Federal Office
for Information Security

# Certification Report

## BSI-DSZ-CC-0880-2013

for

## STARCOS 3.5 ID ECC C1R

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-0880-2013**

Secure Signature Creation Device (SSCD)

**STARCOS 3.5 ID ECC C1R**

| | |
|---|---|
| from | Giesecke & Devrient GmbH |
| PP Conformance: | Protection profiles for secure signature creation device - Part 2: Device with key generation, Version 2.0.1, BSI-CC-PP-0059-2009-MA-01 |
| Functionality: | PP conformant plus product specific extensions Common Criteria Part 2 extended |
| Assurance: | Common Criteria Part 3 conformant EAL 4 augmented by AVA_VAN.5 |

Common Criteria Recognition Arrangement for components up to EAL 4

Common Criteria

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

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

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

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

Bonn, 19 April 2013

For the Federal Office for Information Security

SOGIS IT SECURITY CERTIFIED

Bernd Kowalski
Head of Department

L.S.

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

This page is intentionally left blank.

# Preliminary Remarks

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

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

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

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

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

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

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

# Contents

# A Certification

## 1 Specifications of the Certification Procedure

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

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

## 2 Recognition Agreements

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

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

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

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL 4 resp. E3 (basic). In Addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

---

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

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

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

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

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

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

### 2.2 International Recognition of CC – Certificates (CCRA)

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

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

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

This evaluation contains the component AVA_VAN.5 that is not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL 4 components of these assurance families are relevant.

## 3 Performance of Evaluation and Certification

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

The product STARCOS 3.5 ID ECC C1R has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0769-2012. Specific results from the evaluation process BSI-DSZ-CC-0769-2012 were re-used.

The evaluation of the product STARCOS 3.5 ID ECC C1R was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 3 April 2013. The SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: 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.

[6] Information Technology Security Evaluation Facility

# 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, as specified in the following report and in the Security Target.

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

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

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

# 5 Publication

The product STARCOS 3.5 ID ECC C1R has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

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

[7] Giesecke & Devrient GmbH
Prinzregentenstr. 159
81677 München
Deutschland

This page is intentionally left blank.

# B Certification Results

The following results represent a summary of

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

# 1 Executive Summary

The Target of Evaluation (TOE) is the product STARCOS 3.5 ID ECC C1R provided by Giesecke & Devrient GmbH, based on the hardware platform M7820 A11 from Infineon Technologies AG (Certificate-ID: BSI-DSZ-CC-0813-2012 [15]).

The TOE is a contactless, contact-based or dual interface smart card and is intended to be used as a Secure Signature Creation Device (SSCD) in accordance with the European Directive 1999/93/EC1 [17]. The TOE as SSCD provides functionality for the onboard generation of signature key pairs (Signature Creation Data / Signature Verification Data, SCD / SVD), for the generation of qualified electronic signatures and for a trusted communication channel to the Certification Generation Application (CGA) respective the Signature Creation Application (SCA). The TOE's Signature Application is compliant to EN 14890 [24].

The TOE consists of the part of the implemented software related to the generation of signature key pairs (SCD / SVD), to the generation of qualified electronic signatures and to the establishment and execution of trusted communication channels between the TOE and the external world in combination with the underlying hardware. For CC evaluation, the following application of the corresponding product will be considered: The Signature Application containing the related user data (signature PIN and SCD) as well as the data needed for authentication (authentication keys etc.) as specified in the Generic Application Specifications [14].

In addition, the Smart Card Application Verifier version 2.1 (short: Verifier) is part of the TOE. The Verifier is a configurable comparison tool for initialisation tables installed on the TOE, which is used by the developer in order to verify the created and loaded initialisation table against the Generic Application Specifications [14]. The Generic Application Specifications [14] are implemented in the reference images which are used with according configuration files with the Verifier to approve the correctness of the developed initialisation tables. The Verifier is part of the TOE and has therefore been evaluated, but it is not part of the delivery to the customer. It is only used as a tool within the developer's environment.

