Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0582-2009

for

STARCOS 3.4 Health QES 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-0582-2009

Smart Card with Digital Signature Application

STARCOS 3.4 Health QES 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_MSU.3 and AVA_VLA.4

Common Criteria
Recognition
Arrangement
for components up to
EAL 4

Common Criteria

The IT product identified in this certificate has been evaluated at an accredited and licensed / approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005).

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

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

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

Bonn, 30 April 2009
For the Federal Office for Information Security

IT Security Certified

SOGIS - MRA

Bernd Kowalski
Head of Department

L.S.

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

This page is intentionally left blank.

Preliminary Remarks

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

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

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

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

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

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

[1] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

Contents

A Certification

1 Specifications of the Certification Procedure

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

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)[5] [1]
- Common Methodology for IT Security Evaluation, Version 2.3 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

2 Recognition Agreements

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

---

2 Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

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

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

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

2.1 European Recognition of ITSEC/CC - Certificates

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

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

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

2.2 International Recognition of CC - Certificates

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

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

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

This evaluation contains the components AVA_MSU.3 (Analysis and Testing for insecure States) and AVA_VLA.4 (Highly Resistant) that are not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4 components of these assurance families are relevant.

3 Performance of Evaluation and Certification

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

The product STARCOS 3.4 Health QES C1 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0407-2008-MA01. Specific results from the evaluation process BSI-DSZ-CC-0407-2008-MA01 were re-used.

The evaluation of the product STARCOS 3.4 Health QES C1 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 23 April 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

[6] Information Technology Security Evaluation Facility

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.

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

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

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

5 Publication

The product STARCOS 3.4 Health QES C1 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http://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 related product of the Target of Evaluation (TOE) is the STARCOS 3.4 Health QES C1 Smart Card consisting of the Operating System (OS) and the Digital Signature Application on a Smart Card Integrated Circuit (IC). The TOE differs from the whole product, as the TOE does not include the optionally other applications (for example the “German Health System Applications”) shown in Figure 2 on page 10 of the Security Target [6], marked with the dashed line.

The TOE is implemented as a Smart Card on an IC and is intended to be used as Secure Signature Creation Device Type 3. This includes generation and secure storage of a SCD/ SVD pair and the generation of qualified electronic signatures of 2048 Bit.

The Security Target [6] is the basis for this certification. It is based on but not compliant to the certified Secure Signature-Creation Device Protection Profile Type 3 [10]. The deviation from the Protection Profile has been necessary to fulfil the specifications of the German electronic Health Card.

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_MSU.3 and AVA_VLA.4.

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

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

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

TOE Security Function	Addressed issue
SF.ACCESS	Checks if the operation specific requirements on user authorisation and protection of communication data are fulfilled
SF.ADMIN	The administration of the TOE is managed by this Security Function
SF.AUTH	The authentication of the signatory is managed by this Security Function
SF.SIG	Signature Creation
SF.CRYPTO	Provides the cryptographic support
SF.TRUST	Manages Card-to-Card authentication and protection of the communication data
SF.PROTECTION	Protects the TSF functionality, TSF data and user data
SF.IC_SF	Covers the Security Functions of the IC

Table 1: TOE Security Functions

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

The claimed TOE's Strength of Functions 'high' (SOF-high) for specific functions as indicated in the Security Target [6] and [9], chapter 6.1 is confirmed. The rating of the Strength of Functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). For details see chapter 9 of this report.

The assets to be protected by the TOE are defined in the Security Target [6] and [9], chapter 3. Based on these assets the TOE Security Environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [9], chapter 3.1, 3.2 and 3.3.

The TOE comprises the following parts:

- NXP P5CC080V0B Secure Smart Card Controller, consisting of the circuitry of the 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)
- SSCD application
- Guidance documentation delivered together with the TOE ([16] to [20]) and
- Smart Card Application Verifier Tool[8] (Smart Card Application Verifier, Version 2.1, build 2.1.1, including the configuration file)

This certification covers the following configurations of the TOE: STARCOS 3.4 Health QES C1. For details please refer to chapter 8.

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 QES C1

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW/ SW	NXP P5CC080V0B Secure Smart Card Controller	Mask Identifier: P5CC080X0/ T0B36	Smart card modules, ROM mask of the TOE already mounted into an ID-1 smart card
2	SW	Card Operating System STARCOS 3.4	0103	Software on the smart card

[8] The Smart Card Application Verifier Tool is part of the TOE, but not part of the TOE delivery. Since the TOE may be initialised with different initialisation tables that have to be compliant to the *Spezifikation Generische Applikation* [16] without exceeding the CC certificate, the developer has to ensure this compliance by checking the initialisation table with the Smart Card Application Verifier Tool.

