debis
Services by DaimlerChrysler

Certification Report

STARCOS SPK2.3 with Digital Signature Application StarCert

Giesecke & Devrient GmbH

debisZERT-DSZ-ITSEC-04020-2001

debis Systemhaus Information Security Services GmbH

The Modern Service Provider

Preface

The product STARCOS SPK2.3 with Digital Signature Application StarCert of Giesecke & Devrient GmbH has been evaluated against the *Information Technology Security Evaluation Criteria* and the *Information Technology Security Evaluation Manual*. The evaluation has been performed under the terms of the certification scheme debisZERT of debis Systemhaus Information Security Services GmbH. The certification procedure applied conforms to the rules of service type 4: *Certificates recognised by the BSI*.

The result is:

Security Functionality:	**Identification and Authentication** (authentication of human user; changing, blocking, unblocking and changing the reference data) **Access Control** (commands; extraction; blocking state) **Audit** (secure blocking state; blocked CH authentication) **Object Reuse** **Data Exchange** (key generation and export; digital signature generation)
Assurance Level:	E4
Strength of Mechanisms:	High

This is to certify that the evaluation has been performed compliant to the scheme debisZERT.

Bonn, 21.03.2001

Certifier: Klaus-Werner Schröder

Head of the Certification Body: Dr. Heinrich Kersten

For further information and copies of this report, please contact the certification body:
debis Systemhaus Information Security Services GmbH, - Zertifizierungsstelle -
Rabinstr. 8, D-53111 Bonn, Germany
+49-228-9841-0, Fax: +49-228-9841-60
Internet: www.debiszert.de

Revision List

The following revision list shows the history of this certification report.

Information on re-certifications due to product modifications are given in chapter 7.

Revision	Date	Activity
0.9	14.03.2001	Preversion (based on template report 1.5)
1.0	21.03.2001	Initial release (based on template report 1.5)

Contents

1 Introduction

1.1 Evaluation

1 The evaluation was sponsored by Giesecke & Devrient GmbH, Prinzregentenstraße 159, 81607 München.

2 The evaluation was carried out by the evaluation facility Prüfstelle IT-Sicherheit der and completed on 20.03.2001.

3 The evaluation has been performed against the *Information Technology Security Evaluation Criteria* and the *Information Technology Security Evaluation Manual*. Some explanations concerning the contents of ITSEC and ITSEM can be found in chapter 5.

1.2 Certification

4 The certification was performed under the terms of the certification scheme debisZERT of debis Systemhaus Information Security Services GmbH. The Certification Body of debis Systemhaus Information Security Services GmbH complies to EN 45011 and was accredited with respect to this standard by the Deutsche Akkreditierungsstelle Technik e.V. (DATech) under DAR Registration Number DIT-ZE-005/98-10.

5 The Certification Body applied the certification procedure as specified in the following documents:

- /Z01/ Certification Scheme
- /V04/ Certificates recognised by the BSI

1.3 Certification Report

6 The certification report states the outcome of the evaluation of STARCOS SPK2.3 with Digital Signature Application StarCert - referenced as TOE = Target of Evaluation in this report.

7 The certification report is only valid for the specified version(s) of the TOE. It can be extended to new or different versions as soon as a successful re-evaluation has been performed.

8 The consecutively numbered paragraphs in this certification report are formal statements from the Certification Body. Unnumbered paragraphs contain statements of the sponsor (security target) or supplementary material.

9 The certification report is intended

- as a formal confirmation for the sponsor concerning the performed evaluation,

- to assist the user of STARCOS SPK2.3 with Digital Signature Application StarCert when establishing an adequate security level.

10 The certification report contains pages 1 to 102. Copies of the certification report can be obtained from the sponsor or the Certification Body.

11 The certification report can be supplemented by statements of successful re-certification and by annexes on special technical problems. Such statements and annexes will be published under

- www.debiszert.de.

1.4 Certificate

12 A survey on the outcome of the evaluation is given by the security certificate debisZERT- DSZ-ITSEC-04020-2001.

13 The certificate is published under

- www.debiszert.de.

14 The certificate is formally recognised by the Bundesamt für Sicherheit in der Informationstechnik (BSI) that confirms the equivalence of this certificate to its own certificates in the international context.

15 The rating of the strength of cryptographic mechanisms appropriate for encryption and decryption is not part of the recognition by the BSI.[1]

16 The certificate carries the logo officially authorised by the BSI. The fact of certification will be listed in the brochure BSI 7148.

1.5 Application of Results

17 The processes of evaluation and certification are performed with state-of-the-art expertise, but cannot give an absolute guarantee that the certified object is free of vulnerabilities. With increasing evaluation level however, the probability of undiscovered exploitable vulnerabilities decreases.

18 It is highly recommended to read the certification report carefully to benefit from the evaluation. In particular, the information provided on the intended method of use, the assumed threats, the operational environment and the evaluated configurations are essential for the user.

19 The results of the evaluation are only valid under the assumption that all requirements specified in the certification report are met by the user.

---

1 Due to legal requirements in /BSIG/ BSI must not give ratings to certain cryptographic algorithms or recognise ratings by other certification bodies.

Otherwise, the results of the evaluation are not fully applicable. In this case, there is a need of an additional analysis whether and to which degree the certified object can still offer security under the modified assumptions. The evaluation facility and the Certification Body can give support to perform this analysis.

(This page is intentionally left blank.)

2 Evaluation Findings

2.1 Introduction

20 The outcome of the evaluation is represented by the ETR (Evaluation Technical Report). The evaluation was performed against the security target specified in chapter 3.

2.2 Evaluation Results

21 The evaluation facility came to the following conclusion:

- The TOE meets the requirements of the assurance level E4 according to ITSEC, i.e. all requirements at this assurance level as to correctness and effectiveness are met:

  ITSEC E4.1 to E4.37 for the correctness phases

  Construction - The Development Process (Requirements, Architectural Design, Detailed Design, Implementation),

  Construction - The Development Environment (Configuration Control, Programming Languages and Compiler, Developers Security),

  Operation - The Operational Documentation (User Documentation, Administration Documentation)

  Operation - The Operational Environment (Delivery and Configuration, Start-up and Operation).

  ITSEC 3.12 to 3.37 for the effectiveness with the aspects

  Effectiveness Criteria - Construction (Suitability of Functionality, Binding of Functionality, Strength of Mechanism, Construction Vulnerability Assessment),

  Effectiveness Criteria - Operation (Ease of Use, Operational Vulnerability Assessment).

- The mechanisms of the TOE under the generic heading(s) Identification and Authentication, Data Exchange are critical mechanisms; they are of type A. The mechanisms of the TOE under the generic heading(s) Access Control, Audit, Object Reuse are critical mechanisms; they are of type B.

The mechanisms of type A have a minimal strength of mechanism given by the level High.

For mechanisms of type B no rating of strength is specified in accordance with ITSEM. But even if an attack potential according to level „High“ is considered in the vulnerability assessment phase, no exploitable vulnerability was detected in the assumed environment (cf. chapter 3, Security Target).

2.3 Further Remarks

22 The evaluation facility has formulated **the following requirements** to the **sponsor**:

- It is not allowed to deviate from the procedures of completion, initialization and personalization relevant to “Specification Card Life Cycle for Starcos SPK 2.3 with Signature Application”, Version 1.5.3, 24.01.2001, Giesecke & Devrient GmbH and the “Dokumentation für das Trustcenter Evaluierung SPK 2.3”, Version 1.6.4, 24.01.2001, Giesecke & Devrient GmbH. These procedures exclude mistakes by use and have to be components of the security concept of the Trustcenter.

- The cryptographic mechanisms which are suitable for the use in digital signatures conformable to the SigG are published in accordance with “Verordnung zur digitalen Signatur (Signaturverordnung - SigV) in der Fassung des Beschlusses der Bundesregierung vom 8. Oktober 1997”, § 17 (2) in the Bundesanzeiger (Federal Gazette). Based on the most recent official announcement “Bekanntmachung zur digitalen Signatur nach dem Signaturgesetz und der Signaturverordnung vom 09.02.98, Geeignete Kryptoalgorithmen gemäß § 17 (2) SigV, Bundesanzeiger Nr. 230 – Seite 22.946 v. 07. Dezember 2000” the algorithms implemented in the TOE are suitable until the end of the year 2005 (the hash algorithm SHA-1) and until the middle of the year 2005 (RSA-Algorithm).

- The results of the evaluation of suitability analysis relevant to the security objectives SO6 “Quality of key generation” and SO7 “Provide secure digital signature” only are valid until the middle of 2005 and then have to be checked again.

23 The evaluation facility has formulated **the following requirements** to the **user**:

- The TOE implements the hash function SHA-1 for calculation of hash values for data provided by the terminal together or without intermediate hash values and calculates digital signature for hash values of the hash functions SHA-1 and RIPEMD-160. The cardholder **must not use** the hash function MD5 because it was classified as well as non conformable to the SigG and as insecure.

- The specification of the SigG application in “STARCOS SPK2.3 und DINSIG_SPK Feinentwurf”, Version 1.5.1, Stand 06.11.2000, Giesecke & Devrient GmbH describes in the sections 2, 4.3.4, 4.6, 4.8 and 8 the usage of the TOE with public terminals relevant to “Bekanntmachung zur digitalen Signatur nach dem Signaturgesetz und der Signaturverordnung vom 09.02.98, Geeignete Kryptoalgorithmen gemäß § 17 (2) SigV, Bundesanzeiger Nr. 230 – Seite 22.946 v. 07. Dezember 2000“. The usage of the TOE with public terminals is not allowed according to the security target (cf. chapter 3 of this report). The limitation on private terminals is described in the user documentation for the cardholder “Benutzerdokumentation für den Kartenhalter Evaluierung SPK 2.3”, Version 1.3.6, 15.03.2001, Giesecke & Devrient GmbH (User Manual for Cardholder (with card administration aspects)).

- The cardholder shall be aware that in cases when device authentication is used the device authentication shall take place prior to any cardholder authentication acts. Successful device authentication is made apparent to the cardholder by displaying the user specific display message. Details are given in the user documentation.

24 The evaluation facility has formulated **the following requirements** to a **third party** (vendors of SigG compliant terminals):

- Vendors of SigG compliant terminals shall implement device authentication in such a way that device authentication takes place immediately after starting the communication with the ICC and only once within the session.

(This page is intentionally left blank.)

3 Security Target

25 The Security Target, version 2.7 dated 14.03.2001, supplied by the sponsor for the evaluation was written in English language.

26 The change history of the document "Security Target" is not relevant in this context but might lead the reader to misconception. The change history in section 3.1.1 of the Security Target is, therefore, omitted.

3.1 Preface

This document represents the Security Target for the Smart-Card's operating system STARCOS SPK2.3 and the digital signature application for it StarCert (in short: "SigG application").

This Security Target is based on the Generic Security Target for ICC embedded Software compliant with SigG, SigV and DIN, TeleTrusT Deutschland e.V., Version 0.98 [GST_098].

Note: The enumeration of most of the objects taken from [GST_098] has not been changed and thus sometimes those objects are not numbered consecutively.

3.1.1 Change History

(omitted)[2]

3.1.2 Sections Overview

Section 3.2 describes the product rationale, assumptions about the environment, assumed threats and security features.

Section 3.3 describes the security enforcing functions (informal and semiformal).

Section 3.4 describes the underlying security policy.

Section 3.5 describes the security mechanisms.

Section 3.6 discusses the suitability of the TOE's security features.

In section 3.7 the evaluation target is stated.

Sections 3.8, 3.9 and 3.10 contain abbreviations, glossary and references, respectively.

2 See para 26

3.2 Product Rationale

3.2.1 Product Overview

STARCOS is a complete operation system for integrated circuit cards (ICC). As the ICC operation system, STARCOS controls the data-exchange and the memory areas as well as processes the information in the ICC. As the resource-manager, STARCOS provides the necessary functions for operation and management of any application. STARCOS is used for security applications, e.g. for payment systems, road toll systems or access control systems. STARCOS SPK is an extension to the standard version STARCOS adding asymmetric cryptography (public key cryptography) capabilities to STARCOS. This evaluation focuses on STARCOS SPK2.3 (version 2.3 of STARCOS SPK), which is based on the standard ICC operating system STARCOS S2.1 (version 2.1 of STARCOS). STARCOS SPK2.3 is a further development of STARCOS S2.1 that comprises all functionality of STARCOS S2.1 and adds public key cryptography functionality.

STARCOS SPK2.3 not only implements the symmetric cryptoalgorithm DEA (Data Encryption Algorithm, as defined in DES) as well as Triple-DES, but also the asymmetric cryptoalgorithms RSA and DSA. These algorithms can be used to generate digital signatures as well as to encrypt and decrypt data (PERFORM SECURITY OPERATION: ENCIPHER / DECIPHER according to ISO/IEC 7816-8). The encipher/decipher functionalities do not represent any security relevant functionality. The TOE supports padding according to PKCS 1.0 Vers.1.5 and ISO/IEC 9796-2. In addition, STARCOS SPK2.3 supports mutual device authentication and secure messaging as defined in ISO/IEC 7816-4. The SigG-accredited IFDs using these functionalities are excluded from the evaluation.

STARCOS SPK2.3 together with the digital signature application StarCert (SigG signature application or in short: SigG application) make it possible to generate and to verify digital signatures as defined by the German Signature Law (SigG) and in compliance with SigG, SigV and [DIN].

The ICC may be used as multi-application smart card. In this case other applications may be loaded on the ICC in the operational usage phase. Other applications must not contain any executable code. The TOE prevents the loading of executable data onto the ICC.

3.2.2 Identification of TOE

The ICC contains

(1) the target of the evaluation (TOE) and

(2) the other application's data.

The TOE consists of

(1) all software residing on the card (executable), and

(2) all (non executable) data used for the SigG application on the ICC.

The TOE provides functions

(1) to create the SigG application (including the data being specific for the cardholder during the first personalisation) within the card during the first personalisation,

(2) to generate SigG signing key pairs on the ICC,

(3) to generate digital signatures, and

(4) to provide security for the digital signature generation.

Other parts of the TOE software are needed

(1) to use the SigG application with additional functions (including signature verification),

(2) to provide specific functions for non-SigG applications which may also reside on the card and are different from SigG application, and

(3) to provide other ICC functions which are not specific for the applications.

The data of the non-SigG applications (i) are stored in directories and files of the ICC, (ii) are not executed as code by the TOE, and (iii) are not subject of the evaluation.

Out of all cryptoalgorithms implemented in STARCOS SPK2.3, the SigG application only uses the RSA algorithm and the SHA-1 hash algorithm. DSA is not used by the SigG application.

The TOE is running on the chip "Philips P8WE5032V0G".

The ICC's hardware is not part of the TOE.

There are the following configuration options during the generation of the TOE, which lead to different **configurations** of the TOE:

- **Transmission protocol (T=0 or T=1).**
  The only difference between these two versions are the transmission protocols:
  The TOE supports only the T=1 protocol or
  The TOE supports both the T=0 and T=1 protocols.
  In the latter case (2), the protocol to be used for communication is negotiated between the IFD and the ICC at the beginning of a session and is kept during the rest of the session.

- **Maximum number of signature key pairs.**
  The maximum number *m* of signature key pairs of the cardholder, that can be stored on the TOE, is limited to a fixed number. *m* can be any value between 1 (only

one cardholder signature key pair) and 10 (a maximum of 10 signature key pairs can be generated and stored on the TOE): $1 \le m \le 10$.

Except for the fact that the number of signature key pairs can be different, this number *m* does not have any influence on any other part of the TOE. There are especially no security-relevant differences between a configuration of the TOE with m_1 signature key pairs and a configuration of the TOE with m_2 signature key pairs ($1 \le m_1 < m_2 \le 10$), since the access rights are defined equal for all signature key pairs, independent of the actual value of *m*.

- **Limitation of the number of signatures that can be generated after successful cardholder authentication.**
  The number of digital signatures that can be generated after successful cardholder authentication is either (i) limited to one or (ii) not limited by the TOE itself. The first case (i) will be called **"*limited signature generation configuration*"**, the latter case (ii) will be called **"*unlimited signature generation configuration*"** in the following. The *unlimited signature generation configuration* is used only in a specially secured environment (e.g. usage within a Trust Center) and requires an additional assumption about the environment (see (AE4.2)-(2)).

Considering all combinations of the items listed above, there are 2*10*2 = 40 possible configurations. Since the maximum number of signature key pairs does not affect any security-relevant functionality, there remain 2*2 = 4 different configurations that have to be considered. The Operating System (STARCOS SPK2.3) is constant for all configurations of the TOE (see No. 1 in the following Table 1). The TOE then also comprises one out of two Completion Files, providing support either for only the T=1 protocol or for both the T=0 and T=1 protocols (see No. 2a and 2b). Finally, one out of two Command Sequences (see No. 3a and 3b) are needed that determine whether the actual TOE is a User Version or a TrustCenter Version of the TOE (limited signature generation configuration vs. unlimited signature generation configuration).

The configuration of the TOE is determined during its generation and cannot be changed afterwards (after delivery of the TOE to the trust center).

The following Table 1 lists in detail the components of the TOE:

Table 1: Components of the TOE

No.	Type	Term	Version	Date	Form of delivery
1	Software	STARCOS (Operating System)	SPK2.3	04.05.1999	Loaded into ROM mask
2a	Software	Completion File for T=1 protocol: CP5WxSPKI23-3-0v60.HEX	6.0	29.01.2001	Hex file to be loaded into EEPROM during card completion

No.	Type	Term	Version	Date	Form of delivery
2b	Software	Completion File for T=0/T=1 protocols: CP5WxSPKI23-1-0v60.HEX	6.0	29.01.2001	Hex file to be loaded into EEPROM during card completion
3a	Software	StarCert (SigG application for SPK2.3), User version: Spk23-SigG-User_v161.dat	1.6.1	21.12.2000	Command Sequence to be applied during card initialization, which loads the file system into the EEPROM
3b	Software	StarCert (SigG application for SPK2.3), TrustCenter version: Spk23-SigG-TC_v191.dat	1.9.1	21.12.2000	Command Sequence to be applied during card initialization, which loads the file system into the EEPROM
4	Documentation	User Manual for Cardholder (with card administration aspects), BdCh_spk23 v136.doc	1.3.6	15.03.2001	Paper form
5	Documentation	User Manual for Terminal Developer, BdTe_spk23 v134.doc	1.3.4	07.03.2001	Paper form
6	Documentation	Documentation for Trustcenters, DTc_spk23 v164.doc	1.6.4	24.01.2001	Paper form
7	Documentation	STARCOS SPK2.3 with Digital Signature Application StarCert - Delivery, Generation and Configuration, AGK_spk23 v130.doc	1.3.0	01.02.2001	Paper form

No.	Type	Term	Version	Date	Form of delivery
8	Documentation	Reference Manual Smart Card Operating System STARCOS® S 2.1 ID No. 186466041	Edition Dec. '99	December '99	Paper form
9	Documentation	Reference Manual Smart Card Operating System STARCOS® SPK 2.3 Supplement to the STARCOS® S 2.1 Reference Manual Edition 08/00 ID No. Z188999061	Edition Aug. '2000	22.08.00	Paper form
10	Documentation	Specification Signature Application for STARCOS SPK2.3, SpecApplication-184.doc	1.8.4	24.01.2001	Paper form
11	Documentation	Specification Card Life Cycle of STARCOS SPK2.3 with Digital Signature Application StarCert, SpecCardLifeCycle-153.doc	1.5.3	24.01.2001	Paper form

The TOE communicates with the outside world over the ICC's standardised interface (see [DIN] NI-17.4, sect. 4 "Technical characteristics").

The TOE is a **product**.

3.2.3 Intended method of use

The TOE is intended to provide the digital signature function to the legitimate cardholder acting as owner of the individual ICC equipped with the SigG signature key of the cardholder in accordance with the SigG legislative [SigG], [SigV] and the standard [DIN]. The cardholder is the only subject that is intended to use the TOE for generating signatures.

The TOE is used to generate all cardholder's SigG signing key pair(s) (SK_i.CH.DS, PK_i.CH.DS) on the ICC. Different scenarios of key generation are supported.

3.2.3.1 Card Life Cycle

The development and manufacturing of the ICC's software and hardware leads to the ICC being ready to be used for a specific purpose (application). The ICC will be loaded with the SigG application including data specific to the cardholder in the initialisation and first personalisation phases of the ICC. The TOE implements features to ensure secure initialisation, personalisation (first personalisation and repersonalisation) and operational usage phase of the ICC.

The TOE can contain more than one SigG signing key pair for the cardholder. An additional SigG signing key pair can be generated in the repersonalisation phase (see sec. 3.2.3.6).

The cardholder can use different SigG signing key pairs to perform digital signatures for different purposes.

Thus the life cycle consists of the following phases (in chronological order):

- Production
- Test
- Completion
- Initialisation
- First Personalisation
- Operational Phase
- Zero or more Repersonalisation Phases for additional SigG signature key pairs (the TOE remains in its operational phase for all SigG signature key pairs which are already operational)
- Recycling / TERMINATE CARD USAGE

There can be multiple repersonalisation phases (one for each additional SigG signature key pair). The maximum number of repersonalisation phases is a fixed property of the TOE (see the number *m* in section 3.2.2).