The Security Target [6] (respective [7]) builds the basis for this certification. It is based on the PP Protection profiles for secure signature creation device – Part 2: Device with key generation certified by BSI and registered under the Certification-ID BSI-CC-PP-0059-MA-01 [9]. Within the Security Target [6] the claimed Protection Profile was appropriately supplemented for a trusted channel between the TOE and the Certification Generation Application (CGA) respective the Signature Creation Application (SCA). For details refer to [6] respective [7], chapter 4 and following.

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 and 7.2. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

| Identifier | Addressed issue |
|---|---|
| SF_AccessControl | The TOE provides access control mechanisms that allow among others the maintenance of different users (Administrator, Signatory). The access and usage of TOE related data and the execution of security relevant actions are controlled appropriately. |
| SF_AssetProtection | The TOE supports the calculation of block check values for data integrity checking. The TOE hides information about IC power consumption and command execution time ensuring that no confidential information can be derived from this information. Furthermore, appropriate memory preparation is implemented. |
| SF_TSFProtection | The TOE is resistant to and detects physical tampering of the TSF. The TOE demonstrates the correct operation of the TSF by among others verifying the integrity of the TSF and TSF data and verifying the absence of fault injections. |
| SF_KeyManagement | The TOE supports the onboard generation of RSA and ECC cryptographic key pairs of different key lengths. |
| SF_SignatureGeneration | The TOE supports the SHA hash value calculation and the generation of RSA and ECC based electronic signatures of different key lengths and signature schemes. |
| 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. The trusted channel/path may be used in the framework of the secure communication between the TOE and the Certification Generation Application (CGA) and the Signature Creation Application (SCA). |

Table 1: TOE Security Functionality

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 Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [7], chapter 4.1 to 4.3.

This certification covers the following configurations of the TOE: STARCOS 3.5 ID ECC C1R/360, STARCOS 3.5 ID ECC C1R/800 and STARCOS 3.5 ID ECC C1R/1280 provided by Giesecke & Devrient GmbH and distinguishing between the different available non-volatile memory sizes. The configurations of the TOE are described in detail in the Guidance Documents [10], [11], [12] and [13] and the Generic Application Specifications [14] provided with the TOE (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 3.5 ID ECC C1R**

The following table outlines the TOE deliverables:

| No | Type | Identifier | Release | Form of Delivery |
|---|---|---|---|---|
| 1 | HW/SW | Initialised or uninitialised module with hardware for contact-based, contactless or dual interface.<br>This part of the TOE consists of:<br>Hardware platform:<br>M7820 A11 by Infineon Technologies AG (incl. its IC Dedicated Test Software)<br>TOE Embedded Software:<br>IC Embedded Software (the operating system) STARCOS 3.5 (implemented in ROM/EEPROM of the IC)<br>TOE Embedded Applications:<br>Signature Application as initialisation table<br>Hint: The TOE can be delivered without the initialisation table (in the case of the TOE's delivery as already initialised module). | ROM Mask label CIF9DSCSR35-01c_ V200<br>STARCOS version 3.5<br>TOE Embedded Application as initialisation table see text below | Items as defined on the left-hand side.<br>Hint: The IC and the Embedded Software are providing self-protection mechanisms, ensuring confidentiality and integrity during delivery. The delivery does not need additional security measures and can be considered as normal transport. |
| 2 | SW | Cryptographic keys for initialisation or personalisation, securing the TOE from modification by illegal entities, e.g. during transport | --- | Item in electronic form, encrypted and signed against disclosure and modification. |
| 3 | DOC | Guidance Documentation STARCOS 3.5 ID ECC C1 – Main Document [10] | Version 0.6 | Document in electronic form. |
| 4 | DOC | Guidance Documentation for the Initialization Phase, STARCOS 3.5 ID ECC C1 [12] | Version 1.5 | Document in electronic form. |
| 5 | DOC | Guidance Documentation for the Personalisation Phase, STARCOS 3.5 ID ECC C1 [13] | Version 0.8 | Document in electronic form. |
| 6 | DOC | Guidance Documentation for the Usage Phase, STARCOS 3.5 ID ECC C1 [11] | Version 1.2 | Document in electronic form. |
| 7 | DOC | Generic Application Specifications of STARCOS 3.5 ID ECC C1R [14] | Different versions, refer to [14] | Document in electronic form. |

Table 2: Deliverables of the TOE

The customer specific ROM mask for the STARCOS 3.5 ID ECC C1R on the hardware platform M7820 A11 is labelled CIF9DSCSR35-01c_V200.

