Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0601-2010

for

STARCOS 3.4 Health AHC C1

from

Giesecke & Devrient 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-0601-2010

STARCOS 3.4 Health AHC C1

from	Giesecke & Devrient GmbH
PP Conformance:	None
Functionality:	product specific Security Target 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

The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

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

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

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

Bonn, 25 January 2010

For the Federal Office for Information Security

Bernd Kowalski L.S.
Head of Department

SOGIS - MRA

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

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

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

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

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

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

[5] Proclamation of the Bundesministerium des Innern of 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

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

2.2 International Recognition of CC - Certificates

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

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

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

This evaluation contains the 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 STARCOS 3.4 Health AHC C1 has undergone the certification procedure at BSI.

The evaluation of the product STARCOS 3.4 Health AHC C1 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 18 December 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: Giesecke & Devrient GmbH

The product was developed by: Giesecke & Devrient GmbH

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

4 Validity of the Certification Result

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

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

[6] Information Technology Security Evaluation Facility

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

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

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

5 Publication

The product STARCOS 3.4 Health AHC C1 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] Giesecke & Devrient GmbH
Prinzregentenstraße 159
81677 München

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 STARCOS 3.4 Health AHC C1, a contact based smart card which is intended to be used as Secure Signature Creation Device (SSCD) in accordance with the European Directive 1999/93/EC [17]. This includes the generation and secure storage of a pair of signature creation data (SCD) and corresponding signature verification data (SVD) and the generation of qualified electronic signatures using the ECDSA standard with GF(p) and a key length of 256 bit.

The TOE is based on the STARCOS 3.4 operating system on a smart card integrated circuit. STARCOS 3.4 is a fully interoperable ISO 7816 compliant multiapplication smart card operating system, including a cryptographic library enabling the user to generate high security electronic signatures based on ECDSA with GF(p) and a key length of 256 bit. The various features of the STARCOS 3.4 operating system allow for additional applications. The TOE differs from the whole product, as the TOE does not include the other (optional) applications (for example health system applications) shown in Figure 2 in the Security Target [6] and [7] marked with the dashed line.

The Security Target [6] is the basis for this certification. It does not claim conformance to any certified Protection Profile. However, the Security Target [6] is based on the Secure Signature Creation Device Protection Profile [22].

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 [7], chapter 7.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Function	Addressed issue
SF_AccessControl	The TOE provides access control mechanisms that allow among others the maintenance of different users (Administrator, Signatory).
SF_AssetProtection	The TOE supports the calculation of block check values for data integrity checking, hides information about IC power consumptions and command execution time, and overwriting of the private signature key or the signature PIN when they are no longer needed.
SF_TSFProtection	The TOE detects physical tampering and is resistant to it.
SF_KeyManagement	The TOE supports onboard generation of ECDSA keypairs with a key length of 256 bit under usage of random numbers generated by its K4 (high) deterministic random number generator.
SF_SignatureCreation	The TOE supports the generation of electronic signatures on the base of elliptic curves defined over a field F(p) and with lengths of the parameters p and q of 256 bit. In addition, the TOE supports the calculation of hash values according to SHA-2 (256 bit).

TOE Security Function	Addressed issue
SF_TrustedCommunication	The TOE supports the establishment of a trusted channel/path based on mutual authentication with negotiation of symmetric cryptographic keys used for the protection of the communication data with respect to confidentiality and integrity.

Table 1: TOE Security Functions

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

The assets to be protected by the TOE are defined in the Security Target [6] and [7], chapter 4. 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 [7], chapter 4.1, 4.2 and 4.3.

The TOE comprises the following parts:

- NXP P5CC052V0A Secure Smart Card Controller, consisting of the circuitry of the TOE’s chip (the integrated circuit, IC) and the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software
- IC Embedded Software (operating system STARCOS 3.4)
- Digital signature application (data structures and their content)
- Guidance documentation delivered together with the TOE ([11] to [16]) and
- Smart Card Application Verifier Tool (Smart Card Application Verifier, including the configuration file, [17])

The operating system STARCOS 3.4 is implemented in the ROM area of the IC, whereas some parts of the operating system may also reside in the EEPROM. The file system containing the application data is installed in the EEPROM of the IC. Beside the files for the digital signature application there may be additional files for other applications, e.g. for health systems, which do not belong to the TOE. The file system part of the TOE is represented by the Guidance Documentation and the Generic Application Specification that define the security relevant parts of the file system. The Smart Card Application Verifier verifies the correctness of the file system after installation of the TOE.