3.2.3.2 Initialisation phase

In the initialisation phase the file system and structures are created. All card-related data (not cardholder-related data) are established, including a unique ICC serial number (ICCSN). The signature application is established, but does not already contain all objects, especially the personalisation data of the cardholder. For all keys the key headers are set up. A device authentication key pair (SK.ICC.AUT, PK.ICC.AUT) together with a certificate C.ICC.AUT of the card manufacturer is generated. A SigG signing key pair may or may not be generated in the initialisation phase.

At the end of the initialisation phase there is an unequivocal, verifiable relation between these data and the ICC.

3.2.3.3 First Personalisation Phase

During the first personalisation phase, a cardholder (CH) is being assigned to the ICC and the ICC is being loaded with cardholder-specific data. A SigG signature key pair may or may not be generated in this phase. If no key pair has been generated in the initialization phase, it will be generated in this first personalisation phase. At the end of the first personalisation phase at least one SigG signature key pair will have been generated and be available on the TOE.

The TOE may be used in different scenarios, that differ in the way a signature key certificate (X.509v3) is created and in the fact whether such a certificate is created before the TOE is delivered to the cardholder. When a SigG signature key pair has been generated, then it is unequivocally assigned to the cardholder. To support this, the TOE provides a way to store the registration number (assigned to the CH by the CA) in a key header.

3.2.3.4 Operational Phase

In the operational usage phase of the ICC, the TOE is used by the cardholder by providing it to some IT system containing the message for which the cardholder wishes to apply a digital signature. The TOE and the IT system communicate through the interface device (IFD). The IFD is the human interface to the ICC.

In order to use the SigG signature generation, the cardholder has to authenticate himself to the TOE. The IFD presents the verification data of the cardholder to the TOE. Depending on its configuration (see section 3.2.2), after a successful authentication, the TOE allows (i) to generate **only one digital signature** (in limited signature generation configuration) **or** (ii) to generate **an unlimited number of digital signatures within the current session** (in unlimited signature generation configuration; see also section 3.2.6.2 and [DIN], section 8).

The TOE is equipped with a **transport PIN** that secures the TOE during its delivery to the cardholder. The transport PIN has a length of 5 digits. During his first authentication, the cardholder has to change the PIN to a PIN with a length of at least 6 digits; otherwise the authentication will fail. This ensures that before the TOE can be used to generate signatures, the transport PIN has to be changed. Whenever the PIN is changed in the future, the PIN also has to be at least 6 digits long. By successfully entering his transport PIN while changing the PIN to a PIN with at least 6 digits, the cardholder thus can check that nobody has authenticated before with the transport PIN. In this case he can also be sure that nobody has used the TOE before to generate a digital signature.

The TOE supports **three ways of hashing** the message to be signed: The IT system (i) transforms the message text into the hash-value and transmits the hash-value to the TOE, (ii) calculates an intermediate hash-value of the message text and transmits the remaining message text and the intermediate hash-value to the TOE, or (iii) transmits the complete message text to be hashed to the TOE (see [DIN], section 14.2.1 and annex A). The cardholder is free to choose either of these three ways.

The TOE calculates the digital signature of the hash-value with a SigG signature key of the cardholder (SK_i.CH.DS) stored in the TOE. The TOE returns the digital signature to the IFD. The SigG signature key(s) of the cardholder never leaves the TOE.

3.2.3.5 Office IFDs and Public IFDs

In this context we distinguish between an "**office IFD**" and a "**public IFD**". They differ in environmental usage: An **office IFD** is located in a certain well-known environment, whereas a **public IFD** is located in an unknown environment. The difference between **office IFD** and **public IFD** is not visible to the TOE, it is only known to the cardholder (CH). The cardholder is assumed to always know, whether he is using the TOE in an **office IFD** or in a **public IFD**.

The **SigG application** must be used **with Office IFDs only**. During a repersonalisation phase the TOE may be used at an IFD within a CA/RA.[3] This IFD is not an **office IFD**; the security function will be provided by the secure environment of the CA/RA in this case. – Since the ICC can contain other applications as well (see section 3.2.1), the ICC may also be used with Public IFDs. Since the difference of **office IFD** and **public IFD** is not visible to the TOE, the TOE cannot prevent the use of the SigG application with Public IFDs; the cardholder is responsible for not using the SigG application with Public IFDs.

3.2.3.6 Repersonalisation

Since the TOE supports the storage of multiple SigG signing keys, for each SigG signing key the TOE can be in either one of the three states: (i) SigG signing <u>key pair does not exist</u>: the SigG signing key pair has not been generated, (ii) (re)<u>personalisation phase</u>: the SigG signing key pair has already been generated[4], but the corresponding certificate has not been loaded onto the ICC yet, or (iii) <u>operational phase</u>: SigG signing key pair is operational. A **SigG signing key pair is defined as being operational**, if (i) the SigG signing key pair has been generated successfully and (ii) the certificate of the generated SigG signing key pair's public key has been loaded onto the ICC.

Note: After a SigG signature key pair has been generated, the TOE does not prevent the cardholder from generating signatures with the newly **generated** (but not yet "operational") SigG signature private key (the **TOE does not distinguish between generated and operational key pairs**). But until the certificate over the newly generated SigG signature public key is loaded onto the TOE (or made available through

---

3 The generation of an additional SigG signing key pair may take place at the cardholder's office IFD or at a CA/RA– several options shall be practicable (see section 3.2.3.6).

4 SigG signature key generation requires a preceding authentication of the cardholder by PIN O3.

a directory service), nobody can verify those signatures, so they should not be regarded as SigG compliant signatures.

The generation of an additional SigG signing key pair may take place at the cardholder's office IFD or at a CA/RA – both options shall be practicable whereby the key- header and key record (dummy keys) are always generated by the card manufacturer (CM).before. Only the key body (precisely only the secret and public key) may be generated by another entity. The Signature certificate over the newly generated public key is always produced within the CA/RA, regardless of what IFD has been used for the generation of the additional SigG signing key pair. The public key of a newly generated key pair may be read signed with the SK.ICC.AUT in charge of the card together with the device authentication certificate out of the card and the signature key certificate may be stored on the TOE when the TOE is either inserted into the cardholder's office IFD or into an IFD with Authentication module within the CA/RA. The following three cases shall be possible:

1. An additional SigG signature key pair is being generated while the TOE is inserted into the cardholder's office IFD. The newly generated public key is read out while the ICC is inserted into the cardholder's office IFD and sent electronically to the CA/RA. The CA/RA produces the signature key certificate over this public key and sends it back to the cardholder. The signature key certificate is loaded onto the TOE.

2. An additional SigG signature key pair is being generated while the TOE is inserted into the cardholder's office IFD. The cardholder goes to the CA/RA and inserts his ICC (the TOE) into an IFD at the CA/RA. The CA/RA reads out the public key (that has already been generated at the cardholder's office IFD), produces the signature key certificate over this public key and writes the signature key certificate into the TOE.

3. An additional SigG signature key pair is being generated while the TOE is inserted into an IFD at the CA/RA. The cardholder himself has to enter his PIN O3 to authenticate for SigG signature key generation The CA/RA reads out the public key, produces the signature key certificate over this public key and writes the signature key certificate into the TOE.

The generation of a further cardholder's SigG signing key pair can take place **exclusively in a repersonalisation phase**. The first SigG signing key pair (SK_1.CH.DS, PK_1.CH.DS) is generated in the first personalisation phase (i) by a CA/RA before the delivery of the TOE to the cardholder or (ii) by the cardholder himself after delivery. After delivery of the TOE to the cardholder, within the Sig. Application the only keys, that can be generated, are SigG signature key pairs within the Sig. Application.

If an additional SigG signing key pair (SK_i.CH.DS, PK_i.CH.DS) ($1<i\leq m$, $m \leq 10$ - the maximum number of SigG signing key pairs that can be stored in the TOE, see section 3.2.2) is generated during the operational usage phase of the TOE, the repersonalisation phase for this new SigG signing key pair begins. The new SigG signing key pair is then added to the TOE and the SigG signing key pair(s) already existing on

the TOE continue(s) to exist. The TOE remains in the repersonalisation phase for the new SigG signing key pair until the CA/RA has generated the signature key certificate over the new public SigG signing key of the cardholder. Regarding the existing SigG signing key pair(s) the TOE remains in the operational usage phase. Each additional SigG signing key pair (SK_i.CH.DS, PK_i.CH.DS) ($1<i\leq m$) can be generated at most once (i.e. it can be generated once or it may never be generated). The SigG signing key pairs (including the first SigG signing key pair (SK_1.CH.DS, PK_1.CH.DS)) can never be overwritten. An additional signing key pair can be generated either by the CA/RA or by the cardholder itself.

The security requirements arise from the operational usage of the TOE. This also leads to requirements on the TOE's functionality "Generation of a SigG signing key pair", which has an essential effect on the secure operation of the TOE in the operational usage phase. The generation of a SigG signing key pair takes place in a personalisation (first personalisation for the first SigG signature key pair, repersonalisation for additional SigG signature key pairs) phase only. The first personalisation phase is regarded as being a system generation, i.e. as being part of the delivery and configuration (see [ITSEC], E4.32-E4.34, 6.16, 6.24).

3.2.3.7 Termination phase

The TOE supports a command TERMINATE CARD USAGE that can be used by Somebody (S2) to terminate the card (the card enters a permanent blocking state).

3.2.4 Assumptions about the environment

Some assumptions about conditions being external to the TOE are made in order to ensure the effectiveness of the TOE's security functions (see Table 2).

Table 2: Assumptions about the environment

Id	Assumption
AE1	Life cycle security
AE2	Integrity and quality of key material
AE3	SigG compliant use of the TOE
AE4	Use with SigG compliant IFD
AE5	Security assumption about the ICC hardware

3.2.4.1 Life cycle security (AE1)

The TOE is expected in the first place to enforce the security objectives as described in sect. 3.2.6 within the operational use phase. In order to have the TOE's security objectives effectively fulfilled in operational use, the security of earlier life cycle stages must be relied upon. The following assumption AE1 about the life cycle of the ICC are made:

(AE1.1) The security of procedures in (i) the manufacturing phase, (ii) the initialisation phase (including completion) and (iii) the personalisation phase of the ICC life cycle is assured.

(AE1.2) The personalisation facility and certification authority keep the confidentiality of authentication information of the cardholder[5].

The description the procedures of the TOE for the secure initialisation and personalisation of the ICC is given in [CLC].

3.2.4.2 Integrity and quality of key material (AE2)

The TOE is used in (i) a public key infrastructure for SigG digital signatures. The TOE contains the elements that can be used in (ii) a public key infrastructure for SigG accredited technical components. The following assumption AE2 about the public key infrastructure is made:

(AE2.1) The environment ensures for the device authentication key pair of the root certification authority (RCA)

(1) the cryptographic quality of the key pair and of the cryptographic algorithms,

(2) the confidentiality of the private key (see SK.DEPCA.CS_AUT in [DIN], sections 9),

(3) authenticity (especially origin) of the public key (see PK.DEPCA.CS_AUT in [DIN], sections 9 and 18.3) stored in the TOE.

(AE2.2) The environment ensures for the device authentication key pair of the certification authorities (CA) for mutual device authentication of SigG accredited technical components

(1) the cryptographic quality of the key pair and of the cryptographic algorithms,

(2) the confidentiality of the private key (see SK.CA.AUT in [DIN], sections 3.2),

(3) authenticity (especially origin) of the public key (see PK.CA.CS_AUT in [DIN], sections 9 and 18.3.1) if stored in the TOE,

(4) authenticity (especially origin) of the public key (see PK.CA.CS_AUT in [DIN], sections 9 and 18.3.2) in the authentication certificate C.CA.CS_AUT.

---

5 see also footnote 3

(AE2.3) The environment ensures for the SigG accredited IFD authentication key pair

(1) the cryptographic quality of the key pair and of the cryptographic algorithms,

(2) the confidentiality of the private key in the IFD (see SK.IFD.AUT in [DIN], annex D),

(3) authenticity (especially origin) of the public key (see PK.IFD.AUT in [DIN], annex D) in the device authentication certificate C.IFD.AUT.

(AE2.4) The environment ensures for the ICC authentication key pair

(1) the cryptographic quality of the key pair and

(2) the authenticity (especially origin) of the public key (see PK.ICC.AUT in [DIN], annex D) in the device authentication certificate C.ICC.AUT, generated by the certification authority for mutual device authentication of SigG accredited technical components and stored in the TOE.

(AE2.5) The environment must ensure for the SigG signing key pair of the root certification authority (RCA)

(1) the cryptographic quality of the key pair and of the cryptographic algorithms,

(2) the confidentiality of the private key (see SK.DEPCA.DS in [DIN], section 9),

(3) authenticity (especially origin) of the public key (see PK.DEPCA.DS in [DIN], section 9).

(AE2.6) The environment ensures for the SigG signing key pair of the certification authorities (CA) for SigG signing keys

(1) the cryptographic quality of the key pair and of the cryptographic algorithms,

(2) the confidentiality of the private key (see SK.CA.DS in [DIN], section 3.2),

(3) authenticity (especially origin) of the public key (see PK.CA.DS in [DIN], sections 9 and 18.3.2) in the signature key certificate C.CA.DS.

(AE2.7) The environment ensures authenticity (especially origin) of the public key(s) (see PK.CH.DS in [DIN], annex D) in the signature certificate C.CH.DS, generated by the certification authority for SigG digital signatures. (Note: AE2.7 in this document corresponds to AE2.8 in [GST_098].)

3.2.4.3 SigG compliant use of the TOE (AE3)

The following assumption AE3 about the SigG compliant use of the TOE is made:

(AE3.1) The TOE shall be used by the cardholder in accordance with SigG legislative. The regulations for the cardholder include at least:

(1) The cardholder ensures secure storage and handling of the ICC to prevent misuse and manipulation of the ICC.

(2) The cardholder uses the TOE SigG signature generation function only for signing data of which the integrity or authenticity must be assured.

(3) The cardholder keeps the confidentiality of his authentication information (PIN and PUK) for SigG application.

(4) The cardholder changes his PIN for the SigG application regularly[6].

(5) The cardholder knows whether the used IFD is a SigG accredited IFD and (i) a public IFD or (ii) an office IFD.

(6) The cardholder uses the SigG application with an office IFD only. The generation of an additional SigG signing key pair can also be performed within a CA/RA; in this case the key generation function of the SigG application may be used with an IFD within a CA/RA.

(AE3.2) The authority, which has issued the cardholder signature key certificate and/or the ICC, informs the cardholder about these regulations.

3.2.4.4 Use with a SigG compliant IFD (AE4)

The SigG regulation requires that the TOE shall be used only with SigG compliant technical components. The bodies running the technical components are responsible for setting up and maintaining appropriate security for the SigG compliant technical components. The following assumption AE4 about the use with SigG compliant IFD is made:

(AE4.1) The cardholder uses the SigG application with SigG compliant IFDs only.

(AE4.2) The environment of the TOE ensures:

(1) The office IFD is connected to an IT system that sends to the ICC only messages or hash-values of messages for which the cardholder wishes to apply a digital signature.

---

6 The TOE performs its security functions independently of (AE3.1) (4). But the fact that only the cardholder knows his PIN O3 is of particular importance, so this requirement should be raised and this assumption is rather expedient.

(2) In unlimited signature generation configuration (see section 3.2.2), remaining components of this IT system limit either

- the number of signatures that can be generated after successful cardholder authentication to a fixed number. After this number of signatures has been generated, a renewal of the cardholder authentication is necessary before a new digital signature can be generated.

- or the time within which signatures can be generated. After this time has expired, a renewal of the cardholder authentication is necessary before a new digital signature can be generated.

(3) The office IFD keeps the confidentiality of the cardholder's authentication information (PIN and PUK).

(4) The environment keeps the confidentiality and integrity of the data transferred between the office IFD and the ICC.

(5) If the TOE is in Current Authentication State **CAS6** (see section 3.4.1 Security state) and the TOE makes this transparent to the office IFD, then the office IFD reacts accordingly and makes this state transparent to the user.[7]

(6) If the maximum number of failed authentication attempts allowed for the PIN or the PUK has been exceeded and the TOE makes this transparent to the office IFD by generating the corresponding error code, then the office IFD reacts accordingly and makes this state transparent to the user.

(AE4.3) If a SigG signature key pair of the cardholder is generated (by the cardholder or by the CA/RA) then the certification authority has to verify the SigG accreditation of the ICC presented by the cardholder.

3.2.4.5 Security assumption about the ICC hardware (AE5)

The following assumption AE5 about the ICC hardware is made:

(AE5.1) The ICC hardware is tamper resistant. The tamper resistance

(1) protects the TOE against modification and

(2) ensures the confidentiality of the all private SigG signature key(s) **O2** (SK_i.CH.DS, $1 \leq i \leq m$) of the cardholder as well as the private

7 This assumption is drawn from SigV, §16 Anforderungen an die technischen Komponenten, paragraph (2), sentence 5: "Sicherheitstechnische Veränderungen an den technischen Komponenten müssen für den Nutzer erkennbar werden."

authentication key SK.ICC.AUT stored on the ICC against physical attacks.

(AE5.2) The ICC hardware implements security mechanisms to prevent or reduce illicit information flow due to physical observable characteristics provided by the hardware design.

(AE5.3) The ICC hardware implements security mechanisms detecting potential security violations. The underlying hardware reacts to the following events:
a) lower/higher clock frequency
b) lower/higher supply voltage and
c) lower/higher temperature.
If one of those events was detected, the ICC is being reset as long as the physical conditions are wrong.

3.2.5 Assumed Threats

The assumed threats for the TOE are a consequence of the method of use, the environment of the TOE and the overall security policy, which is derived from the TOE's overall purpose of being technical component to generate digital signatures compliant with SigG legislative and [DIN]. The fundamental threat is therefore that the cardholder's signature might be generated for a piece of data the cardholder does not want to be signed (by him).

The threats are enumerated as Tn.m where n indicates the number of the subsection in the current section and m the number of the threat within this subsection. The following Figure 1 depicts the resulting threat scenario assumed for the TOE. Items with a dotted borderline are forged or otherwise potentially malicious. Items with a normal borderline are "authentic".

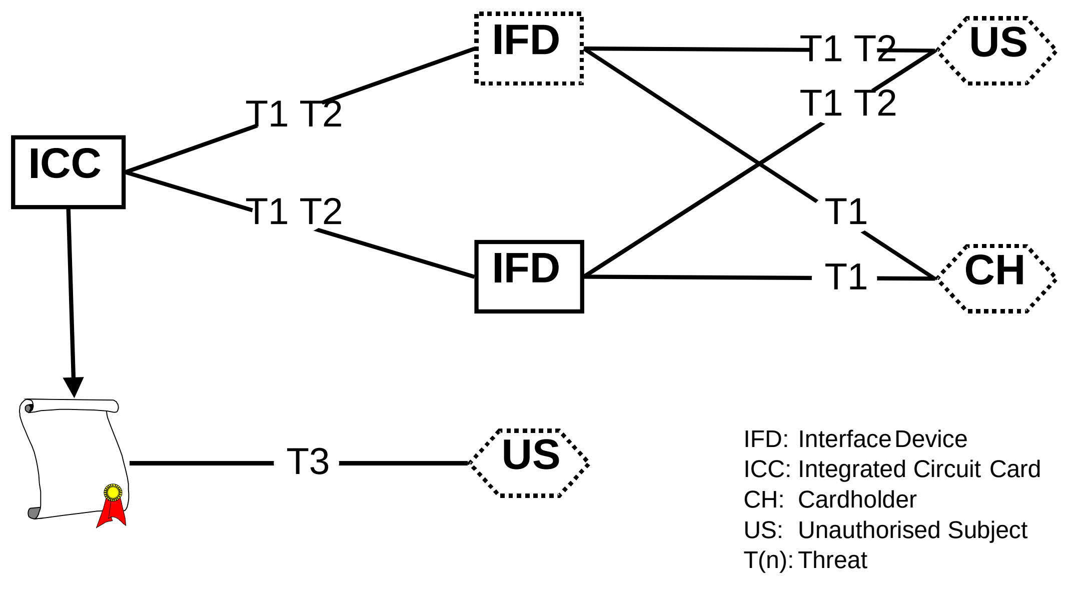

Figure 1: Threat Scenario

Table 3: Security Threats

Id	Security Threat
T1	Extraction of the cardholder's SigG signing private key
T2	Misuse of the signature function
T3	Forging data ascribed to the cardholder

3.2.5.1 Extraction of the cardholder's SigG signing private key (T1)

The ICC stores the SigG signing key pair of the cardholder in the TOE.

(T1.1) The user might try to extract the SigG signing private key of the cardholder used for digital signatures from the ICC.

The extraction of the SigG signing private key of the cardholder T1.1 may be performed by (i) directly reading the key or (ii) copying the key to other devices even if the key is not generally disclosed in the process or (iii) inferring the key by analysing the results of computations performed by the ICC or (iv) inferring the key by analysing a physical observable. Successful key extraction allows an attacker to generate digital signatures ascribed to the cardholder for arbitrary data.

(T1.2) The user might try to modify the SigG signing private key stored in the ICC.

The modification of the SigG signature private key of the cardholder T1.2 might result in a digital signature generated by the TOE, which may not be regarded as compliant to SigG legislative any more.[8]

3.2.5.2 Misuse of the signature function (T2)

The TOE generates digital signatures for the cardholder.

(T2) Somebody might try to misuse the digital signature generation function without permission of the cardholder.

Somebody taking possession of the ICC may try to impersonate the cardholder.

