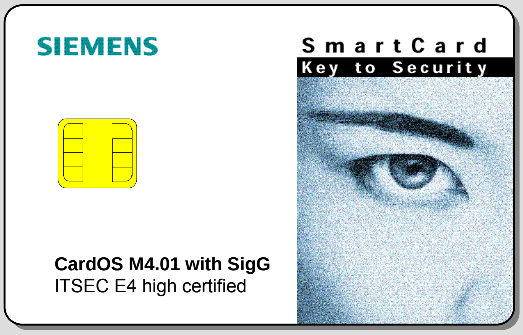
Certification Report

T-Systems-DSZ- ITSEC-04067-2002



CardOS/M4.01 with Application for Digital Signature Creation

Siemens AG

T-Systems ISS GmbH

Preface

The product **CardOS/M4.01 with Application for Digital Signature Creation (as ICC embedded software conforming with German SigG, SigV and DIN V 66291-1)**[1] (TOE) - abbreviated as **CardOS/M4.01 with Application for Digital Signature Creation** in the sequel - of Siemens AG has been evaluated against the ITSEC. The evaluation has been performed under the terms of the certification scheme of T-Systems ISS GmbH. The certification procedure applied conforms to the rules of service type 04: German IT Security Certificate.

The result is:

Security Functions:	**Identification and Authentication, Access Control, Audit, Object Reuse, Data Exchange**
Evaluation Level:	**E4**
Minimum Strength of Mechanisms:	**high**

This is to certify that the evaluation has been performed compliant to the certification scheme of T-Systems ISS GmbH.

Bonn: March 6, 2002

T · · Systems · · ·

Klaus-Werner Schröder

(Certifier)

Dr. Heinrich Kersten

(Head of the Certification Body)

For further information and copies of this report, please contact the certification body:

✉ T-Systems ISS GmbH, - Certification Body -, Rabinstr.8, D-53111 Bonn, Germany
☎ +49-228-9841-0, Fax: +49-228-9841-60
💻 www.t-systems-zert.com

[1] The conformance claim is part of the product name and is not meant to indicate an evaluation result.

Revision List

Revision	Date	Activity
1.0	March 6, 2002	Produced after end of evaluation; Template: Version 3.1

Contents

(This page is intentionally left blank.)

1 Certification

1.1 General Remarks

1 The certification body of T-Systems ISS GmbH was sponsored by Siemens AG for the certification of **CardOS/M4.01 with Application for Digital Signature Creation** (TOE).

2 The certification body complies to EN 45011 and was accredited with respect to this standard by the DATech e.V. for assessments based on ITSEC and CC (DAR registration number DIT-ZE-005/98).

3 The certification scheme is published by the certification body on its web pages (www.t-systems-zert.com).

1.2 Certificate and Certification Report

4 A survey on the outcome of the evaluation of the TOE is given by the security certificate T-Systems-DSZ-ITSEC-04067-2002 as of March 6, 2002.
The certificate carries the logo (German IT Security Certificate) officially authorised by the Bundesamt für Sicherheit in der Informationstechnik (BSI) and is recognised by the BSI as equivalent to its own certificates. Due to legal restrictions for BSI, the rating of the strength of cryptographic algorithms appropriate for encryption and decryption is not part of the recognition by the BSI.

5 The certificate is published on the certification body's web pages (www.t-systems-zert.com) and is referenced in the brochure BSI 7148 of the Bundesamt für Sicherheit in der Informationstechnik (BSI).

6 The certification report is intended

- as a formal confirmation for the sponsor concerning the evaluation performed,
- to assist the user of TOE in establishing an adequate security level.

7 The certification report contains pages 1 to 98. Copies of the certification report can be obtained from the sponsor or the certification body.

8 The consecutively numbered paragraphs in this certification report are formal statements from the certification body. Unnumbered paragraphs contain statements of the sponsor (chapter 3) or informal material.

9 In chapter 3, the certification report addresses the Security Target, version 1.05 as of March 4, 2002, which was the basis for the evaluation.

10 The Security Target was provided by the sponsor in English language.

11 The certification report is only valid for the specified release of the TOE (version number, date of issuance, etc.). However, it can be extended to new or different versions as soon as a successful re-certification has been performed (cf. section 1.6).

1.3 Application of Results

12 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.

13 The results of the evaluation are only valid under the assumption that all stipulations specified in the certification report are observed by the user, especially:

- the precise product name and version (section 1.1),
- the Security Target for the TOE - in particular, the information provided on the adequate use of the certified object, the security objectives and the considered threats, the security environment and the evaluated configurations (cf. chapter 3),
- the specification of the delivery procedure for the TOE (section 1.4),
- the requirements and recommendations of the certification body to the sponsor (section 1.5),
- the requirements and recommendations of the certification body to the user (section 1.5),
- the evaluated configuration (section 2.2),
- the requirements and recommendations of the evaluation facility to the sponsor (section 2.4),
- the requirements and recommendations of the evaluation facility to the user (section 2.4),
- possibly existing technical anneces and re-certifications (cf. explanations in section 1.6).

14 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 in performing this analysis.

1.4 Delivery Procedure

15 The TOE is delivered according to the following procedure:

delivery by messenger

1.5 Requirements and Recommendations

16 The following requirements and recommendations to the sponsor are a result of the certification process.

The certificate T-Systems-DSZ-ITSEC-04067-2002 as well as this certification report are only valid for **CardOS/M4.01 with Application for Digital Signature Creation** embedded into the hardware of the SLE66CX320P chip.

17 The following requirements and recommendations concerning the adequate use of the TOE are a result of the certification process.

If **CardOS/M4.01 with Application for Digital Signature Creation,** embedded into the hardware of the SLE66CX320P chip, is to be used for creation of qualified electronic signatures according to the German Electronic Signature Act /SigG/ the certification service provider shall describe in his security concept all measures necessary for secure personalisation.

1.6 Technical Anneces and Re-Certification

18 When a certified object (including its specified environment and its delivery procedure) has been modified, a re-certification can be performed in accordance with the rules of the certification body. The results of such re-certifications will be documented in technical anneces to this certification report stating the type of modification and the new product version.

19 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 as well.

20 Re-certifications and new technical anneces will be announced on the certification body's web pages (www.t-systems-zert.com). Technical anneces are numbered consecutively (DSZ-ITSEC-04067-2002**/1**, ...**/2**,...).

(This page is intentionally left blank.)

2 Evaluation

2.1 General Remarks

21 The Prüfstelle für IT-Sicherheit of T-Systems ISS GmbH was sponsored by Siemens AG for the evaluation of **CardOS/M4.01 with Application for Digital Signature Creation** (TOE).

22 The evaluation facility was accredited against EN 45001 resp. ISO 17025 and has a valid licence issued by the certification body for the scope of the evaluation.

2.2 Evaluation and Evaluation Technical Report

23 The evaluation has been performed against the ITSEC /ITSEC/ by using the evaluation methodology ITSEM /ITSEM/, the Joint Interpretation Library /JIL/ and the national interpretations (AIS) valid at the time of the evaluation.

24 Basis for the evaluation was the Security Target, version 1.05 as of March 4, 2002 (cf. chapter 3).

25 The evaluation was monitored by the certification body.

26 The outcome of the evaluation is reproduced in the evaluation facility's ETR (Evaluation Technical Report). The ETR is identified by version 1.02 and dated March 4, 2002.

27 The evaluation was completed on March 04, 2002.

28 The evaluated configuration is described as follows:

The TOE is based upon the ROM mask version C803 (CardOS/M4.01) which is unique for all configurations of the TOE. The basic signature application is unique to all configurations of the TOE, too. During the personalisation process a service package will be loaded into the TOE which is unique to all configurations of the TOE as well.

The configurations of the TOE differ with respect to the following aspects:

The personalisation process may be a centralised or a decentralised one.

In case of centralised personalisation the whole process is carried out at the trust center's site (certification authority), and the personalisation script for centralised personalisation shall be used.

In case of decentralised personalisation the pre-personalisation process is carried out at the trust center's site (certification authority), and the personalisation script for pre-personalisation shall be used. The decentralised personalisation will then be continued and finished at a local registration authority's site (LRA) by means of the personalisation script for post-personalisation.

The personal configuration of the TOE (in short **$n = 1$**) was designed for individuals (card holder). After authentication by PIN (Personal Identification Number) the card holder is allowed to generate a single electronic signature. The signature module configuration of the TOE (in short **$n \neq 1$**) designed for use in a specially secured environment (e.g. at a certification service provider) was also evaluated. The authentication by PIN (Personal Identification Number) allows to generate more than one or even an unrestricted number of electronic signatures.

The technical parameter **n** controls the behaviour described above. In the case $n = 0$ and $n = 255$ an unrestricted number of electronic signatures can be generated after a single authentication. In all other possible cases ($1 \leq n \leq 254$) exactly n electronic signatures can be generated. The selection of either the personal configuration or the signature module configuration is done as part of the personalisation process. The authority responsible for the personalisation process is kept informed on the procedure to apply and shall take special care of the delivery process of the TOE to avoid the handover of a signature module to an individual by mistake.

All configurations described above were evaluated.

2.3 Evaluation Result

29 The evaluation facility comes to the following conclusion:

The TOE meets the requirements of the assurance level E4 according to ITSEC, i.e. all requirements of 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 are critical mechanisms. The mechanisms M1, M2, M4, M5, M10, and M11 are of type A, all the other mechanisms 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).

2.4 Requirements and Recommendations

30 The evaluation facility has formulated the following requirements and recommendations to the sponsor.

1. The cryptographic mechanisms suitable for qualified electronic signatures according to the /SigG/ are published regularly in the Federal Gazette as indicated by /SigV/. According to the current publication (Geeignete Kryptoalgorithmen, 05.07.2001, Federal Gazette No. 158, p. 18562, as of August 24th, 2001) the algorithms of the TOE (hash algorithm SHA-1 and RSA algorithm) are suited until end of 2006. The results of the evaluation as to the security objectives SO6 “Quality of Key Generation” and SO7 “Provide Secure Digital Signature” are, therefore, valid until end of 2006. Then, they shall be re-examined.
2. It is necessary to re-evaluate the TOE if and when new discoveries on attacks are found with respect to cryptographic or other security mechanisms the TOE utilises which may lead to suspicion that the minimum strength of high is in question.

31 The evaluation facility has formulated the following requirements and recommendations as to the adequate use of the TOE.

1. The signature module configuration of the TOE (n ≠ 1) designed for a specially secured environment must not be delivered to an individual as

a personal configuration of the TOE. It is the responsibility of the card issuer (e. g. a certification service provider) to ensure secure delivery.

2. The procedures of completion, initialisation, and personalisation as described in *CardOS/M4.01 Delivery, Generation and Configuration* (No. 8 in table 1 of the Security Target, cf. chapter 3 of this certification report) and *CardOS/M4.01 Documentation for Trust Center* (No. 7 in table 1 of the Security Target, cf. chapter 3 of this certification report) must strictly be followed, no deviation is allowed. These procedures avoid mistakes and shall be part of the security concept of the certification service provider. Changes to the personalisation scripts may be applied only at locations and in the sense indicated by a comment.

3. Key generation shall take place within a secure environment, e. g. at a certification service provider's site, only.

4. In the following respect the TOE is not compliant to the DIN V 66291-1 standard: The TOE always allows reading of the certificate of the card holder (C.CH.DS) located in the EF_C_CH_DS without any authentication.

3 Security Target

32 In the sequel, the Security Target, version 1.05 as of March 4, 2002, for **CardOS/M4.01 with Application for Digital Signature Creation** (TOE) is reproduced completely and in authentic layout.

33 The Security Target has a separate table of contents and individual page numbers which are given in the middle of the page footer.

(This page is intentionally left blank.)

CardOS/M4.01 with Application for Digital Signature Creation (as ICC embedded software conforming with German SigG, SigV and DIN V 66291-1)

Security Target

SIEMENS AG
ICM D IS
Hofmanstrasse 51
D-81379 Munich

Version 1.05

Change History

Version	date	Changes
0.10	08.2000	First Edition CardOS M4.0 based on the Version 0.99 of Tele Trust Deutschland
0.11	31.08.2000	Revision through debis; editorial changes, unused options removed
0.12	06.10.2000	Revision through Siemens; editorial changes
0.13	13.10.2000	Revision through debis; editorial changes, some opened questions
0.14	06.11.2000	Revision through Siemens; change from S-Chip to P-Chip and editorial changes
0.15	8.12.2000	Revision through Siemens and debis, editorial changes
0.16	19.12.2000	Revision through Siemens and debis: • OR1.2 changed, hardware assumptions added • IA1.1.1 and IA1.1.2: wording • TOE behaviour with security violation flag A redefined
1.0	15.01.2001	Final revision through Siemens, editorial changes
1.01	20.03.01	print errors (definition of CAS2)
1.02	15.01.2002	Update of Table 1, Update of references to SigG and SigV
1.03	20.02.2002	Footnote to M1: In fact the part of M1 detecting the “Potential attacker” is implemented by the mechanismus M7.
1.04	25.02.2002	Update of Table 1
1.05	04.03.2002	no temperature sensor on the ICC (AE5.3)

Table of Contents

Figures

Tables

1. Product Rationale

1.1. Product Overview

CardOS/M4 is a multifunctional smart card operating system supporting active and passive data protection. The operating system is designed to meet the most advanced security demands. CardOS/M4 complies with the ISO standard family ISO 7816 part 3, 4, 5, 8 and 9.