This certification covers the following configuration of the TOE: STARCOS 3.4 Health AHC C1. 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:

STARCOS 3.4 Health AHC C1

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW/ SW	NXP P5CC052V0A Secure Smart Card Controller (BSI-DSZ-CC-0466)	Mask Identifier: V0A	Smart card modules, ROM mask of the TOE already mounted into an ID-1 smart card
2	SW	Card Operating System STARCOS 3.4	0102	Software on the smart card
3	SW	EEPROM image of STARCOS 3.4 Health AHC	Identifier of valid images published on the G&D web site	Image on the smart card
4	DOC	Guidance Documentation STARCOS 3.4 Health AHC C1 – Main Document	Version 1.2 / 2009-06-12	Document in paper / electronic form
5	DOC	Guidance Documentation for the Usage Phase STARCOS 3.4 Health AHC C1	Version 1.7 / 2009-12-15	Document in paper / electronic form
6	DOC	Guidance Documentation for the Initialisation Phase STARCOS 3.4 Health AHC C1	Version 1.4 / 2009-12-15	Document in paper / electronic form
7	DOC	Guidance Documentation for the Personalisation Phase STARCOS 3.4 Health AHC C1	Version 1.5 / 2009-12-15	Document in paper / electronic form
8	DOC	Generic Application STARCOS 3.4 Health AHC C1	Version 1.6 / 2009-07-09	Document in paper / electronic form
9	DOC	STARCOS 3.4 SmartCard Operating System Reference Manual	Edition 09.2009	Document in paper / electronic form
10	SW	Smart Card Application Verifier (including configuration files)	Version 2.1 (build 2.1.2)	Executable PC software with additional files necessary

Table 2: Deliverables of the TOE

Basically the life cycle of the STARCOS 3.4 Health AHC C1 consists of the development phase and the operational usage phase. The development phase comprises the development and the production of the TOE and ends with the delivery of the TOE parts to the SSCD provision service. The operational usage phase of the TOE covers the preparation phase (i.e. the initialisation and personalisation of the TOE) and the operational phase. The preparation phase of the TOE life cycle processes the TOE from the customer's acceptance of the delivered TOE to a state ready for operation by the signatory. After issuance of the initialised and personalised product, the signatory controls the TOE as an SSCD. For a more detailed description of the TOE's life cycle please refer to the Security Target [6] and [7], chap. 2.2.3 and 2.2.4.

For the evaluation process the whole life cycle of the TOE was considered during evaluation as far as the developer and manufacturer of the TOE is directly involved. Any delivery of the chip modules is done via a G&D security transport or a security transport maintained by another initialiser to avoid the delivery of fake chips.

The user can identify the TOE by retrieving the following information from the TOE:

- IC manufacturer data (Chipherstellerdaten)
- Version of the operating system (Betriebssystemversion)
- Completion state of the operating system (Komplettierungsstand) and

- Initialisation table (Initialisierungstabelle)

To verify the TOE's identification data and in particular of its initialisation table (and therefore also the composite TOE), the user executes the command GET PROTOCOL DATA (see [12], chapter 4.1.1.2, [13], chapter 4.2.2, 5.2.12, [14], chapter 5.2.4). The identification data of valid initialisation tables are published on the Giesecke & Devrient GmbH web site https://certificates.gi-de.com for comparison.

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

- Generation of the signature creation data (SCD) and the corresponding signature verification data (SVD)
- Export of the SVD
- Authentication of the signatory
- Creation of electronic signatures for the selected data to be signed
- Storing, copying, releasing and deriving of the signature creation data by an attacker
- Forgery of the electronic signature, of the signature verification data or of the DTBS-representation
- Repudiation of electronic signatures
- Modification and disclosure of IC assets / smart card embedded software / application data
- Compromise / forge / misuse of confidential user or TSF data including information leakage
- Interception of communication
- Abuse of TOE functionality (including its digital signature application)
- Malfunction due to environmental stress as well as physical tampering
- 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:

- Integrity and authenticity of the signature verification data (SVD) exported to the certification generation application (CGA)
- Generation of qualified certificates by the CGA
- Verification of the correspondence between the signature creation data (SCD) in the SSCD of the signatory and the SVD in the (qualified) certificate by the certificate service provider (pre-initialisation of the TOE as SSCD)
- Integrity and confidentiality of the verification authentication data (VAD)

- Protection of the data to be signed (DTBS)
- Security obligations of the Signatory

Details can be found in the Security Target [6] and [7], chapter 5.2.