3.2.5.3 Forging data ascribed to the cardholder (T3)

A message is characterised by (i) the sender, the (ii) designated receiver and (iii) the message text. The hash-value is a digest of the message text.

[8] Another unintended result of (T1.2) might be that a digital signature is generated which is compliant to SigG, but the card holder generating it might not be the owner of the corresponding certificate.

(T3.1) An unauthorised subject might try to modify the message text originating from the cardholder without the recipient being able to notice it.

The message of the cardholder is exposed to modifications not authorised by the cardholder. The recipient of the message accepts it as original.

(T3.2) An unauthorised subject might claim that a certain message text origins from the cardholder without the cardholder being able to disprove that.

The message will be ascribed to the originator noticed in the message.

3.2.6 Summary of Security Features

The following Table 4 identifies the security objectives. The security objectives are grouped by content and enumerated as SOn.m, where n indicates the number of the security objective group and m the number of the security objective within this security objective group. Each security objective is described later on in a respective subsection by

- stating the security objective,
- giving rationales and explaining the relationship to the security threats previously presented and
- indicating the security functionality used to achieve the security objective.

Table 4: Security objectives

Id	**Security Objective**
SO1	Prevent disclosure, copying or modification of the cardholder's SigG signing private keys SK_i.CH.DS
SO2	Prevent unauthorised use of the SigG digital signature function
SO6	Quality of key generation
SO7	Provide secure digital signature
SO8	React to potential security violation

3.2.6.1 Prevent extraction or modification of the SigG signature key(s) of the cardholder (SO1)

(SO1) The TOE ensures the confidentiality and the integrity of the SigG signature private key(s) SK_i.CH.DS of the cardholder stored in the TOE with two aspects:

(SO1.1) The TOE shall prevent any kind of extraction of a cardholder's SigG signing private key(s) SK_i.CH.DS from the ICC.

(SO1.2) The TOE shall prevent any kind of modification of a cardholder's SigG signing private key(s) SK_i.CH.DS in the ICC.

The cardholder intends to protect the integrity of his message while in transit (either over space or time) to the intended recipient. It is the TOE's primary function to generate digital signatures for data provided by the IFD and related to the message text. The signature enables the recipient to verify the origin and the integrity of the message text. The effectiveness of the digital signature mechanisms is based on the confidentiality and integrity of the cardholder's SigG signature private key. The TOE is intended to be used within the context of SigG legislative, which is strict about the confidentiality: the key must never leave the signature device and must not be disclosed when used[9].

This security objective covers threat T1.1 and T1.2 defined in section 3.2.5.1.

The TOE shall implement the security enforcing functions **AC1** and **AC2** described in sections 3.3.2.2and 3.3.3.2 to fulfil the security objective SO1. The SEF **OR1** described in sections 3.3.2.4 and 3.3.3.4 shall prevent illicit information flow between the SigG application and other application embedded on the ICC through the temporary used storage areas. The SEF **DX1** and **DX2** described in section 3.3.2.5 and 3.3.3.5 shall prevent disclosing of the SigG private signature key of the cardholder in the digital signatures generated by the TOE. The appropriate reaction of the TOE shall ensure the security of the SigG private signature key of the cardholder if a potential attack has been detected (see SEF **AC3** in sections 3.3.2.2 and 3.3.3.2).

3.2.6.2 Prevent unauthorised use of the SigG digital signature function (SO2)

(SO2) The TOE shall allow the use of the digital signature function only to the cardholder. This security objective has the following aspects[10]:

(SO2.1) The TOE shall allow the use of the digital signature function only to the cardholder after successful authentication by knowledge[11].

(SO2.2) Successive authentication failures will be interpreted as an attempted unauthorised access by the TOE and will disable the signature function.

(SO2.3) The authentication data is stored in the TOE and may not to be disclosed.

---

9 see [SigV] §16 (1) Sentence 2 and §16 (2) Sentence 2

10 The security objective SO2 corresponds to [SigV] §16 (2) Sentence 2, 3 and 4, requiring authentication of the cardholder for access to function using the SigG private signature key of the cardholder.

11 PIN **O3** and PUK **O4** are specific to the SigG application and are only used to authenticate the cardholder for the use of the SigG application. Both PIN **O3** and PUK **O4** are not used to authenticate the cardholder for the use of any other application that may be installed on the ICC in addition to the SigG application.

To use the SigG application the cardholder has to authenticate by knowledge (by presenting a PIN or a PUK). The number of digital signatures that can be generated after successful cardholder authentication is either (i) limited to one or (ii) not limited by the TOE itself (see limited signature generation configuration and unlimited signature generation configuration). The cardholder can sign till (i) his authentication is expired[12], (ii) the SigG application is closed, (iii) next ICC reset or (iv) the ICC is deactivated (see also section 3.2.3).

This security objective counters the threat T2 (section 3.2.5.2).

The TOE implements the security enforcing functions **IA1**, **IA2**, **IA3** and **IA4** as well as **AC1** described in sections 3.3.2.1, 3.3.3.1, 3.3.2.2 and 3.3.3.2 to fulfil the security objective SO2. Authentication failures are being made apparent to the cardholder through the security enforcing functions **AU1** and **AU2** described in sections 3.3.2.3 and 3.3.3.3.

Remark to (SO2.2):

The TOE itself can detect if the maximum number of failed authentication attempts allowed for (i) the cardholder reference data and/or (ii) the cardholder reset reference code has been exceeded. In this case (i) the cardholder reference data and/or (ii) the cardholder reset reference code are blocked. If both (i) cardholder reference data and (ii) the cardholder reset reference code are blocked, the cardholder can no longer authenticate himself to the TOE and all functionality that is only available to the cardholder (especially the generation of digital signatures) can no longer be used. – The fact, that (i) the cardholder reference data or (ii) the cardholder reset reference code is blocked, is being made apparent to the IFD and thus to the human user (see (AE4.2) (6)) through the return codes of the commands (i) VERIFY and/or (ii) VERIFY AND CHANGE, respectively (see mechanisms M12 Return Code for VERIFY and M13 Return Code for VERIFY AND CHANGE).

3.2.6.3 Quality of key generation (SO6)

(SO6) Any key material generated by the TOE shall bear a strong cryptographic quality. The cryptographic quality is characterised as follows[13]:

(1) If SigG signature key pairs are generated (either in the first personalisation phase or in a repersonalisation phase after the operational use of the TOE has begun), this process must be performed in a secure way.

(2) The generated SigG signature key pairs must be unique with a very high probability and cryptographically strong.

---

12 case limited signature generation configuration only

13 The security objective SO6 fulfils the requirement of [SigV] §16 (1) Sentence 1 for the SigG signature key pair of the cardholder.

(3) It shall be impossible to calculate the SigG private signature key from the SigG public signature key.

Key generation in a secure way means to ensure (i) the confidentiality of the SigG signing private key, (ii) the integrity of the SigG signing public key, and (iii) cryptographic strength of the key pair. The cryptographic quality for the ICC device authentication key pair is necessary to ensure the cryptographic strength of the signature generated over an additional (generated during the repersonalisation phase) SigG signature key pair.

The security objective SO6 counters the threat T3 ensuring a precondition[14] for the cryptographic strength of the digital signature (see also [BA]).

The TOE implements the security enforcing function **DX1** described in sections 3.3.2.5 and 3.3.3.5 to fulfil the security objective SO6 by means of generation of secure SigG signature key pairs. The appropriate reaction of the TOE shall prevent misuse of this SEF if a potential attack has been detected (see SEF **AC3** in sections 3.3.2.2 and 3.3.3.2).

3.2.6.4 Provide secure digital signature (SO7)

The principal security objective of the TOE is SO7 - the generation of SigG digital signatures.

(SO7.1) The TOE provides a function to generate a SigG digital signature for the data presented by the IFD using the SigG signature private key of the cardholder stored in the TOE.

(SO7.2) The function to generate a SigG digital signature works in a manner that other individuals, not possessing SigG private signature key of the cardholder, cannot generate a SigG digital signature.

The security objective SO7 is drawn from [SigV] §16 (2) Sentence 1. The requirement of [SigV] §16 (2) Sentence 1 that the cardholder's SigG private signature key cannot be derived from the signature is a sub-case of SO1.1 because signature is a part of the TOE's output. In general SO7.2 relates to a cryptoanalytic attack against a signed message independently of the TOE and addresses the cryptographic strength of the signing function of the TOE (see [BA]).

The data presented by the IFD and to be signed is (i) the hash-value of the message text or (ii) an intermediate hash-value of the message text and the remaining message text to be hashed by the TOE or (iii) the complete message text to be hashed by the TOE (see [DIN], section 14).

This is the principal security objective of the TOE directly countering the threat T3.

---

14 Cryptographically weak key material involves danger for the strength of the digital signature.

The TOE implements the security enforcing function **DX2** described in sections 3.3.2.5 and 3.3.3.5 to fulfil the security objective SO7 by means of generation of secure digital signatures. The appropriate reaction of the TOE shall ensure the security of SigG signature generation if a potential attack has been detected (see SEF **AC3** in sections 3.3.2.2 and 3.3.3.2).

3.2.6.5 React to potential security violation (SO8)

The TOE fulfils the following security objective SO8[15]:

(SO8) The TOE can be put into a TERMINATE state (see **CAS6** in section 3.4.1 Security state as well as **SRE10**). If the TOE has been put to **CAS6**, the ICC is irreversibly blocked and no application can be used any longer. The TOE contains a mechanism **M7** that detects **CAS6** at start-up and in this case enters an endless loop. – The fact that the TOE is in its TERMINATE state is being made apparent to the IFD and thus to the human user (see (AE4.2) (5)) by modifying the ATR (see M14 in section 3.5.13).

The TOE therefore recognises a “potential security violation” if somebody **S2** sends the TERMINATE CARD USAGE command to the TOE and every time the TOE is powered up or reset again. This command can be accepted by the TOE only once. After that the ICC is irreversibly blocked and the TOE can not accept any command any more. This is the only way for the TOE to react to a potential security violation.

The TOE implements the security enforcing function **AC3** described in sections 3.3.2.2+3.3.3.2 (informally + formally) to fulfil the security objective SO8.

SO8 is fulfilled independently from and complements (AE5.3).

3.3 Security Functions

3.3.1 Definitions

Note: The names of processes, objects, access-types and security-relevant-events will be presented in **bold face** in this section. The definitions of the terms are collected in the glossary (see section 3.9).

3.3.1.1 Subjects

The IFD as technical process represents the outside world beyond the external interface of the ICC and thus the TOE. The IFD is generally expected to access data and services of the ICC on behalf of and as intended by the human user. Moreover the IT system used by the human user acts on behalf of him or her as a service provider. In the point of view of the TOE security policy the outside world is a combination of two types of subjects: (i) the human users and (ii) the IT-systems. The subjects **S1** Cardholder, **S2** Somebody and **S7** Potential attacker represent human users. The

---

15 The security objective SO8 is drawn from [SigV] §16 (1) Sentence 3 and §16 (2) Sentence 5.

subject **S3** IFD represents an IT-systems. The outside world is represented by a pair $(u,t) \in \{S1, S2, S7\} \times \{S3\}$.

The TOE is aware of the subjects identified in the following Table 5.

Table 5: Subjects

Id	Subject
S1	Cardholder
S2	Somebody
S3	IFD
S7	Potential attacker (anybody using the ICC in its blocking state)

3.3.1.1.1 Subject S1 Cardholder

After the first personalisation (in the operational phase) the **subject S1 Cardholder** is a human user for which the SigG application of the TOE is personalised:

- The cardholder is the only person in legitimate possession of the verification data (PIN and PUK) matching the reference data stored for authentication by knowledge for the SigG application of the TOE in the operational phase. See AE1.2 and AE3.1.

The cardholder is the legitimate owner of a specific ICC running the TOE and the SigG signature key pair(s) of the cardholder stored in the TOE.

3.3.1.1.2 Subject S2 Somebody

The **subject S2 Somebody** is some human user of the ICC different from the subject **S1** Cardholder and **S7** Potential attacker, i. e. (i) being not in legitimate possession of the verification data defined for the cardholder[16] and (ii) using the TOE being not in the blocking state. The subject S2 may be in legitimate possession of other verification data or be able to provide the biometrical characteristics to generate such verification data for a non-SigG application on the ICC.

3.3.1.1.3 Subject S3 IFD

The **subject S3** IFD is an arbitrary IFD (interface device) connected to the ICC, which need not to be able to support mutual device authentication and/or secure messaging.

16 i.e. the verification data that Somebody **S2** will provide to the TOE will not match the reference data stored in the TOE

3.3.1.1.4 Subject S7 Potential attacker

The **subject S7 Potential attacker** stands for an arbitrary subject trying to use the TOE in the blocking state (e. g. after a potential attack is detected, see **SRE10**, **CAS6** and **SO8** for details).

3.3.1.2 Security-relevant-events

The **security-relevant-events** depend on (i) commands presented by the IFD to the TOE, (ii) command data presented by the IFD to the TOE, (iii) data about security relevant events persistently stored in TOE, and (iv) events detected by the ICC hardware or signalled by it to the TOE.

The security-relevant-events given in the following Table 6 are recognised by the TOE.

Table 6: Security-relevant-events

Id	Security-relevant-event
SRE1	Resetting of the ICC
SRE2	Deactivation of the ICC
SRE3	Opening of the SigG application
SRE4	Closing of the SigG application
SRE5	Successful cardholder authentication
SRE6	Cardholder authentication failure
SRE7	Repeated authentication failure
SRE8	Authentication expiration
SRE10	Potential security violation occurred
SRE11	Cardholder authenticated by reset code
SRE12	Cardholder authentication by reset code failed

Security-relevant-event SRE1 Resetting of the ICC

The **SRE1 Resetting of the ICC** is defined as security relevant event when the ICC is powered up by inserting the ICC into a suitable IFD (”activation”) or a hardware reset signal is given to the ICC. The TOE performs a well-defined initialisation procedure (”card reset”) without intervention of the user or the IFD.

Security-relevant-event SRE2 Deactivation of the ICC

The security relevant event **SRE2 Deactivation of the ICC** occurs if the power supply of the ICC is down, e.g. by removal of the ICC from the IFD. After **SRE2** all non-persistent information of the TOE not stored in the EEPROM or ROM is lost.

Security-relevant-event SRE3 Opening of the SigG application

The security relevant event **SRE3 Opening of the SigG application** occurs if (i) no file (EF or DF) of the SigG application has been selected before and (ii) a file in the SigG application (an elementary file (EF) in the SigG application directory or the SigG application directory (DF) itself) is selected or a security environment in the SigG application directory is selected.

Note: If the SigG application is already open, then the selection of a file in the SigG application or of a security environment in the SigG application will not cause the security relevant event SRE3[17]. The security relevant event SRE3 is refined in section 3.4.1 into **SRE3a** and **SRE3b** (depending on the value of RC_{PIN}).

Security-relevant-event SRE4 Closing of the SigG application

The security relevant event **SRE4 Closing of the SigG application** occurs if (i) an elementary file (EF) outside the SigG application directory is selected or (ii) a security environment outside the SigG application directory is selected or (iii) an application directory (DF) different from the SigG application directory is selected.

Security-relevant-event SRE5 Successful cardholder authentication

The security relevant event **SRE5** "**Successful cardholder authentication"** occurs if (i) the authentication of a human user for the SigG application with the verification data was attempted, (ii) the number of consecutive failed authentication attempts with verification data does not exceed the maximum number of failed authentication attempts allowed ($RC_{PIN}>0$), and (iii) the verification data presented for human user authentication matches the reference data (PIN) **O3** stored for the SigG application of the TOE. Due to the TOE supporting only the user authentication by knowledge for the SigG application, condition (iii) is fulfilled if and only if the verification data presented matches the reference data for knowledge based authentication. If **SRE5** occurs the number of consecutive failed authentication attempts with reference data is set to zero (i.e. RC_{PIN} is set to its initial value, $RC_{PIN}:=3$).

For the user authentication by knowledge the cardholder presents his verification data (PIN) to the TOE. The retry counter for PIN RC_{PIN} has the initial value 3, so that there are three successive attempts to input the PIN. A successful attempt (i) resets the retry counter and (ii) authenticates the cardholder (**SRE5**).

Security-relevant-event SRE6 Cardholder authentication failure

The security relevant event **SRE6 Cardholder authentication failure** occurs if (i) the authentication of a human user for the SigG application was attempted and (ii) **SRE5** does not occur and (iii) the retry of the human user authentication for the SigG application is allowed ($RC_{PIN}>0$).

---

17 This especially means that an already authenticated cardholder will not lose this security state since the CAS will not be changed.

Security-relevant-event SRE7 Repeated authentication failure

The security relevant event **SRE7 Repeated authentication failure** occurs if (i) the authentication of a human user for the SigG application was attempted and (ii) **SRE5** does not occur and (iii) the retry of the human user authentication for the SigG application is not allowed (RC_{PIN}=0).

Note: If both the retry counter for PIN **O3** and the retry counter for PUK **O4** reach the value 0 (RC_{PIN} = RC_{PUK} = 0), the cardholder authentication for the SigG application is permanently blocked (see also (SO2.2)).

Security-relevant-event SRE8 Authentication expiration

For a TOE in limited signature generation configuration, the security relevant event **SRE8 "Authentication expiration"** is generated automatically by the TOE after the generation of a digital signature.

For a TOE in unlimited signature generation configuration, the security relevant event **SRE8** is never generated.

<u>Notes:</u>

1. These "configurations" (see also section 3.2.2) cannot be configured by the cardholder, but are properties of the TOE instead which cannot be altered after generation of the TOE.

2. The security-relevant-event SRE8 can only occur after the generation of a digital signature. Therefore SRE8 will not occur in any other state except for CAS3. See also Table 11: State transition table and Figure 2: State transition diagram.

Security-relevant-event SRE10 Potential security violation occurred

The following events cause the security relevant event **SRE10 Potential security violation occurred** to be triggered:

(i) The TOE detects the reception of the command TERMINATE CARD USAGE.

(ii) The TOE detects after the ICC is powered up or a hardware reset signal is given to the ICC, that the ICC has been permanently blocked.

The ICC can be blocked permanently by the subject **S2** Somebody issuing the TERMINATE CARD USAGE command. After the execution of this command, the TOE is in its TERMINATE state **CAS6**, which is permanent and can never be left (besides by reset **SRE1** or deactivation **SRE2** of the ICC; after contacting the ICC the TOE will immediately and automatically transit into the TERMINATE state **CAS6**).

Security-relevant-event SRE11 Cardholder authenticated by reset code

The security relevant event **SRE11 Cardholder authenticated by reset code** occurs if (i) the reset of the retry counter of the SigG application was attempted and (ii) the reset code presented matches the SigG cardholder reference reset code **O4** of the SigG application and (iii) the retry counter $RC_{PUK}>0$ (in the case $RC_{PUK}=0$, the attempt is regarded as unsuccessful, see **SRE12**).

Security-relevant-event SRE12 Cardholder authentication by reset code failed

The security relevant event **SRE12 "Cardholder authentication by reset code failed"** occurs if (i) the authentication with the SigG cardholder reset code was attempted and (ii) the presented reset code does not match the reference reset code **O4** "SigG cardholder reset code" stored in the TOE or (iii) the retry of the human user authentication for the SigG application by presenting the reset code is not allowed ($RC_{PUK}=0$).

The previous paragraph should be understood in such a way that **SRE12** occurs if the following conditions apply: [(i) and (ii)] or [(i) and (iii)]. This especially means, that if the presented cardholder reset code matches the reference reset code **O4**, but $RC_{PUK}=0$, then this will also be regarded as **SRE12**.

3.3.1.3 Objects and related access-types

The following objects and related access-types are identified in the Table 7[18].

Table 7: Objects and related access-types

Id	Object	Access-types
O1	SigG application	open, close
O2	SigG signature private key(s) (SK_i.CH.DS) of the cardholder	use for signature generation, generate, extract
O3	SigG cardholder reference data	use for cardholder authentication, modify, block, unblock
O4	SigG cardholder reference reset code	use for authentication, block
O5	SigG signature key certificate(s) of the cardholder (C_i.CH.DS)	use for signature verification, read, supplement
O6	SigG public key of the root certification authority (PK.RCA.DS)	use for signature verification, read, modify

18 Note that due to the compatibility to the generic security target [GST_098], the object O8, O9, O10, O11 and O13 do not exist in this Security Target.

Id	Object	Access-types
O7	Other credentials for signature verification	use for signature verification, read, modify, supplement
O12	SigG public signature key(s) (PK_i.CH.DS) of the cardholder	use for signature verification, read, generate

SigG application (O1)

The object **O1 SigG application** (SigG signature application, StarCert) includes SigG related data objects as specified in Table 7 (Objects O2 to O7, and O12) and any function or method to access or use that data.

Opening the **O1** enables the access-types to the contained objects, which are not available otherwise. No other function or data not being related to the SigG application is available in an open SigG application.

Closing the **O1** disables these access-types and gives way to other not SigG related activities.

The **O1** is always implicitly closed immediately after resetting the TOE.

SigG signature private key(s) of the cardholder (O2)

The object **O2 SigG signature private key(s) of the cardholder** is part of the object **O1** and is used by the TOE to generate a digital signature on behalf of the cardholder. This object is named SK.CH.DS in [DIN], since there it is assumed that there is only one SigG signature key pair.