CardOS/M4 is designed to meet the requirements of the German Digital Signature Act ([6], [7]).

The versatile and feature rich operating system supports rapid application development on smart cards. Nearly every function of the operating system can easily be parameterized, even after the initial personalization of cards, if required.

A patented scheme for initialization/personalization provides for cost efficient mass card production by card manufacturers.

CardOS/M4 Features

General features:

- CardOS/M4 runs on the Infineon SLE66 chip family. The SLE66CX320P chip with embedded security controller for asymmetric cryptography and true random number generator has successfully been certified against the ITSEC E4 “high” security requirements [14].
- Shielded against all presently known security attacks
- All commands are compliant with ISO 7816-4, -8 and –9 standards.
- PC/SC- compliance and CT-API
- Cleanly structured security architecture and key management
- Customer and application dependent configurability of card services and commands
- Extensibility of the operating system using loadable software components (packages)

File system

CardOS/M4 offers a dynamic and flexible file system, protected by chip specific cryptographic mechanisms:

- Arbitrary number of files (EFs, DFs)
- Nesting of DFs limited by memory only
- Dynamic memory management aids in optimum usage of the available EEPROM.
- Protection against EEPROM defects and power failures

Access control

- Up to 126 distinct programmer definable access rights
- Access rights may be combined with arbitrary Boolean expressions.
- Any command or data object may be protected with an access condition scheme of its own.
- All security tests and keys are stored as so-called key objects in the DF bodies (no reserved file IDs for key- or PIN files).
- Security structure may be refined incrementally after file creation without data loss.

Cryptographic Services

- Implemented algorithms: RSA 1024 Bit (PKCS#11), SHA-1, , Triple-DES (CBC), DES (ECB, CBC), MAC, Retail-MAC
- Protection against Differential Fault Analysis (”Bellcore-Attack”)
- Protection of DES and RSA against SPA[2] and DPA[3]
- Support of ”Command Chaining” following ISO 7816-8
- Asymmetric key generation “on chip” using the onboard true random number generator
- Digital Signature functions “on chip”
- Connectivity to external Public Key certification services

Secure Messaging

- Compatible with ISO 7816-4
- may be defined for every command and every data object (files, keys) independently.

1.2. Identification of TOE

The integrated circuit card (ICC) contains

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

(2) data of other applications.

The TOE consists of

(1) all software residing on the card (executable data including RMS),

[2] Simple Power Analysis

[3] Differential Power Analysis

(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 cardholder specific data) within the card during the initialization and personalization phases in the ICC life cycle, which are represented by the administration phase in CardOS,

(2) to generate digital signatures,

(3) to provide security for the digital signature generation and

(4) to generate asymmetric key pairs on the ICC.

Other parts of the TOE software are needed

(1) to use the SigG application with additional functions which may include signature verification,

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

(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.

The TOE is a product.

The TOE consists of the following components:

Table 1: Components of the TOE

No.	Type	Term	Version	Date	Form of delivery
1	Software (OperatingSystem)	CardOS M4.01	C803	11.06.2001	loaded in ROM / EEPROM
2	Software (Application / Data Structure)	SigG application	0.20	26.09.2001	loaded in EEPROM
3	Documentation	CardOS/M4 User’s Manual with correction sheet	1.0	10/2001	Paper form or PDF-File
4	Documentation	CardOS/M4 User’s Manual - correction sheet	1.0	02/2002	Paper form or PDF-File
5	Documentation	Manual for Cardholder	1.02	27.02.2002	Paper form or PDF-File

6	Documentation	Manual for Terminal Developer	1.12	27.02.2002	Paper form or PDF-File
7	Documentation	Documentation for Trust Center	1.02	27.02.2002	Paper form or PDF-File
8	Documentation	Delivery, Generation and Configuration	1.1	18.12.2001	Paper form or PDF-File

The TOE is running on the Infineon chip SLE66CX320P. The ICC's hardware is not part of the TOE.

CardOS, the first component of Table 1, contains among others a package with corrections of the CardOS system software

1.3. 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 signature key of the cardholder in accordance with the SigG legislative [6], [7] and the standard [9].

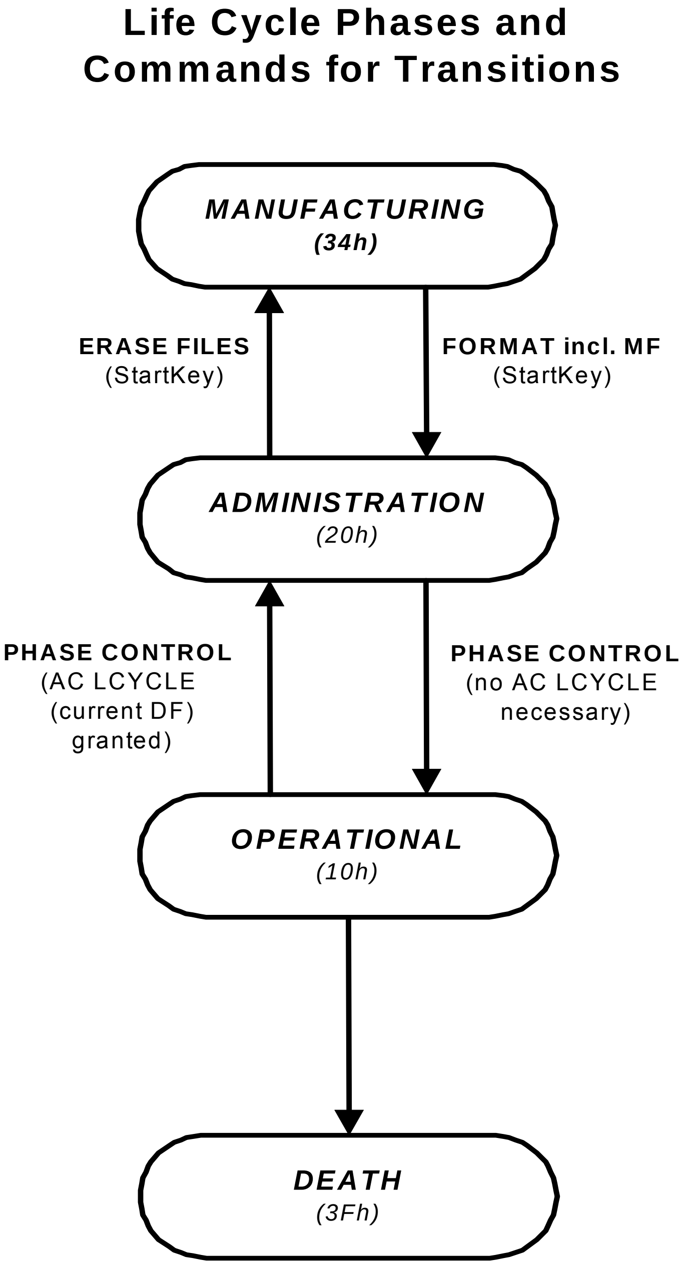
The development and manufacturing of the ICC's software and hardware leads to the ICC being ready to be used for a specific purpose (application). The ICC will be loaded with the SigG application including cardholder specific data in the personalization phase of the ICC. The TOE implements security features to ensure secure personalization of the ICC.

The TOE is used to **generate** the cardholder's signing key pair (SK.CH.DS, PK.CH.DS)

Card Life Cycle

In order to secure the personalization of a CardOS the TOE's different so-called life cycle phases are provided, witch are shown in **Figure 1**.

Figure 1: Card Life Cycle Phases and Transitions between them


Life Cycle Phases and Commands for Transitions
MANUFACTURING (34h)
ERASE FILES (StartKey)
FORMAT incl. MF (StartKey)
ADMINISTRATION (20h)
PHASE CONTROL (AC LCYCLE (current DF) granted)
PHASE CONTROL (no AC LCYCLE necessary)
OPERATIONAL (10h)
DEATH (3Fh)

The administration phase comprises the logical initialization und personalization phases.

The TOE always “knows” of its current life cycle phase.

Transitions between the life cycle phases are possible using the specified commands and system keys. All transitions shown in **Figure 1**, except the transition from the *OPERATIONAL* to the *ADMINISTRATION* phase, are permanent.

A permanent transition means that the current life cycle phase is not affected by a reset of the ICC.

The transition from the *OPERATIONAL* to the *ADMINISTRATION* phase is only temporary. After a reset of the ICC the current life cycle phase will be *OPERATIONAL* again.

CardOS uses two system keys, they are 16 bytes (triple-) DES Keys:

1. StartKey: To change the Life cycle from Manufacturing to Administration and back,
2. LoadPackageKey: To activate the CodePackage.

Table 3: Logical initialization and personalization of the SigG Application

Step	Phase	Action
1.	Manufacturing	Card authentication with StartKey
2.	Manufacturing	change StartKey
3.	Manufacturing	Change life cycle phase to Administration (implicit create MF)
4.	Administration	Bringing in administrative keys[4]
5.	Administration	Read Serial number

[4] e.g. challenge response and secure messaging keys

6.	Administration	Create file structure
7.	Administration	Filling file contents
8.	Administration	Load and activate Packages (with PackageLoadKey)
9.	Administration	Generate key pair
10.	Administration	Read Public Key
11.	Administration	write certificates
12.	Administration	Delete not needed Packages
13.	Administration	Restricting access rights
14.	Administration	Change life cycle phase to Operational
15.	Operational	Initialization and Personalization is completed. When this life cycle phase has been reached then the TOE is issued to the customer. The customer cannot switch to any other phase of the TOE.

It’s allowed to initialise and personalise other file structures besides SigG, e.g. between the steps 4-5 and 5-6 or between the steps 10-11 or 11-12.

DEATH

In this life cycle phase of the TOE all smart card commands except the GET DATA command are disabled. Other TOE functionality is blocked irreversibly.

The life cycle phase DEATH will be reached if one of several special events occur in the TOE (EEPROM weakness, filesystem or EEPROM corrupted or potential security violation flag has been set (Active Shield))

Each life cycle phase has a specific command set.

In the operational phase the cardholder uses the TOE by providing it to some IT system, which contains the message to which the cardholder wishes to apply a digital signature. The TOE and the IT system communicate through an interface device (IFD). Moreover the IFD is the human interface to the TOE.

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 the administration phase the TOE may be used at an IFD within a CA/RA. 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 above), the ICC may also be used with Public IFDs. Since the difference between **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.

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. After a successful authentication and in dependence of the configuration, the TOE allows to generate exactly ***one digital signature***. For special cards (Security model for TrustCenter) the TOE allows to generate (i) 1 till *n* or (ii) an unlimited number of digital signatures.

The IT system (i) transforms the message text into the hash-value and transmits the hash-value to the TOE or (ii) transmits the complete message text to be hashed by the TOE (see [9]). The TOE calculates the digital signature of the hash-value with the SigG private signature key of the cardholder stored in the TOE. The TOE returns the digital signature to the IFD. The SigG private signature key of the cardholder never leaves the ICC.

The ICC may be used as multi-application smart card. In this case an additional application may have been loaded on the ICC in the administration phase. But the TOE prevents the execution of executable data possibly existing in this additional application.

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 enter this transport PIN and to change his operational PIN with a length of at least 6 digits; otherwise the authentication will fail[5]. After the successful authentication with the transport PIN this PIN will be blocked forever. The operational PIN and PUK can only be used after a successful authentication with the transport PIN. This ensures that before the TOE can be used to generate signatures, the operational PIN has to be changed. Whenever the PIN is changed in the future, the PIN also has to be at least 6 digits

[5] After the third consecutive unsuccessful authentication attempt with the transport PIN, it will blocked irreversibly

long. As the transport PIN can be used successfully only once, an accepted first authentication ensures that nobody has authenticated before with the transport PIN. In this case the cardholder can also be sure that nobody has used the TOE before to generate a digital signature.

The TOE does not support the ISO command TERMINATE CARD USAGE. Instead, (i) the expiration of the PUK leads to a state in which the DF_{SigG} is permanently blocked and the SigG Application cannot be used any more. Or (ii) if a potential security violation is detected (AE5.4) the TOE is blocked as described in SO8.

1.4. 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 4).

Table 4: 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	Technical assumption about the ICC hardware

1.4.1. Life cycle security (AE1)

The TOE is expected in the first place to enforce the security objectives as described in section 1.6 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 shall be relied upon. The following assumption AE1 about the life cycle of the ICC is made (see also AE2 in the following sub-section):

(AE1.1) The security of procedures in (i) the manufacturing phase, (ii) the initialization phase and (iii) the personalization phase[6] of the ICC life cycle is assured.

(AE1.2) The personalization facility and the certification authority keep the confidentiality of authentication information of TOE users.

[6] The initialisation and the personalisation phase together are called "administration phase" (see **Table**)

1.4.2. Integrity and quality of key material (AE2)

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

(AE2.1) The environment ensures for the ICC authentication key pair[7]

(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 [9], section 9[8]),

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

(AE2.2) The environment shall ensure for the SigG signing key pair of the root certification authority

(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 [9], section 9),

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

(AE2.3) The environment ensures for the SigG signing key pair of the certification authorities

(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 [9], section 3.2),

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

(AE2.4) For the method of use “Generation of cardholders signing key on the ICC” the environment ensures authenticity (especially origin) of the public key (see PK.CH.DS in [9], annex D) in the certificate C.CH.DS, generated by the certification authority for SigG digital signatures.