The user is provided with guidance for TOE identification in [10], [11], [12] and [13]. The initialisation agent, the personalisation agent and the end user (respective the customer of the product on his behalf) can use the command GET PROTOCOL DATA (with CLA = A0; INS = CA) to read out the identification data stored in the TOE.

The following command parameters can be used to retrieve identification data:

- Command parameters: P1=’9F’ P2=’6B’, Identifier length: 8 bytes, Description: Chip manufacturer data (Chip manufacturer’s ROM mask ID) varying in dependence on the used hardware (different non-volatile memory size).
- Command parameters: P1=’9F’ P2=’6A’, Identifier length: 5 bytes, Description: Version of the operating system (OS manufacturer / OS version number / Version of ROM mask).
- Command parameters: P1=’9F’ P2=’67’, Identifier length: 20 bytes, Description: Version of the completion level of the operating system (first 3 bytes) and initialisation table (last 16 bytes).

Details on the identification data of the different evaluated configurations of the TOE can be found in chapter 8 below.

All initialisation tables listed in [14] have to pass a validation by the Verifier. The functionality of the Verifier has been evaluated and tested as part of the evaluation.

To verify the TOE's identification data and in particular the identification data of its initialisation table (and therefore also of the composite TOE), the user executes the command GET PROTOCOL DATA. The identification data of valid initialisation tables are published on the Giesecke & Devrient GmbH website https://certificates.gi-de.com for comparison.

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 Giesecke & Devrient GmbH security transport or a security transport maintained by another initialiser to avoid the delivery of fake chips.

# 3 Security Policy

The TOE is the composition of an IC and appropriate Smart Card Embedded Software and will be used as Secure Signature Creation Device (SSCD). The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

- Modification and disclosure of IC assets / Smart Card Embedded Software / application data
- Compromise, forgery and misuse of confidential user or TSF data including information leakage
- Physical attacks through the TOE interfaces
- Tamper detection and resistance
- Abuse of TOE functionality
- Malfunction due to environmental stress

- Storage, copy and release of the SCD
- Derivation of the SCD
- Misuse of the signature creation function of the TOE
- Forgery of the DTBS-representation and the electronic signature
- Interception of communication (trusted channel between the TOE and the SCA respective the CGA)
- Life-cycle security

# 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:

- OE.SVD_Auth: Authenticity of the SVD
- OE.CGA_QCert: Generation of qualified certificates
- OE.DTBS_Intend: SCA sends data intended to be signed
- OE.Signatory: Security obligation of the Signatory
- OE.Dev_Prov_Service: Authentic SSCD provided by SSCD Provisioning Service
- OE.CGA_SSCD_Auth: Pre-initialisation of the TOE as SSCD
- OE.CGA_TC_SVD_Imp: CGA trusted channel for SVD import
- OE.HID_confTC_VAD_Exp: Optional trusted channel of HID for VAD export
- OE.SCA_confTC_DTBS_Exp: Optional trusted channel of SCA for DTBS export

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

# 5 Architectural Information

The TOE is a composite product. It is composed from an Integrated Circuit, IC Embedded Software and IC Application Software containing the Signature Application. The IC Embedded Software contains the operating system STARCOS 3.5. For details concerning the CC evaluation of the underlying IC see the evaluation documentation under the certification ID BSI-DSZ-CC-0813-2012 [15].