This TOE allows the cardholder to have **multiple SigG signature key pairs** (see section 3.2.3 Intended method of use), thus there can be multiple SigG signature private keys and, therefore, **O2** is defined as the set of all SigG signature private keys of the cardholder that have already been generated:

$$\mathbf{O2} := \{SK_i.CH.DS \mid 1 \le i \le n\},$$

where $n \le m$ and m denotes the maximum number of SigG signature key pairs that can be stored in the TOE.

When the TOE is delivered to the cardholder, the TOE already contains one operational SigG signing key pair (i = 1)(SK_1.CH.DS, PK_1.CH.DS). The cardholder can generate additional SigG signing key pairs. Those key pairs will be named (SK_i.CH.DS, PK_i.CH.DS) or in short: key pair *i*, where *i* > 1. If an additional key pair (SK_i.CH.DS, PK_i.CH.DS) is generated, its private key SK_i.CH.DS becomes part of the set **O2**[19].

The term “**use for signature generation**“ the **O2** means calling and performing the respective command for transferring the (intermediate or final) hash value and/or the data to be hashed on the card (see section 3.2.3.4), selecting the desired SigG signing key pair and then calling and performing the respective command to generate a digital signature. Only those SigG signing key pairs can be used for signature generation, that have already been generated.

The term “**use for signing**“ the **O2** will be used synonymously with the same meaning as “**use for signature generation**“ the **O2**.

The term “**extract**” the **O2** means (i) to use one of the keys for any other function beside signature generation (in sense of refer) and (ii) any kind of gathering information about the **O2** by observing the TOE’s external behaviour during the computation of a digital signature (e.g. electromagnetic emanation, power consumption and timing, in sense of infer).

The term “**generate”** the **O2** means to use the respective command of the TOE to generate a SigG signing key pair (SK_i.CH.DS, PK_i.CH.DS) ($1 \le i \le m$) of the cardholder **S1** and to store the private key SK_i.CH.DS in object **O2** in the TOE. The generation of a SigG signing key pair *i* is possible only once for each key pair *i*; thus there can be *m* SigG signing key pair generations at most, of which one (the first) SigG signing key pair generation takes place at the CA/RA during the first personalisation phase and a maximum of *m-1* SigG signing key pair generations take place at the cardholder during repersonalisation phases. Since each key pair *i* can be generated only once, only such a signing key pair *i* can be generated that has not already been generated. By generating of each element *i* of the set **O2**, the TOE enters the (first or re-)personalisation phase for the corresponding SigG signing key pair *i*.

SigG cardholder reference data (O3)

The object **O3 SigG cardholder reference data** is the data permanently stored in the TOE to verify the verification data provided for the cardholder authentication (PIN). We will use the term **PIN**[20] (**O3**) synonymously.

To “**use O3 for cardholder authentication”** means to call services, which provide human user authentication by comparing the **O3** with the verification data presented (see IA1 in section 3.3.2.1 and 3.3.3.1).

---

19 If we want to formulate a statement where an arbitrary SigG signature private key SK_i.CH.DS chosen by the cardholder is used, then we will use the notation SK.CH.DS to stand for this arbitrary SK_i.CH.DS chosen by the cardholder.

20 Note the difference between the PIN stored in the TOE (**O3**) and the data input by a user for authentication purposes.

The term “**modify**” the SigG cardholder reference data means (i) to authenticate with the verification data for the actual reference data and (ii) if this cardholder authentication was successful to change the value of O3 to the presented reference data.

The term “**block**” the O3 means to deactivate O3 for the use for cardholder authentication by repeated authentication failure (see **SRE7**).

The term “**unblock**” the O3 means (i) to perform cardholder authentication by reset code and (ii) if this cardholder authentication was successful to change the value of O3 to the presented reference data.

SigG cardholder reference reset code (O4)

The object **O4 SigG cardholder reference reset code** is the data permanently stored in the TOE to verify the reset code provided by the user to reset of the retry counter for PIN RC_{PIN}. We will use the term **PUK**[21] (**O4**) synonymously.

The term “**use O4 for authentication**” means to call services (see mechanism M5), which compare the O4 with the presented reset code, and, if they match, (i) reset the retry counter (for PIN as well as for PUK: $RC_{PIN} = RC_{PUK} = 3$), (ii) unblock and allow to change **O3** (see **IA4** in section 3.3.2.1 and 3.3.3.1) and (iii) perform the cardholder authentication by reset code (see **IA1** in section 3.3.2.1 and 3.3.3.1).

The term “**block**” the **O4** means to deactivate **O4** for the use for authentication by failure of authentication by reset code (see **SRE12**, case (iii)), if the retry of the authentication by reset code is not allowed any more (RC_{PUK}=0).

Note: PIN (**O3**) and PUK (**O4**) are used for the SigG application only. If other applications are installed on the ICC as well, they may or may not have their own, independent PIN and/or PUK.

SigG signature key certificate of the cardholder (O5)

The object **O5 SigG signature key certificate(s) of the cardholder** is the set of certificates of the SigG public key(s) PK_i.CH.DS of the cardholder for the signing algorithm RSA. This set of certificates is stored in the TOE and may be used by an external party to verify the cardholder’s signatures[22].

The **use for signature verification** of the object **O5** means calling and performing the respective commands for transferring the (intermediate or final) hash value and/or the data to be hashed on the card (see section 3.2.3.4), selecting the desired SigG public key to be used for the signature and then calling and performing the respective command to verify a digital signature.

---

21 Note the difference between the PUK stored in the TOE (**O4**) and the data input by a user for authentication purposes.

22 This object is named C.CH.DS in [DIN]

To **supplement** the **O5** means to use the respective command of the TOE to (I) load an (additional) or to (II) update signature key certificate C_i.CH.DS for an (additional) SigG signing public key PK_i.CH.DS generated by the cardholder **S1** into the ICC, where $1 \le i \le m$.

To **read** the **O5** means to use the respective command of the TOE to transmit the signature key certificate C_i.CH.DS for the signing public key (PK_i.CH.DS) of the cardholder **S1** to the IFD.

SigG public key of the root certification authority (O6)

The object O6 **SigG public key of the root certification authority** is a public key of the root certification authority for the signing algorithm supported by the TOE, which is stored in the TOE and may be used by an external party. This object O6 is named PK.RCA.DS in [DIN].

The **use for signature verification** of the object **O6** means calling and performing of the respective command to verify a digital signature.

To **modify** the **O6** means to use the respective command of the TOE to load the SigG public key of the root CA into the ICC.

To **read** the **O6** means to use the respective command of the TOE to transmit the SigG public key of the root CA to the IFD.

Other credentials for signature verification (O7)

The object O7 **Other credentials for signature verification** are defined as additional public keys or certificates, which may be stored in the SigG application directory for the purpose of signature verifications. The object O7 is an optional object for the TOE, e. g. it may not exist in the SigG application directory. The certificate, which directly refers to the cardholder's public key is part of this and is called the **SigG cardholder's certificate** (signature key certificate). Other certificates are called collectively **SigG CA certificates of the cardholder**.

The **use for signature verification** of object O7 means calling and performing of the respective command to verify the relevant digital signature.

To **modify** to the **O7** means to use of the respective command of the TOE to load the object **O7** into the ICC.

To **read** to the **O7** means to use of the respective command of the TOE to transmit the object **O7** to the IFD.

The term "**supplement**" means to add any data (independent whether the data are public keys or certificates) to **O7**.

SigG public key of the cardholder (O12)

The object **O12 SigG public key of the cardholder** is part of the object **O1** and is used by the TOE to verify digital signatures of the cardholder. This object is named PK.CH.DS in [DIN].

In accordance to the definition of the object **O2 SigG signature private key(s) of the cardholder** (see also the definition of **O2**!), the cardholder can have one or **multiple SigG signing key pairs** (see section 3.2.3 Intended method of use) and thus there can be multiple SigG signature public keys.**O12** is defined as the set of all SigG signature public keys of the cardholder that have already been generated:

$$\mathbf{O12} := \{PK_i.CH.DS \mid 1 \le i \le n\},$$

where $n \le m$, m as in the definition of **O2**.

If an additional key pair (SK_i.CH.DS, PK_i.CH.DS) is generated, its public key PK_i.CH.DS becomes part of the set **O12**[23].

The term "**use for signature verification**" of object **O12** means calling and performing the respective command for selecting the desired SigG signing key pair and then calling and performing the respective command to verify the cardholder's digital signature. Only those SigG signing public keys can be used for signature verification, that have already been generated.

To **read** to the **O12** means to use the respective command of the TOE to transmit a public key header and public key body inside the object **O12** to the IFD. Optionally the public key export can be secured by a signature with a secret key (secure public key export).

The term "**generate"** the **O12** means to use the respective command of the TOE to generate a SigG signing key pair (SK_i.CH.DS, PK_i.CH.DS) ($1 \le i \le m$) of the cardholder **S1** and to store the public key PK_i.CH.DS in object **O12** in the TOE (see also the definition of "generate" for object **O2**!). By generating of the each element *i* of the set O12, the TOE enters the (first or re-)personalisation phase for the corresponding SigG signing key pair *i*.

3.3.2 Informal Description

3.3.2.1 Identification and Authentication

IA1 Authentication of human user

The SEF **IA1** contains four sub-functions: IA1.1 (i.e. IA1.1.1 and IA1.1.2; remark of the certifier), IA1.2 and IA1.3

---

23 If we want to formulate a statement where an arbitrary SigG signature public key PK_i.CH.DS chosen by the cardholder is used, then we will use the notation PK.CH.DS to stand for this arbitrary PK_i.CH.DS chosen by the cardholder.

(1) SEF IA1.1 authenticates the **S1** “Cardholder”,

(2) SEF IA1.2 assumes the default identity **S2** “Somebody”,

(3) SEF IA1.3 detects **S7** “Potential attacker”.

ad (1): The TOE will contain an authentication function SEF IA1.1 that detects the **S1** “Cardholder” in two different ways: (a) by PIN and (b) by PUK.

(a) The SEF IA1.1.1 allows the S1 “Cardholder” to authenticate himself for the SigG application presenting the verification data. If the number of consecutive failed authentication attempts with reference data does not exceed the maximum number of allowed failed authentication attempts (RC_{PIN}>0), the SEF IA1.1.1 will verify the verification data by means of O3 “SigG cardholder reference data” (PIN) using the mechanism M1 defined in paragraph 3.5.1. If the number of consecutive failed authentication attempts with reference data (PIN) exceeds the maximum number of allowed failed authentication attempts (RC_{PIN}=0) the authentication attempt fails (independently of the presented verification data). Successful authentication of the cardholder is defined as SRE5 “Successful cardholder authentication”. A failure of the authentication attempt as the cardholder is defined as SRE6 “cardholder authentication failure” or **SRE7** “Repeated authentication failure”, depending on the value of RC_{PIN}. The SEF IA1.1.1 uses the mechanism M1 described in section 3.5.1.

(b) The SEF IA1.1.2 allows the S1 “Cardholder” to authenticate himself for the SigG application presenting data as reset code. The presented data is verified by means of O4 “SigG cardholder reset code”. If the presented data matches O4 “SigG cardholder reset code” and the retry of authentication by presenting the reset code is still allowed (RC_{PUK}>0) then this will be interpreted as SRE11 “Cardholder authenticated by reset code”. If the presented data does not match O4 “SigG cardholder reset code” or the retry of authentication by presenting the reset code is not allowed (RC_{PUK}=0) then this will be interpreted as SRE12 “Cardholder authentication by reset code failed”. The SEF IA1.1.2 uses the mechanism M4 described in section 3.5.4.

ad (2): The TOE assumes for the SigG application the default identity of the human user **S2** “Somebody” after the following SRE: **SRE1** “Resetting of the ICC”, **SRE2** “Deactivation of the ICC”, **SRE3** “Opening of the SigG application”, **SRE4** “Closing of the SigG application”, **SRE6** “Cardholder authentication failure”, **SRE7** “Repeated authentication failure”, **SRE8** "Authentication expiration" and **SRE12** “Cardholder authentication by reset code failed”. This SEF IA1.2 uses the mechanism M1 defined in paragraph 3.5.1.

ad (3): If a **SRE10** Potential security violation occurred, the TOE will assume the **S7** Potential attacker as the human user of the ICC. (If the ICC has been terminated, it is intended not to be used anymore.) This SEF IA1.3 uses the mechanism **M7** defined in paragraph 3.5.7.

IA2 Changing reference data

The TOE will contain an authentication function SEF **IA2** that permits the cardholder **S1** “Cardholder” to change his or her **O3** “SigG cardholder reference data”. The cardholder changes the reference data by means of SEF IA2 (i) presenting the verification data matching the actual **O3** “SigG cardholder reference data” and (ii) defining the new **O3** “SigG cardholder reference data” using the mechanism M2 defined in paragraph 3.5.2. The SEF IA2 permits the change of SigG cardholder reference data only after successful authentication of the cardholder defined as **SRE5** Successful cardholder authentication[24]. A failure of the authentication attempt as the cardholder is defined as **SRE6** “Cardholder authentication failure” (if RC_{PIN}>0) or **SRE7** “Repeated authentication failure” (if RC_{PIN}=0).

IA3 Blocking the reference data

This TOE contains a SEF **IA3** that will prevent the subject **S2** Somebody to use of object **O3** SigG cardholder reference data after **SRE7** Repeated authentication failure using the mechanism M3 defined in paragraph 3.5.3.

IA4 Unblocking and changing the reference data

The SEF **IA4** permits the successfully authenticated cardholder **S1** with the reference data matching the cardholder reset code (PUK) **O4** (i) to unblock the cardholder reference data (PIN) **O3** and (ii) to modify the PIN **O3** using the mechanism M4 defined in paragraph 3.5.4. The successful authentication of the cardholder with PUK **O4** is defined as **SRE11**. This will in addition (i) reset the retry counter RC_{PUK} for the PUK **O4** and (ii) perform the cardholder authentication by PUK **O4** (see also **IA1**). The unsuccessful authentication of the cardholder with PUK **O4** is defined as **SRE12**. Repeated unsuccessful authentication of the cardholder with PUK **O4** leads to RC_{PUK}=0 and the blocking of the SEF IA4. Note that in the case RC_{PUK}=0 it is still possible to have RC_{PIN}>0.

3.3.2.2 Access Control

AC1 Access control of commands

The SEF **AC1** contains the sub-function AC1.1 (to conform with the [GST_098]):

SEF AC1.1 will control the access of the subjects **S1**, **S2** and **S7** representing a human user.

---

24 Note: The authentication data used for **IA2** is the same as that used for **IA1.1.1** (namely the PIN **O3**). After the cardholder has successfully changed his PIN, he is authenticated as cardholder **S1** and can also generate digital signatures.

The SEF AC1.1 will **permit** that the subjects *s* access the object *o* by the access-type acy(*s*,*o*) defined in the Table 8. The SEF AC1.1 will **prevent** that the subjects *s* access the object *o* by the access-type acn(*s*,*o*) defined in the Table 9.

The SEF AC1 uses the mechanism M6 defined in paragraph 3.5.6.

Note that these access-sets concern a requested access and do not guarantee the possibility of an access request. This does not contradict the security policy because the reliability of service is not a security objective of the TOE.

Note that these access-sets are defined for the operational phase and the re-personalisation phase only.

The access-type "extract" is prevented by **AC2** for all subjects and not mentioned here.

Note that the TOE recognises the subject Potential attacker **S7** only if the TOE is in its permanent blocking state (TERMINATE state) **CAS6** (see the definition of **S7** in section 3.3.1.1). Thus **S7** is only listed to complete Table 8, further description is given in **AC3**[25]. The TOE will detect the subject **S7** “Potential attacker” if the **SRE10** Potential security violation has occurred.

The formal model of security policy [FMSP] and the underlying security policy both permit to open and to close the SigG application in the **CAS6**, because the TOE may be operational in **CAS6** – but this is not the case for this TOE (see also the definition of **CAS6** in 3.4.1). Since TOE does not permit even to open or close the SigG application, this adds even more security to the TOE.

This security target **does not cover the privileged IFD** authenticated with RoleID=02 defined in [DIN], annex C. Therefore the TOE does not allow to modify or supplement the objects **O6** and **O7**.

Table 8: Access-set acy(*s*,*o*) of SEF AC1.1 (permit-table)

Object		**S1** Cardholder	**S2** Somebody	**S7** Potential attacker
O1	SigG application	open, close	open, close	-
O2	SigG private signature key(s) of the	use for signa-ture generation,	-	-

[25] If the TOE is in its TERMINATE state **CAS6**, caused by the command TERMINATE CARD USAGE, the TOE is non-operational at all, besides the functionalities recognising of the TERMINATE state and doing it apparent for the IFD.

Object		S1 Cardholder	S2 Somebody	S7 Potential attacker
	cardholder	generate		
O3	SigG cardholder reference data (PIN)	modify, block, unblock	use for cardholder authentication, block	-
O4	SigG cardholder reset code (PUK)	-	use for authentication, block	-
O5	SigG signature key certificate(s) of the cardholder	read, use for signature verification, supplement	read, use for signature verification	-
O6	SigG public key of the root certification authority	read, use for signature verification	read, use for signature verification	-
O7	Other credentials for signature verification	read, use for signature verification	read, use for signature verification	-
O12	SigG public key(s) of the cardholder	read, use for signature verification, generate	use for signature verification, read	-

Table 9: Access-set acn(*s*,*o*) of SEF AC1.1 (prevent-table)

Object		S1 Cardholder	S2 Somebody	S7 Potential attacker
O1	SigG application	-	-	open, close
O2	SigG private signature key(s) of the cardholder	-	generate, use for signature generation	generate, use for signature generation
O3	SigG cardholder reference data (PIN)	use for cardholder authentication	modify, unblock	use for cardholder authentication, modify, block, unblock
O4	SigG cardholder reset code (PUK)	use for authentication, block	-	use for authentication, block

Object		**S1** Cardholder	**S2** Somebody	**S7** Potential attacker
O5	SigG signature key certificate(s) of the cardholder	-	supplement	read, supplement, use for signature verification
O6	SigG public key of the root certification authority	modify	modify	read, modify, use for signature verification
O7	Other credentials for signature verification	modify, supplement	modify, supplement,	read, modify, supplement, use for signature verification
O12	SigG public signature key(s) of the cardholder	-	generate	generate, use for signature verifica-tion, read

AC2 Access control of extraction

The SEF **AC2** will prevent the extraction of the SigG private signature key(s) **O2** of the cardholder. The SEF AC2 uses the mechanism M5 defined in paragraph 3.5.5.

The cardholder may use his signing private key(s) for generation of digital signatures performed by the TOE.

In order to prevent any disclosure or modification of the cardholder's private key the TOE never allows any access to that data except for its implicit use within the SigG security functions as specified by those functions. This includes also the prevention of any sort of inference of the private key by observing the TOE's behaviour while generating a digital signature.

The operating system only can access the file ISF_SigG, which stores the private signature key(s) of the cardholder SK_i.CH.DS.

During a usage (e.g. during the generation of signatures) the relevant private signature key of the cardholder is being protected against Differential Power Analysis (DPA). Besides, the relevant private signature key of the cardholder is being protected against Simple Power Analysis (SPA) during its generation.

AC3 Blocking state

The SEF **AC3** prevents a Potential attacker **S7** from using any functionality of the TOE (besides recognising of the TERMINATE state, switching into the state **CAS6** as well as **AU1**). The SEF AC3 uses the mechanism M7 defined in paragraph 3.5.7.

Somebody **S2** can submit the TERMINATE CARD USAGE command that blocks the ICC completely and permanently (**CAS6**), besides generating and sending a modified ATR. The TOE checks for being in its blocking state **CAS6** at every start-up (after the ICC is powered up or a hardware reset signal is given to the ICC) – see **SRE10**. If the **SRE10** has occurred, the TOE will react appropriate by entering an endless loop that prevents the execution of any other command.

3.3.2.3 Audit

AU1 Information about secure blocking state

The SEF **AU1** will inform the human user about the secure blocking state **CAS6** of the TOE by means of a blocking information (modified ATR) that the ICC is completely disabled (besides recognising of the TERMINATE state and **AU1** itself).

(i) If the **SRE10** (i) has occurred, the TOE will enter an endless loop and will not process any further commands. The IFD knows that it has sent the TERMINATE CARD USAGE command and thus knows from the behaviour of the TOE that it is in its permanent blocking state.

(ii) If the **SRE10** (ii) has occurred, the TOE will react appropriate by sending a modified ATR to the IFD.

The SEF AU1 will use the mechanism **M14** defined in paragraph 3.5.13.

AU2 Information about blocked CH authentication

The SEF **AU2** will inform the IFD about the fact that the cardholder (CH) authentication by

(AU2.1) reference data (PIN **O3**) or by

(AU2.2) reset code (PUK **O4**)

is blocked by means of a corresponding return code to the command. SEF (AU2.1) uses the mechanism M12 defined in paragraph 3.5.11 (Return Code for VERIFY), SEF (AU2.2) uses mechanism M13 defined in paragraph 3.5.12 (Return Code for VERIFY AND CHANGE).

Note that, according to (AE4.2) (6), the SigG compliant IFD shall inform the cardholder about the blocked authentication function.

3.3.2.4 Object Reuse

The SEF **OR1** will clear the cardholder's private signing key(s) SK.CH.DS (**O2**), the PIN **O3** and the PUK **O4** from temporary used storage areas in any case before the action of closing the SigG application caused by **SRE4** will be finished. The SEF **OR1** will use the mechanism M9 defined in paragraph 3.5.8.