1.4.3. SigG compliant use of the TOE (AE3)

The following assumptions about the SigG compliant use of the TOE are made:

[7] The current version of the TOE does not support the authentication key pair.

[8] The use of the object in [9] is not consistent. Sometimes RCA is used instead of DEPCA and AUT instead of CS_AUT.

(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 shall be assured.

(3) The cardholder keeps the confidentiality of all PINs and PUKs.

(4) The cardholder changes the PIN regularly.

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

(6) The cardholder uses the TOE only with an office IFD.

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

1.4.4. Use with SigG compliant IFD (AE4)

The SigG regulations require 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 shall use the TOE's SigG application only with SigG compliant office IFDs.

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

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

(2) In unlimited signature generation configuration (see section 1.3), 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 **O3** and PUK **O4**).

(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 3.1) and the TOE makes this transparent to the office IFD, then the office IFD reacts accordingly and makes this state transparent to the user.[9]

(6) If the maximum number of failed authentication attempts allowed for the cardholder reference data (PIN **O3**) or the cardholder reset code (PUK **O4**) 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 CA/RA) then the certification authority has to verify the SigG accreditation of the ICC presented by the cardholder.

1.4.5. Security assumption about the ICC hardware (AE5)

The following assumptions about the ICC hardware are made:

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

(1) protects the TOE against modification and

(2) ensures the confidentiality of the SigG private signature key of the cardholder and the private authentication key stored on the ICC against physical attacks.

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

(AE5.3) The ICC hardware implements mechanisms detecting and reacting to the following events:

- lower or higher clock frequency (than allowed / specified),
- lower or higher supply voltage

by generating a continuous reset signal as long as the physical conditions stay out of the specified range.

(AE5.4) The ICC hardware implements security mechanisms which

(1) detect any physical modification of the Active Shield and

(2) signal that to the TOE.

[9] This assumption is drawn from SigV, §15 (4): “Sicherheitstechnische Veränderungen an technischen Komponenten nach Absätzen 1 bis 3 müssen für den Nutzer erkennbar werden.”

(AE5.5) The ICC hardware ensures that the private signature key does not have to be stored (temporarily) in any other place than in the key object within the EEPROM.

1.5. 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 [9]. 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 2 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”.

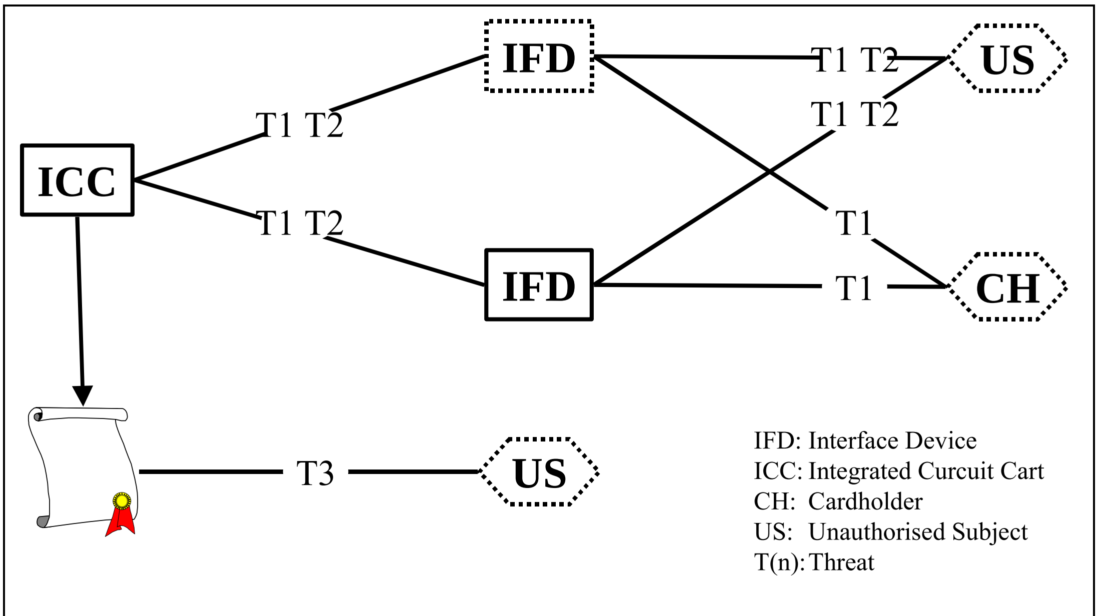


Figure 2: Threat Scenario (in case of method of use “Office IFD only”)

Table 5: Security Threats

Id	Security Threat
T1	Extraction of the cardholder’s private key
T2	Misuse of the signature function
T3	Forged data ascribed to the cardholder

1.5.1. Extraction of the cardholder’s private key (T1)

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

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

The extraction of the SigG private signature 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 private key stored in the ICC.

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

1.5.2. Misuse of the signature function (T2)

The TOE generates digital signatures of the cardholder.

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

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

1.5.3. Forged 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 an image of the message text.

(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 modification of the message cannot be averted but this may be noticed by the recipient of the message.

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

The message will be ascribed to the originator indicated in the message. If the message is signed by a SigG digital signature, the originator of the message will be identified as the owner of the certificate containing the public key matching the digital signature.

1.6. Summary of Security Features

The following Table 6 identifies the security objectives. The security objectives are enumerated as SOn.m where n indicates the number of the subsection in the current section and m the number of the security objective within this subsection. 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 6: Security objectives

Id	Security Objective
SO1	Prevent disclosure, copying or modification of the cardholder's private key
SO2	Prevent unauthorised use of the SigG digital signature function
SO6	Quality of key generation
SO7	Provide secure digital signatures
SO8	React to potential security violations

1.6.1. Prevent disclosure, copying or modification of the cardholder's private key (SO1)

(SO1) The TOE ensures the confidentiality and the integrity of the SigG private signature key of the cardholder stored in the TOE under two aspects:

(SO1.1) The TOE shall prevent any kind of extraction of the cardholder's private key from the ICC.

(SO1.2) The TOE shall prevent any kind of modification of the cardholder's private key in the ICC.

The cardholder intends to protect the integrity of his message while it transits (either over space or time) to the intended recipient. It is the TOE's principal 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 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 (see [7] §15 (1) Sentence 2).

This security objective covers threat T1.1 and T1.2 defined in section 1.5.1.

The TOE shall implement the security enforcing function AC1 and AC2 described in sections 2.2.2 and 2.3.2 to fulfil the security objective SO1. The SEF OR1 described in sections 2.2.4 and 2.3.4 shall prevent illicit information flow between the SigG application and other application embedded on the ICC through temporarily used storage areas. The SEF DX1 and DX2 described in section 2.2.5 and 2.3.5 shall prevent disclosing of the SigG private signature key of the cardholder in the digital signatures generated by the TOE. The secure blocking state of the TOE shall ensure the security of the SigG private signature key of the cardholder if a potential attack was detected (see SEF AC3 and AU1 in sections 2.2.2, 2.2.3, 2.3.2 and 2.3.3).

1.6.2. 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.

(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 are stored in the TOE and shall not be disclosed.

This security objective counters the threat T2 (section 1.5.2).

[10] The security objective SO2 corresponds to [7] §15 (1) Sentences 1 and 3, and (2) 1. a) and b), requiring authentication of the cardholder for access to functions using the SigG private signature key of the cardholder.

To use the SigG application the cardholder has to authenticate by knowledge (by presenting a PIN).

The TOE implements the security enforcing functions IA1, IA2, IA3 and IA4 as well as AC1 described in sections 2.2.1, 2.3.1, 2.2.2 and 2.3.2 to fulfil the security objective SO2. Authentication failures are being made apparent to the cardholder through the security enforcing function AU1 described in section 2.2.3. The **secure blocking state**[11] of the TOE shall ensure the security of the SigG signature function if a ***potential security violation*** (see (SO8.1) below) has been detected (see SEF AC3 and AU1 in sections 2.2.2, 2.2.3, 2.3.2 and 2.3.3).

1.6.3. Quality of key generation (SO6)

The TOE shall fulfil the following security objective concerning the quality of key material generated by the TOE:

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

(1) If private keys are generated either in the personalization phase or in operational use phase by means of the TOE then this process shall be performed in a confidential way.

(2) The private keys generated by the TOE shall be unique with a very high probability and cryptographically strong.

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

The key pair shall be generated by appropriate algorithms and parameters according to [7] Anlage 1, Abschnitt I Nr. 2 (see [9]). The cryptographic quality for the ICC device authentication key pair is necessary to ensure the cryptographic strength of the mutual device authentication, see [9].

The security objective SO6 counters the threat T3 ensuring a precondition[12] for the cryptographic strength of the digital signature (see also [8]).

The TOE implements the security enforcing function DX1 described in sections 2.2.5 and 2.3.5 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 section 2.2.2).

[11] See Glossary for the definition.

[12] Cryptographically weak key material involves danger for the strength of the digital signature.

1.6.4. Provide secure digital signatures (SO7)

The principal security objective of the TOE is the generation of secure SigG digital signatures (SO7)[13].

(SO7.1) The TOE provides a function to generate a SigG digital signature for the data presented by the IFD using the SigG private signature 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 the SigG private signature key of the cardholder cannot generate the signature.

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 [8]).

The data presented by the IFD and to be signed are (i) the hash-value of the message text or (ii) the complete message text to be hashed by the TOE (see [9], section 14).

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

The TOE implements the security enforcing function DX2 described in sections 2.2.5 and 2.3.5 to fulfil the security objective SO7 generating secure digital signatures. The appropriate reaction of the TOE shall ensure the security of SigG signature generation if a potential attack was detected (see SEF AC3 and AU1 in sections 2.2.2, 2.2.3, 2.3.2 and 2.3.3).

1.6.5. React to potential security violations (SO8)

The TOE fulfils the following security objective SO8[14]:

(SO8.1) The TOE detects a potential security violation, which is identified by the TOE itself.

For this TOE, a **potential security violation** is defined in the following way:

[13] The security objective SO7 is drawn from [7] §15 (1) Sentence 4. The requirement of [7] §15 (1) Sentence 4 that the cardholder's secret key cannot be derived from the signature is a sub-case of SO1.1 because the signature is a part of the TOE's output.

[14] The security objective SO8 is drawn from [7] §15 (4).

Somebody is trying to use the TOE when a potential security violation flag is set (see Glossary).

(SO8.2) If a potential security violation is detected then

(1) the TOE has already reached a ***secure blocking state*** (see Glossary) by
(i) disabling all functionalities of the SigG Application (security violation flag A is set)[15] or
(ii) disabling all functionalities of the ICC, with the exception of sending the ATR and the command “Get Data”.

(2) the secure blocking state is made apparent to the user. The blocked TOE will send an appropriate Return Code to the IFD.

The security objective SO8 counters the threats T1 to T3 in case of detected potential security violation

The TOE implements the security enforcing functions IA1.3, AC3 and AU1 described in sections 2.2.1, 2.3.1, 2.2.2, 2.2.3, 2.3.2 and 2.3.3 to fulfil the security objective SO8.

SO8 is fulfilled independently from and complements (AE5.3). If the ICC hardware detects any abnormal physical condition and prevents the execution of the TOE by the reset signal (see (AE5.3)(1)), than the SO8 is also fulfilled because this is a secure state of the ICC discernible by the cardholder.

[15] Only the command Get Data is still executable referring to the DF_{SigG}

2. Security Functions

2.1. Definitions and Global Substitutions

Note: The names of processes, objects, access-types and security-relevant-events will be presented in **bold face** in a chapter when introduced and explained for the first time. They are printed *italic* when referred to outside of tables to point out the keywords to the reader. The definitions of the terms are collected in the glossary (see section 8).

2.1.1. Subjects

The IFD presents as technical process the outside world beyond the 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 and as intended by the human user. In the point of view of the TOE's 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 subject **S3** IFD represents an IT system. The outside world is represented by a pair $(u,t) \in \{S1, S2, S7\} \times \{S3\}$. The term "Anybody" is introduced for the set of the two subjects S1 and S2 to make some descriptions easy.

The TOE is aware of the subjects identified in the following table.

Table 7: Subjects

Id	**Subject**
S1	Cardholder
S2	Somebody
S3	IFD
S7	Potential attacker

Subject S1 Cardholder

In the operational phase the **subject S1 Cardholder** is a human user, for whom 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 (AE3.1)).

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

Subject S2 Somebody

The **subject S2 Somebody** is any human user of the ICC different from the subject **S1** Cardholder and **S7** Potential attacker, i.e. (i) not being in legitimate possession of the verification data (PIN and PUK) defined for the cardholder[16] and (ii) using the TOE not being in the secure 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 authentication data for a non-SigG application on the ICC.

Subject S3 IFD

The **subject S3 IFD** is an interface device connected to the ICC, which (i) doesn't have initiated mutual device authentication according to [9], section 18, or (ii) is not a SigG accredited IFD (see definition in the glossary, section 8). The subject **S3** IFD may be an office IFD or an arbitrary public IFD connected to the ICC.

Subject S7 Potential attacker

The **subject S7 Potential attacker** is an arbitrary subject (among others a human user) trying to use the TOE in the secure blocking state (e.g. after a potential security violation is detected, see SO8, **CAS6** and **SRE10** for details).

