Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0767-2011

for

GeGKOS A6 Electronic Health Card 6.20

from

Gemalto 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-0767-2011

GeGKOS A6 Electronic Health Card 6.20

from	Gemalto 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, 17 November 2011

For the Federal Office for Information Security

INFORMATION TECHNOLOGY SECURITY
SOGIS
IT SECURITY CERTIFIED
MUTUAL RECOGNITION AGREEMENT

Bernd Kowalski L.S.
Head of Department

This page is intentionally left blank.

Preliminary Remarks

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

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

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

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

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

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

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

Contents

A Certification

1 Specifications of the Certification Procedure

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

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 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 EAL 1 to EAL 4 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 EAL 4 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 EAL 4 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 GeGKOS A6 Electronic Health Card 6.20 has undergone the certification procedure at BSI.

The evaluation of the product GeGKOS A6 Electronic Health Card 6.20 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 11 October 2011. 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 GmbH.

The product was developed by: Gemalto 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, where 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 GeGKOS A6 Electronic Health Card 6.20 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 GmbH
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 the GeGKOS A6 Electronic Health Card 6.20, a contact based smart card with applications for the German Health Care System according to the “Gesetz zur Modernisierung der Gesetzlichen Krankenversicherung” (GKV-Modernisierungsgesetz – GMG), the “Sozialgesetzbuch” (SGB) and the privacy legislation (“Datenschutzgesetze des Bundes und der Länder”). The TOE is intended to be used as electronic Health Card (eHC) within the German Health Care System and is therefore based on the specification documents [18] and [19].

The TOE contributes to the health application management by providing the following services:

- Mutual authentication between the eHC and an Health Professional Card (HPC) or a Security Module Card (SMC).
- Mutual authentication between the eHC and a security device (e. g. for online update of contractual data in the card).
- Authentication of the card holder by use of one or two PINs (PIN.CH and PIN.home: specific PINs for eHC functions).
- Secure storage of contractual and medical data, with respect to confidentiality, integrity and authenticity of these data.
- Authentication of the card using private key and X.509 certificate.
- Document content key decipherment using a private key.
- Management of applications.
- File content protection via access conditions.
- Confidentiality of the PINs and the cryptographic keys.
- Integrity of PINs, cryptographic keys and file contents.

The TOE GeGKOS A6 Electronic Health Card 6.20 comprises a Smart Card Integrated Circuit (IC with contacts) with Smart Card Embedded Software, consisting of the operating system platform and the dedicated electronic Health Card applications (eHC applications) set up and running on the operating system platform. More detailed:

The TOE GeGKOS A6 Electronic Health Card 6.20 is composed of the components

- Integrated Circuit (IC) SLE78CX800P provided by Infineon Technologies AG (Infineon smart card IC (Security Controller) M7801 A12 with specific IC dedicated software, see BSI-DSZ-CC-0606-2010, but without usage of the Infineon crypto library) and
- Smart Card Embedded Software GeGKOS comprising the operating system platform (designed as native implementation) and the dedicated eHC applications for the German Health Care System provided by Gemalto GmbH.

The TOE's operating system platform and applications and their technical functionality and inherently integrated security features are designed and developed under consideration of the specifications, standards and requirements as stated in the specifications [18] and [19] respective in the Security Target [6] and [8], chapter 1.3.2.

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 6.2. 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 Functionalities:

TOE Security Functionality	Addressed issue
LIFE CYCLE STATE MACHINE	The ES (embedded software) incorporates a state machine to reflect the TOE life-cycle phases. It ensures the secure evolution of the TOE from the IC manufacturing phase to the usage phase.
PRODUCTION COMMANDS	The production of the TOE is accomplished via a dedicated set of production commands. Together with the Life Cycle State Machine they tie up the specified production flow. Each production command is implemented with a hard coded check for the necessary authentication state and the exact production phase(s) where it can be executed.
INITIAL SETTINGS	During initialisation phase an EEPROM image is loaded onto the card. This image contains preset data relevant for TOE scope, e.g. access conditions or PIN counter.
RANDOM NUMBERS	For the cryptographic computations and authentication protocols the TOE has to generate random numbers that meet a defined quality metric. This is achieved by utilising the AIS31 TRNG of the hardware platform fulfilling class P2.
CRYPTOGRAPHIC COMPUTATIONS	The ES contains a cryptographic library to implement the cryptographic procedures made available via the respective APDU commands. The basic RSA and DES operations are performed by the respective hardware co-processor.
CARD HOLDER AUTHENTICATION	The card holder authenticates himself by correctly presenting PIN.CH or PIN.home. Further, the TOE features a retry counter, an unblocking code and a PIN transport state.
ASYMMETRIC AUTHENTICATION	Asymmetric authentication is used by the components of the health professionals to prove their authenticity to the card and to secure the subsequent communication.
SYMMETRIC ADMINISTRATOR AUTHENTICATION	In usage phase the administrator can authenticate himself by a symmetric one-time challenge-response protocol.
ACCESS MANAGEMENT	As this product is a smart card complying with ISO 7816 the external world can only communicate with it via APDU commands. No direct access to the resources of the smart card, which in essence are file contents, PINs, and keys, is possible.
SECURE MESSAGING	This component provides the functionality to ensure protection of the data exchanged via APDUs by authenticity, integrity and confidentiality, (trusted channel) using 3TDES cryptography.
TSF PROTECTION	The ES is designed to protect the TOE against fraudulent attacks. Supported features are among others:

TOE Security Functionality	Addressed issue
	• On each reset the TOE is set to a secure state before the normal operation of the TSF starts. • If during TSF execution an unexpected error occurs, the secure state of the TSF will be preserved by halting their execution. • Sensitive operations like the RSA and 3TDES computations or PIN verification are programmed in a way that processing timing, electromagnetic radiation, or power consumption of the chip cannot be used to discover any PIN or secret/private key.

Table 1: TOE Security Functionalities

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

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

This certification covers the following configurations of the TOE: GeGKOS A6 Electronic Health Card 6.20. For details refer to 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:

GeGKOS A6 Electronic Health Card 6.20

The following table outlines the TOE deliverables:

No.	Type	Identifier	Release	Form of Delivery
1	HW/SW	Infineon smart card IC (Security Controller) M7801 A12 with specific IC dedicated software (BSI-DSZ-CC-0606-2010) Hint: The crypto library from Infineon as covered within the HW certificate BSI-DSZ-CC-0606-2010 (RSA2048/4096 v1.1.18, EC v1.1.18 and SHA-2 v1.1) is not used by the TOE.	Mask Identifier M7801 A12 (produced in Dresden) '05 73 10 65 47 4B 61 36'	---

No.	Type	Identifier	Release	Form of Delivery
2	SW	Card operating system of GeGKOS A6 Electronic Health Card 6.20		---
3	SW	EEPROM image of GeGKOS A6 Electronic Health Card 6.20	'A6 20 FF 00 00 21 07 11'	---
The TOE is delivered in form of initialised cards in ID-1 format, i.e. including the IC, the operating system platform in the ROM resp. EEPROM (for patches) and the EEPROM image.				
4	DOC	AGD - Guidance documents Electronic Health Card - GeGKOS A6 Electronic Health Card 6.20	Version 6.0 / 2011-05-12	Hardcopy or document in electronic form
5	DOC	Operational User Guidance Electronic Health Card - GeGKOS A6 Electronic Health Card 6.20	Version 6.3 / 2011-09-26	Hardcopy or document in electronic form
6	DOC	End User Guidance Electronic Health Card - GeGKOS A6 Electronic Health Card 6.20	Version 6.3 / 2011-09-26	Hardcopy or document in electronic form
7	DOC	Preparative Procedures Electronic Health Card - GeGKOS A6 Electronic Health Card 6.20	Version 6.3 / 2011-07-27	Hardcopy or document in electronic form
8	DOC	Key Setting Up	Version 10.0 / January 2011	Hardcopy or document in electronic form Note: only delivery to the personalisation center
9	DOC	Key Management Process for Gemalto industrial activities	Version 12.0 / December 2010	Hardcopy or document in electronic form Note: only delivery to the personalisation center

Table 2: Deliverables of the TOE

Basically the life-cycle of the TOE GeGKOS A6 Electronic Health Card 6.20 consists of the development phase and the operational phase. The initialisation of the TOE completely belongs to the development phase and the TOE will be delivered in initialised form to the personaliser for its personalisation. More detailed, the TOE will be delivered as an IC already embedded in the plastic card and containing all software and data structures as defined in the specifications [18] and [19]. In addition, the TOE related guidance documentation as outlined in Table 2 will be provided. No modifications of the TOE by a third party are possible.