5 Architectural Information

The TOE STARCOS 3.4 Health AHC C1 is composed of the already certified NXP P5CC052V0A Secure Smart Card Controller, the operating system STARCOS 3.4 and the digital signature application from Giesecke & Devrient. The TOE is composed of the following subsystems:

- System Library
- Runtime System
- Chip Card Commands
- Security Management
- Key Management
- File System
- Non-Volatile Memory Management
- Transport Management (Protocols)
- Secure Messaging
- Crypto Functions

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

7.1 Test Configurations

The tests were performed with the composite smart card product STARCOS 3.4 Health AHC C1 consisting of the NXP Chip P5CC052V0A, the operating system STARCOS 3.4 and the digital signature application.

Test configurations:

- CD0: Not fully initialised (only MF present), not personalised
- CD1: Personalised as ecard (Usage Phase)
- CD2: Personalised as Admin card (Usage Phase)
- CD3: Personalised as ecard (Personalisation Phase)
- CD4: Plain (i.e. not initialised and not personalised)

Test target categories:

- Operating system (contained in ROM code and EEPROM patch code)
- Initialization and personalization process (PDI and ISO) as defined in [15]
- Applications initialized / loaded as defined in [15]
- Completion state:
  - Completed card: Card in usage phase (completion state “COMPLETED")
  - Uncompleted card: Card in uncompleted state (completion state "INITIAL")
- Physical format:
  - Card (usable for all automatic or non-recoverable test cases)
  - Simulator (required for all interactive test cases)

7.2 Developer Tests according to ATE_FUN

Developer's testing approach:

- Tests to cover all actions defined in the developer's functional specification
- One good case test and one bad case for each command defined in the developer's functional specification and executable on the TOE
- Access Rules test as part of the requirements on TSF data
- Tests covering all TSF subsystems in the TOE design

Verdict for the activity:

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

7.3 Evaluator Tests

7.3.1 Independent Testing according to ATE_IND

Test configurations:

- The tests were performed with the composite smartcard product STARCOS 3.4 Health AHC C1 consisting of the NXP Chip P5CC052V0A, the operating system STARCOS 3.4 and the digital signature application.

Subset size chosen:

- The evaluators have tested 126 TSFI.

TSFI subset selection criteria:

- The evaluators have chosen a subset of interfaces so that the most all TSF could be covered by at least one test case in order to confirm that the TOE operates as specified. The valid cases as well as invalid cases were considered.

TSFI tested:

- The evaluator tested all 126 TSFI documented in the developer's functional specification.

Evaluator's testing approach:

- The developer performed tests of all TSF with card based tests and simulator test cases. The evaluator selected all tests of the developer's testing documentation for sampling due to the fact that all developer tests are implemented in scripts that can run without many manual interactions within days.

Verdict for the activity:

- During the evaluator’s testing the TOE operated as specified.
- The evaluators have verified the developer’s test results by executing a sample of tests in the developer’s test documentation.

7.3.2 Penetration Testing according to AVA_VAN

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 ST, 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 the list of potential vulnerabilities applicable to the TOE in its operational environment the evaluator devised the attack scenarios for penetration tests in the case that those potential vulnerabilities could be exploited in the TOE’s operational environment.

While doing this, also the aspects of the security architecture description 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 penetration tests covered in particular the cryptographic functionality implemented in the TOE. Hereby, the TOE's SHA-256 functionality was out of scope under the aspect of confidentiality.

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. As result of these activities, the evaluator defined a penetration test framework and produced penetration tests to verify the vulnerabilities.

