T · · Systems · · ·

Certification Report

T-Systems-DSZ-ITSEC-04016-2003

Setec Signature Card SetEID v1.0

Setec Oy

Certification report: T-Systems-DSZ-ITSEC-04016-2003, version 1.0, July 18, 2003

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

✉ Certification Body of T-Systems
c/o T-Systems GEI GmbH
BU ITC Security
Rabinstr.8, D-53111 Bonn, Germany

☎ +49-228-9841-0, Fax: +49-228-9841-60

💻 www.t-systems-zert.com

Deutsches IT-Sicherheitszertifikat

anerkannt vom
Bundesamt für Sicherheit in der Informationstechnik

T · · Systems · · ·

The Certification Body of T-Systems

hereby certifies that

Setec Signature Card SetEID v1.0

of

Setec Oy
Suometsäntie 1, FIN- 01741 Vantaa

has been evaluated against a specific Security Target in accordance with the Information Technology Security Evaluation Criteria (ITSEC) and the Information Technology Security Evaluation Manual (ITSEM); the following result was achieved:

Security Functions:	**Identification and Authentication, Access Control, Audit, Object Reuse, Data Exchange**
Evaluation Assurance Level:	**E3**
Minimum Strength of Mechanisms:	**high**

This certificate meets the requirements of the Mutual Recognition Agreement (SOGIS-MRA) as of 03.03.1998, signed by Finland, France, Germany, Great Britain, Greece, Italy, the Netherlands, Norway, Portugal, Spain, Sweden and Switzerland.

This certificate is valid only for the configurations and the environment described in the certification report, and in connection with the complete certification report under the registration code below. The stipulations and recommendations in the certification report should be observed. The certification report contains the security target which was the basis for the evaluation. The rating of the strength of cryptographic algorithms suitable for encryption as well as decryption is excluded from the recognition by BSI. For copies of this certificate and the certification report contact the sponsor or the certification body.

Registration:
T-Systems-
DSZ-ITSEC-04016-2003

Bonn: July 18, 2003

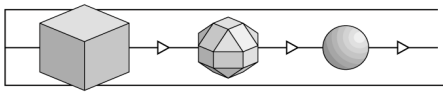
T · · Systems · · ·

Dr. Heinrich Kersten
Head of Certification Body

Certification Body of T-Systems
c/o T-Systems GEI GmbH, BU ITC Security, Rabinstr.8, D-53111 Bonn, Germany
☎ +49-228-9841-0, Fax: +49-228-9841-60, Internet: www.t-systems-zert.com
accredited against EN 45011 unter DAR registration DIT-ZE-005/98 by DATech e.V.

(This page is intentionally left blank.)

Contents



Abbreviations

AIS	Anwendungshinweise und Interpretationen zum Schema [Guidance and Interpretations of Scheme Issues] (BSI procedure)
BGBl	Bundesgesetzblatt [German Federal Gazette]
BS	British Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
DAR	Deutscher Akkreditierungsrat [German Accreditation Council]
DATech	Deutsche Akkreditierungsstelle Technik e.V. [German Accreditation Body Technology]
DIN	Deutsches Institut für Normung e.V. [German Standards Institute]
ETR	Evaluation Technical Report
ISO	International Organization for Standardization
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	IT Security Evaluation Facility
ITSEM	Information Technology Security Evaluation Manual
JIL	Joint Interpretation Library
RegTP	Regulierungsbehörde für Telekommunikation und Post [(German) Regulatory Authority for Telecommunications and Posts]
SigG	German Electronic Signature Act
SigV	German Electronic Signature Ordinance
TOE	Target of Evaluation

References

/AIS/ Anwendungshinweise und Interpretationen zum Schema [Guidance and Interpretations of Scheme Issues], Bundesamt für Sicherheit in der Informationstechnik, endorsed version

/ALG/ Geeignete Kryptoalgorithmen [Approved Crypto-Algorithms], published in the Bundesanzeiger [German Federal Gazette] by the (German) Regulatory Authority for Telecommunications and Posts, 02.01.2003

/BS7799/ BS7799-1:2000 Information technology - Code of practice for information security management (ISO/IEC 17799:2000)
BS7799-2:2002 Information security management systems - Specification with guidance for use

/CC/ Common Criteria for Information Technology Security Evaluation (ISO 15408), August 1999
Part1: Introduction and general model
Part2: Security functional requirements
Part3: Security assurance requirements

/CEM/ Common Methodology for Information Technology Security Evaluation

Part1: Introduction and general model, version 0.6, January 1997
Part2: Evaluation Methodology, version 1.0, August 1999

/EU-DIR/ Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

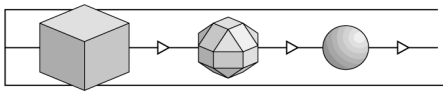
/ITSEC/ Information Technology Security Evaluation Criteria (ITSEC), version 1.2 (1991), ISBN 92-826-3004-8

/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

/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.)