No	Type	Identifier	Release	Form of Delivery
3	SW	EEPROM image of STARCOS 3.4 Health QES C1	Identifier of valid images published on the G&D website	Image on the smart card
4	DOC	Administrator Guidance, Part 1: Initialisation, STARCOS 3.4 Health eGK C1, STARCOS 3.4 Health QES C1	Version 1.5 / 2009-02-09	Document in paper / electronic form
5	DOC	Administrator Guidance, Part 2: Personalisation, STARCOS 3.4 Health eGK C1, STARCOS 3.4 Health QES C1	Version 1.4 / 2009-02-06	Document in paper / electronic form
6	DOC	Benutzerhandbuch STARCOS 3.4 Health QES C1	Version 1.6 / 2009-04-01	Document in paper / electronic form
7	DOC	Spezifikation Generische Applikation, STARCOS 3.4 Health QES C1	Version 0.71 / 2009-04-01	Document in paper / electronic form
8	DOC	Installation, generation and startup, STARCOS 3.4 Health eGK C1 / STARCOS 3.4 Health QES C1	Version 1.7 / 2009-02-09	Document in paper / electronic form

Table 2: Deliverables of the TOE

Basically the life cycle of STARCOS 3.4 Health QES C1 consists of the development phase and the operational phase. The development phase includes OS Design and Application Design (responsibility: G&D), HW design (responsibility: Chip Manufacturer), HW Fabrication as well as OS and Application Implementation (responsibility: Chip Manufacturer). The initialisation phase completely belongs to the operational use. The TOE will be delivered as a smart card with initialisation data already embedded in the TOE. No modifications by a third party are possible (e.g. by the party loading the initialisation data into the hardware).

For the evaluation process the whole life-cycle of the TOE was considered during evaluation as far as the developer/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 faked chips.

To verify the ID of the initialisation table of the TOE (and therefore also the composite TOE), the user executes the command GET PROTOCOL DATA (see [19], chap. 5).

The user can check the version of the

- IC manufacturer data (*Chipherstellerdaten)*
- OS version (*Betriebssystemversion*)
- completion state (*Komplettierungsstand)* and
- initialisation table *(Initialisierungstabelle)*

The numbers of valid initialisation tables are published on the Giesecke & Devrient GmbH website https://certificates.gi-de.com for comparison.

3 Security Policy

The TOE is the composition of an IC, IC Dedicated Software and Smart Card Embedded Software and is intended to be used as a Secure Signature Creation Device (SSCD) for

the generation of signature creation data (SCD) and the creation of qualified electronic signatures. 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 / forge / misuse of confidential user or TSF data including information leakage
- interception of communication
- abuse of TOE functionality (including its SSCD application)
- storing, copying, releasing and deriving the signature creation data by an attacker
- forgery of the electronic signature, of the signature-verification data, or of the DTBS-representation
- repudiation of signatures,
- 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 security objectives related to the environment of the TOE´s dedicated SSCD Application can be found in the Security Target [6] and [9], chapter 4.2.

5 Architectural Information

The TOE STARCOS 3.4 Health QES C1 is composed of the already certified NXP P5CC080V0B Secure Smart Card Controller, the operating system STARCOS 3.4 and the SSCD application from Giesecke & Devrient, see also figure 1 in [6].

The TOE is composed of the following subsystems:

- Access Control
- Setup
- Commands
- Application Data and Basic Functions
- Crypto Functions
- Secure Messaging
- Hardware

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. 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
- a simulator which is required for all interactive test cases.

The test targets (TT) were:

- TT1a: Card completed / initialized / personalized with eHC and SSCD application, (TOE TT), plus test applications loaded onto the TOE by the tests
- TT1b: Simulator completed / initialized / personalized with eHC and SSCD application, (Non-TOE TT), plus test applications loaded onto the TOE by the tests
- TT2a: Uncompleted card + eHC and QES applications in form of an initialization image, (non-TOE TT)
- TT2b: Simulator in uncompleted state + eHC and QES application in form of an initialization image (non-TOE TT)

These four different test targets were necessary to test the single aspects of the TOE relevant for testing:

- Operating system contained in ROM code and EEPROM patch code
- Applications which were initialized / loaded
- Completion state: card in usage phase or in uncompleted state

7.1 Developer Tests according to ATE_FUN

All TSF as specified in [6] with related subfunctions and subsystems were tested in order to assure complete coverage. The test strategy was that all commands stated in the functional specification were tested to cover the requirements on TSF data, the security functional effects and the most important return codes given there and moreover all interfaces described in the high-level design.