2.1.2. Security-relevant-events

A security-relevant-event depends on (i) commands presented by the IFD to the TOE, (ii) command data presented by the IFD to the TOE, (iii) data concerning security relevant events persistently stored in TOE and (iv) events signalled by the ICC hardware to the TOE (see AE5).

The security-relevant-events given in the following Table 8 are recognised by the TOE.

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

Table 8: 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 (i) ICC is powered up by inserting the ICC into a suitable IFD (”activation”) or (ii) a hardware reset signal is given to the ICC. The TOE performs a well-defined start-up 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 cut off as by removal 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.

Note: if the SigG application is already open, then the selection of a file in the SigG application will not cause the security relevant event **SRE3**[17]. The security

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

relevant event **SRE3** is refined in section 3.1 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 (EF) file outside the SigG application is selected or (ii) 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 and (iii) the verification data presented for human user authentication match the reference data **O3** stored for the SigG application of the TOE in the operational phase. Since the TOE supports only user authentication by knowledge for the SigG application, condition (iii) is fulfilled if and only if the verification data presented match 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 PIN retry counter 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 with the verification data was attempted and (ii) **SRE5** does not occur and (iii) the maximum number of allowed consecutive failed authentication attempts with reference data is not exceeded (RC-PIN > 0). If **SRE6** occurs, the number of authentication attempts with reference data remaining is decreased by one.

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 with verification data was attempted, (ii) **SRE5** does not occur and (iii) the retry of the human user authentication for the SigG application is not allowed anymore (PIN retry counter RC-PIN:=0).

If the **SRE7** has occurred then the cardholder can reset the PIN retry counter RC-PIN and input a new PIN using the cardholder reset code **O4** (PUK), see **SRE11**. The PUK retry counter RC-PUK also has the initial value 3, so that there are three successive attempts to input the PUK. A successful attempt (i) resets the PUK retry counter RC-PUK to its initial value, (ii) resets the PIN retry counter RC-PIN to its initial value and (iii) authenticates the cardholder by reset code (**SRE11**)[18].

Note: If the retry counter for PUK **O4** reaches the value 0 (RC-PUK = 0), the cardholder authentication for the SigG application is permanently blocked and, thus, the TOE is in the secure blocking state (see also (SO2.2) and (SO8.1), (SO8.2)). The current value of the RC-PIN is not significant.

Security-relevant-event SRE8 Authentication expiration

The security relevant event **SRE8 "Authentication expiration"** occurs

(case_one): if a digital signature has been generated (not configurable by the cardholder) or

(case_n): if the following event occurs according to the configuration selected by the card manufacturer[19]

n digital signatures have been generated, where *n* ≥ 1 and ≤ 255.

If the card manufacturer has personalized the card with an ARA Counter = 0 for the PIN, which means an unlimited usage of the granted access right, then it is possible to generate an unlimited number of signatures (only for Trust Center use).

Security-relevant-event SRE10 Potential security violation occurred

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

(1) The retry of the authentication for unblocking and changing of PIN (**SRE11**) by presenting the reset code (PUK) is <u>not</u> allowed any longer (RC-PUK has been decremented and equals zero, in short: "RC-PUK reaches 0"). Moreover, an opening of the DF_{SigG} is not possible any more, because the **Potential security violation flag A** is set in the header of the DF_{SigG}. This flag will be automatically set, if the RC-PUK reaches 0 (RC-PIN can be zero or greater than zero).

(2) A signal provided by the underlying hardware indicates a modification of the active shield and the TOE sets the **Potential security violation flag B** (see (AE5.4) for further details).

(3) After the ICC is powered up or a hardware reset signal is given to the ICC the TOE detects that the **Potential security violation flag B** is set.

[18] this authentication by reset code does not allow to generate a digital signature, but only to change the PIN.

[19] configurable in ARA Counter of PIN

Security-relevant-event SRE11 Cardholder authenticated for PIN unblocking and changing by reset code

The security relevant event **SRE11** “**Cardholder authenticated for PIN unblocking and changing by reset code”** occurs if (i) the authentication for the PIN unblocking and changing by the reset code (PUK) of the SigG application has been attempted, (ii) the human user authentication for the SigG application by presenting the reset code is allowed (RC-PUK>0) and (iii) the reset code presented matches the stored reset code **O4** (PUK) of the SigG application of the TOE.

The authentication of the cardholder **S1** presenting verification data matching the **O4** SigG cardholder reset code (PUK) (i) will reset the retry counters RC-PIN and RC-PUK (for PIN as well as for PUK)[20] and (ii) will change the cardholder reference data (PIN) **O3** (see IA4 in section 2.2.1 and 2.3.1). The authentication by reset code allows only to change the PIN, but does not allow to generate digital signatures.

Security-relevant-event SRE12 Authentication for PIN unblocking and changing by reset code failed

The security relevant event **SRE12 “Authentication for PIN unblocking and changing by reset code failed”** occurs if (i) the authentication with the SigG cardholder reset code has been attempted, (ii) the presented reset code does not match the reset code **O4** “SigG cardholder reset code” stored in the TOE and (iii) the retry of authentication for PIN unblocking and changing by reset code is still allowed (RC-PUK > 0).

Note that the **SRE10** “Potential security violation occurred” represents the repeated failure of authentication attempts by reset code (PUK) if the retry of the human user authentication by presenting the reset code (PUK) is not allowed any longer (RC-PUK reaches 0).

2.1.3. Substitutions for the placeholders ”*object*” and ”*access-types*”

The following objects and related access-types are identified (see Table 9) and used to replace the respective placeholders within the claims section 2.3.

Table 9: Objects and related access-types

Id	Object	access-types
O1	SigG application	open, close

[20] i.e. it will unblock the PIN

Id	Object	access-types
O2	SigG private signature key of the cardholder (SK.CH.DS)	generate, use for signature generation, extract
O3	SigG cardholder reference data (PIN)	use for cardholder authentication, modify, block, unblock
O4	SigG cardholder reference reset code (PUK)	use for authentication, block
O5	SigG signature key certificate of the cardholder (C.CH.DS)	read, modify
O6	SigG public key of the root certification authority (PK.RCA.DS)[21]	read, modify
O12	SigG public key of the cardholder (PK.CH.DS)	read, modify, generate

Object O1 SigG application

The object **O1 SigG application** includes SigG related data objects as specified in Table 9 and any function or method to access or use that data.

The term “**open**” the **O1** means to enable 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.

The term “**close**” the **O1** means to disable these access-types and gives way to other not SigG related activities.

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

Object O2 SigG private signature key of the cardholder

The object **O2 SigG private signature key 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 [9].

The term “**generate**” of the **O2** means the generation of a SigG key pair of the cardholder on the ICC and storing the SigG private signature key of the cardholder in the TOE. The access type “generate” is applicable only in the administration phase.

The term “**use for signature generation**” of the **O2** means calling and performing of the respective command to generate a digital signature. Only such SigG signing key pair can be used for signature generation that has already been generated.

The term “**extract**” to the **O2** means (i) to use the key 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

[21] This public key is wrapped in the corresponding certificate

computation of a digital signature (e.g. electromagnetic emanation, power consumption and timing, in sense of infer).

Object O3 SigG cardholder reference data

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.

The term "**use for cardholder authentication**" the **O3** means to call a service, which provides human user authentication by comparing the **O3** with the verification data presented (see IA1 in sections 2.2.1 and 2.3.1).

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

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

The term "**unblock**" the **O3** means (i) to perform cardholder authentication by reset code (PUK **O4**) and (ii) if this cardholder authentication was successful to change the value of **O3** to the new reference data presented.

Object O4 SigG cardholder reference reset code

The object **O4 SigG cardholder reset code** (PUK) is the data permanently stored in the TOE and used to verify the reset code provided for the unblocking and changing of the reference data (PIN).

The term "**use for authentication**" the **O4** means to call the service (see mechanism 4.4), which (i) compares the **O4** (PUK) with the reset code presented (see IA1 in sections 2.2.1 and 2.3.1) and if it matches (ii) allows to unblock and change **O3** (PIN) (see IA4 in section 2.2.1 and 2.3.1).

Note that an authentication with **O4** allows only to unblock and change **O3**, but does not authenticate the cardholder for the generation of digital signatures, i.e. after entering the correct PUK **O4** it is not possible to generate a digital signature.

The term "**block**" the **O4** means to deactivate **O4** for the use for authentication through failure of authentication by reset code, if the retry of the authentication by reset code is not allowed any more (RC-PUK reaches 0, see **SRE10**). This triggers the secure blocking state of the TOE.

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.

Object O5 SigG signature key certificate of the cardholder

The object **O5 SigG signature key certificate of the cardholder** is a certificate of the SigG public key PK.CH.DS of the cardholder for the signing algorithm supported by the TOE (RSA), which is stored in the TOE and may be used by an external party to verify the cardholder’s signatures. This object is named C.CH.DS in [9].

The term “**read**” means to export the object **O5** to the IFD.

The term “**modify**” means to change the stored value of **O5**. The access type modify is applicable only in the administration phase.

Object O6 SigG public key of the root certification authority

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 wrapped in the certificate C.RCA.DS and may be used by an external party. This object **O6** is named PK.RCA.DS in [9].

The term “**read**” means to export the object O6 to the IFD.

The term “**modify**” means to change the stored value of **O6**. The access type modify is applicable only in the administration phase.

Object O12 SigG public key of the cardholder

The **object O12 SigG public key of the cardholder** can be used by an external party to verify the digital signature of the cardholder. This object is named PK.CH.DS in [9].The term “**read**” the **O12** means the use of the respective command of the TOE to transmit the object **O12** to the IFD.

The term “**generate**” the **O12** means the generation of a SigG key pair of the cardholder on the ICC and storing the SigG public signature key of the cardholder in the TOE. The access type generate is applicable only in the administration phase.

The term “**modify**” means to change the stored value of **O12**. The access type modify is applicable neither in the administration nor in the operational phase.

2.2. Informal Description

2.2.1. Identification and Authentication

IA1 Authentication of human user

The SEF IA1 contains three sub-functions: IA1.1, IA1.2 and IA1.3

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

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

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

The TOE will contain an authentication function SEF IA1.1 that detects the **S1** “Cardholder” in two different ways:

(1) The SEF **IA1.1.1** allows a subject S2 “Somebody” to authenticate himself as S1 “Cardholder” 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, the SEF IA1.1.1 will verify the verification data by means of O3 “SigG cardholder reference data” using the mechanism defined in paragraph 4.1. If the number of consecutive failed authentication attempts with reference data exceeds the maximum number of allowed failed authentication attempts (RC-PIN=0), the authentication attempt fails (independently of the presented verification data). If RC-PIN>0 and the presented verification data match the O3, the authentication attempt is successful. Successful authentication of the cardholder is defined as SRE5 “Successful cardholder authentication”. A failure of the authentication attempt as cardholder causes (see SEF IA3) either (i) SRE6 “cardholder authentication failure” if the maximum number of allowed consecutive failed authentication attempts with reference data is not yet exceeded (RC-PIN>0) or (ii) SRE7 “Repeated authentication failure”, if the maximum number of allowed consecutive failed authentication attempts with reference data is exceeded (RC-PIN=0). The SEF IA1.1.1 uses the mechanism M1 described in section 4.1.

(2) The SEF **IA1.1.2** allows a subject S2 “Somebody” to authenticate himself for PIN change for the SigG application presenting data as reset code. This means that after successful authentication with PUK (O4), the subject S2 “Somebody” is granted the right to change the PIN (O3), but not the right to generate a digital signature. If the retry of authentication by presenting the reset code is allowed (RC-PUK>0), then the presented data are verified by means of O4 “SigG cardholder reset code”. If the presented data match O4 then this will be interpreted as SRE11 “Cardholder authenticated by reset code”. If the presented data do not match O4 then this will be interpreted as SRE12 “Cardholder authentication by reset code failed”. If the presented data do not match O4 and the number of consecutive failed authentication attempts with reference data exceeds the maximum number of allowed failed authentication attempts this will be interpreted as the **SRE10** “Potential security violation occurred” (see SEF IA3). The SEF IA1.1.2 uses the mechanism M4 described in section 4.4.

SEF **IA1.2**: The TOE assumes for the SigG application the default identity of the human user **S2** “Somebody” after the following SREs: **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"[22]. This SEF IA1.2 uses the mechanism M1 defined in paragraph 4.1.

SEF **IA1.3**: After **SRE10** “Potential security violation occurred”, the TOE will assume the **S7** Potential attacker as the human user of the TOE. This SEF IA1.3 uses the mechanism M1 defined in paragraph 4.1.

[22] therefore the PIN must be in DF_DinSig

IA2 Changing reference data

The TOE will contain an authentication function SEF IA2 that permits the **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 stored **O3** (PIN) and (ii) defining the new **O3** using the mechanism M2 defined in paragraph 4.2. The SEF IA2 permits the change of SigG cardholder reference data only after successful authentication of the cardholder defined as SRE5 “Successful cardholder authentication”. A failure of the authentication attempt as the cardholder causes either (i) SRE6 “cardholder authentication failure” if the maximum number of allowed consecutive failed authentication attempts with reference data is not exceeded (RC-PIN>0) or (ii) SRE7 “Repeated authentication failure” if the maximum number of allowed consecutive failed authentication attempts with reference data is exceeded (RC-PIN=0).