According to the TOE Design the security functionality of the TOE is enforced by the following subsystems:

- System Library (contains the application framework)
- Runtime System (main loop and command interpreter)
- Chip Card Commands (pre-processor and processor of all implemented commands)
- Security Management (manages the security environment, security states and rule analysis)
- Key Management (search, pre-process, use and post-process of keys)
- Secure Messaging (SM handling)

- Crypto Functions (library with an API to all cryptographic operations, e.g. signature generation)

# 6 Documentation

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

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

# 7 IT Product Testing

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

Since much of the security functionality can be tested by APDU command sequences, the evaluators performed these tests with real cards. This is considered to be a reasonable approach because the developer tests include a full coverage of all security functionality. Furthermore, penetration tests were chosen by the evaluators for that security functionality where internal secrets of the card could maybe be modified or observed during testing. During their independent testing, the evaluators covered

- testing APDU commands related to Key Management and Crypto Functions,
- testing APDU commands related to NVM Management and File System,
- testing APDU commands related to Security Management,
- testing APDU commands related to Secure Messaging,
- testing APDU commands related to Runtime System and System Library,
- penetration testing related to verify the Reliability of the TOE,
- source code analysis performed by the evaluators,
- testing the commands which are used to execute the PACE protocol,
- side channel analysis for SHA, RSA and ECC (including ECC key and signature generation),
- fault injection attacks (laser attacks),
- testing the Verifier,
- testing APDU commands for the initialization, personalization and usage phase,
- testing APDU commands for the commands using cryptographic mechanisms.

The evaluators have tested the TOE systematically against high attack potential during their penetration testing.

The achieved test results correspond to the expected test results.

# 8 Evaluated Configuration

The TOE evaluated configuration is defined by the notation:

STARCOS 3.5 ID ECC C1R on the hardware platform M7820 A11 and configured as described in the document Generic Applications STARCOS 3.5 ID ECC C1R [14] and in the Guidance Documents [10], [11], [12] and [13] provided with the TOE.

The initialisation and personalisation agent as well as the end user or the card issuer on his behalf can use the command GET PROTOCOL DATA as described in chapter 2 (above) to read out the chip information and identify the chip. The following information describes the evaluated configuration:

- Chip manufacturer data (chip manufacturer's ROM mask ID) varying in dependence on the used hardware (different non-volatile memory size):
  - for TOE STARCOS 3.5 ID ECC C1R/360, Identifier Data: '05 77 33 00 B1 00 8B 01',
  - for TOE STARCOS 3.5 ID ECC C1R/800, Identifier Data: '05 77 33 00 A9 00 8A 01',
  - for TOE STARCOS 3.5 ID ECC C1R/1280, Identifier Data: '05 77 33 00 A7 00 23 00',
- Version of the operating system (OS-manufacturer / OS version number / Version of ROM mask), Identifier Data: '47 44 00 B5 02',
- Version of the completion level of the operating system, Identifier Data: '02 00 00'.
- Version of the initialisation table, Identifier Data: see G&D website.

# 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 5 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the technology was used:

- Application of CC to Integrated Circuits,
- Smart Card evaluation guidance,
- Application of Attack Potential to Smart Cards,
- Composite product evaluation for Smart Cards and similar devices,
- Functionality classes and evaluation methodology of deterministic random number generators

(see [4], AIS 20, AIS 25, AIS 26, AIS 32, AIS 34, AIS 36, AIS 38).

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

To support composite evaluations according to AIS 36 the document ETR for composite evaluation [16] was provided and approved. This document provides details of this

platform evaluation that have to be considered in the course of a composite evaluation on top.

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

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

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0769-2012 [26], re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on

- the change of the Generic Applications in comparison to the base certification and
- the rating of the TOE's DRNG as DRG.4.

