Erasable Programmable Read Only Memory
eHC	electronic Health Card
ES	Embedded Software
IC	Integrated Circuit
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
OS	Operating System

PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest Shamir Adleman Algorithm
SF	Security Function
SFP	Security Function Policy
SHA	Secure Hash Algorithm
SOF	Strength of Function
SSCD	Secure Signature Creation Device
SCD	Signature Creation Data
ST	Security Target
SVD	Signature Verification Data
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 BSI-DSZ-CC-0425-2009, Electronic Health Card and SSCD, TOE version 2.10, document version 2.15, 2009-05-26, Gemalto (confidential document)

[7] Evaluation Technical Report, Version 4, Date: 2009-10-02, BSI-DSZ-CC-0425, Electronic Health Card and SSCD 2.10 (confidential document)

[8] Configuration list for the TOE: Configuration Check Electronic Health Card and SSCD, version 3.6 2009-10-02, Gemalto; and STD Configuration Check List For GeGKOS on INFINEON SLE66CX680 PE, version 3.0 2008-04-08, Gemalto (confidential documents)

[9] Security Target BSI-DSZ-CC-0425-2009, Document Reference: ASE02R10559 V0.9, Date 08. September 2009, Electronic Health Card and SSCD 2.10, Developer Name (sanitised public document)

[10] Common Criteria Protection Profile electronic Health Card (eHC) – elektronische Gesundheitskarte (eGK), BSI-PP-0020-V2-2007-MA02, Version 2.6, 2008-07-29, BSI

---

[8] specifically

- AIS 20, Version 1, 2 December 1999, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 6, 07.09.2009, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 6, 07.05.2009, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 1, 25 Sept. 2001 Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 1, 2 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.
- AIS 34, Version 2, 24.10.2008, Evaluation Methodology for CC Assurance Classes for EAL5+
- AIS 35, Version 2.0, 12 November 2007, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 2, 12 November 2007, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

[11] Protection Profile – Secure Signature-Creation Device Type 3, EAL 4+, BSI-PP-0006-2002, Version 1.05, July 25th 2001

[12] Smartcard IC Platform Protection Profile, Version 1.0, July 2001, registered and certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-PP-0002-2001

[13] ETR-lite for composition according to AIS 36 for the Product SLE66CX680PE / m1534-a14, SLE66CX360PE / m1536-a14, SLE66CX482PE / m1577-a14, SLE66CX480PE / m1565-a14, SLE66CX182PE / m1564-a14, All Products with RSA2048 V1.5 library, Version 1, 2008-04-02, TÜVIT (confidential document)

[14] Infineon Technologies AG, Security and Chipcard ICs, Security Target, SLE66CX680PE/m1534-a14, SLE66CX360PE/m1536-a14, SLE66CX482PE/m1577-a14, SLE66CX480PE / m1565-a14, SLE66CX182PE / m1564-a14 All Products with RSA2048 library, Version 1.3, Date 2007-03-22

[15] Certification Report BSI-DSZ-CC-0437-2008 for SLE66CX680PE / m1534-a14,SLE66CX360PE / m1536-a14, SLE66CX482PE / m1577-a14,SLE66CX480PE / m1565-a14, SLE66CX182PE / m1564-a14, all optional with RSA2048 V1.5 and all with specific IC dedicated software from Infineon Technologies AG, including Maintenance Addendum BSI-DSZ-CC-0437-2008-MA-01 and BSI-DSZ-CC-0437-2008-MA-02

[16] User guidance Electronic Health Card and SSCD, version 1.41, 2009-10-01

[17] Administrator guidance, Electronic Health Card and SSCD, version 1.41, 2009-10-01

[18] The Specification of the German Electronic Health Card eHC Part 1: Commands, Algorithms and Functions of the COS Platform, Release 2.2.2, 16/09/2008

[19] The Specification of the German Electronic Health Card eHC Part 2: Applications and application related structures, Release 2.2.1, 19/06/2008

[20] Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen - Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 17. November 2008, Veröffentlicht am 27. Januar 2009 im Bundesanzeiger Nr. 13, Seite 346

[21] BSI - Technische Richtlinie 03116 für die eCard-Projekte der Bundesregierung, Version 2.0, 03.04.2009, Bundesamt für Sicherheit in der Informationstechnik

[22] Geeignete Algorithmen zur Erfüllung der Anforderungen nach §17 Abs.1 bis 3 SigG vom 22. Mai 2001 in Verbindung mit Anlage 1 Anschnitt I Nr. 2 SigV vom 22. Nov. 2001, 17.11.2008, published in the Bundesanzeiger No 13, page 346, 27.01.2009

[23] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, Amtsblatt der Europäischen Gemeinschaften, L13/12-L13/20, 19.01.2001, Europäisches Parlament und Rat der Europäischen Union

[24] Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften, Bundesgesetzblatt Nr. 22, S. 876, 16.05.2001, Dtsch. Bundestag

[25] Verordnung zur elektronischen Signatur, Bundesgesetzblatt Nr. 509, S. 3074, 16.11.2001, Dtsch. Bundestag

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 33

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0425-2009

Evaluation results regarding development and production environment

The IT product Electronic Health Card and SSCD Version 2.10 (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 07 October 2009, 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.1, ALC_LCD.1, ALC_TAT.1),

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

(a) Site Gémenos (module production, card production, embedding, initialisation), Avenue du Pic de Bertagne – BP 100, 13881 GEMENOS CEDEX, France

(b) Site La Vigie / La Ciotat (lib development), Avenue des Jujubiers - Z.I. ATHELIA IV, 13705 LA CIOTAT CEDEX, France

(c) Site Ismaning (OS development), Adalperostraße 45, 85737 Ismaning, Germany

(d) Site Filderstadt (card personalization), Mercedesstraße 13, 70794 Filderstadt, Germany

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.