IA3 Blocking the reference data

The SEF IA3 counts the consecutive failed authentication attempts and prevents the subjects **S1** “Cardholder” and **S2** “Somebody” from using the object **O3** “SigG cardholder reference data” if the maximum number of allowed consecutive failed authentication attempts with reference data is exceeded (e. g. **SRE7** has occurred, RC-PIN=0). If **SRE7** has occurred, the SEF IA3 will reject the authentication attempt independent of whether the presented data match O3 or not. The SEF IA3 uses the mechanism M3 defined in paragraph 4.3.

IA4 Unblocking and changing the reference data (Reset Retry Counter)

After successful “*authentication for PIN unblock and change*” with the **O4** “Reset code of the cardholder” (PUK) the SEF IA4 permits (i) to unblock the SigG cardholder reference data **O3** and (ii) to modify **O3** (PIN) using the mechanism M4 defined in paragraph 4.4. The successful *authentication for PIN unblock and change* with the reset code is defined as **SRE11** “Cardholder authenticated by reset code”. A failure of the authentication attempt by reset code (PUK) causes **SRE12** “Cardholder authentication by reset code failed”[23] or SRE10 “Potential security violation occurred”[24]. The SEF IA4 uses the mechanism M4.

2.2.2. Access Control

AC1 Access control of commands

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

[23] if RC-PUK > 0

[24] if RC-PUK = 0

The SEF AC1 will ***permit*** that the subjects ***s*** access the object ***o*** by the access-type acy(***s,o***) defined in the **Table 10**.
The SEF AC1 will ***prevent*** that the subjects ***s*** access the object ***o*** by the access-type acn(***s,o***) defined in the **Table 11**. [25]

The SEF AC1 uses the mechanism M6 defined in paragraph 4.6.

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.

The underlying security policy permits to open and to close the SigG application in the **CAS6** because the TOE may still be partly operational in **CAS6** (see **SRE10**).

Note that these access-sets are defined for the ***operational phase only***. The TOE will detect the subject **S7** "Potential attacker" if the TOE is in the **Blocking state of the TOE**. The access-type "*extract*" is prevented by **AC2** for all subjects and, hence, not mentioned here. This security target does not cover the privileged IFD authenticated with RoleID=02 defined in [9], annex C. Therefore the TOE does not allow to *modify* or *supplement* the objects **O5**, **O6**.

Table 10: Access-set acy(*s,o*) of SEF AC1

Object		**S1** Cardholder	**S2** Somebody	**S7** Potential attacker
O1	SigG application	open, close	open, close	close[26]
O2	SigG private signature key of the cardholder	use for signature generation		
O3	SigG cardholder reference data	use for cardholder authentication, modify, block, unblock	use for cardholder authentication, block	
O4	SigG cardholder reset code	use for authentication, block	use for authentication, block	
O5	SigG signature key certificate of the cardholder	read	read	
O6	SigG public key of the root certification authority	read	read	

[25] acy() and acn() mean access yes and access no, respectively

[26] Only if the potential security violations flag A is set

Object		S1 Cardholder	S2 Somebody	S7 Potential attacker
O12	SigG public key of the cardholder	read	read	

Table 11: Access-set acn(o,s) of SEF AC1

Object		**S1** Cardholder	**S2** Somebody	**S7** Potential attacker
O1	SigG application			open
O2	SigG private signature key of the cardholder	generate	generate, use for signature generation	generate, use for signature generation
O3	SigG cardholder reference data		modify, unblock	use for cardholder authentication, modify, block, unblock
O4	SigG cardholder reset code			use for authentication, block
O5	SigG signature key certificate of the cardholder	modify	modify	read, modify
O6	SigG public key of the root certification authority	modify	modify	read, modify
O12	SigG public key of the cardholder	modify, generate	modify, generate	modify, generate, read

AC2 Access control of extraction

The SEF AC2 will prevent the extraction of the SigG private signature key SK.CH.DS (**O2**) of the cardholder. The SEF AC2 uses the mechanism M5 defined in paragraph 4.5.

The cardholder may use his private signing key 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 TOE’s security functions as specified by those functions. This also includes the prevention of any sort of inference of the private key by observing the TOE’s behaviour during the generating of a digital signature.

The TOE doesn't provide any command that could be used to select and to read a key-record. The SigG private signature key SK.CH.DS is only used implicitly.

The corresponding modules for signature generation are implemented in a way which is resistant against all known attacks: The RSA algorithm which is used for signature generation is implemented in a DPA- and SPA-resistant way; and the SigG private signature key (O2) is protected against DFA (Differential Fault Analysis, ”Bellcore-Attack”). (see M5).

AC3 Secure blocking state

The Secure Blocking State occurs, if one of the potential security violation flags is set.

These flags prevent the object **O1** from being opened. The SEF AC3 uses the mechanism M7 defined in paragraph 4.7.

2.2.3. Audit

AU1 Information about secure blocking state

The SEF AU1 will inform the human user about the secure blocking state of the TOE by means of a blocking information.

The appropriate Return Code will be generated by the TOE if it is in the Secure Blocking State (if **SRE10** has occurred).

The SEF AU1 uses the mechanism M7 defined in paragraph 4.7.

Note that, according to (AE4.2)-(5) the SigG compliant IFD shall inform the cardholder about the secure blocking state of the TOE.

2.2.4. Object Reuse

The SEF OR1 ensures that sensitive data (PIN, PUK and SK.CH.DS (O2)) will not remain in temporary used storage areas and be read accidentally by another application or by Somebody S2.

OR1.1 The values of PIN and PUK, which have been entered by the user, will immediately be actively erased from the RAM or XRAM areas after their use.

OR1.2 The TOE does not store the SK.CH.DS (O2) in any other place than in the key object within the EEPROM.

The SEF OR1 will use the mechanism M9 defined in paragraph 4.8.

2.2.5. Data Exchange

DX1 Key Generation

The SEF DX1 generates the cardholder's signature key pair on the ICC. The cardholder's signature key pair consists of the SigG private signature key SK.CH.DS of the cardholder (**O2**) and the SigG public signature key PK.CH.DS of the cardholder (**O12**). During the key-generation the key-header and the key-body are written, where the key-header specifies the attributes of the key, including its allowed usage (digital signature creation), the algorithm (RSA) and the modulus length of the key pair (1024 bit). This SEF DX1 shall be used only in the personalization phase; the cardholder cannot generate any key pair.

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 personalization phase (see sec. 1.3). The SEF DX1 implements the security objective **SO6** and has an essential effect on the secure operation of the TOE in the operational phase. Because of that the inclusion of the SEF DX1 into Security Target is easily to justify.

The SEF DX1 will use the mechanism M10 defined in paragraph 4.9.

DX2 Digital signature generation

The cardholder generates a SigG compliant digital signature by means of the SEF DX2 using SigG private signature key (SK.CH.DS). The SEF DX2 receives the data to be signed from the IFD and returns the signature of these data to the IFD. Only the cardholder is allowed to execute SEF DX2 (DX2 can only be executed after successful cardholder authentication by PIN **SRE5**; after successful cardholder authentication by PUK **SRE11** it is not possible to use SEF DX2). The TOE allows to generate

(case_one) only one digital signature (after this signature has been generated, SRE8 "Authentication expiration" occurs) or

(case_n) a configurable number *n* of digital signatures (where *n* can be ≥ 1 and ≤ 255 or unlimited)

Witch case is implemented for a concrete issue of the TOE is defined only by the card manufacturer in the administrative phase and cannot be changed in the operational phase (see also the definition of SRE8 in section 2.1.2 for these two cases).

The TOE supports two 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 or (ii) transmits the complete message text to be hashed by the TOE.

SEF DX2 will use the mechanism M11.

2.3. Semiformal specification of the security function

2.3.1. 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 *{user, process}* = **S1** Cardholder *process* = SigG application *security relevant event* = **SRE5** Successful cardholder authentication *paragraph* = 4.1	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 4.1. Note that the SigG application as process means here 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 IA1.1.2 *{user, process}* = **S1** Cardholder *process* = SigG application *security relevant event* = **SRE11** Cardholder authenticated by reset code *paragraph* = 4.4	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 4.4. Note that the SigG application as process means here the usage of all objects accessible within the opened SigG application. Note that the subject **S1** "Cardholder" in the context of IA1.1.2 can not directly generate digital signatures, but since he has gained the right to change the PIN, he can change the PIN, authenticate with a new PIN and then generate digital signatures.
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**:	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",

Construction	**Security claim**
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, **SRE8** Authentication expiration, **SRE12** Cardholder authentication by reset code failed *n* = 4.1	**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 4.1.
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 IA1.3 *{user, process}* = **S7** Potential attacker *process* = (i) authentication attempt or (ii) activation of the Active Shield of the ICC to the TOE *security relevant event* = **SRE10** Potential security violation occurred *n* = 4.1	The TOE contains a SEF IA1.3 that will detect the identity of the subject **S7** “Potential attacker” requesting (i) an authentication attempt or (ii) activation of the Active Shield of the ICC to the TOE after **SRE10** “Potential security violation occurred” using the mechanism defined in paragraph 4.1.
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	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 4.2.

Construction	Security claim
cardholder authentication *n* = 4.2	
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* = 4.3	This TOE contains a SEF IA3 that will prevent the use for cardholder authentication of the object **O3** “SigG cardholder reference data” by the **S1** “Cardholder” and **S2** “Somebody” after **SRE7** “Repeated authentication failure” using the mechanism defined in paragraph 4.3.
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* = 4.4	This TOE contains a SEF IA4.1 that will permit a subject **S1** “Cardholder” to unblock the object **O3** “SigG cardholder reference data” after **SRE11** “Cardholder authenticated by reset code” using the mechanism defined in paragraph 4.4.
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	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 4.4.

Construction	Security claim
security relevant event = **SRE11** Cardholder authenticated by reset code *n* = 4.4	

2.3.2. 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*) *{user, process}* = subject *s* *n* = 4.6	This TOE contains a SEF AC1.1 that will permit the access-set acy(*s*,*o*) of a subject *s* using the mechanism defined in paragraph 4.6. 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* represents **O1** to **O12** in **Table 10**.
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 AC1.2 *access set* = acn(*s*,*o*) *{user, process}* = subject *s* *n* = 4.6	This TOE contains a SEF AC1.2 that will prevent the access-set acn(*s*,*o*) of a subject *s* using the mechanism defined in paragraph 4.6. 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* represents **O1** to **O12** in **Table 11**.
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**	This TOE contains a SEF AC2 that will prevent the **S1** "Cardholder", **S2** "Somebody", **S3** "IFD", **S7** "Potential attacker" to extract the **O2** "SigG private signature key of the cardholder" using the mechanism defined in paragraph 4.5.

Construction	Security claim
IFD, **S7** Potential attacker; extract *object* = **O2** SigG private signature key of the cardholder *n* = 4.5	
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* = 4.6	This TOE contains a SEF AC3 that will prevent the **S7** “Potential attacker” to open the object **O1** “SigG application” using the mechanism defined in paragraph 4.7.

2.3.3. 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**. The SEF AU1 uses the mechanisms defined in paragraph 4.7.

2.3.4. Object Reuse

Construction	Security claim
Action Phrase: The TOE contains a *function* that *will ensure* ... after *security-relevant-event* using the mechanism defined in paragraph *n*. **Target Phrase:** 21: clearing of information from	The TOE contains a SEF OR1.1 that will ensure the clearing of the information after **SRE5** or **SRE11** from temporary used storage areas using the mechanism defined in paragraph 4.8.

Construction	Security claim
an *object*. **Substitution:** *function* = SEF OR1.1 *security-relevant-event* = **SRE5** or **SRE11** *object* = temporary used storage areas *n* = 4.8	Note that OR1.1 refers to PIN and PUK.
Action Phrase: The TOE contains a *function* that *will prevent* ... using the mechanism defined in paragraph *n*. **Target Phrase:** 15: the *access-type* by {*user, process*} in respect of an *object*. **Substitution:** *function* = SEF OR1.2 *access-type* = extraction *user* = **S1**, **S2**, **S7** *process* = empty set *object* = **O2** *n* = 4.8	The TOE contains a SEF OR1.2 that will prevent the extraction by **S1**, **S2**, **S7** in respect of **O2** using the mechanism defined in paragraph 4.8.

2.3.5. Data Exchange

Construction	Security claim
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 DX1 *access-set* = **S2** “Somebody”, generate *object* = **O2** “SigG private signature key of the cardholder”, **O12** “SigG public key of the cardholder” *security-relevant-event* = operational phase	The TOE contains a SEF DX1 that will permit the subject **S2** “Somebody” to generate an object **O2** “SigG private signature key of the cardholder” and **O12** “SigG public key of the cardholder” before the operational phase. The SEF DX1 uses the mechanisms defined in paragraph 4.9. Note that the objects **O2** “SigG private signature key of the cardholder” and **O12** “SigG public key of the cardholder” can be generated only together and only before the operational phase of the TOE.
Action Phrase: The TOE contains a *function* that *will permit* ... before *security-relevant-event* **Target Phrase:** 13 ... the *access-set* of an *object*	The TOE contains a SEF DX2 that will permit **S1** “Cardholder” to use for signature generation the object **O2** “SigG private signature key of the cardholder”

Construction	Security claim
object **Substitution:** *function* = SEF DX2 *access-set* = **S1** Cardholder, use for signature generation *security-relevant-event* = **SRE8** *object* = **O2** SigG private signature key of the cardholder	before **SRE8**. The SEF DX2 uses the mechanisms defined in paragraph 4.10. Note that the TOE automatically generates **SRE8** after one digital signature has been generated in (case_one) or after *n* digital signatures have been generated in (case_n).