Test configurations:

The evaluators used TOE samples for testing that were configured according to the ST. The TOE samples were identified by using the identification procedure in the operational guidance [12], chap. 4.1.1.2. The application of the evaluated verification tool Smart Card Application Verifier ensured that the configuration of the TOE samples matches the required specifications.

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.
- Simulator based tests 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.

Verdict for the sub-activity:

- During the evaluator's penetration testing based on the evaluator's vulnerability analysis the TOE operated as specified.
- The vulnerabilities discussed in the evaluator's vulnerability analysis are not exploitable in the intended environment for the TOE. None of the penetration tests was successful.
- The TOE is resistant to attackers with high attack potential in the intended environment for the TOE.

8 Evaluated Configuration

This certification covers the following configurations of the TOE: The TOE has only one fixed configuration, namely the composite smartcard product STARCOS 3.4 Health AHC C1 consisting of the NXP chip P5CC052V0A, the operating system STARCOS 3.4 and the digital signature application. 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**, **Documentation** and the **Smart Card Application Verifier Tool** as described below:

TOE_IC: The HW part of the TOE consists of the circuitry of the smart card's chip, the NXP P5CC052V0A and the related IC Dedicated Software with its parts IC Dedicated Test Software and IC Dedicated Support Software (Certification ID: BSI-DSZ-CC-0466-2008).

The TOE_IC firmware contains an RSA crypto library, which is not used in this evaluation project.

TOE_ES: The IC Embedded Software covers the operating system STARCOS 3.4 from Giesecke & Devrient GmbH.

TOE_APP: The application part consists of the digital signature application including the related data structures and their content.

Documentation: The documentation covers all documents delivered together with the TOE ([11] to [16]).

Smart Card Application Verifier Tool: The verification tool consists of the Smart Card Application Verifier, version 2.1 (build 2.1.2) and includes the TOE`s configuration file.

As indicated in chapter 2 the identification data of the TOE consist of information on the underlying chip, operating system, completion state and initialisation table. The following table shows the TOE's identification data as relevant for the TOE's certification:

Identification Data	Identifier
IC manufacturer data	04 11 05 39 00 30 30 35
Version of the operating system	47 44 00 B4 02
Completion state of the operating system	01 02 1x (first 3 bytes of 12 bytes in total)
Initialisation table	Refer to G&D's web site

Table 3: TOE identification data

For details please refer to [12], chapter 4.1.1.2, [13], chapter 4.2.2, 5.2.12, [14], chapter 5.2.4.

To reach this version of the TOE, different initialisation tables can be used which differ only in non-security relevant parts. The requirements for those initialisation tables are listed as generic initialisation tables in [15]. As different versions of initialisation tables may lead to the same TOE version no fixed reference values can be provided in this document. The response data given by the TOE are a unique reference value for every initialisation table. All references for valid initialisation tables are published on the dedicated G&D's web site at https://certificates.gi-de.com/. New initialisation tables have to be checked with the evaluated Smart Card Verifier Tool before updating the above mentioned web site.

Please note that the usage of the TOE within the scope of this certification is limited in accordance with the validity of the used cryptographic algorithms, see chapter 10 of this report.

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [8] 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 4 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:

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

- Composite product evaluation for Smart Cards and similar devices

(see [4], AIS 1, AIS 14, AIS 19, AIS 20, AIS 25, AIS 26, AIS 34, AIS 36, AIS 37, AIS 38.)

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

The ETR [8] builds up on the ETR-for-Composition document of the evaluation of the underlying platform certification [19] supplemented by a recent Re-Assessment [9].

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: None
- for the Functionality: product specific Security Target
  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 were part of the rating:

- SF_KeyManagement: Generation of asymmetric cryptographic keys for digital signatures (ECDSA according to EN 14890 [18])
- SF_SignatureGeneration: Calculation of hash values and generation of digital signatures (ECDSA with SHA-256 according to EN 14890 [18])

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). This holds for:

- SF_TrustedCommunication Challenge-response based mutual authentication with negotiation of symmetric cryptographic keys and following data exchange under secure messaging

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

- Algorithms for message integrity and confidentiality:
  Triple-DES with cryptographic key size of 168 bits according to FIPS 46-3 used for secure messaging
- Algorithms for mutual authentication:
  Triple-DES with cryptographic key size of 168 bits according to FIPS 46-3 used within mutual authentication protocols