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

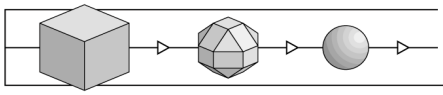


Glossary

This glossary provides explanations of terms used within the certification scheme of BU ITC Security, but does not claim completeness or general validity. The term *security* here is always used in the context of information technology.

Accreditation	A process performed by an accreditation body to confirm that an evaluation facility [resp. a certification body] complies with the requirements of the relevant standard ISO 17025 [resp. EN 45011].
Audit	A procedure of collecting evidence that a process works as required.
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 a 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	An institution (named “certification service provider” in the German Electronic Signature Act) that confirms the relationship between signature keys and individuals by means of electronic certificates.
Certifier	Employee at a certification body authorised to monitor evaluations and to carry out the certification.
Confidentiality	Classical security objective: Data should only be accessible to authorised persons.
Evaluation	Assessment of an (IT) product, system or service against published IT security criteria.

Evaluation (Assurance) Level	Level of assurance gained by evaluation; part of a rating system in security criteria ITSEC / CC; level of trust that a TOE meets its security target.
Evaluation Facility	The organisational unit which performs evaluations (ITSEF).
Evaluation Technical Report	Final report written by an evaluation facility on the procedure and results of an evaluation.
Evaluator	Person in charge of an evaluation at an evaluation facility.
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 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 supported by IT systems.
IT System	An inherently functional combination of IT products. (ITSEC:) A real installation of IT products with a known operational environment.
License Agreement	Agreement between an Evaluation Facility and a Certification Body concerning the procedure and responsibilities of a joint evaluation and certification project.
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 ratings 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	Sequence of networked activities (process elements) performed within a given environment – with the objective to provide a certain service.
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.
Security Certificate	Cf. „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 for Business	Security Initiative that offers to companies security service modules (Basic Security, Standard Security, Professional Security). These modules include consulting, analyses, penetration testing, audits as well as procedures of registration, issuance of a seal and certification after successful assessments. Details can be obtained from the web-site of the Initiative. (www.s4b.org)
Security Function	Function counteracting certain threats.
Security Target	Document describing a set of security requirements and specifications to be used as the basis for the evaluation of an identified TOE.
Service	Here: activities offered by a company, provided by its (business) processes and usable by a client.
System Certification	Certification of an installed IT system.
Target of Evaluation	An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.
Trust Centre	Cf. Certification Service Provider

Security Criteria Background

This chapter gives a survey on the criteria used in the evaluation and their rating system. Original ITSEC and ITSEM text is printed in quotes.

- Fundamentals

In the view of ITSEC security is provided if there is sufficient assurance that the target of evaluation (TOE) 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 an IT product evaluation is the product's developer or vendor; in case of an IT 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, modify data objects or prevent other authorised subjects to access such objects.

Security (enforcing) functions provided by the TOE are intended to counter these threats.

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

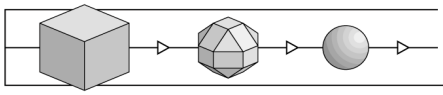
Thus, an adequate assurance that the security objectives are met can be achieved by evaluating correctness and effectiveness.

- 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; it would be as well inadequate to use very low resources for a high level security need.

Thus, it is reasonable to define different assurance levels: 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 TOE 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."

- Security Functions and Security Mechanisms

Security functions of a TOE are intended to counter threats.

Functionality classes are formed by combining 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, 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.

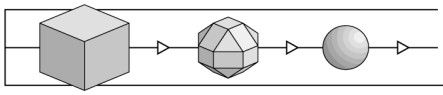
Type B „A type B mechanism is a security mechanism which, if perfectly conceived and implemented, will have no weaknesses. A type B mechanism can be considered to be impregnable to direct attack regardless of the level of resources, expertise and opportunity deployed. … However, these type B mechanisms can be defeated by indirect attacks which are the subject of other effectiveness analyses."