The evaluation has confirmed:

- PP Conformance: Protection profiles for secure signature creation device - Part 2: Device with key generation, Version 2.0.1, BSI-CC-PP-0059-2009-MA-01 [9]
- for the Functionality: PP conformant plus product specific extensions Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant EAL 4 augmented by AVA_VAN.5

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

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

## 9.2 Results of cryptographic assessment

The following cryptographic algorithms are used by STARCOS 3.5 ID ECC C1R to enforce its security policy:

| Algorithm | Bit Length | Purpose | Security Functionality | Standard of Implementation | Standard of Usage |
|---|---|---|---|---|---|
| EC Key Generation | 256, 320, 384, 512, 521 | EC Keys for signature creation | Cryptographic key generation – ECC<br><br>(FCS_CKM.1/ECC) | G&D standard | --- |
| RSA Key Generation | 2048-4096 | RSA key for signature creation | Cryptographic key generation – RSA<br><br>(FCS_CKM.1/RSA) | G&D standard | --- |
| ECDSA | 256, 320, 384, 512, 521 | ECC based signature creation | Cryptographic operation – Signature creation<br><br>(FSC_COP.1/ECC, FIA_API.1) | TR-03111 [18], [22], TR-03110 [20] | [9], [18], [22], [20] |

| Algorithm | Bit Length | Purpose | Security Functionality | Standard of Implementation | Standard of Usage |
|---|---|---|---|---|---|
| RSA | 2048-4096 | RSA based signature creation | Cryptographic operation – Signature creation<br><br>(FSC_COP.1/RSA, FIA_API.1) | PKCS #1 [19], TR-03110 [20] | [9], [19], [20] |
| SHA-2 | 224, 256, 384, 512 | Hash value calculation | Cryptographic operation – Signature creation<br><br>(FSC_COP.1/ECC, FCS_COP.1/RSA, FIA_API.1) | FIPS PUB 180-2 [23] | [9], [23] |
| ECDH | 224, 256, 320, 384, 512, 521 | Diffie-Hellman Keys for PACE, Terminal and Chip Authentication | Authentication including cryptographic key gener-ation – Diffie-Hellman for PACE, Terminal and Chip Authentication<br><br>(FIA_API.1) | TR-03110 [20] | [20] |
| AES | 128, 192, 256 | Symmetric Authentication<br><br>Secure Messaging | Symmetric Authentication<br><br>Secure Messaging with keys derived during PACE, Terminal and Chip Authentication resp. Symmetric Authentication<br><br>(FIA_API.1, FTP_ITC.1/SVD, FTP_ITC.1/Conf_VAD, TP_ITC.1/Conf_DTBS) | NIST 197 [21], EN 14890 [24] | [21], [24] |

Table 3: Cryptographic Algorithms used by the TOE

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 3, Clause 2).

According to [25] the algorithms which are related to the explicit signature creation are suitable for the calculation of hash values and the creation of digital signatures. The validity period of each algorithm is mentioned in the official catalogue [25].

According to [20] and [24] the algorithms which are related to PACE, to Terminal and Chip Authentication, to Symmetric Authentication as well as to Secure Messaging are suitable for authentication purposes and securing integrity, authenticity and confidentiality of data exchange and storage. For that reason an explicit validity period for these algorithms is not given.

# 10 Obligations and Notes for the Usage of the TOE

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

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

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

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

# 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

| | |
|---|---|
| **AES** | Advanced Encryption Standard |
| **APDU** | Application Protocol Data Unit |
| **AIS** | Application Notes and Interpretations of the Scheme |
| **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 |
| **CMAC** | Cipher-based Message Authentication Code |
| **DRNG** | Deterministic Random Number Generator |
| **DTBS** | Data To Be Signed |
| **EAL** | Evaluation Assurance Level |
| **EC** | Elliptic Curve |
| **ECC** | Elliptic Curve Cryptography |
| **ECDH** | Elliptic Curve Diffie-Hellman |
| **ECDSA** | Elliptic Curve Digital Signature Algorithm |
| **EEPROM** | Electrically Erasable Programmable Read-Only Memory |
| **ETR** | Evaluation Technical Report |
| **HID** | Human Interface Device |
| **IC** | Integrated Circuit |
| **IT** | Information Technology |
| **ITSEC** | Information Technology Security Evaluation Criteria |