- Hash functions:
  SHA-256 according to FIPS 180-2
- Algorithms for signature generation:
  ECDSA with SHA-256 and cryptographic key size of 256 bits according to EN 14890 [18]
- Algorithms for key generation:
  ECDSA with cryptographic key size of 256 bits according to EN 14890 [18]

This holds for the following security functions:

● SF_TrustedCommunication	Challenge-response based mutual authentication with negotiation of symmetric cryptographic keys and following data exchange under secure messaging
● SF_KeyManagement:	Generation of asymmetric cryptographic keys for electronic signatures
● SF_SignatureGeneration:	Calculation of hash values and generation of electronic signatures

The strength of the cryptographic algorithms was not rated in the course of this evaluation (see BSIG Section 9, Para. 4, Clause 2). According to “Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen)” [23], TR-02102 [20] and TR-03111 [21] the algorithms are suitable for the hash value calculation and the generation of electronic signatures. The validity period of each algorithm is mentioned in the official catalogue [23] and summarized in chapter 10 of this report.

10 Obligations and Notes for the Usage of the TOE

The operational documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. There are no further requirements for the TOE usage to be taken into account except those provided for users and administrators in the guidance documentation [12], [13] and [14].

In particular, related to the generation of electronic signatures the signatory has to consider the following security constraints required in [12], chap. 5.1.1:

- STARCOS 3.4 Health AHC C1 cards may only be used in a trusted environment. The signatory has to ensure, that the environment is trusted before using the card. He must not use the card in an untrusted environment.
- The signature PIN as authentication data for the signatory shall be handled confidentially. Especially when entering the PIN, it is recommended to ensure confidentiality.
- In case confidentiality is required (e.g. for privacy reasons) for the documents sent to the card for hashing or signing the signatory has to ensure that the trusted environment he uses provides sufficient measures to ensure the confidentiality of the documents.

In chapter 9.2 of this report, the “Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen)” [23] is referenced for the considerations concerning the suitability of the implemented cryptographic algorithms. According to this paper, the following validity periods apply:

Security Function (SF)	Algorithm	Valid to
SF_SignatureGeneration	SHA-256	End of 2015
SF_SignatureGeneration, SF_KeyManagement	ECDSA 256 bit	End of 2015
SF_SignatureGeneration, SF_KeyManagement	Random number generation, AIS 20, K4	No restriction

Table 4: Validity periods of cryptographic algorithms

In the case that the official catalogue [23] has to be taken into account the usage of the TOE within the scope of this certification is limited in accordance with the validity of the used cryptographic algorithms as outlined in table 4.

For the expiry of the cryptographic algorithms please refer to the relevant and applicable national directives at the particular current status.

The automatic verification tool cannot check the validity of the used cryptographic algorithms, hence by-and-by less of the initialisation tables on the above mentioned web site will fall under this certificate. If a valid CC certificate is required, the card issuer is responsible for only using initialisation tables where the used cryptographic algorithms are valid according to the then effective version of [23].

11 Security Target

For the purpose of publishing, the Security Target [7] 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

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
CGA	Certification Generation Application
DEMA	Differential Electromagnetic Analysis
DPA	Differential Power Analysis
DTBS	Data To Be Signed
EAL	Evaluation Assurance Level
ECDSA	Elliptic Curve Digital Signature Algorithm
HW	Hardware
IT	Information Technology

ITSEC	Information Technology Security Evaluation Criteria
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
QES	Qualified Electronic Signature
SAR	Security Assurance Requirement
SCA	Signature Creation Application
SCD	Signature Creation Data
SEMA	Simple Electromagnetic Analysis
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SPA	Simple Power Analysis
SSCD	Secure Signature Creation Device
ST	Security Target
SVD	Signature Verification Data
SW	Software
TOE	Target of Evaluation
TSF	TOE Security Functions
VAD	Verification Authentication Data

12.2 Glossary

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 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, Revision 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, BSI 7149), periodically updated list published also in the BSI web site

[6] Security Target BSI-DSZ-CC-0601, Version 2.3, 17.12.2009, Security Target STARCOS 3.4 Health AHC C1, Giesecke & Devrient GmbH (confidential document)