7.2 Evaluator Tests

7.2.1 Independent Testing according to ATE_IND

The approach for the evaluator’s independent testing was:

- Examination of the developer’s testing amount, depth and coverage analysis and of the developer’s test goal 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 performed by the evaluator in the evaluation facility with the TOE development environment using script based developer test tools with automated comparison of expected and actual test results

During sample testing the evaluator has chosen to repeat all developer functional tests at the Evaluation Body for IT-Security. The evaluator has verified the developer's test results by executing all tests in the developer's test documentation and verifying the test log files of a sample thereof.

The independent test results demonstrate that the TOE performs as expected.

7.2.2 Penetration Testing according to AVA_VLA

The approach for the evaluator's penetration testing was:

- Examination of the developer's vulnerability analysis and of the developer's rationale based on for why the vulnerabilities are not exploitable in the intended environment of the TOE
- Examination whether the TOE, in its intended environment, is susceptible to vulnerabilities not considered by the developer by considering current information regarding obvious public domain vulnerabilities

Penetration testing was performed by the evaluator at the Evaluation Body for IT-Security with the TOE development environment using script based developer test tools with automated comparison of expected and actual test results. All security functions were penetration tested.

During the penetration testing the TOE operated as specified. The vulnerabilities discussed in the vulnerability analysis are not exploitable in the intended environment for the TOE.

8 Evaluated Configuration

The TOE as a Secure Signature Creation Device only features one fixed configuration STARCOS 3.4 Health QES C1 which cannot be altered by the user. 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: Consists of the circuitry of the chip, the NXP P5CC080V0B and the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software (Certification ID: BSI-DSZ-CC-0410-2007-MA-04). The chip hardware of TOE_IC includes:

- Security logic (SEC)
- Microcontroller with an 8-bit architecture (CPU) that has an extended instruction set compared with the 80C51 family instruction set
- External memory comprising:
  - 224 kBytes ROM
  - 6144 Bytes RAM, 3584 Bytes general purpose RAM and 2560 FameXE RAM
  - 200 kBytes Application-ROM and 24 kBytes Test-ROM
  - a total of 80 kBytes EEPROM, with 128 Bytes of the EEPROM are always reserved for the manufacturer and can not be read and written by the smart card embedded software
  - True random number generator (RNG), SOF-high, AIS 31

- FameXE co-processor

The TOE_IC firmware consists of a RSA crypto library, which is not used in this evaluation project.

TOE_ES: The IC Embedded Software (operating system), STARCOS 3.4

TOE_APP: The SSCD application

Documentation: Documents delivered together with the TOE ([16] to [20])

Smart Card Application Verifier Tool: Smart Card Application Verifier (Version 2.1, build 2.1.1), including the configuration file (Version 0.71)

However, 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 [16]. The initialisation tables listed in Table 3 all fulfil the requirements of [16].

Table Identifier
01 03 03 e1 ff e8 89 ea 76 cb 4a 1b
01 03 03 e2 d2 16 c9 9d 3e 69 0c c1
01 03 03 e4 96 b3 2a d5 0b 1d 4e 70
01 03 03 e9 4f d6 4a b5 49 14 da b1

Table 3: Identifiers for valid Initialisation Tables

The identification of the TOE is described in [19], chapter 5.2. The relevant identifier for the evaluated initialisation table can be found on the dedicated web page: https://certificates.gi-de.com. New initialization tables have to be checked with the evaluated Smart Card Verifier Tool before updating the above mentioned web page.

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

The Evaluation Methodology CEM [2] was used for those components up to EAL4 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the technology was used:

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

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

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

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

- All components of the class ASE
- All components of the EAL 4 package as defined in the CC (see also part C of this report)
- The components AVA_MSU.3 and AVA_VLA.4 augmented for this TOE evaluation

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0407-2008-MA01, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the change of the underlying hardware platform [12], integration of the new gematik specifications of the German Health Card [13] and [14] and changes in the bitlength of the used hash and cryptographic algorithms.

The evaluation has confirmed:

- 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_MSU.3 and AVA_VLA.4
- The following TOE Security Functions fulfil the claimed Strength of Function: high
  - SF.ADMIN - The administration of the TOE is managed by this Security Function
  - SF.AUTH - The authentication of the signatory is managed by this Security Function
  - SF.CRYPTO - Provides the cryptographic support
  - SF.IC_SF - Covers the Security Functions of the IC

In order to assess the Strength of Function the scheme interpretations AIS 20 and AIS 26 (see [4]) were used.