| | |
|---|---|
| **ITSEF** | Information Technology Security Evaluation Facility |
| **NVM** | Non-Volatile Memory |
| **PACE** | Password Authenticated Connection Establishment |
| **PP** | Protection Profile |
| **RAD** | Reference Authentication Data |
| **RNG** | Random Number Generator |
| **ROM** | Read Only Memory |
| **SAR** | Security Assurance Requirement |
| **SCA** | Signature Creation Application |
| **SCD** | Signature Creation Data |
| **SFP** | Security Function Policy |
| **SFR** | Security Functional Requirement |
| **SSCD** | Secure Signature Creation Device |
| **SVD** | Signature Verification Data |
| **ST** | Security Target |
| **TOE** | Target of Evaluation |
| **TSF** | TOE Security Functionality |
| **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** - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

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

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

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

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

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

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

# 13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Revision 4, September 2012

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

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[8]

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

[6] Security Target BSI-DSZ-CC-0880, STARCOS 3.5 ID ECC C1R Security Target, Version 2.2, 21.03.2013, Giesecke & Devrient GmbH (confidential document)

[7] Security Target BSI-DSZ-CC-0880, STARCOS 3.5 ID ECC C1R Security Target Lite, Version 2.3, 21.03.2013, Giesecke & Devrient GmbH (sanitised public document)

[8] Evaluation Technical Report (ETR), Product: STARCOS 3.5 ID ECC C1R, Certification ID: BSI-DSZ-CC-0880, Version 1.2, Date: 27.03.2013, Evaluation Facility: SRC Security Research & Consulting GmbH (confidential document)

[9] Protection profiles for secure signature creation device – Part 2: Device with key generation, Version 2.0.1, January 2012, BSI-CC-PP-0059-2009-MA-01

[10] Guidance Documentation STARCOS 3.5 ID – Main Document, Version 0.6, 11.10.2011, Giesecke & Devrient GmbH

[11] Guidance Documentation for the Usage Phase STARCOS 3.5 ID ECC C1,Version 1.2, 27.06.2012, Giesecke & Devrient GmbH

[12] Guidance Documentation for the Initialization Phase STARCOS 3.5 ID EAC+AA C1, STARCOS 3.5 ID SAC+EAC+AA C1, STARCOS 3.5 ID ECC C1, Version 1.5, 15.06.2012, Giesecke & Devrient GmbH

[8] specifically

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

[13] Guidance Documentation for the Personalisation Phase STARCOS 3.5 ID ECC C1, Version 0.8, 15.06.2012, Giesecke & Devrient GmbH

[14] Generic Application Specifications for different TOE configurations of STARCOS 3.5 ID ECC C1R:

- STARCOS 3.5 ID ECC C1R Application Specification ESignK international, Version 0.16, 09.01.2013, Giesecke & Devrient GmbH
- STARCOS 3.5 ID ECC C1R Application Specification ESignK international 1PIN, Version 0.10, 09.01.2013, Giesecke & Devrient GmbH
- STARCOS 3.5 ID ECC C1R Application Specification ESignK national, Version 0.16, 09.01.2013, Giesecke & Devrient GmbH
- STARCOS 3.5 ID ECC C1R Application Specification ESignK national 1PIN, Version 0.10, 09.01.2013, Giesecke & Devrient GmbH
- STARCOS 3.5 ID ECC C1R Application Specification EACv2 international, Version 0.20, 09.01.2013, Giesecke & Devrient GmbH
- STARCOS 3.5 ID ECC C1R Application Specification EACv2 international 1PIN, Version 0.10, 09.01.2013, Giesecke & Devrient GmbH
- STARCOS 3.5 ID ECC C1R Application Specification EACv2 national, Version 0.20, 09.01.2013, Giesecke & Devrient GmbH
- STARCOS 3.5 ID ECC C1R Application Specification EACv2 national 1PIN, Version 0.10, 09.01.2013, Giesecke & Devrient GmbH
- STARCOS 3.5 ID ECC C1R Application Specification PACE international, Version 0.20, 09.01.2013, Giesecke & Devrient GmbH
- STARCOS 3.5 ID ECC C1R Application Specification PACE international 1PIN, Version 0.10, 09.01.2013, Giesecke & Devrient GmbH
- STARCOS 3.5 ID ECC C1R Application Specification PACE national, Version 0.20, 09.01.2013, Giesecke & Devrient GmbH
- STARCOS 3.5 ID ECC C1R Application Specification PACE national 1PIN, Version 0.10, 09.01.2013, Giesecke & Devrient GmbH