For the evaluation process the whole life-cycle of the TOE was considered during evaluation as far as the developer respective manufacturer of the TOE is directly involved. Any delivery of TOE intermediate or final components is done via a sufficiently secure transport to avoid the delivery of fake chips.

The user can identify the TOE by retrieving the following identification data from the TOE:

- IC

- Operating system platform GeGKOS
- EEPROM image data

To verify the TOE's identification data, the user executes the card command GET DATA, for details refer to chapter 8.

3 Security Policy

The TOE is the composition of an IC and appropriate Smart Card Embedded Software 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. It covers the following issues:

- Modification and disclosure of IC assets / Smart Card Embedded Software / application data.
- Compromise / forgery / misuse of confidential user or TSF data including information leakage.
- Misuse of TOE functions.
- Interception of communication.
- Abuse of TOE functionality (including its eHC applications).
- Malfunction due to environmental stress.
- Physical attacks through the TOE interfaces.

4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE environment. The following topics are of relevance:

- Adequate usage of TOE and IT-Systems in the environment.
- Legal responsibility of authorised persons.
- Protection of sensitive data outside of the eHC.
- Secure handling of data during personalisation and additional personalisation.

The Security Objectives related to the operational environment of the TOE and its dedicated eHC applications can be found in the Protection Profile [7], chapter 4.2 as well as in the Security Target [6] and [8], chapter 4.3.

5 Architectural Information

The TOE GeGKOS A6 Electronic Health Card 6.20 is composed of the already certified SLE78CX800P Smart Card Controller from Infineon Technologies AG, the GeGKOS operating system platform and the eHC applications from Gemalto GmbH, see also Figure 3 in [6] and [8], chapter 1.4.7.

The TOE is composed of the following subsystems:

- APDU Container

- Error
- File System
- Hardware Abstraction Layer
- Security Kernel
- Process Handling
- Toolbox
- System Services

6 Documentation

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

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

7 IT Product Testing

The tests were performed with the composite smart card product GeGKOS A6 Electronic Health Card 6.20. The physical format of the test configuration for TOE testing was either

- a card which is usable for all automatic or non-recoverable test cases or
- an emulator which is required for all interactive test cases.
- Test target categories:
- Operating system (contained in ROM code and EEPROM patch code).
- Initialisation and personalisation process.
- Applications initialised respective loaded.
- Completion states / life-cycle states.

7.1 Developer Tests according to ATE_FUN

TOE configurations tested:

The tests were performed with the composite smart card product GeGKOS A6 Electronic Health Card 6.20 on the IC Infineon SLE78CX800P. The TOE embedded software part consists of the operating system platform GeGKOS (ROM/EEPROM) and the file system including data structures and access conditions (EEPROM).

To run the test validation campaign the TOE had an additional test patch applied.

Test target categories:

- Interface tests for usage phase (interface commands and RSA library).
- Interface tests for initialisation and personalisation (different completion states and patch loading).
- Alternative tests (emulator tests, required for cases where it is not possible to stimulate or to observe the behaviour to be tested via the external interfaces of the chip).

- T=1 tests (protocol tests).

Developer's testing approach:

- All use cases of the TSFI as described in the functional specification are tested with at least one test case.
- All SFR-enforcing use cases of the SFR-enforcing module interfaces from TDS.

Verdict for the activity:

- All test cases in each test category were run successfully on this TOE version.
- The developer's testing results demonstrate that the TOE performs as expected.

7.2 Evaluator Tests

7.2.1 Independent Testing according to ATE_IND

Approach for independent testing:

- Examination of developer's testing amount, depth and coverage analysis and of the developer's test goals and plan for identification of gaps.
- Examination whether the TOE in its intended environment, is operating as specified using iterations of developer's tests.
- Independent testing was performed by the evaluator at the ITSEF in Essen with the TOE development environment using script based developer test tools with automated comparison of expected and actual test results.