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

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

9.2 Results of cryptographic assessment

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

Hash functions:

- SHA-256

Algorithms for signature creation:

- RSA 2048

This holds for the following security function:

- SF.SIG - Signature Creation
- SF.CRYPTO - Provides the cryptographic support
- SF.TRUST - Manages Card-to-Card authentication and protection of the communication data

The strength of the cryptographic algorithms was not rated in the course of this evaluation (see BSIG Section 4, Para. 3, Clause 2).

According to "*Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen)"* [15] the algorithms are suitable for signature creation. The validity period of each algorithm is mentioned in the official catalogue [15] 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. In particular, the user and administrator guidances make the following constraints for users of the TOE:

- The ChipPWD shall be kept confidential ([18], chapter 4.1.4)
- The Initialiser must perform the self tests of the TOE ([17], chapters 6.2, 6.3 and 6.15)
- The chosen User PIN has to be random. It should not be possible to guess it ([19], chapter 2.2.2)

In addition, the following aspects need to be fulfilled when using the TOE:

- The identification of the TOE is described in [19], chapter 5.2. The relevant identifier for the evaluated initialisation table can be found on the dedicated web page: https://certificates.gi-de.com
- The card issuer is responsible for choosing only values which are permitted by [16]
- When Giesecke & Devrient GmbH modifies the non-TOE part of the initialization table (e.g. when Giesecke & Devrient GmbH implements the initialisation table with the values of the card issuer), that initialization table has to be checked before updating the above mentioned web page
- Giesecke & Devrient GmbH is supported in this task with an automatic verification tool that checks the consistency to [16], e.g. FCPs for MF/DFs or the access rules for MF/DFs

As mentioned in Chapter 9.2 of this report, the "*Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen)"* [15] is applied.

The following restrictions arise from that paper:

Security Funciton (SF)	Algorithm	Valid to
SF.Crypto 1	SHA-256	End of 2015
SF.Crypto 2	RSA, 2048 bit	End of 2015
SF.Crypto 4	Random number generation, AIS 20, K4	valid

Table 4: Validity period of the used cryptographic and hash algorithms

For the expiry of the cryptographic algorithms please refer to the relevant and applicable national directives. The usage of the TOE within the scope of this certification is limited in accordance with the validity of the used cryptographic algorithms.

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 [15].

11 Security Target

For the purpose of publishing, the Security Target [9] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12 Definitions

12.1 Acronyms

APDU Application Protocol Data Unit

AS Application Software

ATE Assurance class Test Activity

ATE_IND Independant testing

AVA Assurance class Vulnerability Assessment Activity

AVA_VLA Vulnerability analysis

BSI Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany

BSIG BSI-Errichtungsgesetz

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation

CEM Evaluation Methodology

DES Data Encryption Standard

DFA Differential Fault Analysis

DOC Document

DPA Differential Power Analysis

EAL Evaluation Assurance Level

EEPROM	Electronically Erasable Programmable Read Only Memory
eHC	electronic Health Card
ES	Embedded Software
ETR	Evaluation Technical Report
IC	Integrated Circuit
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
JIL	Joint Interpretation Library
OS	Operating System
PP	Protection Profile
QES	Qualified Electronic Signature
RSA	Rivest Shamir Adleman Algorithmus
SCD	Signature Creation Data
SF	Security Function
SFP	Security Function Policy
SHA	Secure Hash Algorithm
SOF	Strength of Function
SPA	Simple Power Analysis
SSCD	Secure Signature Creation Device
ST	Security Target
SVD	Signature Verification Data
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

12.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

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

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

Informal - Expressed in natural language.

Object - An entity within the TSC that contains or receives information and upon which subjects perform operations.

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

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

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

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

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

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

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

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

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

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

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

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

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

13 Bibliography

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

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

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

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

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Website

[6] Security Target BSI-DSZ-CC-0582-2009, Version 0.8, 19.03.2009, Security Target STARCOS 3.4 Health QES C1, Giesecke & Devrient GmbH (confidential document)

[7] Evaluation Technical Report, Version 3, 23.04.2009, Evaluation Technikal Report for STARCOS 3.4 Health QES C1, TÜV Informationstechnik GmbH (confidential document)

[8] Configuration list for the TOE, Version 1.2, 16.04.2009, Configuration List STARCOS 3.4 Health QES C1 (confidential document)

[9] Security Target BSI-DSZ-CC-0582-2009, Version 0.8, 19.03.2009, Security Target Lite STARCOS 3.4 Health QES C1, Giesecke & Devrient GmbH (sanitised public document)

[10] Protection Profile Secure Signature Creation Device Type 3, EAL 4+, BSI-PP-0006-2002, Version 1.05, 25.07.2001, CEN/ISSS