[15] Certification Report for BSI-DSZ-CC-0813-2012 for Infineon smart card IC (Security Controller) M7820 A11 with optional RSA2048/4096 v1.02.008, EC v1.02.008, SHA-2 v1.01 and Toolbox v1.02.008 libraries and with specific IC dedicated software from Infineon Technologies AG, 6 June 2012, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[16] ETR for composition according to AIS36, M7820 A11, BSI-DSZ-CC-0813, Version 1, 1 June 2012, TÜViT 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] Technical Guideline TR-03111: Elliptic Curve Cryptography, Version 1.11, 17.04.2009, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[19] PKCS #1 v2.1: RSA Cryptographic Standard, 14.6.2002

[20] Technical Guideline TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), Version 2.05, 14.10.2010, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[21] NIST Specification for the Advanced Encryption Standard (AES), FIPS PUB 197, 2001

[22] Standards for efficient cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters, Certicom Research, September 20, 2000, Version 1. http://www.secg.org/collateral/sec2_final.pdf

[23] NIST. Secure hash standard (and Change Notice to include SHA-224), FIPS PUB 180-2, 2002

[24] EUROPEAN STANDARD, EN 14890-1:2008, Application Interface for smart cards used as secure signature creation devices – Part 1: Basic services (EN 14890-1)

[25] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), 30 December 2011, published in Bundesanzeiger no. 10, pp. 243 following on 18 January 2012

[26] Certification Report for BSI-DSZ-CC-0769-2012 for STARCOS 3.5 ID ECC C1 from Giesecke & Devrient GmbH, 31 August 2012, Bundesamt für Sicherheit in der Informationstechnik (BSI)

This page is intentionally left blank.

# C Excerpts from the Criteria

CC Part1:

### Conformance Claim chapter 10.4

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

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

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

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

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

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

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

CC Part 3:

**Class APE: Protection Profile evaluation** (chapter 10)

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

| Assurance Class | Assurance Components |
|---|---|
| Class APE: Protection Profile evaluation | APE_INT.1 PP introduction |
| | APE_CCL.1 Conformance claims |
| | APE_SPD.1 Security problem definition |
| | APE_OBJ.1 Security objectives for the operational environment<br>APE_OBJ.2 Security objectives |
| | APE_ECD.1 Extended components definition |
| | APE_REQ.1 Stated security requirements<br>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<br>ASE_OBJ.2 Security objectives |
| | ASE_ECD.1 Extended components definition |
| | ASE_REQ.1 Stated security requirements<br>ASE_REQ.2 Derived security requirements |
| | ASE_TSS.1 TOE summary specification<br>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<br>ADV_FSP.2 Security-enforcing functional specification<br>ADV_FSP.3 Functional specification with complete summary<br>ADV_FSP.4 Complete functional specification<br>ADV_FSP.5 Complete semi-formal functional specification with additional error information<br>ADV_FSP.6 Complete semi-formal functional specification with additional formal specification |
| | ADV_IMP.1 Implementation representation of the TSF<br>ADV_IMP.2 Implementation of the TSF |
| | ADV_INT.1 Well-structured subset of TSF internals<br>ADV_INT.2 Well-structured internals<br>ADV_INT.3 Minimally complex internals |
| | ADV_SPM.1 Formal TOE security policy model |
| | ADV_TDS.1 Basic design<br>ADV_TDS.2 Architectural design<br>ADV_TDS.3 Basic modular design<br>ADV_TDS.4 Semiformal modular design<br>ADV_TDS.5 Complete semiformal modular design<br>ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation |

| Assurance Class | Assurance Components |
|---|---|
| AGD:<br>Guidance documents | AGD_OPE.1 Operational user guidance |
| | AGD_PRE.1 Preparative procedures |
| ALC: Life cycle support | ALC_CMC.1 Labelling of the TOE<br>ALC_CMC.2 Use of a CM system<br>ALC_CMC.3 Authorisation controls<br>ALC_CMC.4 Production support, acceptance procedures and automation<br>ALC_CMC.5 Advanced support |
| | ALC_CMS.1 TOE CM coverage<br>ALC_CMS.2 Parts of the TOE CM coverage<br>ALC_CMS.3 Implementation representation CM coverage<br>ALC_CMS.4 Problem tracking CM coverage<br>ALC_CMS.5 Development tools CM coverage |
| | ALC_DEL.1 Delivery procedures |
| | ALC_DVS.1 Identification of security measures<br>ALC_DVS.2 Sufficiency of security measures |
| | ALC_FLR.1 Basic flaw remediation<br>ALC_FLR.2 Flaw reporting procedures<br>ALC_FLR.3 Systematic flaw remediation |
| | ALC_LCD.1 Developer defined life-cycle model<br>ALC_LCD.2 Measurable life-cycle model |
| | ALC_TAT.1 Well-defined development tools<br>ALC_TAT.2 Compliance with implementation standards<br>ALC_TAT.3 Compliance with implementation standards - all parts |
| ATE: Tests | ATE_COV.1 Evidence of coverage<br>ATE_COV.2 Analysis of coverage<br>ATE_COV.3 Rigorous analysis of coverage |
| | ATE_DPT.1 Testing: basic design<br>ATE_DPT.2 Testing: security enforcing modules<br>ATE_DPT.3 Testing: modular design<br>ATE_DPT.4 Testing: implementation representation |
| | ATE_FUN.1 Functional testing<br>ATE_FUN.2 Ordered functional testing |
| | ATE_IND.1 Independent testing – conformance<br>ATE_IND.2 Independent testing – sample<br>ATE_IND.3 Independent testing – complete |
| AVA: Vulnerability assessment | AVA_VAN.1 Vulnerability survey<br>AVA_VAN.2 Vulnerability analysis<br>AVA_VAN.3 Focused vulnerability analysis<br>AVA_VAN.4 Methodical vulnerability analysis<br>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-0880-2013

## Evaluation results regarding development and production environment

The IT product STARCOS 3.5 ID ECC C1R (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 19 April 2013, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.1, ALC_LCD.1, ALC_TAT.1)

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

- Giesecke & Devrient GmbH, Development Centre Germany, Zamdorferstrasse 88, 81677 Munich, Germany, Site Certificate BSI-DSZ-CC-S-0009-2012 (development).
- Smartrac Technology, 142 Moo, Hi-Tech Industrial Estate Tambon Ban Laean, Amphor Bang-Pa-In, 13160 Ayutthaya, Thailand, Site Certificate BSI-DSZ-CC-S-0007-2011 (inlay embedding).
- Smartrac Technology Germany GmbH, Gewerbeparkstr. 10, 51580 Reichshof-Wehnrath, Germany, Site Certificate BSI-DSZ-CC-S-0008-2011 (inlay embedding).
- HID Global Ireland Teoranta, Pairc Tionscail na Tulaigh, Baile na hAbhann, Co. Galway, Ireland, Site Certificate BSI-DSZ-CC-S-0015-2012 (inlay embedding).
- Giesecke & Devrient Slovakia, s.r.o., Dolné Hony 11, 949 01 Nitra, Slovakia, Site Certificate BSI-DSZ-CC-S-0012-2012 (inlay embedding, initialisation and card production).
- Giesecke & Devrient GmbH, G&D Dienstleistungscenter, Prinzregentenstraße 159, 81677 Munich, Germany, Site Certificate BSI-DSZ-CC-S-0010-2012 (initialisation and card production).
- For development and productions sites regarding the smart card IC (Security Controller) M7820 A11 from Infineon Technologies AG refer to the certification report BSI-DSZ-CC-0813-2012 [15].

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6] and [7]. 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.