The “temporary used storage areas” is the whole part of the XRAM which is used to save the temporary data including the buffered objects O2, O3 and O4. The TOE will actively overwrite this area of memory. All temporary data are thereby lost.

3.3.2.5 Data Exchange

DX1 Key Generation and Export

The SEF **DX1** consists of two sub-functions, DX1.1 and DX1.2:

The **SEF DX1.1 Key generation** is used to generate asymmetric key pairs. SEF DX1.1 can be used to generate SigG signing key pairs (SK_i.CH.DS, PK_i.CH.DS) as well as the key pair (SK.ICC.AUT, PK.ICC.AUT). In a first step the key header is written, specifying the attributes of the key, including its allowed usage (digital signature creation or device authentication), the algorithm (RSA), and the modulus length of the key pair (1024 bit). In a second step the key body is generated.

The SEF **DX1.1** generates the cardholder’s signature key pair(s) (SK_i.CH.DS, PK_i.CH.DS) on the ICC whereby $1 \leq i \leq m$ and *m* is the maximum number of signing key pairs that can be stored within the TOE. A cardholder’s signature key pair consists of the SigG private signature key of the cardholder (SK_i.CH.DS, part of **O2**) and the SigG public key of the cardholder (PK_i.CH.DS, part of **O12**). It is possible for the cardholder to have only one signature key pair or to have multiple key pairs.

The execution of the DX1 means the beginning of the (first or re-)personalisation phase for the key pair *i* (SK_i.CH.DS, PK_i.CH.DS) which is about to be generated. The TOE remains in the personalisation phase for this key pair *i* until the CA generates the signature key certificate C_i.CH.DS over the new public signing key (PK_i.CH.DS) of the cardholder. After the corresponding signature key certificate C_i.CH.DS has been generated by the CA, the personalisation phase for this key pair (SK_i.CH.DS, PK_i.CH.DS) is over and the operational usage phase for it begins. The new key pair will be added to the TOE and the key pair(s) which are already on the ICC will continue to exist (see sect. 3.2.3.6). It is not allowed to replace any existing key pair. The number *m* of key pairs, which can be generated, has been specified by the card manufacturer during the generation of the TOE (in the initialisation phase).

In order to distinguish different signing key pairs, the SEF DX1 will use a parameter *i*, where $1 \leq i \leq m$ and *m* is the number of signing key pairs.

The security requirements arise from the operational usage of the TOE. This also leads to requirements on the TOE’s functionality “Generation of a SigG signing key pair”, which has an essential effect on the secure operation of the TOE in the operational usage phase. On the other hand the security enforcing function DX1 is used per definitionem only in a personalisation phase (see sect. 3.2.3.6). The SEF DX1 implements the security objective **SO6** and has an essential effect on the secure operation of the TOE in the operational usage phase. Because of that the inclusion of the SEF DX1 into Security Target is easily to justify.

The SEF DX1.1 is implemented using the mechanism **M10** defined in paragraph 3.5.9.

The **SEF DX1.2 Read Public Key** allows to read out a public key (key header and key body). This function can be used to read out PK.ICC.AUT and PK_i.CH.DS signed with SK.ICC.AUT (secure public key export). The SEF DX1.2 is implemented using the mechanisms M15 and **M11** defined in paragraphs 3.5.14 and 3.5.10, respectively.

DX2 Digital signature generation

The cardholder generates a digital signature (using one of his SigG private signature key(s) SK.CH.DS) for data transmitted to the TOE by means of the SEF **DX2**. The TOE returns the digital signature to the IFD. If the TOE contains more than one signing key pair, the cardholder has to choose a private signature key (security environment) with which he will sign. The cardholder only is allowed to execute the SEF DX2. Depending on the configuration of the TOE (see section 3.2.2), after a successful authentication, the TOE allows to generate (i) only one digital signature in case of limited signature generation configuration or (ii) an unlimited number of digital signatures in case of unlimited signature generation configuration within the current session[26]. In case of limited signature generation configuration of the TOE the SEF DX2 will generate **SRE8** "Authentication expiration" after generation of a digital signature.

The TOE supports three ways of hashing the message to be signed: The IT system (i) transforms the message text into the hash-value and transmits the hash-value to the TOE, (ii) calculates an intermediate hash-value of the message text and transmits the remaining message text and the intermediate hash-value to the TOE, or (iii) transmits the complete message text to be hashed to the TOE.

The SEF DX2 uses the mechanism M11 defined in paragraph 3.5.10.

3.3.3 Semiformal specification of the security functions

3.3.3.1 Identification and Authentication

Construction	Security claim
Action Phrase: This TOE contains a *function* that *will detect ...* after *security relevant event* using the mechanism defined in paragraph *n* **Target Phrase**: 3 ... the identity of the *{user, process}* requesting a *process* **Substitution**: *function* = SEF IA1.1.1	The TOE contains a SEF IA1.1.1 that will detect the identity of the subject **S1** “Cardholder” requesting a SigG application after **SRE5** “Successful cardholder authentication” using the mechanism defined in paragraph 3.5.1. Note that the SigG application as process in this context means the usage of all

26 Note: Once the cardholder is authenticated, he can change the private signature key (security environment) used for the generation of his next (in limited signature generation configuration) or of his further (in unlimited signature generation configuration) digital signatures. The cardholder does not have to re-authenticate after changing the security environment.

Construction	**Security claim**
{user, process} = **S1** Cardholder *process* = SigG application *security relevant event* = **SRE5** Successful cardholder authentication *n* = 3.5.1	objects accessible within the opened SigG application.
Action Phrase: This TOE contains a *function* that *will detect ...* after *security relevant event* using the mechanism defined in paragraph *n* **Target Phrase**: 3 ... the identity of the *{user, process}* requesting a *process* **Substitution**: *Function* = SEF IA1.1.2 *{user, process}* = **S1** Cardholder *process* = SigG application *security relevant event* = **SRE11** Cardholder authenticated by reset code *n* = 3.5.4	The TOE contains a SEF IA1.1.2 that will detect the identity of the subject **S1** “Cardholder” requesting a SigG application after **SRE11** “Cardholder authenticated by reset code” using the mechanism defined in paragraph 3.5.4. Note that the SigG application as process in this context means the usage of all objects accessible within the opened SigG application.
Action Phrase: This TOE contains a *function* that *will detect ...* after *security relevant event* using the mechanism defined in paragraph *n* **Target Phrase**: 3 ... the identity of the *{user, process}* requesting a *process* **Substitution**: *Function* = SEF IA1.2 *{user, process}* = **S2** Somebody *process* = SigG application *security relevant event* = **SRE1** Resetting of the ICC, **SRE2** Deactivation of the ICC, **SRE3** Opening of the SigG application, **SRE4** Closing of the SigG application, **SRE6** Cardholder authentication failure, **SRE7** Repeated authentication failure, and **SRE12** Cardholder authentication by reset code failed *n* = 3.5.1	The TOE contains a SEF IA1.2 that will detect the identity of the subject **S2** “Somebody” requesting a SigG application after **SRE1** “Resetting of the ICC”, **SRE2** “Deactivation of the ICC”, **SRE3** “Opening of the SigG application”, **SRE4** “Closing of the SigG application”, **SRE6** “Cardholder authentication failure”, **SRE7** “Repeated authentication failure”, **SRE8** "Authentication expiration" and **SRE12** “Cardholder authentication by reset code failed” using the mechanism defined in paragraph 3.5.1.
Action Phrase: This TOE contains a *function* that *will detect ...* after *security relevant event*	The TOE contains a SEF IA1.3 that will detect the identity of the subject **S7** “Potential attacker” requesting an

Construction	Security claim
using the mechanism defined in paragraph *n*. **Target Phrase**: 3 ... the identity of the *{user, process}* requesting a *process* **Substitution**: *Function* = SEF IA1.3 *{user, process}* = **S7** Potential attacker *process* = activation of the ICC *security relevant event* = **SRE10** Potential security violation occurred *n* = 3.5.7	activation of the ICC after **SRE10** "Potential security violation occurred" using the mechanism defined in paragraph 3.5.7.
Action Phrase: This TOE contains a function that will permit ... after security relevant event using the mechanism defined in paragraph *n*. **Target Phrase:** 13... the *access-set* of an *object* **Substitution:** *Function* = SEF IA2 *Access-set* = S1 Cardholder, modify *Object* = object O3 SigG cardholder reference data *Security relevant event* = SRE5 Successful cardholder authentication *n* = 3.5.2	This TOE contains a SEF IA2 that will permit the subject S1 "Cardholder" to modify an object O3 "SigG cardholder reference data" after SRE5 "Successful cardholder authentication" using the mechanism defined in paragraph 3.5.2.
Action Phrase: This TOE contains a *function* that *will prevent ...* after *security relevant event* using the mechanism defined in paragraph *n* **Target Phrase:** 13 ... the *access-set* of an *object* **Substitution:** *Function* = SEF IA3 *Access-set* = S1 Cardholder, **S2** Somebody; use for cardholder authentication *Object* = **O3** SigG cardholder reference data *Security relevant event* = **SRE7** Repeated authentication failure *n* = 3.5.3	The TOE contains a function SEF IA3 that will prevent the use for cardholder authentication of the object **O3** "SigG cardholder reference data" by the **S2** "Somebody" after **SRE7** "Repeated authentication failure" using the mechanism defined in paragraph 3.5.3.

Construction	Security claim
Action Phrase: This TOE contains a *function* that *will permit* ... after *security relevant event* using the mechanism defined in paragraph *n* **Target Phrase** 13 ... the *access-set* of an *object* **Substitution:** *Function* = SEF IA4.1 *Access-set* = subject **S1** Cardholder, unblock *Object* = object **O3** SigG cardholder reference data *Security relevant event* = **SRE11** Cardholder authenticated by reset code *n* = 3.5.4	This TOE contains a SEF IA4.1 that will permit a subject **S1** "Cardholder" to unblock an object **O3** "SigG cardholder reference data" after **SRE11** "Cardholder authenticated by reset code" using the mechanism defined in paragraph 3.5.4.
Action Phrase: This TOE contains a *function* that *will permit* ... after *security relevant event* using the mechanism defined in paragraph *n* **Target Phrase** 13 ... the *access-set* of an *object* **Substitution:** *Function* = SEF IA4.2 *Access-set* = **S1** Cardholder, modify *Object* = **O3** SigG cardholder reference data *Security relevant event* = **SRE11** Cardholder authenticated by reset code *n* = 3.5.4	This TOE contains a SEF IA4.2 that will permit the subject **S1** "Cardholder" to modify the object **O3** "SigG cardholder reference data" after **SRE11** "Cardholder authenticated by reset code" using the mechanism defined in paragraph 3.5.4.

3.3.3.2 Access Control

Construction	Security claim
Action Phrase: This TOE contains a *function* that *will permit ...* using the mechanism defined in paragraph *n* **Target Phrase:** 12 ... the access-set of a *{user,process}* **Substitution:** *Function* SEF AC1.1 *Access set* acy(*s*,*o*)	This TOE contains a SEF AC1.1 that will permit the access-set acy(*s*,*o*) of a subject *s* (human user) using the mechanism defined in paragraph 3.5.6. Note that for each subject **S1**, **S2** and **S7** the access-set acy(*s*,*o*) lists the allowed access-types to an object *o*, where *o* stands for an O1 to O12 in Table 8.

Construction	Security claim
{user,process} subject *s* *n* 3.5.6	
Action Phrase: This TOE contains a *function* that *will prevent* ... using the mechanism defined in paragraph *n* **Target Phrase:** 12 ... the *access-set* of a *{user,process}* **Substitution:** *function* SEF AC1.1 *access set* acn(*s*,*o*) *{user,process}* subject *s* *n* 3.5.6	This TOE contains a SEF AC1.1 that will prevent the access-set acn(*s*,*o*) of a subject *s* (human user) using the mechanism defined in paragraph 3.5.6. Note that for each subject **S1**, **S2** and **S7** the access-set acn(*s*,*o*) lists the access-types which are not allowed to an object *o*, where *o* stands for an O1 to O12 in Table 9.
Action Phrase: This TOE contains a *function* that *will prevent* the ... using the mechanism defined in paragraph *n* **Target Phrase:** 13 ... the *access-set* of an *object* **Substitution:** *function* SEF AC2 *access set* **S1** Cardholder, **S2** Somebody, **S3** IFD, **S7** Potential attacker; extract *object* **O2** SigG private signature key(s) of the cardholder *n* 3.5.5	This TOE contains a SEF AC2 that will prevent the **S1** “Cardholder”, **S2** “Somebody”, **S3** “IFD”, **S7** “Potential attacker” to extract of the **O2** “SigG private signature key(s) of the cardholder” using the mechanism defined in paragraph 3.5.5.
Action Phrase: This TOE contains a *function* that *will prevent* the ... using the mechanism defined in paragraph *n* **Target Phrase:** 13 ... the *access-set* of an *object* **Substitution:** *function* SEF AC3 *access set* **S7** Potential attacker; open *object* **O1** SigG application *n* 3.5.6	This TOE contains a SEF AC3 that will prevent the **S7** “Potential attacker” to open an object **O1** “SigG application” using the mechanism defined in paragraph 3.5.6.

3.3.3.3 Audit

Construction	Security claim
Action Phrase: This TOE contains a *function* that *will ensure* **Target Phrase:** 1 ... *audit-information* concerning *security-relevant-events* **Substitution:** *function* = SEF **AU1** *audit-information* = blocking information *security-relevant-events* = **SRE10**	This TOE contains a SEF **AU1** that will ensure blocking information concerning **SRE10**. **Note:** The SEF AU1 uses the mechanism M14 described in 3.5.13
Action Phrase: This TOE contains a *function* that *will ensure* **Target Phrase:** 1 ... *audit-information* concerning *security-relevant-events* **Substitution:** *function* = SEF AU2.1 *audit-information* = return code *security-relevant-events* = **SRE7**	This TOE contains a SEF AU2.1 that will ensure the return code concerning **SRE7**. **Note:** The SEF AU2.1 uses the mechanism M12 described in 3.5.11.
Action Phrase: This TOE contains a *function* that *will ensure* **Target Phrase:** 1 ... *audit-information* concerning *security-relevant-events* **Substitution:** *function* = SEF AU2.2 *audit-information* = return code *security-relevant-events* = **SRE12** with RC_{PUK}=0	This TOE contains a SEF AU2.2 that will ensure the return code concerning **SRE12** with RC_{PUK}=0. **Note:** If **SRE12** occurs and RC_{PUK}=0, then the cardholder authentication by reset code is permanently disabled. The SEF AU2.2 uses the mechanism M13 described in 3.5.12.

3.3.3.4 Object Reuse

Construction	Security claim
Action Phrase: The TOE contains a *function* that *will ensure* ... before *security-relevant-event* using the mechanism defined in paragraph *n*. **Target Phrase:** 21: clearing of information from an *object*. **Substitution:** *function* = SEF **OR1** *security-relevant-event* = **SRE4** *object* = temporary used storage areas *n* = 3.5.8	The TOE contains a SEF **OR1** that will ensure the clearing of information before **SRE4** from temporary used storage areas using the mechanism defined in paragraph 3.5.8. **Notes:** the “temporary used storage areas” is the whole part of the XRAM, which is used to save the temporary data incl. the buffered cardholder’s signing private key(s) **O2**.

3.3.3.5 Data Exchange

Construction	Security claim
Action Phrase: The TOE contains a *function* that *will permit* ... **Target Phrase:** 13... the *access-set* of an *object* **Substitution:** *function* SEF **DX1.1** *access-set* **S1** Cardholder, generate *object* **O2** SigG private signature key(s) of the cardholder, **O12** SigG public key(s) of the cardholder	The TOE contains a SEF **DX1.1** that will permit the subject **S1** “Cardholder” to generate an element of the object **O2** “SigG private signature key(s) of the cardholder” and **O12** “SigG public signature key(s) of the cardholder” as specified by the parameter *i*. **Notes:** The corresponding elements of the objects **O2** “SigG private signature key(s) of the cardholder” and **O12** “SigG public key(s) of the cardholder” can be generated only together, only once and only in the (first or re-) personalisation phase of the TOE. The SEF **DX1.1** uses a parameter *i* indicating which element of the object **O2** (i.e. which SigG signing key pair) is to be generated. The SEF **DX1.1** uses the mechanism

Construction	Security claim
	defined in paragraph 3.5.9.
Action Phrase: The TOE contains a *function* that *will permit* ... **Target Phrase:** 13... the *access-set* of an *object* **Substitution:** *function* SEF **DX1.2** *access-set* **S2** Somebody, read *object* **O12** SigG public key(s) of the cardholder	The TOE contains a SEF **DX1.2** that will permit the subject **S2** "Somebody" to read an element of the object **O12** "SigG public signature key(s) of the cardholder" as specified by the parameter *i*. The SEF **DX1.2** uses the mechanisms defined in paragraphs 3.5.14 and 3.5.10.
Action Phrase: The TOE contains a *function* that *will permit* ... **Target Phrase:** 13 ... the *access-set* of an *object* **Substitution:** *function* SEF **DX2** *access-set* **S1** Cardholder, use for signature generation *object* **O2** SigG private signature key(s) of the cardholder	The TOE in <u>unlimited signature generation configuration</u> contains a SEF **DX2** that will permit **S1** "Cardholder" to use for signature generation an element of the object **O2** "SigG private signature key(s) of the cardholder". **Note:** The SEF **DX2** uses the mechanism defined in paragraph 3.5.10. The SEF **DX2** uses a parameter *i* indicating which element of the object **O2** (i.e. which SigG signing private key) shall be used to generate the signature. In unlimited signature generation configuration the TOE does not generate **SRE8** at all.
Action Phrase: The TOE contains a *function* that *will permit* ... before *security-relevant-event* **Target Phrase:** 13 ... the *access-set* of an *object* **Substitution:** *function* SEF **DX2** *access-set* **S1** Cardholder, use for signature	The TOE in <u>limited signature generation configuration</u> contains a SEF **DX2** that will permit **S1** "Cardholder" to use for signature generation an element of the object **O2** "SigG private signature key(s) of the cardholder" before **SRE8**. Note: ▪ The SEF **DX2** uses the mechanism

Construction	Security claim
generation *object* **O2** SigG private signature key(s) of the cardholder *security-relevant-event* **SRE8**	defined in paragraph 3.5.10. ▪ The SEF **DX2** uses a parameter *i* indicating which element of the object **O2** (i.e. which SigG signing private key) shall be used to generate the signature. ▪ In limited signature generation configuration the TOE automatically generates **SRE8** after a digital signature has been generated.

3.4 Underlying Security Policy

The ITSEC [ITSEC] states in paragraph 2.81 that at evaluation levels E4 and above, a TOE must implement an underlying model of security policy, i.e. there must be an abstract statement of the important principles of security that the TOE will enforce. This shall be expressed in a formal style, as a formal model of security policy.

This security target refers to a Formal Model of Security Policy (FMSP) together with its Informal Interpretation of the FMSP. The Informal Interpretation of the FMSP and a reference to the FMSP are given in [InformInt] and [AddInformInt].

This Security Target provides the underlying security policy on the basis of the security objectives in section 3.2.6 and the security functions in chapter 3.3 and in accordance with [JIL]. The underlying security policy describes the security principles of the TOE's dynamic behaviour. Each time the TOE makes an assumption about the human user. This is expressed in the current authentication state and the rights the outside world has.

3.4.1 Security state

The **current internal state** is the tupel of (i) the **current authentication state *CAS*** reflecting the results of the authentication attempts of the subjects currently using the TOE, (ii) the retry counter RC_{PIN} and (iii) and the retry counter RC_{PUK}.

The **assumption about the subjects currently using the TOE** depends on (i) the currently selected application context and (ii) the results of the authentication attempts of human user.

The **retry counter for the reference data** RC_{PIN} (i) stores the number of remaining authentication attempts to present the verification data (PIN) **O3** after the last successful authentication attempt with the verification data[27] or (ii) will be equal to zero if the number of failed authentication attempts to present the verification data exceeds the maximum number of failed authentication attempts with the verification data allowed. The **reset retry counter** RC_{PUK} (i) stores the number of remaining authentication attempts[28] to present the reset code (PUK) **O4** or (ii) will be equal to zero if the number of failed authentication attempts with the reset code exceeds the maximum number of failed authentication attempts with reset code allowed. The retry counter for the reference data and the retry counter of the reset code are persistently stored in the TOE.

The following table identifies the different current authentication states described later on.

Table 10: Identification of different current authentication states

	Current authentication state
CAS1	Somebody using the TOE
CAS2	Somebody using the SigG application
CAS3	Cardholder using the SigG application
CAS6	A potential attacker / Card is TERMINATEd
CAS7	Somebody using the SigG application with blocked Cardholder reference data (PIN) O3

A human user is authenticated if (i) the human user has performed a successful authentication presenting the verification data defined for this subject and (ii) this authentication is not deemed as expired by the TOE for any reason.

The **current authentication state CAS1 Somebody using the TOE** represents the state of the TOE in which (i) the TOE is operational but the SigG application is currently not opened and (ii) the human user is not authenticated as **S1**. RC_{PIN} and RC_{PUK} can be any value (either zero or greater than zero).