3. Underlying Security Policy

The ITSEC [1] 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 provides the underlying security policy on the basis of the security objectives in section 1.6 and the security functions in chapter 2 and in accordance with [3]. 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 and the IFD expressed in the current authentication state and the rights the outside world has.

The formal model of the security policy of the TOE and its informal interpretation are provided in [4]. The additional informal interpretation of the formal model of the security policy of the TOE is given in [5].

3.1. Security state

The **current internal state** is the tuple of (i) the **current authentication state *CAS*** (see Table 12) reflecting the assumption about the subjects currently using the TOE and (ii) the retry counters (values of RC-PIN and RC-PUK).

The parameter **assumption about the subjects currently using the TOE** depends on (i) the currently selected application context (e.g.: Is the $\mathrm{DF}_{\mathrm{SigG}}$ selected?) and (ii) the results of the authentication attempts of human users (see Table 12).

The **retry counter for the reference data** RC-PIN (i) stores the number of failed authentication attempts by presenting the verification data after the last successful authentication attempt with this data or (ii) is equal to a fixed value if the number of failed authentication attempts by presenting the verification data exceeds the maximum allowed number of failed authentication attempts with this data.

The **retry counter for the reset code** RC-PUK (i) stores the number of failed authentication attempts by presenting the reset code after the last successful authentication attempt with this code or (ii) is equal to a fixed value if the number of failed authentication attempts with the reset code exceeds the maximum allowed number of failed authentication attempts with reset code. The retry counter for the reference data RC-PIN and the retry counter for the reset code RC-PUK are persistently stored in the TOE.

The **potential security violation flags** *pa* will be set by the TOE indicating that a potential security violation was detected. These flags are persistently set and cannot be reset[27].

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

Table 12: Identification of different current authentication states

	Current authentication state
CAS1	Somebody using the TOE
CAS2	Somebody using the SigG application
CAS3	Cardholder using an IFD
CAS6	A potential attacker (Secure Blocking State)
CAS7	Somebody using the SigG application with blocked Cardholder reference data (RC-PIN=0)

A human user is authenticated if (i) the human user has performed a successful authentication by 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) and the **Potential security violation flag** A is not set.

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**. RC-PIN and RC-PUK are 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 both RC-PIN and RC-PUK can only be greater than zero, since a successful authentication by PIN (**SRE5**) always implies that RC-PIN is reset to its initial value (RC-PIN:=3) and that RC-PUK > 0 (the TOE is not in the secure blocking state **CAS6**).

The **current authentication state CAS6 Potential attacker** represents the secure **Blocking state of the TOE** in which (i) the SigG application is not operational (this is ensured by the secure blocking state of the TOE) and (ii) no human user is successfully authenticated for the SigG application. The **CAS6** is a permanent

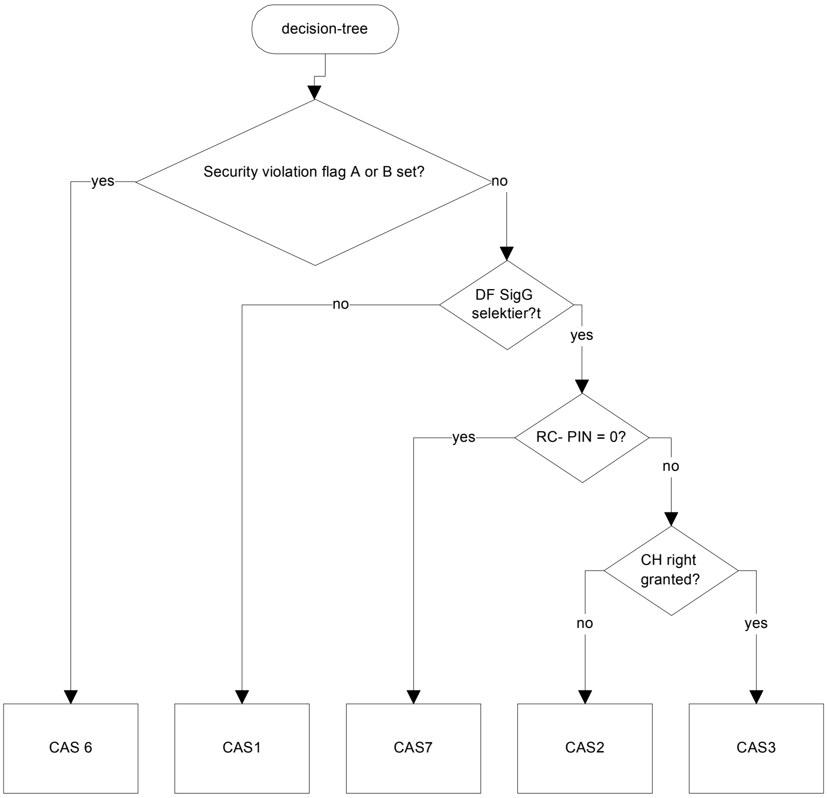
[27] these flags will be set if (i) the RC-PUK= 0 or (ii) by receiving the appropriate signal from the ICC (AE5.4).

state of the TOE. This state is indicated by the potential security violation flags *pa* persistently stored in the TOE. See also **SRE10**.

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 for cardholder authentication (i.e. RC-PIN=0, RC-PUK > 0).

The following **Figure 4** illustrates the decisions for the current authentication state.

Figure 4: Logical decision-tree diagram



The current authentication state will be set and changed by security relevant events as described by the following state transition table (**Table 13**). The complete definition of the state transition is based on the SEF under the generic heading identification and authentication as described in sub-sections 2.2.1 and 2.3.1 and the following rules:

(1) If the SRE is not expected in the CAS but does not indicate a security relevant error then the SRE does not change the CAS.

(2) If the SRE indicates a security relevant error in the CAS then the CAS is changed into CAS6. Such a security relevant error occurs especially if

cardholder authentication succeeds or fails without opening the SigG application.

The state transition in **CAS1** caused by **SRE3** depends on the value of the retry counter for the reference data (RC-PIN). That's why the security relevant event CAS3 is divided into two security relevant events:

SRE3a: the security relevant event SRE3a "**Opening of the SigG application with blocked reference data"** (RC-PIN=0) occurs if (i) no file of the SigG application has been selected before and (ii) a file in the SigG application directory is selected and (iii) the retry counter for the reference data RC-PIN 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 allowed number of failed authentication attempts with the verification data, RC-PIN=0).

SRE3b: the security relevant event SRE3b "**Opening of the SigG application with unblocked reference data"** (RC-PIN>0) occurs if (i) no file of the SigG application has been selected before and (ii) a file in the SigG application directory is selected and (iii) the retry counter for the reference data RC-PIN 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 allowed number of failed authentication attempts with the verification data, RC-PIN>0).

Table 13: State transition table

	CAS1 **Smb. → TOE**	**CAS2** **Smb. → Sig. app.**	**CAS3** **CH → IFD**	**CAS6** **Secur. violation**	**CAS7** **Smb. → Sig. app. RC-PIN=0**
SRE1	CAS1	CAS1	CAS1	CAS6	CAS1
SRE2	CAS1	CAS1	CAS1	CAS6	CAS1
SRE3a	CAS7	-	-	CAS6	(CAS7)
SRE3b	CAS2	(CAS2)	(CAS3)	CAS6	-
SRE4	-	CAS1	CAS1	CAS6	CAS1
SRE5	-	CAS3	CAS3	(CAS6)	-
SRE6	-	CAS2	CAS2	(CAS6)	-
SRE7	-	CAS7	-	(CAS6)	(CAS7)
SRE8	-	-	CAS2	(CAS6)	-

	CAS1 **Smb. → TOE**	**CAS2** **Smb. → Sig. app.**	**CAS3** **CH → IFD**	**CAS6** **Secur. viola-tion**	**CAS7** **Smb. → Sig. app. RC-PIN=0**
SRE10	CAS6	CAS6	CAS6	CAS6	CAS6
SRE11	-	CAS2	CAS3	(CAS6)	CAS2
SRE12	-	CAS2	CAS3	(CAS6)	CAS7

Comments to **Table 13**

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**

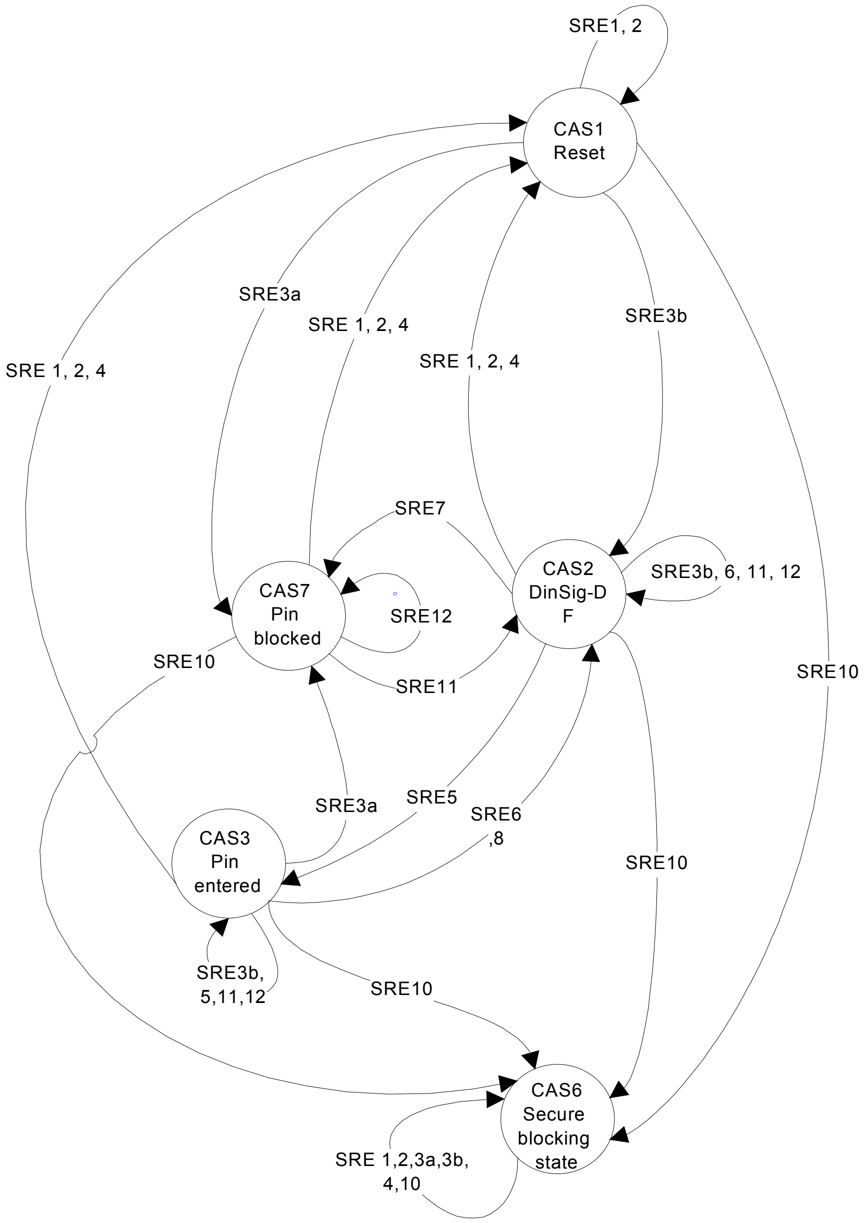
A → B means human user A uses IT-System B as short hint to the definition of the CAS,

RC-PIN value of the retry counter RC-PIN, 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 by presenting the verification data exceeds the maximum allowed number of failed authentication attempts with the verification data then RC-PIN=0

(CASx) The SRE defined for this row is not expected in the CAS defined for this column. In this case the TOE will (i) remain in CAS6 if a potential attack was detected (i. e. the TOE was already in CAS6) and (ii) revoke the cardholder and IFD authentication if the TOE was not in CAS6 (i. e. the TOE goes into CAS1). These state transitions are defined for completeness of the formal model [4] and are not shown in **Figure 5**.

Figure 5 illustrates the state transition with exception of the security relevant events marked with brackets in **Table 13**.

Figure 5: State transition



SRE1: Reset
SRE2: deactivate
SRE3a: open RC-PIN=0
SRE3b: Open, RC-PIN>0
SRE4: Close
SRE5: Authenticate
SRE6: Auth. failed
SRE7: repeated auth. failed
SRE8: Auth. expired
SRE10: Security Violation
SRE11: PUK authentication
SRE12: PUK auth. failed

3.2. 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 2.1.3) and the current authentication state.

Table 14 and **Table 14** 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 deny 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. In CAS6 the SigG Application cannot be opened any more (see **SRE10**).