[11] ETR-lite for composition according to AIS 36 for the Product NXP P5CD080V0B Secure Smart Card Controller, Version 1.1, 23.04.2008, BSI-DSZ-CC-430-2008, T-Systems (confidential document)

---

[9] specifically

- AIS 20, Version 1, 2 December 1999, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 3, 6 August 2007, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 3, 6 August 2007, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 1, 25 Sept. 2001 Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 1, 2 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.
- AIS 34, Version 1.00, 1 June 2004, Evaluation Methodology for CC Assurance Classes for EAL5+
- AIS 35, Version 2.0, 12 November 2007, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 2, 12 November 2007, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

[12] Certification Report for NXP Secure Smart Card Controller P5CD080V0B, P5CN080V0B and P5CC080V0B each with specific IC Dedicated Software, BSI-DSZ-CC-410-2007, 05.07.2007, BSI

[13] Spezifikation der elektronischen Gesundheitskarte, Teil 1: Spezifikation der elektrischen Schnittstelle, Version 2.2.2, 16.09.2008, gematik

[14] Spezifikation der elektronischen Gesundheitskarte, Teil 2: Grundlegende Applikationen, Version 2.2.1, 19.06.2008, gematik

[15] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 17. Dezember 2007, veröffentlicht am 27. Januar 2009 im Bundesanzeiger Nr. 13, Seite 346

[16] Spezifikation Generische Applikation STARCOS 3.4 Health QES C1 (includes document & verifier files), Version 0.71, 01.04.2009, Giesecke & Devrient

[17] Administrator Guidance Part 1: Initialisation, STARCOS 3.4 Health eGK C1, STARCOS 3.4 Health QES C1, Version 1.5, 09.02.2009, Giesecke & Devrient

[18] Administrator Guidance Part 2: Personalisation, STARCOS 3.4 Health eGK C1, STARCOS 3.4 Health QES C1, Version 1.4, 05.02.2009, Giesecke & Devrient

[19] Benutzerhandbuch STARCOS 3.4 Health QES C1, Version 1.6, 01.04.2009, Giesecke & Devrient

[20] Installation, generation and startup STARCOS 3.4 Health eGK C1 / STARCOS 3.4 Health QES C1, Version 1.7, 09.02.2009, Giesecke & Devrient

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

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

The conformance result consists of one of the following:

- **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.
- **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

- **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.
- **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

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

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

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

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

CC Part 3:

Protection Profile criteria overview (chapter 8.2)

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

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

Table 3 - Protection Profile families - CC extended requirements”

Security Target criteria overview (Chapter 8.3)

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

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

Table 5 - Security Target families - CC extended requirements ”

Assurance categorisation (chapter 7.5)

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

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

Table 1: Assurance family breakdown and mapping”

Evaluation assurance levels (chapter 11)

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

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

Evaluation assurance level (EAL) overview (chapter 11.1)

“Table 6 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

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

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

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

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

Table 6: Evaluation assurance level summary”

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

“Objectives

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

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

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.”

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

“Objectives

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

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

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 11.5)

“Objectives

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

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

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 11.6)

“Objectives

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

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

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 11.7)

“Objectives

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

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

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 11.8)

“Objectives

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

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

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 11.9)

“Objectives

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

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

“Objectives

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

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

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

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

"Application notes

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

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

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development and production environment 37

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0582-2009

Evaluation results regarding development and production environment

The IT product STARCOS 3.4 Health QES C1 (Target of Evaluation, TOE) has been evaluated at an accredited and licensed / approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005).

As a result of the TOE certification, dated 30 April 2009, the following results regarding the development and production environment apply. The Common Criteria Security Assurance Requirements

- ACM – Configuration management (i.e. ACM_AUT.1, ACM_CAP.4, ACM_SCP.2),
- ADO – Delivery and operation (i.e. ADO_DEL.2, ADO_IGS.1) and
- ALC – Life cycle support (i.e. ALC_DVS.1, ALC_LCD.1, ALC_TAT.1),

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

(a) Giesecke & Devrient GmbH (Site: “GDTC”), Prinzregentenstraße 159, 81677 Munich (Development and Production)

(b) Giesecke & Devrient GmbH (Site: “ZAM”), Zamdorfer Straße 88, 81677 Munich (Development)

For development and productions sites regarding the NXP chip P5CC080V0B refer to the certification report BSI-DSZ-CC-0410-2007 [12].

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. The evaluators verified, that the Threats, Security Objectives and Requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6] and [9]) are fulfilled by the procedures of these sites.

This page is intentionally left blank.