[7] Security Target BSI-DSZ-CC-0601, Version 2.3, 17.12.2009, Security Target Lite STARCOS 3.4 Health AHC C1, Giesecke & Devrient GmbH (sanitised public document)

[8] Evaluation Technical Report STARCOS 3.4 Health AHC C1, Version 3, 17.12.2009, TÜViT GmbH (confidential document)

[9] ETR-lite for composition according to AIS 36 for the Product STARCOS 3.4 Health AHC C1, Version 1.2, 21.08.2009, ETR for composition according to AIS36 / NXP P5CC052V0A Secure Smart Card Controller, T-Systems GEI GmbH (confidential document)

[10] Configuration list for the TOE, Version 1.4, 17.12.2009, Configuration List STARCOS 3.4 Health AHC C1 (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 6, 07 May 2009, Evaluations Methodologie 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 3, 12 May 2009, CC-Interpretationen im deutschen Zertifizierungsschema.
- AIS 34, Version 2, 24 October 2008, Evaluation Methodology for CC Assurance Classes for EAL5+
- AIS 35, Version 2, 12 November 2007, Öffentliche Fassung eines Security Target (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 37, Version 2, Terminologie und Vorbereitung von Smartcard-Evaluierungen
- AIS 38, Version 2, 28 September 2007, Reuse of evaluation results

[11] Guidance Documentation STARCOS 3.4 Health AHC C1 – Main Document, Version 1.2, 12.06.2009, Giesecke & Devrient GmbH

[12] Guidance Documentation for the Usage Phase STARCOS 3.4 Health AHC C1, Version 1.7, 15.12.2009, Giesecke & Devrient GmbH

[13] Guidance Documentation for the Initialisation Phase STARCOS 3.4 Health AHC C1, Version 1.4, 15.12.2009, Giesecke & Devrient GmbH

[14] Guidance Documentation for the Personalisation Phase STARCOS 3.4 Health AHC C1, Version 1.5, 15.12.2009, Giesecke & Devrient GmbH

[15] Generic Application STARCOS 3.4 Health AHC C1, Version 1.6, 09.07.2009, Giesecke & Devrient GmbH

[16] STARCOS 3.4 SmartCard Operating System Reference Manual, Edition 09.2009, Giesecke & Devrient GmbH

[17] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures

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

[19] Certification Report BSI-DSZ-CC-0466-2008 for Smart Card Controller P5CC052V0A with specific IC Dedicated Software from NXP Semiconductors Germany GmbH, 24 June 2008

[20] BSI Technische Richtlinie TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 1.0, 20.06.2008

[21] Technical Guideline TR-03111 Elliptic Curve Cryptography, Version 1.11, 17.04.2009, Bundesamt für Sicherheit in der Informationstechnik

[22] Protection Profiles for Secure Signature Creation Device - Part 2: Device with Key Generation, Version 1.03, December 2009, BSI registration ID: BSI-CC-PP-0059-2009

[23] “Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen)”, 27.01.2009, Bundesanzeiger Nr. 13 S. 346

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance Claim (chapter 9.4)

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

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

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

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

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

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

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

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

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

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

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

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

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

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

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

The following table shows the assurance class decomposition.

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

Assurance Class	Assurance Components
	level design presentation
AGD: 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_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
ATE: Tests	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

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

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

Evaluation assurance level (EAL) overview (chapter 8.1)

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

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

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

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

Assurance Class	**Assurance Family**	**Assurance Components by Evaluation Assurance Level**						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	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-0601-2010

Evaluation results regarding development and production environment

The IT product STARCOS 3.4 Health AHC C1 (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 25 January 2010, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.1, ALC_LCD.1, ALC_TAT.1, ALC_COMP.1) are fulfilled for the development and production sites of the TOE listed below:

a) Giesecke & Devrient GmbH, Zamdorfer Straße 88, 81677 Munich, Germany (short name: ZAM; development of evaluation documents and sourcecode)

b) Giesecke & Devrient GmbH, Prinzregentenstraße 159, 81677 Munich, Germany (short name: GDM; system administration)

For development and production sites regarding the underlying NXP chip P5CC052V0A refer to the certification report BSI-DSZ-CC-0466-2008.

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

This page is intentionally left blank.