Table 14: Access-sets ssy(o,t) defined in terms of the security states

	CAS1	**CAS2**	**CAS3**	**CAS6**	**CAS7**
O1	open, close	open, close	open, close	close	open, close
O2			use for signature generation		
O3		use for cardholder authentication, block	use for cardholder authentication, modify, block, unblock		unblock
O4		use for authentication, block	use for authentication, block		use for authentication, block
O5		read	read		read
O6		read (only with Cert)	read (only with Cert)		read (only with Cert)
O12[28]		read	read		read

[28] if still present (could have been deleted by the card manufacturer)

Table 15: Access-sets ssn(o,t) defined in terms of the security states

	CAS1	CAS2	CAS3	CAS6	CAS7
O1				open	
O2	extract, generate, use for signature generation	extract, generate, use for signature generation	extract, generate	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, modify, block, unblock	use for cardholder authentication, modify, block
O4	use for authentication, block			use for authentication, block	
O5	modify, read	modify	modify	modify, read	modify
O6	modify, read	modify	modify	modify, read	modify
O12	generate, modify, read	generate, modify	generate, modify	generate, modify, read	generate, modify

4. Security Mechanisms

The security functions specified in chapter 2 shall be implemented using the following mechanisms.

Table 16: Security mechanisms

ID	Mechanism
M1	Human user authentication
M2	Change the unblocked 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	Secure blocking state
M9	Clearing of memory
M10	Signature key pair generation
M11	Signature generation

4.1. M1: Human user authentication

The human user authenticates himself using a knowledge-based authentication mechanism.

Note that the human user chooses the kind of authentication information and the mechanism he wants to use for authentication: (i) O3 “SigG cardholder reference data” (PIN) with mechanism M1 or (ii) O4 “SigG cardholder reset code” (PUK) with mechanism M4.

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

In accordance with [9] the verification data consist of a string of minimal 6 ASCII characters.

The mechanism M1 will detect the S7 “Potential attacker”, if the TOE is in the **Blocking state of the TOE** (see **SRE10** and **CAS6**)[29].

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.

4.2. M2: Change the unblocked reference data

The mechanism M2 implements the following security sub-functions with one command:

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

(2) modification of the **O3** (PIN) to the presented new string of characters.

The command sent to the TOE contains (i) the verification data and (ii) a string of characters as new reference data of the cardholder. If (a) the number of consecutive failed authentication attempts with reference data does not exceed the maximum number of allowed failed authentication attempts (RC-PIN>0) and (b) the verification data presented for human user authentication match the reference data **O3** (PIN) stored for the SigG application of the TOE, then (i) the retry counter (see mechanism M3) will be reset to the initial value (RC-PIN:=3) and (ii) the presented string will be stored as new value of the **O3** (PIN). 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.

4.3. M3: Locking of the reference data

The mechanism M3 implements the following security sub-functions:

(1) detection of **SRE6** "Cardholder authentication failure" and **SRE7** “Repeated authentication failure“ by means of a retry counter (RC-PIN) for the reference data (PIN),

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

An authentication by the **O3** “SigG cardholder reference data” is attempted by use of mechanism M1 or M2. The retry counter for the reference data RC-PIN counts the number of failed authentication attempts by presenting the verification data. Each time a successful authentication by presenting the verification data takes place this retry counter is reset to a defined initial value (RC-PIN:=3). The retry counter for the reference data is equal 0 (RC-PIN=0), if the number of consecutive

[29] In fact the part of M1 detecting the “Potential attacker” is implemented by the mechanism M7 (see below).

failed authentication attempts reaches or exceeds the maximum number of allowed failed authentication attempts.

If the authentication attempt has failed and the retry counter after this authentication attempt is not equal 0 (RC-PIN>0), then this event is the **SRE6**. If the authentication attempt failed and the retry counter after this authentication attempt is equal 0 (RC-PIN=0), then this event is the **SRE7**.

If the **SRE7** occurs the **O3** (PIN) will be blocked for the use for cardholder authentication. This blocking remains stored in the TOE and may only be reset by mechanism M4.

4.4. M4: Unblocking and changing of the reference data

The mechanism M4 implements the following security sub-functions with two commands:

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

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

2.2 modifying the **O3** (PIN) to the presented new string of characters.

The human user authenticates himself using a knowledge based authentication mechanism.

Note that the human user chooses the kind of authentication information and the mechanism he wants to use for authentication: (i) O3 (PIN) with mechanism M1 or (ii) O4 (PUK) with mechanism M4.

If the mechanism M4 is used, then the first command sent to the TOE will contain the reset code and the second command a string of characters as new reference data of the cardholder.

If the retry counter of the reset code indicates that human user authentication by presenting the reset code is not allowed (RC-PUK=0), then (i) the authentication attempt will be rejected (independently whether the presented reset code matches the stored reset code or not), (ii) the retry counter for the reference data (RC-PIN, see mechanism M3) will not be reset and (iii) the **O3** (PIN) will not be modified. Moreover **SRE10** will occur in this case.

If (a) the retry counter of the reset code indicates that human user authentication by presenting the reset code is still allowed (RC-PUK>0) and (b) the presented reset code matches **O4** (PUK) then (i) the retry counters for the reference data and for the reset code will be reset to the initial value (RC-PIN:=3, RC-PUK:=3), (ii) the **O3** (PIN) will be unblocked for the use for cardholder authentication and (iii) the presented string will be stored as new value of the **O3**.

If the reset code presented does not match **O4** “SigG cardholder reset code” (PUK) then (i) the authentication failure with reset code is counted by decrementing the retry counter for the reset code (RC-PUK := RC-PUK - 1), (ii) the **O3** (PIN) will remain blocked for the use for cardholder authentication and (iii) the **O3** (PIN) will not be changed. If the retry counter of the reset code indicates that human user authentication by presenting the reset code is still allowed (RC-PUK>0) then **SRE12** “Cardholder authentication by reset code failed” will occur. If the retry counter of the reset code indicates that human user authentication by presenting the reset code is not allowed any longer (e. g. the defined maximum number of authentication failures by presenting the reset code is exceeded, RC-PUK reaches 0) then this event triggers the **SRE10** “Potential security violation occurred”.

4.5. M5: Extraction resistance

The TOE will implement security mechanisms (summarised as M5) to prevent extraction of the SigG private signature keys (O2) of the cardholder as required for SEF AC2.

There is no command for reading a key-record (SK.CH.DS).

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) as well as Simple Power Analysis (SPA) during its use (i.e. during the generation of signatures).

The SigG private signature key (O2) is also protected against DFA (Differential Fault Analysis, ”Bellcore-Attack”).

Note that though the DPA, SPA and DFA countermeasures are provided by the TOE, they can be tested only on the ICC, but not in a simulator environment.

4.6. M6: Access control for command execution

The TOE will implement security mechanisms (summarized as M6) as required for SEF AC1. These mechanisms will, according to the underlying security policy,

(1) implement a security **state machine** as described in section 3.1 and

(2) control the access as described in section 3.2.

4.7. M7: Secure blocking state

The TOE will implement a security mechanism M7 as required for SEF AC3 and AU1.

a) If the retry counter RC-PUK of the **O4** (PUK) reaches the value 0, the DF_{SigG} is blocked definitely and permanently by setting the potential security violation flag A in the header of the DF_{SigG}.

b) The security violation flag B is persistently set if the TOE receives the appropriate signal by the hardware described in (AE5.4).

These states of the TOE are called the Secure Blocking State of the TOE.

c) If the TOE is in its secure blocking state, M7 will generate a corresponding return code and send it to the IFD.

4.8. M9: Clearing of memory

The TOE will implement security mechanism M9 as required for SEF OR1.

a) PIN and PUK will be immediately actively erased from the RAM or XRAM areas after their use.

b) The TOE does not store the key SK.CH.DS in any temporary area.

4.9. M10: Signature key pair generation

The TOE will implement the following security mechanisms (summarised as M10) as required for SEF DX1 in accordance with [8].

a) Generation of random numbers using the onboard true random number generator.

b) Quality check of the prime number (Rabin-Miller-Test)

c) RSA Algorithm with a key length of 1024 Bit.

This approach is described in [8], section 1.4 (RSA) and considered as being adequate.

Note that the mechanism M10 uses the output of the hardware true random number generator and, hence, can be tested only on the ICC.

4.10. M11: Signature generation

The TOE will implement security mechanisms (summarised as M11) as required for SEF DX2 in accordance with [8] and [9].

a) RSA Algorithm with a key length of 1024 Bit (see [8], section 1.4).

b) Hash SHA-1 (see [8], section 1.3).

c) PKCS1 BT1 Padding according to [9] (Appendix A, section A.1.2).

5. Suitability of the TOE's security features

This section describes the suitability of the TOE's security features to counter all assumed threats. A simple mapping between the threats, the security objectives and the SEF and threats is shown based on the explanations given in section 1.6 in the following table.

Table 17: Mapping between the threats, the security objectives and the SEF

	SO1 ”Prevent disclosure, copying or modification of the cardholder's private key”	SO2 ”Prevent unauthorised use of the SigG digital signature function”	SO6 ”Quality of key generation”	SO7 ”Provide secure digital signatures”	SO8 ”React to potential security violations”
T1 ”Extraction of the cardholder's private key”	AC1, AC2, OR1			DX1, DX2	AC3, AU1
T2 ”Misuse of the signature function”		IA1 – IA4, AC1			AC3, AU1
T3 ”Forged data ascribed to the cardholder”			DX1	DX2	AC3, AU1

Threat T1

The threat T1 ”Extraction of the cardholder's private key” will be countered by the security objectives SO1, SO7 and SO8.

The TOE shall implement the security enforcing function AC1 “Access control of commands” and AC2 “ Access control of extraction” described in sections 2.2.2 and 2.3.2 to prevent misuse of ICC commands implemented by the TOE and the extraction of the SigG private signature key. The SEF OR1 described in sections 2.2.4 and 0 shall prevent illicit information flow between the SigG application including the SigG private signature key and other applications embedded on the ICC through temporary used storage areas. The SEF DX1 and DX2 described in section 2.2.5 and 2.3.5 shall prevent disclosing of the SigG private signature key of the cardholder by cryptoanalytic attacks against the digital signatures generated by the TOE. The secure blocking state of the TOE CAS6 shall ensure the security of the SigG private signature key of the cardholder if a potential attack was detected (see SEF AC3 and AU1 in sections 2.2.2, 2.2.3, 2.3.2 and 2.3.3).

Threat T2

The threat T2 ”Misuse of the signature function” will be countered by the security objectives SO2, SO8 in case that the Option Public IFD is not supported.

The TOE implements the security enforcing function IA1, IA2, IA3 and IA4 for cardholder authentication (described in sections 2.2.1 and 2.3.1) and AC1 for access control over the usage of the SigG signature key of the cardholder (described in sections 2.2.1, 2.3.1, 2.2.2 and 2.3.2) to fulfil the security objective SO2. The (AE4.2)(4) assumes that the environment keeps the confidentiality and integrity of the data transferred between the office IFD and the ICC. The secure blocking state of the TOE CAS6 shall ensure the security of the SigG signature function if a potential attack was detected (see SEF AC3 and AU1 in sections 2.2.2, 2.2.3, 2.3.2 and 2.3.3).

Threat T3

The threat T3 “Forged data ascribed to the cardholder” will be countered by the security objectives (i) SO7 “Provide secure digital signatures” and (ii) SO6 “Quality of key generation”. The TOE implements the security enforcing function DX1 described in sections 2.2.5 and 2.3.5 to fulfil the security objective SO6 by means of generating a secure SigG signature key pair. The AE2 assumes the reliable public key infrastructure needed to check whether the cardholder was the sender of a signed message or not. SEF DX2 ensures cryptographic security of the digital signature. Therefore the forgery of digital signatures is prevented. The confidentiality of the SigG private signature key and limitation of access to the signature function prevent the repudiation of valid digital signatures addressed by threat T3. The secure blocking state of the TOE CAS6 shall prevent misuse of the TOE if a potential attack was detected (see SEF AC3 and AU1 in sections 2.2.2, 2.2.3, 2.3.2 and 2.3.3).

6. Evaluation Target

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

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

7. List of abbreviations

AC	Access Control
ACE	Advanced Crypto Engine
AE1	Life cycle security
AE2	Integrity and quality of key material
AE3	SigG compliant use of the TOE
AE4	Use with SigG accredited IFD
AE5	Security assumption about the ICC hardware
AEn.m	Assumption about the Environment (No. n)
CAS1	Somebody using the TOE
CAS2	Somebody using the SigG application
CAS3	Cardholder using an IFD
CAS6	A potential attacker
CAS7	Somebody using the SigG application with blocked Cardholder reference data
CH	Cardholder
DX	Data Exchange
IA	Identification and Authentication
IC	Integrated Circuit
ICC	Integrated Circuit Card
IFD	Interface Device
ITSEC	Information Technology Security Evaluation Criteria
M1	Human user authentication
M10	Signature key pair generation
M11	Signature generation
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	Secure blocking state
M9	Clearing of memory

O1	SigG application
O2	SigG private signature key of the cardholder
O3	SigG cardholder reference data
O4	SigG cardholder reset code
O5	SigG signature key certificate of the cardholder
O6	SigG public key of the root certification authority
On	Object (No. n)
OR1	Object Reuse
PIN	Personal identification number
PK	Public Key
PUK	Personal unblocking key
S1	Cardholder
S2	Somebody
S3	IFD
S7	Potential attacker
SEF	Security Enforcing Function
SigG	Signaturgesetz
SigV	Signaturverordnung
SK	Secret Key
Mn	Security Mechanism (No. n)
SO1	Prevent disclosure, copying or modification of the cardholder's 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)
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
SRE3a	Opening of the SigG application with blocked reference data

SRE3b	Opening of the SigG application with unblocked reference data
SRE4	Closing of the SigG application
SRE5	Successful cardholder authentication
SRE6	Cardholder authentication failure
SRE7	Repeated authentication failure
SRE8	Authentication expiration
SREn	Security Relevant Event (No. n)
T1	Extraction of the cardholder’s private key
T2	Misuse of the signature function
T3	Forged data ascribed to the cardholder
Tn.m	Threat (No. n)
TOE	Target of Evaluation

8. Glossary

ACE

Advanced Crypto Engine

Anybody

The set of the two subjects **S1** Cardholder and **S2** Somebody.