TOE test configurations:

- TOE smart cards with test patch.
- TOE smart cards (without test patch) in different life-cycle states.
- Because the real PKI of the eHC was not available for testing, a self-chosen root CA key pair was used. In fact, for repeated test cases the original productive image was taken and just the root CA's public key inside was replaced.

Subset size chosen:

- During sample testing the evaluator chose to repeat the script-based developer functional tests covering the usage phase of the TOE in evaluation at the ITSEF in Essen.
- During independent testing the evaluator focussed on the main security functionality as described in the ST, with 30 evaluator tests cases so that all TSF could be covered by at least one test case in order to confirm that the TOE operates as specified.

Security functions tested:

- LIFE CYCLE STATE MACHINE
- PRODUCTION COMMANDS
- INITIAL SETTINGS
- RANDOM NUMBERS

- CRYPTOGRAPHIC COMPUTATIONS
- CARD HOLDER AUTHENTICATION
- ASYMMETRIC AUTHENTICATION
- SYMMETRIC ADMINISTRATOR AUTHENTICATION
- ACCESS MANAGEMENT
- SECURE MESSAGING
- TSF PROTECTION

Evaluator tests performed:

- The evaluator performed tests of all TSF and interfaces with script based tests and emulator test cases.
- The evaluator selected all usage phase and initialisation/personalisation script-based tests that can run without manual interactions of the developer's testing documentation for sampling.

Verdict for the activity:

- During the evaluator's TSF subset testing the TOE operated as specified.

7.3.2 Penetration Testing according to AVA_VAN

Overview:

The penetration testing was performed using the test environment of the ITSEF.

All configurations of the TOE being intended to be covered by the current evaluation were tested.

The overall test result is that no deviations were found between the expected and the actual test results; moreover, no attack scenario with the attack potential 'high' was actually successful.

Penetration testing approach:

The evaluator used the information on potential vulnerabilities collected by the evaluator during the evaluation that should be considered in the vulnerability analysis. Hereby, the evaluator took into account the Security Target, guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify possible potential vulnerabilities in the TOE.

The evaluator applied the following procedure while creating a list of potential vulnerabilities applicable to the TOE in its operational environment: the raw list of vulnerabilities was checked whether there are any measures in the operational environment, either IT or non-IT, which prevent exploitation of the potential vulnerability in that operational environment. The evaluator records any reasons for exclusion of potential vulnerabilities from further consideration if the evaluator determines that the potential vulnerability is not applicable in the operational environment. Otherwise the evaluator records the potential vulnerability for further consideration.

Based on a list of potential vulnerabilities applicable to the TOE in its operational environment created within the work unit AVA_VAN.5-5 the evaluators devised the attack scenarios for penetration tests when they were of the opinion, that those potential vulnerabilities could be exploited in the TOE's operational environment.

While doing this, also the aspects of the security architecture described in ADV_ARC were considered for penetration testing. All other evaluation input was used for the creation of the tests as well. Specifically the test documentation provided by the developer was used to find out if there are areas of concern that should be covered by tests of the evaluation body.

The source code reviews of the provided implementation representation accompanied the development of test cases and were used to find test input. The code inspection also supported the testing activity by enabling the evaluator to verify implementation aspects that could hardly be covered by test cases.

In addition the evaluator applied tests and performed code reviews during the evaluation activity of ADV_COMP.1 to verify the implementation of the requirements imposed by the ETR and the guidance of the underlying platform. This ensured confidence in the security of the TOE as a whole.

The primary focus for devising penetration tests was to cover all potential vulnerabilities identified as applicable in the TOE's operational environment for which an appropriate test set was devised.

TOE test configurations:

The evaluators used TOE samples for testing that were configured according to the Security Target. The samples had not the test patch applied and were identified using the method as described by the evaluator in its guidance [13] und [15].