There is a special kind of the state CAS1 – **$CAS1_{TCU}$**. This special state $CAS1_{TCU}$ means the state CAS1 for an already terminated TOE by the TERMINATE CARD USAGE command. If the TOE is already terminated and the ICC will be contacted (state $CAS1_{TCU}$), the TOE (yet before the ATR) will immediately recognise by event **SRE10**, that it was terminated and pass over in the state **CAS6**. In the state $CAS1_{TCU}$ the only event that is possible (besides reset and deactivate) and that will be automatically performed by the TOE – is the **SRE10**. I.e. the state $CAS1_{TCU}$ is a brief between-state after the

---

27 RC_{PIN} does this by counting the retries left for PIN **O3** entry. RC_{PIN} is initialised with the value 3 and decremented for each failed authentication attempt by PIN. If RC_{PIN}=0, the PIN is blocked.

28 RC_{PUK} for the PUK **O4** works analogous to RC_{PIN} for the PIN **O3**.

contacting of the ICC that will be at once left, so that the TOE can transit in the durable-state **CAS6**. CAS1$_{TCU}$ shall be considered as being a part of CAS1 that could also be identified with CAS1 without losing any security functionality, but which makes some descriptions easier to understand. For that reason, RC$_{PIN}$ and RC$_{PUK}$ can of course be also any value.

The **current authentication state CAS2 Somebody using the SigG application** represents the state of the TOE in which (i) the SigG application is currently opened and (ii) the human user is not authenticated as **S1**. In this case RC$_{PIN}$ is always greater than zero (RC$_{PIN}$>0); RC$_{PUK}$ can be any value (either zero or greater than zero).

The **current authentication state CAS3 Cardholder using an IFD** represents the state of the TOE in which (i) the SigG application is currently opened and (ii) the human user is authenticated as **S1**. In this case RC$_{PIN}$ is always greater than zero (RC$_{PIN}$>0), since successful authentication by PIN (**SRE5**) or PUK (**SRE11**) always implies that RC$_{PIN}$ is reset to its initial value (RC$_{PIN}$:=3); RC$_{PUK}$ can be any value (either zero or greater than zero).

The **current authentication state CAS6 Potential attacker** represents the secure **Blocking state of the TOE** in which the TOE has detected that it is in its terminated state and in which the command interface of the TOE is not operational (see SO8). No human user is successfully authenticated as well as no human user can successfully authenticate any more. The **CAS6** occurs after the TOE usage has been terminated completely (besides recognising the blocking state, generating and sending a modified ATR as well as automatically switching into the **CAS6**) with the command TERMINATE CARD USAGE (see also **SRE10**). The **CAS6** is the permanent blocking state of the TOE. RC$_{PIN}$ and RC$_{PUK}$ can be any value.

The **current authentication state CAS7 Somebody using the SigG application with blocked Cardholder reference data** represents the state of the TOE in which (i) the SigG application is currently opened, (ii) the human user is not authenticated as **S1** and (iii) the **O3** SigG cardholder reference data are blocked to use for cardholder authentication (RC$_{PIN}$=0). RC$_{PUK}$ can be any value (either zero or greater than zero).

The current authentication state will be set and changed by security relevant events as described by the following State Transition Table (see Table 11). The definition of the state transition is based on the SEF under the generic heading identification and authentication as described in sub-sections 3.3.2.1 and 3.3.3.1.

Remark on SRE3: The state transition in **CAS1** caused by **SRE3** depends on the value of the retry counter for the reference data. That's why the security relevant event SRE3 is divided into two security relevant events:

SRE3a: the security relevant event SRE3a "**Opening of the SigG application with unblocked reference data**" occurs if (i) no file of the SigG application has been selected before, (ii) a file in the SigG application directory is selected or a security environment of the SigG application directory is selected and (iii) the retry counter for the reference data allows authentication by presenting the verification data (i. e. the number of failed authentication attempts by presenting the verification data does not exceed the maximum number of failed authentication attempts with the verification data allowed; in other words the retry counter for the PIN is still greater than zero: $RC_{PIN}>0$).

SRE3b: the security relevant event SRE3b "**Opening of the SigG application with blocked reference data"** occurs if (i) no file of the SigG application has been selected before, (ii) a file in the SigG application directory is selected or a security environment of the SigG application directory is selected and (iii) the retry counter for the reference data does not allow authentication by presenting the verification data (i. e. the number of failed authentication attempts by presenting the verification data exceeds the maximum number of failed authentication attempts with the verification data allowed, $RC_{PIN}=0$).

Remark on unexpected SRE: Because of the definition of the CAS and the SRE, some security relevant events can not occur in specific CAS (e.g. in CAS7 the PIN is blocked, thus a successful authentication with PIN is *per definitionem* not possible).

Table 11: State transition table

	CAS1 Smb. → TOE	**$CAS1_{TCU}$** (CAS1 for an already terminated TOE)	**CAS2** Smb. → Sig. app.	**CAS3** CH → IFD	**CAS6** Secur. violation	**CAS7** Smb. → Sig. app. $RC_{PIN}=0$
SRE1	CAS1	$CAS1_{TCU}$	CAS1	CAS1	$CAS1_{TCU}$	CAS1
SRE2	CAS1	$CAS1_{TCU}$	CAS1	CAS1	$CAS1_{TCU}$	CAS1
SRE3a	CAS2	-	(CAS2)	(CAS2)	-	-
SRE3b	CAS7	-	(CAS7)	(CAS7)	-	(CAS7)
SRE4	(CAS1)	-	CAS1	CAS1	-	CAS1
SRE5	-	-	CAS3	CAS3	-	-
SRE6	-	-	CAS2	CAS2	-	-
SRE7	-	-	CAS7	CAS7	-	CAS7
SRE8	-	-	-	CAS2	-	-
SRE10	CAS6	CAS6	CAS6	CAS6	(CAS6)	CAS6
SRE11	-	-	CAS3	CAS3	-	CAS3
SRE12	-	-	CAS2	CAS2	-	CAS7

Comments to **Table 11**:
If the SRE*m* occurs in the CAS*n* then the CAS*n* is changed into the CAS shown in the row *m* and the column *n*.

Notation:

Smb.	Somebody **S2**,
CH	Cardholder **S1**,
A → B	means human user A uses IT-System B as short hint to the definition of the CAS,
RC_{PIN}	value of the retry counter for the PIN **O3**, where it is assumed that (i) the retry counter is set by **SRE5** and **SRE11** to the initial value, (ii) is decremented by **SRE6** and **SRE7** and (iii) if the number of failed authentication attempts to present the verification data exceeds the maximum number of failed authentication attempts with the verification data allowed then RC_{PIN}=0.
"-"	Because of the definition of the CAS and the SRE, the security relevant event defined for this row can not occur in this CAS. These state transitions are not shown in **Figure 2**.
(CASx)	The SRE defined for this row is not expected in the CAS defined for this column. These state transitions are not shown in **Figure 2**.

Figure 2 illustrates the state transition with exception of the security relevant events enclosed in brackets in Table 11: State transition table.

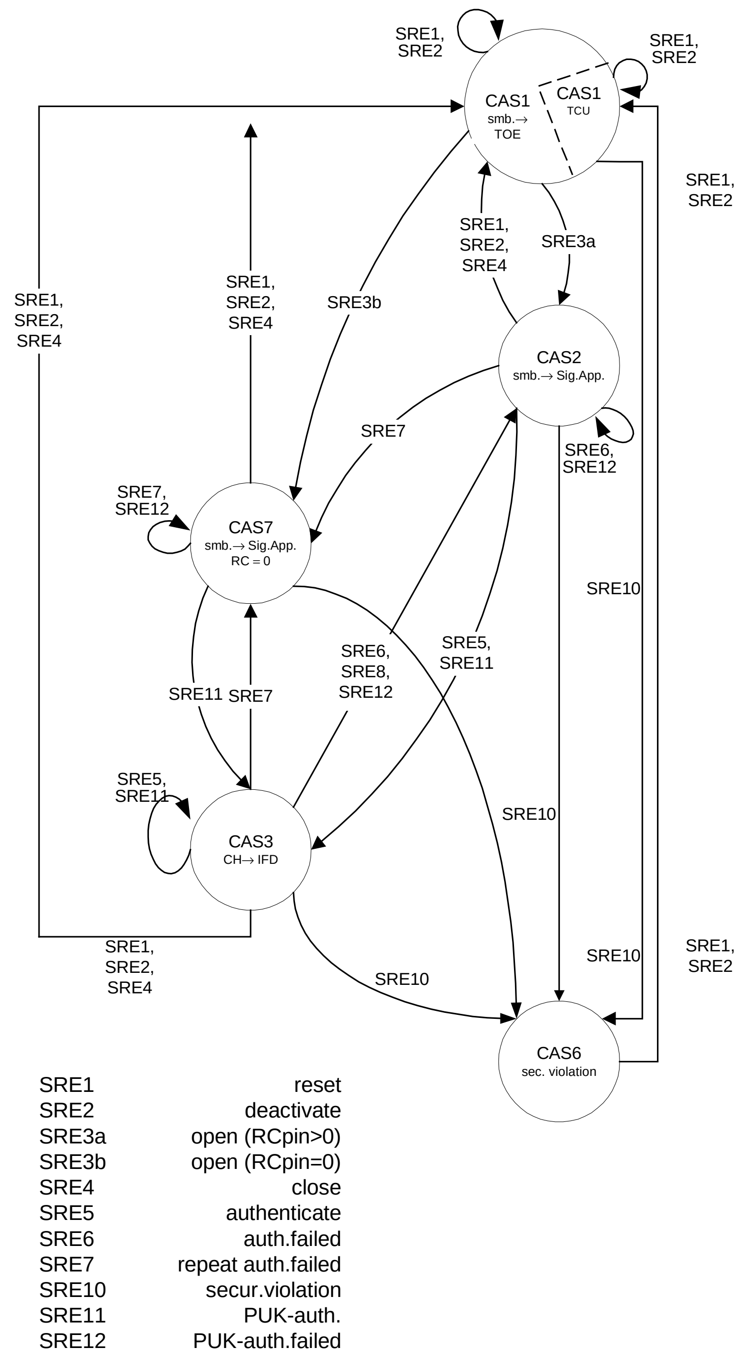

Figure 2: State transition diagram

3.4.2 Access control for command execution

The access control decisions take place within the command execution. Access control decisions are based on the type of object associated with the access type (see paragraph) 3.3.1.3 and the current authentication state.

The Table 12 and Table 13 define access-sets in terms of the security states:

(1) The TOE in the current authentication state in column *t* will permit the requested access-type ssy(*o*,*t*) to the object in the row *o*.

(2) The TOE in the current authentication state in column *t* will prevent the requested access-type ssn(*o*,*t*) to the object in the row *o*.

Note that these access-sets concern a requested access and do not guarantee the possibility of an access request. This does not contradict the security policy because the reliability of service is not a security objective of the TOE. If the **CAS6** is caused by the command TERMINATE CARD USAGE, the TOE is non-operational at all (besides recognising of blocking state, generating and sending of the appropriate ATR and automatically switching in the **CAS6**; see also **SRE10**).

Table 12: Access-sets ssy(*o*,*t*) defined in terms of the security states

	CAS1	**CAS2**	**CAS3**	**CAS6**	**CAS7**
O1	open, close	open, close	open, close		open, close
O2			use for signature generation, generate		
O3		use for cardholder authentication, block	modify, unblock		unblock
O4		use for authentication, block			use for authentication, block
O5		use for signature verification, read	use for signature verification, read, supplement		use for signature verification, read
O6		read, use for signature verification	read, use for signature verification		read, use for signature verification
O7		read, use for signature verification	read, use for signature verification		read, use for signature verification

	CAS1	CAS2	CAS3	CAS6	CAS7
O12		use for signature verification, read	use for signature verification, read, generate		use for signature verification, read

Note: If the TOE is in its TERMINATE state **CAS6**, the SigG application **O1** can neither be opened nor closed. In the formal model of security policy (FMSP) which applies to the [GST_098] as well as to this Security Target, in **CAS6** the Potential Attacker **S7** is also able to open and close the **O1**. Thus this TOE offers even more restrictive security, since it offers less functionality to the Potential Attacker S7 than the [GST_098].

Table 13: Access-sets ssn(*o*,*t*) defined in terms of the security states

	CAS1	CAS2	CAS3	CAS6	CAS7
O1				open, close	
O2	extract, generate, use for signature generation	extract, generate, use for signature generation	extract	extract, generate, use for signature generation	extract, generate, use for signature generation
O3	use for cardholder authentication, modify, block, unblock	modify, unblock	use for cardholder authentication, block	use for cardholder authentication, modify, block, unblock	use for cardholder authentication, modify, block
O4	use for authentication, block		use for authentication, block	use for authentication, block	
O5	supplement, read, use for signature verification	supplement		supplement, read, use for signature verification	supplement
O6	modify, read, use for signature verification	modify	modify	modify, read, use for signature verification	modify
O7	modify, supplement, read, use for signature verification	modify, supplement	modify, supplement	modify, supplement, read, use for signature verification	modify, supplement

	CAS1	CAS2	CAS3	CAS6	CAS7
O12	generate, use for signature verification, read	generate		generate, use for signature verification, read	generate

3.5 Security Mechanisms

The security functions specified in chapter 3.3 shall be implemented using the following mechanisms:

Table 14: Security mechanisms

ID	Mechanism
M1	Human user authentication (PIN)
M2	Change unblocked the reference data
M3	Locking of the reference data
M4	Unblocking and changing of the reference data
M5	Extraction resistance
M6	Access control for command execution
M7	Blocking state
M9	Clearing of memory
M10	SigG Signature key pair generation
M11	Signature generation
M12	Return Code for VERIFY
M13	Return Code for VERIFY AND CHANGE
M14	Modified ATR
M15	Public Key Export

3.5.1 M1: Human user authentication (PIN)

The human user authenticates himself using a knowledge-based authentication mechanism. The human user can choose the kind of authentication information and the mechanism he wants to use for authentication: (i) O3 “SigG cardholder reference data” with mechanism M1 or (ii) O4 “SigG cardholder reset code” with mechanism M4.

The human user using mechanism M1 presents his verification data (PIN (O3)) and the mechanism M1 compares the presented verification data with the stored reference data in the SigG application. Successful authentication of the cardholder with O3 “SigG cardholder reference data” is defined as **SRE5** “Successful cardholder authentication”. If an authentication attempt with O3 “SigG cardholder reference data” fails, the mechanism M3 will define whether the **SRE6** “Cardholder authentication failure” or **SRE7** “Repeated authentication failure” occurs.

In accordance with [DIN] the verification data (PIN) consists of a string of minimal 6, maximal 8 ASCII characters.

Note: The mechanism M7 will detect the S7 “Potential attacker”, if the TOE is in the Blocking state of the TOE. If the TOE is not in the Blocking state of the TOE, then the mechanism M1 will detect the default identity S2 “Somebody” until the cardholder is successfully authenticated.

3.5.2 M2: Change the unblocked reference data

The mechanism M2 implements the following security sub-functions by means of one command:

(1) authentication of the cardholder by knowledge of the verification data matching **O3** “SigG cardholder reference data” (old PIN),

(2) modification of the **O3** “SigG cardholder reference data” to the presented new string of characters (new PIN).

The command sent to the TOE contains (i) the verification data and (ii) a string of characters as new reference data of the cardholder.

The new reference data **O3** shall have a length of at least 6 characters. Note that mechanism M2 accepts old PINs with a length of only 5 characters, too.

If the RC_{PIN}=0 then **SRE7** will occur and the mechanism M2 will not change the **O3**. If the RC_{PIN} > 0 and the presented verification data matches **O3** “SigG cardholder reference data”, then (i) the retry counter RC_{PIN} (see mechanism M4) will be reset to the initial value (RC_{PIN}:=3), (ii) the presented string will be stored as new value of the **O3** “SigG cardholder reference data”. Successful authentication of the cardholder is defined as **SRE5** “Successful cardholder authentication”. If an authentication attempt fails the mechanism M3 will define whether the **SRE6** “Cardholder authentication failure” or **SRE7** “Repeated authentication failure” occurs.

3.5.3 M3: Locking of the reference data

The mechanism M3 implements the following security sub-functions:

(1) detection of **SRE7** “Repeated authentication failure“ by means of a retry counter RC_{PIN},

(2) blocking the **O3** SigG cardholder reference data (PIN) for the use for cardholder authentication.

An authentication attempt is any use of mechanism M1 or M2. The retry counter RC_{PIN} counts (going down from its initial value) the number of failed authentication attempts of the Cardholder **S1** after the last successful authentication attempt. The retry counter is equal to a fixed value RC_{PIN} =0, if the number of consecutive failed authentication attempts reaches or exceeds the maximum number of failed authentication attempts allowed (3). Each time a successful authentication takes place the retry counter is reset to a defined initial value =3.

If the authentication attempt has failed and the retry counter after this authentication attempt is not equal to 0, then this event is the **SRE6** “Cardholder authentication failure”. If the authentication attempt failed and the retry counter after this authentication attempt is equal to 0, then this event is the **SRE7** “Repeated authentication failure”.

The retry counter RC_{PIN} is persistently stored in the TOE and may be reset by mechanism M4.

If the **SRE7** “Repeated authentication failure” occurs, the **O3** “SigG cardholder reference data” (PIN) will be blocked for the use for cardholder authentication. This blocking is persistently stored in the TOE and may be reset by mechanism M4.

3.5.4 M4: Unblocking and changing of the reference data

The human user authenticates himself using a knowledge based authentication mechanism. The human user can choose the kind of authentication information and the mechanism he wants to use for authentication: (i) “SigG cardholder reference data” (PIN) **O3** with mechanism M1 or (ii) “SigG cardholder reset code” (PUK) **O4** with mechanism **M4**.

The mechanism M4 implements the following security sub-functions by means of one command:

(1) authentication of the cardholder by knowledge of the reset code matching **O4** “SigG cardholder reference reset code” (PUK),

(2) unblocking the **O3** “SigG cardholder reference data” (PIN) for the use for cardholder authentication,

(3) modifying the **O3** “SigG cardholder reference data” to the presented new string of characters.

If the mechanism M4 is used, then the command sent to the TOE will contain (i) a reset code and (ii) a string of characters as new reference data (PIN) of the cardholder.

The retry counter of the reset code RC_{PUK} will be checked by the TOE.

- If RC_{PUK} indicates that human user authentication by presenting the reset code is not allowed (RC_{PUK}=0, see **SRE12**), then the (i) authentication attempt will be rejected (independently whether the presented reset code PUK matches the reference reset code **O4** or not), (ii) the retry counter for the reference data (RC_{PIN}, see mechanism M3) will not be reset and (iii) the “SigG cardholder reference data” (PIN) **O3** will not be modified.

- If (a) RC_{PUK} indicates that human user authentication by presenting the reset code is still allowed (**RC_{PUK}>0**) and (b) the presented reset code **matches** “SigG cardholder reference reset code” (PUK) **O4**, then (i) the retry counters RC_{PIN} as well as RC_{PUK} will be reset to their initial values (=3), (ii) the “SigG cardholder reference data” (PIN) **O3** will be unblocked for the use for cardholder authentication, (iii) the presented string will be stored as new value of the “SigG cardholder reference data” (PIN) **O3** and (iv) the **SRE11 Cardholder authenticated by reset code** will occur. Thus after successful authentication M4 will always lead to a new value of the PIN **O3**.

- If (a) RC_{PUK} indicates that human user authentication by presenting the reset code is still allowed (**RC_{PUK}>0**) and (b) the presented reset code does **not match** “SigG cardholder reference reset code” (PUK) **O4**, then (i) the authentication failure with reset code is counted by decrementing the reset retry counter RC_{PUK} (see **SRE12**), (ii) the “SigG cardholder reference data” (PIN) **O3** will remain blocked for the use for cardholder authentication, and (iii) the “SigG cardholder reference data” (PIN) **O3** will not be changed.

  - If – after decrementing RC_{PUK} – the retry counter of the reset code RC_{PUK} indicates that human user authentication by presenting the reset code is not allowed any longer (e. g. the defined maximum number of authentication failure by presenting the reset code is exceeded, RC_{PUK}=0), then the cardholder authentication by reset code is permanently disabled.

Note: In the case RC_{PUK}=0, it is still possible for the cardholder to authenticate using the SigG cardholder reference data (PIN) **O3** if RC_{PIN}>0. But in case RC_{PUK}=0 the retry counter for the reset code RC_{PUK} can never be reset to its initial value and will remain zero (RC_{PUK}=0) for the rest of the ICC use.

3.5.5 M5: Extraction resistance

The TOE will implement security mechanisms to prevent extraction of the SigG private signature key of the cardholder as required for SEF **AC2**.

The operating system only can access the file ISF_SigG where the SigG private signature key(s) of the cardholder SK_i.CH.DS is stored.

The appropriate measures are implemented by the TOE, which provide the protection of the relevant SigG private signature key of the cardholder against Differential Power Analysis (DPA) during its using (i.e. during the generation of signatures). Besides, the relevant SigG private signature key of the cardholder is being protected against Simple Power Analysis (SPA) during its generation by the appropriate measures implemented by the TOE.

3.5.6 M6: Access control for command execution

The TOE shall implement security mechanisms as required for SEF **AC1**. According to the underlying security policy this mechanism shall

(1) implement a security state machine as described in section 3.4.1 and

(2) control the access as described in section 3.4.2.

The access control information is stored in the header of each file in the file system of the TOE. Besides the TOE contains a special subroutine to realise the security state machine as well as access control.

3.5.7 M7: Blocking state

The TOE will implement security mechanisms as required for SEF **AC3** and **IA1.3**.