ARA Counter

Acces Right Applicability Counter

Authenticated User

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

Authentication information

Information used to prove or to verify the identity of a subject by means of authentication. The user authentication information is the verification data provided by the cardholder to prove her or his identity and the reference data used by the TOE to verify this identity. The authentication information for the mutual authentication (see [9], 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.

Blocking state of the TOE

Secure State of the ICC disabling the Signature application of the ICC. This state is apparent to the cardholder by means of an appropriate return code.

Cardholder

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. In case of the (optional for the TOE) authentication by biometrical characteristics the assumption AE4.5 assumes that the cardholder is the only person who is able to provide the biometrical characteristics to generate the verification data matching the verification data stored for the SigG application of the TOE.

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 Artikel 1 §2 SigG [6]).

Certification authority

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 Artikel 1 § 4 of the SigG [6].

Credentials for signature verification

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

Current authentication state

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 key pair

Pair of a private key and a public key of a SigG accredited technical component for the mutual device authentication according to [9].

DFA

Differential Fault Analysis

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 [9].

Digital Signature

A digital signature is a seal affixed to digital data which is generated by the 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.

Display message of the cardholder

Secret string (i) stored in the SigG application of the TOE, (ii) displayed by the IFD after reading from the ICC and (iii) checked by the cardholder to verify the successful conduction of the mutual authentication procedure between ICC and IFD. See [9], section 18 and annex D for more details.

DPA

Differential Power Analysis

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.

FMSP

Formal Model of the Security Policy

IFD

abbreviation for: Interface Device

Infer

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

Integrated Circuit Card

A smart card equipped with the TOE.

Interface Device

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

Non-SigG application

Application which resides on the card and is different from SigG signature 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

The life cycle phase of the ICC, when it is ready to be used by the cardholder for SigG digital signature generation (e. g. (i) TOE has been personalised for the cardholder and (ii) the SigG private signature key of the cardholder is stored in the TOE). The ICC will have been transferred to the cardholder typically involving some „smart card issuer“.

Personalization phase

The life cycle phase, when the ICC is equipped with SigG application related data and data related to the specific cardholder. The TOE is personalised for the cardholder (e. g. The TOE stores the reference data for authentication by knowledge for the SigG application of the TOE which matches the verification data (Transport-PIN and PUK) given to the cardholder as the legitimate person in the operational phase). In case of Method of Use “Generation of cardholders signature key on the ICC” the TOE is used to generate the cardholder’s signature key pair on the ICC.

Potential security violation flags

These flags are set by the TOE if:

A The flag A is persistently set if the RC-PUK is decremented from 1 to 0 (i.e. reaches the value RC-PUK=0). The flag A is set in the header of the DF_{SigG} and cannot be reset[30].

B The flag B is persistently set if the TOE receives the appropriate signal by the hardware described in (AE5.4)

Potential security violations

A set of specified events to be deemed as potential tries to penetrate the TOE using logical interfaces to the TOE.

[30] We distinguish between the verb “set” and “reach” in relation to the RC-PUK: “set” the RC-PUK means to assign a value to the RC-PUK, “reach” means that RC-PUK equals a value after decrementing.

For this TOE, the term potential security violation is defined in (SO8.1). When a potential security violation occurs, the TOE assumes the Potential Attacker **S7** as user of 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 for 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.

RC-PIN

Retry Counter for the PIN, synonym for Retry counter for the reference data

RC-PUK

Retry Counter for the PUK, synonym for Retry counter for the reset code

Reference data

Data stored in the SigG application of the TOE for checking the verification data presented by the human user for authentication as cardholder.

Reset code

Data required to unlock the reference data and used for the authentication of the cardholder. The reset code is also named PUK.

Retry counter for the reference data

The retry counter for the reference data (i) stores the number of allowed failed authentication attempts by presenting the verification data after the last successful authentication attempt with the verification data or (ii) will be equal to a fixed value if the number of failed authentication attempts by presenting the verification data exceeds the maximum number of allowed failed authentication attempts with the verification data.

Retry counter for the reset code

The retry counter of the reset code (i) stores the number of allowed failed authentication attempts by presenting the reset code or (ii) will be equal to a fixed value if the number of failed authentication attempts with the reset code exceeds the maximum number of allowed failed authentication attempts with reset code. The retry counter for the reference data and the retry counter of the reset code are persistently stored in the TOE.

Secure Blocking State

The TOE is defined to be in its secure blocking state, if one of the potential security violation flags is set.

Session

Time frame from external reset by power supply on or reset signal to the ICC until next external reset or power supply down of the ICC on wich the TOE runs.

RMS

Resource Management System

SigG compliant digital signature

A digital signature compliant with the German digital signature legislative [6], [7], [8]. It shall be generated by SigG compliant technical components.

SigG accredited ICC

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 [9], section 18 and annex D).

SigG accredited IFD

Public IFD (i) being a SigG accredited technical component and (ii) acting as customer IFD according to [9], section 18, and (iii) supporting the mutual device authentication and secure messaging according to [9], annex D).

SigG accredited technical component

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

SigG application services

The functions provided for 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 (i) by knowledge or (ii) by biometrical characteristics.

SigG signature key pair of the cardholder

Pair of asymmetric keys consisting of the SigG private signature key of the cardholder and the SigG public key of the cardholder.

SigG compliance of technical component

A property of technical components adhering to 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 [7]

Anlage 1. The SigG compliance of a technical component is usually not directly apparent to the user or to another technical component. Note that a SigG compliant technical component is not necessarily a SigG accredited technical component.

SigG private signature key of the cardholder

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 of the SigG signature key pair of the cardholder.

SigG public key of the cardholder

Public key corresponding to the SigG private signature key of the cardholder and used to verify a digital signature of the cardholder. The SigG public key of the cardholder is part of the SigG signature key pair of the cardholder and the SigG certificate of the cardholder.

SigG signature verification

Process established with the help of an associated public key provided by a signature key certificate of a certification authority: (i) whether the digital signature of the message was generated by the owner of the 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.

SPA

Simple Power Analysis

Verification data

Data presented by a human user for authentication as cardholder and corresponding to the reference data stored in the TOE. The verification data are also named PIN.

9. References

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

[2] Information Technology Security Evaluation Manual (ITSEM); Provisional Harmonised Methodology, Version 1.0, September 1993

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

[4] 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

[5] CardOS/M4.0 Additional explanations to informal interpretation of the formal model, Siemens AG, Version 1.0, 21.12.2000

[6] Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (in Kraft getr. am 22.05.2001) Artikel 1 Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG)

[7] Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) (in Kraft getreten am 22.11.2001)

[8] Bekanntmachung zur digitalen Signatur nach Signaturgesetz und Signaturverordnung vom 09.02.98, Bundesanzeiger Nr. 31 vom 14.02.98

[9] Spezifikation der Schnittstelle zu Chipkarten mit Digitaler Signatur-Anwendung / Funktion nach SigG und SigV; DIN 66291-1, Version 1.0, 15th December 1998

[10] International Organization for Standardization: Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 2: Dimensions and location of contacts, International Standard ISO/IEC 7816-2 (1996)

[11] International Organization for Standardization: Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocols, International Standard ISO/IEC 7816-3 (1997)

[12] International Organization for Standardization: Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interchange, International Standard ISO/IEC 7816-4 (1995)

[13] International Organization for Standardization: Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 8: Security related interindustry commands, International Standard ISO/IEC 7816-8 FDIS (1998)

[14] Certification report for Smart Card Infineon IC SLE 66CX320P, version m1421b14, certification file TUVIT-DSZ-ITSEC-9115, TUVIT, 04.08.2000

End of Security Target

4 Annex

4.1 Glossary

This glossary provides explanations of the terms 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.

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.

Business process

Cf. process

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 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.

Certification Service Provider

Cf. Trust Center.

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, being an internationally accepted security evaluation standard.

Component according to SigG

A logical unit in an IT system performing a task defined in SigG/SigV (signature-creation device, signature-application component, 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.

Electronic Signature Act – SigG
German Act to regulate the application of electronic signatures.

Electronic Signature Ordinance – SigV
Official regulations concerning the implementation of the German Electronic Signature Act.

EN 45000
A series of European standards applicable, in particular, to evaluation facilities and certification bodies.

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.
License Agreement	Agreement between an Evaluation Facility and a Certification Body concerning the procedure and responsibilities of a joint evaluation and certification project.
Licensing	Assessment of organisation and qualification of an evaluation facility with respect to an intended licence agreement.
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.).
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 (Business ~)	Sequence of linked activities (process elements) performed within a given environment – with the objective to provide a certain service.
Process ID	ID designating a certification or confirmation process.
Product Certification	Certification of IT products.
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 German authority responsible in the field of electronic signatures.
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
SigG: A legally binding document stating conformity 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 rating 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.

Service (Enterprise ~)
Here: activities offered by a company, provided by its (business) processes and usable by a client.

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
An institution (named “certification service provider” in the German Electronic Signature Act) that confirms the relationship between signature keys and persons by means of electronic certificates.

4.2 References[31]

/ALG/ Geeignete Kryptoalgorithmen [Approved Crypto-Algorithms], published in the Bundesanzeiger [German Federal Gazette] by the (German) Regulatory Authority for Telecommunications and Posts, endorsed version

/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, August 1999
Part 1: Introduction and general model

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

Part 2: Security functional requirements
Part 3: Security assurance requirements

/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

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

/Mkat12/ Maßnahmenkatalog nach §12 Abs. 2 [Catalogue of Security Measures in accordance with §12 Sec. 2], Regulatory Authority for Telecommunications and Posts, http://www.regtp.de/

/Mkat16/ Maßnahmenkatalog nach §16 Abs. 6 [Catalogue of Security Measures in accordance with §16 Sec. 6], Regulatory Authority for Telecommunications and Posts, http://www.regtp.de/

/SigG/ Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (Signaturgesetz – SigG) [German Electronic Signature Act] as of May 16, 2001 (BGBl. I, S. 876 ff.)

(earlier version:)
Gesetz zur digitalen Signatur (Signaturgesetz – SigG) [German Digital Signature Act] as of July 22, 1997 (BGBl. I., S. 1870, 1872)

/SigV/ Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) [German Electronic Signature Ordinance] as of 16.11.2001 (BGBl. I., S. 3074 ff.)

(earlier version:)
Verordnung zur digitalen Signatur (Signaturverordnung – SigV) [German Digital Signature Ordinance] as of October 08, 1997 (BGBl. I., S. 2498 ff.)

4.3 Abbreviations

AIS	Anforderung einer Interpretation von Sicherheitskriterien [Request for an interpretation of security criteria] (BSI procedure)
BGBl	Bundesgesetzblatt [German Federal Gazette]
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 Technology]
ETR	Evaluation Technical Report
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	IT Security Evaluation Facility
ITSEM	Information Technology Security Evaluation Manual
RegTP	Regulierungsbehörde für Telekommunikation und Post [Regulatory Authority for Telecommunications and Posts]
SigG	German Electronic Signature Act
SigV	German Electronic Signature Ordinance
TOE	Target of Evaluation

5 Security Criteria Background

This chapter gives a survey on the criteria used in the evaluation and its different metrics. Original ITSEC and ITSEM text is printed in quotes.

5.1 Fundamentals

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

In general, the security objectives for a product or system consist of requirements for confidentiality, availability and / or integrity of certain data objects. Such security objectives are defined by the sponsor of the evaluation. Normally, the sponsor of a product evaluation is the product's developer or vendor; in case of a system evaluation it is the owner of the system.

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

Principal threats become *attacks*, when unauthorised subjects try to read or modify data objects or prevent other authorised subjects to access such objects.

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

There are two basic questions: Do the security functions operate correctly? Are the security functions effective?

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

5.2 Assurance level

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; an only “superficial” evaluation, however, would be as well inadequate for a high level security need.

Therefore, it is reasonable to define a rating system of hierarchical assurance levels that can be used to reflect the individual security need. In ITSEC, six assurance levels are given for the evaluation of correctness and effectiveness. E1 is the lowest, E6 the highest level.

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

The following excerpts from the ITSEC show which aspects are covered during the evaluation process and which depth of analysis corresponds to each assurance level. („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."

In addition, effectiveness aspects have to be evaluated for each level E1 to E6 according to the following requirements:

"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

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.

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.

For a specific security function there are normally many ways of implementation: Example: The function *Identification and Authentication* can be realised by a password procedure, by usage of smartcards with a challenge response scheme or by biometrical algorithms.

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

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

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, type B mechanisms in this sense 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.“

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."

End of certification report for T-Systems-DSZ-ITSEC-04067-2002.

Certification Report
T-Systems-DSZ-ITSEC-04067-2002

Address: Rabinstr.8, D-53111 Bonn
Germany
Phone: +49-228-9841-0
Fax: +49-228-9841-60
Web: www.t-systems-iss.com
www.t-systems-zert.com