The tests were performed in different test scenarios:

- TOE smart card based on ROM mask tested in the TOE development environment at the evaluator's site using script based developer test tools with automated comparison of expected and actual test results.
- TOE smart card with dedicated images for the SPA/DPA and SEMA/DEMA tests at evaluator's site.

The TOE was tested in different life-cycle configurations: before initialisation, initialised, personalised, in usage phase.

Verdict for the sub-activity:

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential 'high' was actually successful in the TOE's operational environment as defined in the ST [6] and [8] provided that all measures required by the developer are applied.

8 Evaluated Configuration

This certification covers the following configurations of the TOE: The TOE as an electronic Health Card only features one fixed configuration, the composite smart card product GeGKOS Electronic Health Card 6.20 consisting of the Infineon chip SLE78CX800P, the operating system platform GeGKOS and the eHC applications from Gemalto GmbH. This configuration cannot be altered by the user, and the evaluation is therefore only valid for this configuration of the TOE.

The TOE comprises the parts **TOE_IC**, **TOE_ES**, **TOE_APP** and **TOE_GD** as described in the following:

- **TOE_IC**: Consists of the Integrated Circuit of the eHC's chip (IC), the SLE78CX800P from Infineon Technologies AG with its IC dedicated test and support software (Certification ID: BSI-DSZ-CC-0606-2010). The TOE_IC firmware contains a crypto library which is not used in this composite TOE.
- **TOE_ES**: The IC Embedded Software, the GeGKOS operating system platform.
- **TOE_APP**: The eHC applications, i.e. their data structures and content (not including card individual data like PIN and key values).
- **TOE_GD**: The guidance documentation delivered together with the TOE (refer to [12] to [15]).

The TOE can be identified by its ROM data and the EEPROM image identifier. For this case, the GET DATA card command provides responses in the following way:

The GET DATA command, sent with tag ‘DF7X’ coded in P1P2, retrieves card production statistic data from a GeGKOS A6 Electronic Health Card 6.20 card. This command can be played during all possible life-cycle states without any access restrictions. The data objects with tags 'DF71' and 'DF75' identify the underlying IC, the operating system platform and the EEPROM image data, all together identifying the TOE.

To identify the IC and operating system platform of the TOE the GET DATA command with P1P2=’DF71’ has to be used, and the data returned have to be checked against the following 8 byte value: '05 73 10 65 47 4B 61 36'.

For identification of the EEPROM image data the GET DATA command with P1P2=’DF75’ has to be issued and the bytes 1-8 of the data returned (image identifier) have to be compared against the following value: 'A6 20 FF 00 00 21 07 11'.

9 Results of the Evaluation

9.1 CC specific Results

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

The Evaluation Methodology CEM [2] was used for those components up to EAL 5 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the technology was used:

- Application of CC to Integrated Circuits
- Smart Card evaluation guidance
- Application of Attack Potential to Smart Cards
- Composite product evaluation for Smart Cards and similar devices
- Functionality classes and evaluation methodology of physical and deterministic 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, AIS 38.)

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

To support composite evaluations according to AIS 36 the document ETR for composite evaluation [10] was provided and approved. This document provides details of this platform evaluation that have to be considered in the course of a composite evaluation on top.

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 component AVA_VAN.5 augmented for this TOE evaluation.

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:

Hash functionalities:

- SHA-256 hash value calculation according to [20]

Algorithms for encryption and decryption:

- 3TDES (168 bit) according to [20]
- Retail-MAC (168 bit) according to [20]
- RSA 2048 bit according to [20]

Algorithms for signature generation and verification:

- RSA 2048 bit according to [20]

This holds for the following security functions:

- Cryptographic computations (SHA, RSA, 3TDES, RNG)
- Asymmetric Authentication (SHA, RSA, RNG)
- Symmetric Administrator Authentication (3TDES, RNG)

- Secure Messaging (3TDES)

Random number generation e. g. for generation of session keys, padding mechanisms and authentication protocols is performed by a physical and by a deterministic random number generator provided by the underlying hardware respective by the GeGKOS operating system platform. The rating for the PRNG is P2 with resistance against attack potential ‘high’ according to AIS 31 (see [4] and the certification report for the hardware BSI-DSZ-CC-0606-2010). The DRNG is only used for integrated security measures and rated as sufficient during the vulnerability analysis of the product.