The TOE enters the Blocking State **CAS6** after the successful execution of the command TERMINATE CARD USAGE given to the ICC. In the blocking state, the TOE is permanently and completely disabled, besides recognising of its blocking state, generating and sending a modified ATR and switching into the state **CAS6**, i.e. the other functionality of the TOE cannot be used anymore. See also **M14** in section 3.5.13.

3.5.8 M9: Clearing of memory

The TOE will implement security mechanisms as required for SEF **OR1**.

In order to clear the RAM, that contains the buffered cardholder's signing private key SK_i.CH.DS, the TOE fills the whole part of the XRAM, which is used to save the temporary data, with 0x00. All temporary data are thereby lost. This clearing of the part of the XRAM occurs immediately before the execution of the commands GENERATE PUBLIC KEY PAIR and PERFORM SECURITY OPERATION/COMPUTE SIGNATURE is completed.[29]

3.5.9 M10: Signature key pair generation

The TOE will implement security mechanisms as required for SEF DX1.1.

In order to generate the SigG signature key pair of the cardholder (an RSA key pair with a length of 1024 bit), the TOE implements a software pseudo random number generator which again uses input from a hardware random number generator and does a cryptographic subsequent treatment. This approach is described in [BA], section 1.4 (RSA) and 1.5 (Random number generation) and considered as being adequate. The TOE uses the Lehman test to check the primality of the random numbers.

---

29 Note, that these events take place in any case before **SRE4** has occured.

This mechanism M10 is also used to generate an RSA key pair (SK.ICC.AUT, PK.ICC.AUT) in the initialisation phase; this key pair has a length of 1024 bit.

3.5.10 M11: Signature generation

The TOE will implement security mechanisms as required for SEF **DX2** and **DX1**.

The TOE distinguishes between both types of operations – digital signature generation and secure public key export – by means of different ISO commands and input parameters.

In order to **generate a SigG compliant digital signature**, the TOE uses the SHA-1 hash algorithm and the RSA algorithm with a key-length of 1024 bit as described in [BA], section 1.3 (SHA-1) and 1.4 (RSA). Both RSA and SHA-1 are considered as being adequate. The TOE supports padding according to PKCS#1.0 Block Type 01 Version 1.5 and [DIN] based on ISO/IEC 9796-2.

In order to **read out a public key with a signature** (**secure public key export**, DX1.2), the TOE uses a similar algorithm, but the signature will be distinguishable from a digital signature through its format.

3.5.11 M12: Return Code for VERIFY

The TOE will implement a security mechanism as required for **(AU2.1)**. The VERIFY command will return a return code[30] indicating to the IFD and thus to the human user that the authentication by reference data (PIN **O3**) is blocked.

3.5.12 M13: Return Code for VERIFY AND CHANGE

The TOE will implement a security mechanism as required for **(AU2.2).** The VERIFY AND CHANGE command will return a return code[31] indicating to the IFD and thus to the human user that the authentication by reference data (PUK **O4**) is blocked.

3.5.13 M14: Modified ATR

The TOE will implement a security mechanism as required for **AU1**. If the **SRE10** has occurred, the TOE will react appropriate by sending a modified ATR to the IFD and entering an endless loop by switching in the state **CAS6**.

3.5.14 M15: Public Key Export

The TOE will implement a security mechanism as required for **DX1.2**. This mechanism allows (i) to read the key record of a public key, and (ii) to generate and export a

---

30 status bytes ’63 Cx’, x represents the number of retries and is valued from 0 to 2, whereby x=0 means that the PIN **O3** is blocked; incorrect PIN.

31 status bytes ’63 Cx’, x represents the number of retries and is valued from 0 to 2, whereby x=0 means that the PUK **O4** is blocked; incorrect PUK.

signature of a public key record using the private key SK.ICC.AUT ("secure public key export"). In the latter case (ii), this mechanism is supported by M11 Signature generation (see section 3.5.10) with appropriate parameters.

3.6 Suitability of the TOE's security features

This section describes the suitability of the TOE's security features to counter all assumed threats. An easy mapping between the threats, the security objectives and the SEF based on the explanations given in section 2.6 is shown in the following Table 15:

Table 15: Mapping between the threats, the security objectives and the SEF

	SO1 "Prevent disclosure, copying or modification of the cardholder's SigG signature private key"	SO2 "Prevent unauthorised use of the SigG digital signature function"	SO6 "Quality of key generation"	SO7 "Provide secure digital signature"	SO8 "React to potential security violations"
T1 "Extraction of the cardholder's private key(s)"	AC1, AC2, OR1			DX1, DX2	AC3
T2 "Misuse of the signature function"		IA1 – IA4, AC1			AC3
T3 "Forged data ascribed to the cardholder"			DX1	DX2	AC3

Threat T1

The threat T1 "Extraction of the cardholder's SigG signature private key" will be covered by the security objectives SO1, SO7 as well as SO8 and countered by the security enforcing functions **AC1**, **AC2**, **AC3**, **OR1**, **DX1** as well as **DX2**.

The TOE shall implement the security enforcing function **AC1** "Access control of commands" and **AC2** "Access control of extraction" described in sections 3.3.2.2 and 3.3.3.2 to prevent misuse of ICC commands implemented by the TOE and the extraction of the SigG private signature key(s) **O2**.

The SEF **OR1** described in sections 3.3.2.4 and 3.3.3.4 shall prevent illicit information flow between the SigG application including the SigG private signature key(s) **O2** and other applications eventually embedded on the ICC through temporarily used storage areas.

The SEF **DX1** and **DX2** described in section 3.3.2.5 and 3.3.3.5 shall prevent disclosing of the SigG private signature key(s) of the cardholder **O2** by cryptoanalytic attacks against the digital signatures generated by the TOE.

The blocking state of the TOE shall ensure the security of the SigG private signature key(s) of the cardholder **O2** after a potential attack has been detected (see SEF **AC3** in sections 3.3.2.2 and 3.3.3.2).

Threat T2

The threat T2 "Misuse of the signature function" will be covered by the security objectives SO2, SO8 as well as by the environmental measure (AE4.2)(3) and countered by the security enforcing functions **IA1**-**IA4**, **AC1** and **AC3**.

The TOE implements the security enforcing functions **IA1**, **IA2**, **IA3** and **IA4** for cardholder authentication (described in sections 3.3.2.1 and 3.3.3.1) and **AC1** for access control over the usage of the SigG signature private key(s) of the cardholder **O2** (described in sections 3.3.2.2 and 3.3.2.2) to fulfil the security objective SO2.

The assumption AE4.2(2) ensures that the environment keeps the confidentiality and integrity of the data transferred between the office IFD and the ICC.

The blocking state of the TOE shall ensure the security of the SigG signature function after a potential attack has been detected (see SEF **AC3** in sections 3.3.2.2 and 3.3.3.2).

Threat T3

The threat T3 "Forged data ascribed to the cardholder" will be covered by the security objectives SO6, SO7, SO8 and countered by the security enforcing functions **DX1**, **DX2** and **AC3**.

The TOE implements the security enforcing function **DX1** described in sections 3.3.2.5 and 3.3.3.5 to fulfil the security objective SO6 by means of generation of secure SigG signature key pairs.

The TOE implements the security enforcing function **DX2** described in sections 3.3.2.5 and 3.3.3.5 to fulfil the security objective SO7 by means of generation of secure SigG digital signature.

The blocking state of the TOE shall prevent misuse of this SEF if a potential attack has been detected (see SEF **AC3** in sections 3.3.2.2 and 3.3.3.2).

3.7 Evaluation Target

The TOE's security mechanisms are expected to provide a strength of mechanisms, which is HIGH.

The TOE will be evaluated using level E4 ("E four").

3.8 List of abbreviations

AC	Access Control

AE1	Life cycle security
AE2	Integrity and quality of key material
AE3	SigG compliant use of the TOE
AE4	Use with SigG compliant IFD
AE5	Security assumption about the ICC hardware
AEn.m	Assumption about the Environment (No. n)
ATR	Answer to Reset
CA	Certificate Authority
CA/RA	Certification Authority / Registration Authority
CAS	Current Authentication State (See also section 3.4.1, especially Table 10)
CAS1	Somebody using the TOE
CAS2	Somebody using the SigG application
CAS3	Cardholder using an IFD
CAS6	Security violation
CAS7	Somebody using the SigG application with blocked Cardholder reference data
CH	Cardholder
DEA	Data Encryption Algorithm
DEPCA	Germany Root Certificate Authority (RegTP)
DES	Data Encryption Standard
DF	Dedicated File
DPA	Differential Power Analysis
DSA	Digital Signature Algorithm
DX	Data Exchange
EDC	Error Detection Code
EF	Elementary File
IA	Identification and Authentication
IC	Integrated Circuit
ICC	Integrated Circuit Card
IFD	Interface Device
ISF	Internal Secret File
ITSEC	Information Technology Security Evaluation Criteria

M1	Human user authentication
M10	SigG Signature key pair generation
M11	SigG Signature generation
M12	Return Code for VERIFY
M13	Return Code for VERIFY AND CHANGE
M14	Modified ATR
M2	Change the unblocked reference data
M3	Locking of the reference data
M4	Unblock and change of the reference data
M5	Extraction resistance
M6	Access control for command execution
M7	Blocking state
M9	Clearing memory
Mn	Security Mechanism (No. n)
O1	SigG application
O12	SigG public signature key(s) of the cardholder (({PK_i.CH.DS | $1 \leq i \leq n$})
O2	SigG private signature key(s) of the cardholder ({SK_i.CH.DS | $1 \leq i \leq n$})
O3	SigG cardholder reference data (PIN)
O4	SigG cardholder reset code (PUK)
O5	SigG signature key certificate of the cardholder (C.CH.DS)
O6	SigG public key of the root certification authority (PK.DEPCA.DS)
O7	Other credentials for signature verification
On	Object (No. n)
OR	Object Reuse
PIN	Personal identification number
PK	Public Key
PUK	Personal unblocking key
RC_{PIN}	Retry counter for cardholder reference data (PIN) **O3**; if RC_{PIN}=0, then the PIN is blocked
RC_{PUK}	Retry counter for cardholder reset code (PUK) **O4**; if RC_{PUK}=0, then the PUK is blocked
RN	Registration number

RSA	Rivest, Shamir, Adleman Algorithm (asymmetrical cryptoalgorithm)
S1	Cardholder
S2	Somebody
S3	an IFD
S7	Potential attacker
SigG	Signaturgesetz
SigV	Signaturverordnung
SK	private key (also known as: secret key)
SO1	Prevent disclosure, copying or modification of the cardholder's SigG signature private key
SO2	Prevent unauthorised use of the SigG digital signature function
SO6	Quality of key generation
SO7	Provide secure digital signature
SO8	React to potential security violations
SOn.m	Security Objective (No. n)
SPA	Simple Power Analysis
SRE1	Resetting of the ICC
SRE10	Potential security violation occurred
SRE11	Cardholder authenticated by reset code
SRE12	Cardholder authentication by reset code failed
SRE2	Deactivation of the ICC
SRE3	Opening of the SigG application
SRE4	Closing of the SigG application
SRE5	Successful cardholder authentication
SRE6	Cardholder authentication failure
SRE7	Repeated authentication failure
SREn	Security Relevant Event (No. n)
StarCert	Digital Signature Application by Giesecke & Devrient according to SigG (SigG application)
T1	Extraction of the cardholder's SigG signing private key
T2	Misuse of the signature function
T3	Forged data ascribed to the cardholder
TCU	Terminate Card Usage

Tn.m	Threat (No. n)
TOE	Target of Evaluation
US	Unauthorised User

3.9 Glossary

In this glossary sometimes multiple terms (printed in boldface) are explained together; then all of these terms are used synonymously.

Authenticated User

Human user providing for the authentication by knowledge the verification data matching the reference data stored in the TOE for (a) an application or (b) in a global context.

Authentication information, authentication data

Information used to prove or to verify the identity of a subject by means of authentication. The user authentication information are the verification data provided by the cardholder to prove her or his identity and the reference data (PIN **O3** or PUK **O4**) used by the TOE to verify this identity. The authentication information for the mutual authentication (see [DIN], annex D) are the private device key used by the prover to calculate the authentication token and the public device key used by the verifier to verify this token. See also verification data and reference data.

Blocking state of the TOE

The state of the ICC disabling the ICC completely (after TERMINATE CARD USAGE) besides recognising of this state, generating and sending of the appropriate ATR and automatically switching into the state **CAS6**. This state is apparent to the cardholder by means of an error message (see sect. 3.2.6.5).

Cardholder (CH)

The legitimate owner of a specific ICC running the TOE. The cardholder is the only person in legitimate possession of the reference data (PIN and PUK) matching the stored verification data for the SigG application of the TOE in the operational phase.

Cardholder authentication data

PIN (O3) and PUK (O4)

Certificate

A digital certificate bearing a digital signature and pertaining to the assignment of a public signature key to a natural person (signature key certificate) or a separate digital certificate containing further information and clearly referring to a specific signature key certificate (attribute certificate) (see §2 SigG [SigG]).

Certification authority (CA)

A natural or legal person who certifies the assignment of public signature keys to natural persons and to this end holds a licence pursuant to § 4 of the SigG [SigG].

Credentials for signature verification

Public keys or certificates stored in the ICC for the purpose of SigG signature verifications.

Current authentication state (CAS)

A status of the TOE representing the current assumption about the subject currently using the TOE. The CAS is changed by security relevant events SRE and used for access control decisions.

Device authentication certificate

A certificate for a public key of a SigG compliant technical component to be used for the mutual device authentication according to [DIN].

Digital Signature

A digital signature is a seal affixed to digital data which is generated by the SigG private signature key of the cardholder (a private signature key) and establishes the owner of the signature key (the cardholder) and the integrity of the data with the help of an associated public key provided with a signature key certificate of a certification authority.

Extraction (of a key)

The extraction of the SigG private signature key of the cardholder covers (i) directly reading the key or (ii) copying the key to other devices even if the key is not generally disclosed in the process or (iii) inferring the key by analysing the results of computations performed by the ICC or (iv) inferring the key by analysing a physical observable.

Infer

Any form of determination of private keys by analysing the results of computations performed by the ICC or analysing physical characteristics in the course of computation.

Integrated Circuit Card (ICC)

A smart card equipped with the TOE.

Interface Device (IFD)

Collectively all the devices and other equipment, to which the TOE is presented for the purpose of performing ICC related services.

Key body

The key itself (either a public key or a secret key), encoding the exponent and the modulus. See also key header and key record.

Key header

Information about the key, including its intended purpose and the access conditions for using the key. Optionally a registration number can be stored in the key header. Key header and key body together build a key record. See also key body and key record.

Key record

The concatenation of the key header and the key body. See also key header and key body.

Non-SigG application

Application which resides on the card and is different from SigG application. The TOE may provide specific functions for this application by its specific software components. The data of the other applications (i) are stored in directories and files of the ICC, (ii) are not executed as code by the TOE and (iii) are not subject of the evaluation.

office IFD

A SigG compliant IFD under custody and responsibility of the cardholder.

Operational phase, operational usage phase

The life cycle phase of the ICC, when it is ready to be used by the cardholder for SigG digital signature generation (e. g. at least one SigG signature key pair is operational).

Personalisation phase

A generic term for first personalisation phase (see section 3.2.3.3) and re-personalisation phase (see section 3.2.3.6). See also the term “re-personalisation phase” in this glossary.

Potential security violations

A set of specified events to be deemed as potential tries to penetrate the TOE using physical deficiencies of the underlying hardware or using logical interfaces to the TOE.

Private key

Part of a key pair of an asymmetric cryptographic algorithm. The private key shall be kept confidential.

public IFD

A public IFD runs on behalf of a service provider to provide commercial services the user. The cardholder is assumed to know whether the used IFD is (i) a public IFD or (ii) an office IFD.

Public key

Part of a key pair of an asymmetric cryptographic algorithm. The public key may be published, usually in form of a certificate to keep its authenticity and integrity.

RA

Registration Authority

Reference data

The values of PIN **O3** and PUK **O4** stored on the TOE, that are used during the authentication process. See also verification data.

Registration Number

The registration number (RN) is a structured unique number given by a Registration Authority for each Certification request (containing certification raw data) for a specific cardholder. The special format is out of scope of this document.

Re-personalisation / Repersonalisation

The life-phase of the TOE (precisely of a SigG signature key pair in the TOE), during which a new SigG signature key pair is being generated or has just been generated by the TOE. The first personalisation phase is called “first personalisation”, all following personalisation phases are called repersonalisation (see also the term “Personalisation phase” in this glossary). The SigG signature key certificate (over the public key which has just been generated) of the CH is not yet stored in the TOE or does not exist at all, respectively. The TOE does not distinguish between a SigG signature key pair, for which the certificate has yet been loaded into the TOE, and a SigG signature key pair, for which the certificate has not been loaded yet. The CH is assumed always to know whether the certificate is available or not.

retry counter (RC_{PIN}, RC_{PUK})

A persistently stored parameter of the TOE. The retry counter (i) holds the number of failed authentication attempts of the Cardholder **S1** after the last successful authentication attempt or (ii) equals to a fixed value if the number of failed authentication attempts of the human user after the last successful authentication attempt of the human user exceeds the maximum number of failed authentication attempts allowed.

For STARCOS SPK2.3, there are two retry counters, one for the cardholder authentication data / PIN (RC_{PIN}) and one for the cardholder reset code / PUK (RC_{PUK}). The retry counters are realised as follows: The retry counter is initialised with the number of failed authentication attempts allowed (e.g. RC_{PIN}:=3). For each unsuccessful authentication attempt by PIN, RC_{PIN} is decremented by one (RC_{PIN}:=RC_{PIN}-1). If RC_{PIN} reaches the value zero (RC_{PIN}=0), then the PIN is blocked. – RC_{PUK} is realised analogous to RC_{PIN} and works the same way for the cardholder reset code / PUK.

Secret key

In this document: used as a synonym for an (asymmetric) private key; in other context, the term secret key is also used very often to designate a symmetric key, which has to be kept secret.

SigG accredited ICC

An ICC (i) being a SigG accredited technical component and (ii) equipped with the TOE supporting the Option Public IFD (especially supporting the mutual device authentication and secure messaging according to [DIN], section 18 and annex D).

SigG accredited IFD

A Public IFD (i) being a SigG accredited technical component and (ii) acting as customer IFD according to [DIN], section 18, and (iii) supporting the mutual device authentication and secure messaging according to [DIN], annex D).

SigG accredited technical component

A technical component which (1) is produced as an example of an SigG compliant technical component, (2) is being able to prove its own SigG accreditation by means of (2.i) a secret authentication key, and (2.ii) an device authentication certificate of a policy certification authority for SigG accredited devices and (3) is being able to verify the SigG accreditation of other devices by means of a public authentication key of the DEPCA (see [DIN]) for certificates of policy certification authorities for SigG accredited devices.

SigG application services

The function provided to the cardholder by the TOE. The SigG application services are at least (i) SigG signature generation and (ii) reading SigG digital signature certificates

SigG cardholder reference data

Data permanently stored in the TOE to verify the cardholder authentication.

SigG cardholder verification data

Data provided by the user to authenticate himself as cardholder by knowledge.

SigG compliance of technical component

A property of a technical component to adhere the given SigG legislative with respect to its implementation and configuration. The SigG compliance of a technical component shall be evaluated and conformed according to [SigV] §17 (1). The SigG compliance of a technical component is usually not directly apparent to the user or to an other technical component. Note that a SigG compliant technical component is not necessary a SigG accredited technical component.

SigG private signature key of the cardholder, SigG signature private key

Part of the SigG application and used by the TOE to generate a digital signature on behalf of the cardholder. The signature key is the private key (secret key) of the SigG signature key pair of the cardholder.

SigG public signature key of the cardholder, SigG signature public key

Part of the SigG application and used by the TOE to verify a digital signature. The signature public key is the public key of the SigG signature key pair of the cardholder.
Note: The functionality signature verification is not part of this evaluation (see also SigG signature verification).

SigG signature key pair, SigG signing key pair

A key pair (consisting of a SigG public signature key and a SigG private signature key) used to generate SigG compliant digital signatures.

SigG signature verification

A process, which is established with the help of an associated SigG signature public key provided by a SigG signature key certificate of a certification authority and checks (i) whether the digital signature of the message was generated by the owner of the SigG signature key (the cardholder) and (ii) the integrity of the data. The TOE may provide a signature verification function, but this function is not a subject of this evaluation as a security enforcing function.

signing key

Synonym for signature key

TC

Trust Center

Verification data

The authentication data (PIN or PUK) that is entered by the subject (user) trying to authenticate and that is sent to the TOE. The TOE will compare the verification data entered by the user to the reference data (PIN **O3** or PUK **O4**) stored on the ICC and the authentication will be successful, if verification data and reference data match. See also reference data and authentication data.