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 “Technische Richtlinie für die eCard-Projekte der Bundesregierung” BSI TR-03116 [20] the algorithms are suitable for encryption and decryption of eHC related data stored by the TOE or exchanged with the TOE as well as for authentication protocols implemented by the TOE. The validity period of each algorithm is mentioned in the official catalogue [20].

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 Policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

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

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.

In addition, the following aspects need to be fulfilled when using the TOE: Principally, the user has to follow the instructions in the user guidance documents [12] to [15] and has to ensure the fulfilment of the Assumptions about the environment as outlined in the Security Target [6] and [8], chapter 3.4.

Particular constraints derive from security requirements in the guidance documents [12] to [15]. The guidance documents for TOE users is separated in guidance documents for users in different roles, see the summarising document [12] respective the role-oriented guidance documents [13] and [14]. For preparative procedures, the guidance document [15] was set up.

Notably the guidance document for the end user [14] gives in its chapter 2.2.8 requirements, recommendations and hints concerning the security objectives for the operational environment with the following aspects:

- Communication in insecure networks.
- PIN concept onto the TOE.
- Delivery procedures of TOE inclusive PIN and PUK.
- Environment for entering the PIN.
- Communication without secure messaging.
- Data decryption.

- Data storage outside of the TOE.
- Management access to the TOE.

For the personalisation of the TOE, the following obligation in addition to the requirements, recommendations and hints given in [13] and [15] has to be taken into account:

- The personalisation of the TOE is restricted to the sites Gemalto GmbH Mercedesstraße 13, 70794 Filderstadt and Systemform MediaCard GmbH, Systemformstraße 5, 83209 Prien am Chiemsee (refer to Annex B, e) and f)) whereby the technical, organisational and personnel security measures as they were part of the evaluation of the TOE have to be applied. The TOE's personalisation process or parts of this process must not be performed at other sites.
- In addition to the user guidance documents [12] to [15] as they are outlined in the Security Target, the documents [16] and [17] covering in particular the key management related to the personalisation of the TOE are delivered to the personalisation center.

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
DEMA	Differential Electromagnetic Analysis
DES	Data Encryption Standard
3TDES	Three Key DES
DPA	Differential Power Analysis
DRNG	Deterministic Random Number Generator
EAL	Evaluation Assurance Level
eHC	electronic Health Card
ES	Embedded Software
ETR	Evaluation Technical Report

HPC	Health Professional Card
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
PRNG	Physical Random Number Generator
RNG	Random Number Generator
RSA	Rivest Shamir Adleman Algorithm
SAR	Security Assurance Requirement
SEMA	Simple Electromagnetic Analysis
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMC	Security Module Card
SPA	Simple Power Analysis
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionalities

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[8]

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

[6] Security Target BSI-DSZ-CC-0767-2011, ASE - Security Target GeGKOS A6 Electronic Health Card 6.20, Version 7.3, 6 October 2011, Gemalto 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

[8] Security Target BSI-DSZ-CC-0767-2011, ASE - Security Target lite GeGKOS A6 Electronic Health Card 6.20, Version 7.3, 6 October 2011, Gemalto GmbH (sanitised public document)

[9] Evaluation Technical Report GeGKOS A6 Electronic Health Card 6.20, Version 3, 11 October 2011, TÜViT GmbH (confidential document)

[10] ETR for composite evaluation according to AIS 36 for the product SLE/B78C(I/F)XxxxP / M7801 A12xxx, BSI-DSZ-CC-0606-2010, Version 6, 17 May 2011, TÜViT GmbH (confidential document)

[8] specifically

- AIS 20, Version 1, 2 December 1999, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 6, 7 September 2009, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 8, 8 June 2011, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 1, 25 September 2001, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 7, 8 June 2011, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, 3 September 2009, Evaluation Methodology for CC Assurance Classes for EAL5+ (CCv2.3 & CCv3.1) and EAL6 (CCv3.1)
- AIS 35, Version 2.0, 12 November 2007, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 3, 19 October 2010, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2.9, 8 June 2011, Reuse of evaluation results