3.10 References

[GST_098] Generic Security Target for ICC embedded Software compliant with SigG, SigV and DIN, TeleTrusT Deutschland e.V., Version 0.98

[DIN] DIN: Spezifikation der Schnittstelle zu Chipkarten mit Digitaler Signatur - Anwendung/Funktion nach SigG und SigV, DIN V 66291-1, April 2000

[SigG] Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-gesetz - IuKDG) (in Kraft getr. am 1.8.97) Artikel 3 Gesetz zur digitalen Signatur (Signaturgesetz - SigG)

[SigV] Verordnung zur digitalen Signatur (Signaturverordnung - SigV) (in Kraft getr. am 1.11.97)

[BA] Bekanntmachung zur digitalen Signatur nach Signaturgesetz und Signaturverordnung vom 09.02.98, Bundesanzeiger Nr. 31 vom 14.02.98: Geeignete Kryptoalgorithmen gemäß §17 Abs. 2 SigV

[CLC] Specification Card Life Cycle of Starcos SPK 2.3 with Signature Application, Giesecke & Devrient GmbH, Version 1.5.3, 24.01.2001

[ITSEC] Information Technology Security Evaluation Criteria (ITSEC); Provisional Harmonised Criteria, Version 1.2, June 1991

[JIL] ITSEC Joint Interpretation Library (ITSEC JIL); Version 2.0, November 1998

[AddInformInt] Additional Informal Interpretation of the Formal Model, Giesecke&Devrient GmbH, Version 0.50, 15.08.2000

[FMSP] Generic Formal Model of Security Policy and its Informal Interpretation Target of Evaluation: ICC embedded software for Signature Creation conforming with German SigG, SigV and DIN V 66391-1 Version 1.1 September 12, 2000

[InformInt] ICC embedded software for Signature Creation conforming with German SigG, SigV and DIN V 66391-1. Generic Formal Model of Security Policy and its Informal Interpretation in terms of the Generic Security Target, Vers. 0.98 (draft), DFKI GmbH, 15.02.2000

(This page is intentionally left blank.)

4 Remarks and Recommendations concerning the Certified Object

27 The statements given in chapter 2 are to be considered as the outcome of the evaluation.

28 The Certification Body has the following additional information and recommendations for the **user**:

- With respect to AE4.2 (2) the user is reminded that the TOE supports different SigG signature key pairs. Thus, if the user is authenticated as the cardholder the SigG signature key may be changed and used for signature generation without re-authentication.

- With respect to AE5.1 the chip Philips Smart Card Controller P8WE5032V0G is to be used as the ICC hardware[32]. The validity of the evaluation results, and therefore, of the certificate, is restricted to the implementation of the TOE on the platform of the Philips Smart Card Controller P8WE5032V0G. The restrictions as stated in the “Security Target of Philips P8WE5032 Secure 8-bit Smart Card Controller Version P8WE5032V0G, BSI-DSZ-ITSEC-0158, Version 1.3.1, 16th January, 2001”, section 4.2, and in the “Certification Report BSI-DSZ-ITSEC-0158-2001 for Philips Smart Card Controller P8WE5032V0G from Philips Semiconductors Hamburg Unternehmensbereich der Philips GmbH, Bonn, 17th January, 2001”, part B, chapter 3, apply.

- The term “security relevant event” of the security target, chapter 3 of this certification report, is used to denote an event, an action or a state transition.

- There may be implemented different applications on the smart card supported by the STARCOS® SPK2.3 operating system. The user is strongly recommended to define a PIN for the digital signature application StarCert which is different from all other PINs for other applications on the smart card.

- With respect to the number of digital signatures which may be generated without re-authentication of the cardholder, there are two different configurations of the TOE (cf. section 3.2.2: limited signature generation configuration, unlimited signature generation configuration). The unlimited signature generation configuration of the TOE shall be used only in connection with additional security measures supplied by the environment as described in (AE4.2)-(2) of the security target, section 3.2.4.4 of this certification report.

- Although the TOE accepts MD5 hash values as an input for digital signature generation the cardholder is recommended not to use MD5 as a hash function. Moreover, application of MD5 is not compliant to SigG requirements.

---

32 The Philips Smart Card Controller P8WE5032V0G fulfils the assumption AE5.1 proved by the certificate Deutsches IT-Sicherheitszertifikat BSI-DSZ-ITSEC-0158-2001 as of 17.01.2001.

- The Trust Center is required to hand over a personalised TOE to the cardholder face-to-face, exclusively.
- The cardholder is advised to reject any other form of delivery than face-to-face.

5 Security Criteria Background

29 This chapter gives a survey on the criteria used in the evaluation and its different metrics.

5.1 Fundamentals

30 In the view of ITSEC security is given if there is sufficient assurance that a product or system meets its security objectives.

31 The security objectives for a product or system are a combination of requirements for

- confidentiality
- availability
- integrity

of certain data objects. The security objectives are defined by a vendor or developer for his product and by the user for his (installed) system.

32 The defined security objectives are exposed to *threats*, i.e. loss of confidentiality, loss of availability and loss of integrity of the considered data objects.

33 These threats become real, when subjects read, deny access to or modify data without authorisation.

34 Security (enforcing) functions provided by the considered product or system are intended to counter these threats.

35 There are two basic questions:

- Do the security functions operate correctly?
- Are they effective?

Thus, an adequate assurance that the security objectives are met can be achieved if correctness and effectiveness have been evaluated.

5.2 Assurance level

36 An evaluation can only be performed with limited resources, especially limited time. Thus, the depth of an evaluation is always limited. On the other hand, it is not reasonable to perform an evaluation with extremely high resources when there is only need for low level security - and vice versa.

37 Therefore, it is reasonable to define a metric of assurance levels based on the depth of the evaluation and resources needed. In ITSEC six assurance levels are given for the evaluation of correctness and effectiveness. E1 is the lowest, E6 the highest level.

38 Thus, the trustworthiness of a product or system can be „measured“ by such assurance levels.

39 The following excerpt from the ITSEC shows which aspects are covered during the evaluation process and which depth of analysis corresponds to the assurance levels.

40 The enumeration contains certain requirements as to correctness and gives a first idea of the depth of the corresponding evaluation („TOE“ is the product or system under evaluation):

E1 „At this level there shall be a security target and an informal description of the architectural design of the TOE. Functional testing shall indicate that the TOE satisfies its security target.“

E2 „In addition to the requirements for level E1, there shall be an informal description of the detailed design. Evidence of functional testing shall be evaluated. There shall be a configuration control system and an approved distribution procedure.“

E3 „In addition to the requirements for level E2, the source code and/or hardware drawings corresponding to the security mechanisms shall be evaluated. Evidence of testing of those mechanisms shall be evaluated.“

E4 „In addition to the requirements for level E3, there shall be an underlying formal model of security policy supporting the security target. The security enforcing functions, the architectural design and the detailed design shall be specified in a semiformal style.“

E5 „In addition to the requirements for level E4, there shall be a close correspondence between the detailed design and the source code and/or hardware drawings.“

E6 „In addition to the requirements for level E5, the security enforcing functions and the architectural design shall be specified in a formal style, consistent with the specified underlying formal model of security policy."

41 Effectiveness aspects have to be evaluated according to the following requirements identical for each level E1 to E6 :

"Assessment of effectiveness involves consideration of the following aspects of the TOE:

a) the suitability of the TOE's security enforcing functions to counter the threats to the security of the TOE identified in the security target;

b) the ability of the TOE's security enforcing functions and mechanisms to bind together in a way that is mutually supportive and provides an integrated and effective whole;

c) the ability of the TOE's security mechanisms to withstand direct attack;

d) whether known security vulnerabilities in the *construction* of the TOE could in practice compromise the security of the TOE;

e) that the TOE cannot be configured or used in a manner which is insecure but which an administrator or end-user of the TOE would reasonably believe to be secure;

f) whether known security vulnerabilities in the *operation* of the TOE could in practice compromise the security of the TOE."

5.3 Security Functions and Security Mechanisms

42 Typical examples for security functions are *Identification and Authentication* (of subjects), *Access Control*, *Accounting* and *Auditing*, *(Secure) Data Exchange*. Such security functions can be implemented in IT products and systems.

43 Functionality classes are formed by grouping a reasonable set of security functions.

Example: The functionality class F-C2 covers the generic headings *Identification and Authentication*, *Access Control*, *Accounting* and *Auditing*, and *Object Reuse*. This class is typical for many commercial operating systems.

44 For every security function there are many ways of implementation:

Example: The function *Identification and Authentication* can be realised by a password procedure, usage of chipcards with a challenge response scheme or by biometrical algorithms.

45 The different implementations are called *(security) mechanisms* of the security function *Identification and Authentication*.
For other security functions the term mechanism is used similarly.

46 The rated ability of a security mechanism to counter potential direct attacks is called *strength* of (this) mechanism.

47 In ITSEM two types of mechanisms are considered: type B and type A.

Type B „A *type B mechanism* is a security mechanism which, if perfectly conceived and implemented, will have no weaknesses. A type B mechanism can be considered to be impregnable to direct attack regardless of the level of resources, expertise and opportunity deployed. A potential example of a type B mechanism would be access control based on access control lists: if perfectly conceived and implemented, this type B mechanism cannot be defeated by direct attack. However, these type B mechanisms can be defeated by indirect attacks which are the subject of other effectiveness analyses."

Considering direct attacks only, type B mechanisms cannot be defeated.

Type A „A *type A mechanism* is a security mechanism with a potential vulnerability in its algorithm, principles or properties, whereby the mechanism can be overcome by the use of sufficient resources, expertise and opportunity in the form of a direct attack. An example of a type A mechanism would be an authentication program using a password: if the password can be guessed by attempting all possible passwords in succession, the authentication mechanism is of type A. Type A mechanisms often involve the use of a "secret" such as a password or cryptographic key.“

„All type A mechanisms ... have a strength, which corresponds to the level of resources, expertise and opportunity required to compromise security by directly attacking the mechanism.“

48 How is the strength for type A mechanisms defined?

„All critical security mechanisms (i.e. those mechanisms whose failure would create a security weakness) are assessed for their ability to withstand direct attack. The minimum strength of each critical mechanism shall be rated either *basic*, *medium* or *high*.“

basic: „For the minimum strength of a critical mechanism to be rated *basic* it shall be evident that it provides protection against random accidental subversion, although it may be capable of being defeated by knowledgeable attackers.“

medium: „For the minimum strength of a critical mechanism to be rated *medium* it shall be evident that it provides protection against attackers with limited opportunities or resources.“

high: „For the minimum strength of a critical mechanism to be rated *high* it shall be evident that it could only be defeated by attackers possessing a high level of expertise, opportunity and resources, successful attack being judged to be beyond normal practicability."

6 Annex

6.1 Glossary

This glossary provides descriptions of the expressions used in this brochure, but does not guarantee their completeness or general validity. The term *security* here is always used in the context of information technology.

Accreditation	A process to confirm that an evaluation facility complies with the requirements stipulated by the EN 45001 standard. Accreditation is performed by an *accreditation body.* Accreditations from bodies represented in the German Accreditation Council (DAR) are generally recognised.
Associated Laboratory	A development laboratory co-operating with debisZERT under a contract, using optimised procedures to prepare for an evaluation.
Availability	Classical security objective: Data should always be available to authorised persons, i.e. this data should neither be made inaccessible by unauthorised persons nor be rendered unavailable due to technical defects.
Certificate	Summary representation of a certification result, issued by the certification body.
Certification	Independent confirmation of the correctness of an evaluation. This term is also used to describe the overall process consisting of evaluation, monitoring and subsequent issue of certificates and certification reports.
Certification Body	An organisation which performs certifications.
Certification ID	Code designating a certification process.
Certification Report	Report on the object, procedures and results of certification; this report is issued by the certification body.
Certification Scheme	A summary of all principles, regulations and procedures applied by a certification body.
Certifier	Employee at a certification body authorised to carry out certification and to monitor evaluations.
Common Criteria	Security criteria derived from the US Orange Book / Federal Criteria, European ITSEC and Canadian CTCPEC, and intended to form an internationally accepted security evaluation standard.
Component According to SigG	A logical unit in an IT system performing a task defined in SigG/SigV (display component, component for key generation, etc.).

Confidentiality	Classical security objective: Data should only be accessible to authorised persons.
Confirmation Body	Body that issues security confirmations in accordance with SigG and SigV for technical components (suitability) and trust centres (implementation of security concepts)
Confirmation Procedure	Procedure with the objective to award a security confirmation.
debisZERT	Name of the debis IT Security Services Certification Scheme.
Digital Signature Act - SigG	§3 of legislation on Information and Communications Services Act (IuKDG).
Digital Signature Ordinance – SigV	Official regulations concerning the implementation of the German Digital Signature Act, having the force of law.
EN 45000	A series of European standards applicable, in particular, to evaluation facilities and certification bodies.
Enterprise process	Cf. process
Evaluation	Assessment of an (IT) product, system or service against published IT security criteria or IT security standards.
Evaluation (Assurance) Level	Refer to „Security Level“.
Evaluation Facility	The organisational unit which performs evaluations.
Evaluation Report	Report on a single aspect of an evaluation (see Individual evaluation report) or evaluation technical report (ETR).
Evaluation Technical Report	Final report written by an evaluation facility on the procedure and results of an evaluation (abbreviated as „ETR“ in the ITSEC context).
Evaluator	Person in charge of an evaluation at an evaluation facility.
Individual Evaluation Report	Report written by an evaluation facility on individual evaluation aspects as part of an evaluation.
Initial Certification	The first certification of an (IT) product, system or service.
Integrity	Classical security objective: Only authorised persons should be capable of modifying data.
IT Component	Security criteria: A discrete part of an IT product or IT system, well distinguished from other parts.
IT Product	Software and/or hardware which can be procured from a supplier (manufacturer, distributor).
IT Security Management	Implemented procedure to install and maintain IT security within an organisation.

IT Service	A service depending on the support by IT products and / or IT systems.
IT System	An inherently functional combination of IT products. (ITSEC:) A real installation of IT products with a known operational environment.
ITSEC	Information Technology Security Evaluation Criteria: European de facto standard for the evaluation of IT products and IT systems.
ITSEM	Information Technology Security Evaluation Manual. This manual on ITSEC applies in particular to evaluation processes.
Licence (personal)	Confirmation of a personal qualification (in the context of debisZERT here, cf. licenced engineer).
Licence Agreement	An agreement between an evaluation facility and a certification body specifying procedures and responsibilities for evaluation and certification.
Licenced Engineer	A person with qualifications in the context of evaluation approved by debisZERT.
Licensing	Evaluation of organisation and qualification of an evaluation facility with respect to an intended licence agreement (to become a CLEF).
Manufacturer's Laboratory	An organisational unit belonging to the manufacturer of a product /system or the supplier of a service, charged with performing evaluation of that product, system or service.
Milestone Plan	A project schedule for the implementation of evaluation and certification processes.
Monitoring	Procedure implemented by the certification body in order to check whether an evaluation is performed correctly (compliance with criteria, use of standard processes and appraisal techniques etc.).
Pre-Certification	Confirmation of the results of a preliminary investigation of a product-specific or process-specific security standard or a security-related tool (with a view to later certification).
Problem Report	Report sent by an evaluation facility to the certification body and concerning special problems during evaluation, e. g. concerning the interpretation of IT security criteria.
Process (Enterprise~)	Sequence of linked activities (prozess elements) performed within a given environment – with the objective to provide a certain service.
Process ID	ID designating a certification or confirmation process within debisZERT.

Product Certification	Certification of an IT product.
Re-Certification	Renewed certification of a previously certified object due to a new version following modification; re-certification might also be required after a change of tools, production / delivery processes and security criteria.
Recognition (Agreement)	Declaration and confirmation (of the equivalence of certificates and licences).
Regulatory Authority for Telecommunications and Posts	The authority responsible in accordance with §66 of the German Telecommunications Act (TKG).
Right of Disposal	In this case: Authorisation to allow all inspections of a product, system or service as part of evaluation and certification.
Security Certificate	Refer to „Certificate".
Security Confirmation	In debisZERT: A legally binding confirmation of security features extending beyond the scope of a certificate, e. g. a confirmation according to SigG / SigV.
Security Criteria	Normative document that may contain technical requirements for products, systems and services, but at least describes the evaluation of such requirements.
Security Function	Function of an IT product or IT system for counteracting certain threats.
Security Level	A metric defined in security criteria to indicate various levels of security relating to different requirements for the object to be certified and the degree of detail needed during evaluation.
Security Specification	Security-related functional requirements for products, systems and services.
Security Standards	A joint expression encompassing security criteria and security specifications.
Service (Enterprise ~)	Here: activities offered by a company, provided by its (enterprise) processes and useable by a client..
Service Type	Particular type of service (DLB) offered by debisZERT.
Sponsor	A natural or legal person who (in this case) issues an order for certification or evaluation, and who must possess a sufficient right of disposal for the object to be certified or evaluated, respectively.
System Accreditation	Procedure of accepting an IT system or IT service for usage (considered here from the perspective of adequate security) in a specific environment and/or application.

System Certification	Certification of an IT system (considered here from the perspective of adequate security).
Trust Centre	A centre which confirms the relationship between signature keys and persons by means of electronic certificates - such a centre is termed „certification authority" in the Digital Signature Act.

6.2 References[33]

/A00/ Lizenzierungsschema [Licensing Scheme], debisZERT, version 1.6, 31.03.2000, http://www.debiszert.de/

/ALG/ Bekanntmachung zur digitalen Signatur nach dem Signaturgesetz und der Signaturverordnung vom 09.02.98, Geeignete Kryptoalgorithmen gemäß § 17 (2) SigV, Bundesanzeiger Nr. 230 – Seite 22.946 v. 07. Dezember 2000 [Official Announcement concerning the Digital Signature according to the Digital Signature Act and Signature Ordinance by February 9, 1998 published in Bundesanzeiger No. 230, December 07, 2000"]

/BSIG/ Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz - BSIG) [Act on the Establishment of the German Information Security Agency], BGBl. I. of 17.12.1990, page 2834 ff.

/CC/ Common Criteria for Information Technology Security Evaluation, version 2.1, Part 1 (Introduction and general model), Part 2 (Security functional requirements), Part 2 : Annexes, Part 3 (Security assurance requirements) , August 1999

/CEM/ Common Methodology for Information Technology Security Evaluation, Part 1 (Introduction and general model), version 0.6, January 1997, Part 2 (Evaluation Methodology), version 1.0, August 1999

/ITSEC/ Information Technology Security Evaluation Criteria (ITSEC), version 1.2 (1991), ISBN 92-826-3004-8

/ITSEM/ Information Technology Security Evaluation Manual (ITSEM), version 1.0 (1993), ISBN 92-826-7087-2

/IuKDG/ Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz - IuKDG) [Information and Communication Services Act], BGBl. I. of 28.07.1997, page 1872 ff.

/JIL/ Joint Interpretation Library, version 2.0, November 1998

[33] in brackets [...] translation of title into English, if there is no English document

/Mkat12/ Maßnahmenkatalog nach §12 Abs. 2 [Catalogue of Security Measures in accordance with §12 Sec. 2], Regulierungsbehörde für Telekommunikation und Post, 15.07.1998

/Mkat16/ Maßnahmenkatalog nach §16 Abs. 6 [Catalogue of Security Measures in accordance with §16 Sec. 6], Regulierungsbehörde für Telekommunikation und Post, 15.07.1998

/SigG/ Digital Signature Act, Article 3 of /IuKDG/

/SigV/ Digital Signature Ordinance, BGBl. I. of 27.10.1997, page 2498 ff.

/TKG/ Telekommunikationsgesetz (TKG) [Telecommunications Act], BGBl. I. of 25.7.1996, page 1120

/V01/ Certificates according to ITSEC/CC, service type 1 of debisZERT, version 1.6E, 31.03.2000, http://www.debiszert.de/

/V02/ Security Confirmations for Components according to the German Digital Signature Act, service type 2 of debisZERT, version 1.6E, 31.03.2000, http://www.debiszert.de/

/V03/ Sicherheitsbestätigungen für Zertifizierungsstellen gemäß dem Signaturgesetz [Security Confirmations for Trust Centers according to the German Digital Signature Act], service type 3 of debisZERT, version 1.6, 31.03.2000, http://www.debiszert.de/

/V04/ Certificates recognised by the BSI, service type 4 of debisZERT, version 1.6E, 31.03.2000, http://www.debiszert.de/

/V05/ Zertifizierung von Unternehmensprozessen und Dienstleistungen [Certification of Enterprise Processes and Services], service type 5 of debisZERT, version 1.6, 31.03.2000, http://www.debiszert.de/, in German only

/Z01/ Certification Scheme, debisZERT, version 1.6E, 31.03.2000, http://www.debiszert.de/

6.3 Abbreviations

AA	Work instructions
AIS	Request for an interpretation of security criteria
BSI	Bundesamt für Sicherheit in der Informationstechnik [German Information Security Agency]
BSIG	Act on the Establishment of the BSI
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CTCPEC	Canadian Trusted Computer Products Evaluation Criteria
DAR	Deutscher Akkreditierungsrat [German Accreditation Council]

DATech	Deutsche Akkreditierungsstelle Technik e.V. [German Accreditation Body for Technology]
debisZERT	Certification Scheme of debis Systemhaus Information Security Services GmbH
ETR	Evaluation Technical Report
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	IT Security Evaluation Facility
ITSEM	Information Technology Security Evaluation Manual
IuKDG	German Information and Communication Services Act
RegTP	Regulierungsbehörde für Telekommunikation und Post [Regulatory Authority for Telecommunications and Posts]
SigG	German Digital Signature Act
SigV	German Digital Signature Ordinance
TKG	German Telecommunications Act
TOE	Target of Evaluation

(This page is intentionally left blank.)

7 Re-Certification

49 When a certified object has been modified, a re-certification can be performed in accordance with the rules of debisZERT. The annexes to this chapter 7 (ordered by date of issuance) describe the type of modification, the new product version and the certification status.

50 If current findings in the field of IT security affect the security of a certified object, a technical annex to this certification report can be issued.

51 Re-certification and new technical annexes will be announced under www.debiszert.de.

52 The annexes are numbered consecutively.

End of initial version of the certification report.