[11] Configuration list for the TOE, Configuration Check GeGKOS A6 Electronic Health Card 6.20, Version 6.6, 6 October 2011, Gemalto GmbH (confidential document)

[12] AGD - Guidance documents Electronic Health Card - GeGKOS A6 Electronic Health Card 6.20, Version 6.0, 12 May 2011, Gemalto GmbH

[13] Operational User Guidance Electronic Health Card - GeGKOS A6 Electronic Health Card 6.20, Version 6.3, 26 September 2011, Gemalto GmbH

[14] End User Guidance Electronic Health Card - GeGKOS A6 Electronic Health Card 6.20, Version 6.3, 26 September 2011, Gemalto GmbH

[15] Preparative Procedures Electronic Health Card - GeGKOS A6 Electronic Health Card 6.20, Version 6.3, 27 July 2011, Gemalto GmbH

[16] Key Setting Up, Version 10.0, January 2011, Gemalto GmbH

[17] Key Management Process for Gemalto industrial activities, Version 12.0, December 2010, Gemalto GmbH

[18] Die Spezifikation der elektronischen Gesundheitskarte, Teil 1: Spezifikation der elektrischen Schnittstelle, Version 2.2.0, 20.03.2008, supplemented by SRQ 1070, 1069, 1067, 1066, 1065, 1064, 1047, 0959, 0842, 0841, 0840, 0838, 0837, 0836, 0835, 0834, 0833, 0832, 0831, 0829, 0828, 0827, 0826, 0825, 0824, 0823, 0822, 0821, 0820, 0819, 0818, 0817, 0816, 0815, 0814, 0810, 0809, 1154, 1153, 1094, gematik

[19] Die Spezifikation der elektronischen Gesundheitskarte, Teil 2: Grundlegende Applikationen, Version 2.2.0, 25.03.2008, supplemented by SRQ 1030, 950, 949, 948, 947, 946, 945, 944, 890, 889, 888, 887, 886, 885, 884, 883, 882, 881, 1085, gematik

[20] BSI TR-03116, Technische Richtlinie für die eCard-Projekte der Bundesregierung, Version 3.04, 11.06.2010

[21] Certification report BSI-DSZ-CC-0606-2010, “Infineon smart card IC (Security Controller) M7801 A12 with optional RSA2048/4096 v1.1.18, EC v1.1.18 and SHA-2 v1.1 libraries and with specific IC dedicated software”, 14 September 2010, BSI

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

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-0767-2011

Evaluation results regarding development and production environment

The IT product GeGKOS A6 Electronic Health Card 6.20 (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 17 November 2011, 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:

a) Gemalto, Avenue Pic de Bertagne, BP 100, 13881 Gémenos, France (module manufacturing, card manufacturing, pre-initialisation, documentation)

b) Gemalto, Adalperostraße 45, 85737 Ismaning (development)

c) Gemalto, 6 Rue Verrerie, 92197 Meudon, France (development)

d) Gemalto, Avenue du Jujubier, Z.I Athelia IV, 13705 La Ciotat, France (IT infrastructure)

e) Gemalto GmbH Mercedesstraße 13, 70794 Filderstadt (pre-initialisation, initialisation and personalisation)

f) Systemform MediaCard GmbH, Systemformstraße 5, 83209 Prien am Chiemsee (initialisation and personalisation)

g) Swiss Post Solutions GmbH, Division Cards, Kronacher Str. 61, 96052 Bamberg (only embedding of cards)

h) Gemalto Singapore, 12 Ayar Rajah Crescent, 139941 Singapore, Singapore (module manufacturing, card manufacturing, pre-initialisation)

For the development and production sites regarding the "Infineon smart card IC (Security Controller) M7801 A12 with optional RSA2048/4096 v1.1.18, EC v1.1.18 and SHA-2 v1.1 libraries and with specific IC dedicated software” from Infineon Technologies AG refer to the certification report BSI-DSZ-CC-0606-2010 [21].

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. The evaluators verified, that the Threats, Security Objectives and requirements for the TOE life-cycle phases up to delivery (as stated in the Security Target [6] and [8]) are fulfilled by the procedures of these sites.

This page is intentionally left blank.