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. … 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."

1 Sponsor and Target of Evaluation

1 **Sponsor** of the certification was Setec Oy, Suometsäntie 1, FIN- 01741 Vantaa.

2 The **type of certificate** applied for was a „Deutsches IT-Sicherheitszertifikat [German IT Security Certificate]“.

3 Target of Evaluation (TOE) was the **product „**Setec Signature Card SetEID v1.0” .

4 The TOE is a Signature Card.

5 The sponsor provided the **security target** for the TOE in English language. The security target, final version 1.2 as of July 09, 2003, is reproduced in the annex.

6 The security target references the **ITSEC** as **criteria** and **E3** as **assurance level**. The (minimum) **strength of mechanism** is claimed to be “**high**“.

2 Relevant Normative Documents for the Assessment

7 As applied by the sponsor, the evaluation of the TOE was carried out against the

- Information Technology Security Evaluation Criteria (ITSEC) /ITSEC/.

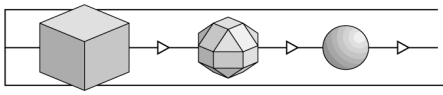
8 In addition, the following documents were relevant for the evaluation and certification:

- Information Technology Security Evaluation Manual (ITSEM) /ITSEM/,
- Joint Interpretation Library /JIL/,
- Anwendungshinweise und Interpretationen zum Schema [Guidance and Interpretations of Scheme Issues], Bundesamt für Sicherheit in der Informationstechnik /AIS/,
- Work instruction „Deutsches IT-Sicherheitszertifikat [German IT Security Certificate]“ by T-Systems GEI GmbH, BU ITC Security (endorsed version).

3 Evaluation

9 The evaluation of the TOE by the Prüfstelle für IT-Sicherheit of T-Systems GEI GmbH, BU ITC Security was sponsored by Setec Oy.

10 The evaluation facility accredited against ISO 17025 has a valid **licence** of the certification body and the BSI for the scope of the evaluation.



11 The evaluation was carried out under the terms of the certification scheme of T-Systems.

12 In compliance with the criteria, the evaluation was monitored by the certification body.

13 The **Evaluation Technical Report** (ETR), version 1.01 and dated July 14, 2003, provided by the evaluation facility, contains the outcome of the evaluation.

14 The evaluation was completed on July 14, 2003.

4 Certification

15 The **certification scheme** of T-Systems is described on the web pages of the certification body (www.t-systems-zert.com).

16 The **certification body** of T-Systems operates in compliance with EN 45011 and has a corresponding accreditation by DATech e.V. for assessments against ITSEC and Common Criteria (DAR registration code DIT-ZE-005/98).

17 The **certification** of the TOE was carried out according to service type 04: „Deutsches IT-Sicherheitszertifikat [German IT Security Certificate]“ as applied for by the sponsor.

18 The certification was carried out under **registration code** T-Systems-DSZ-ITSEC-04016-2003.

19 The certification of the TOE may be subject to **stipulations and recommendations**; cf. chapter 5 for details.

20 A **summary** of the results is given by the security certificate T-Systems-DSZ-ITSEC-04016-2003 as of July 18, 2003 reproduced on page 3 in this certification report.

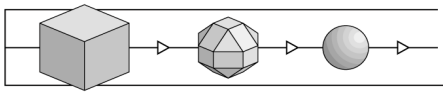
21 The certificate carries the logo „Deutsches IT-Sicherheitszertifikat” [German IT Security Certificate] officially approved by the Bundesamt für Sicherheit in der Informationstechnik (BSI) and is recognised by the BSI as equal to their own certificates. As contractually agreed, the BSI explicitly confirms this equivalence in the international context.

22 The certificate and the certification report are posted on the web pages of the certification body (www.t-systems-zert.com) and are referenced in the brochures BSI 7148 / 7149 of the Bundesamt für Sicherheit in der Informationstechnik (BSI).

23 It is hereby certified that

- the evaluators and certifiers who have participated in this procedure, have not been involved in developing, selling or applying the TOE,
- all rules of the certification scheme, of the specific type of procedure and the relevant criteria have been met.

Klaus-Werner Schröder	Dr. Heinrich Kersten
(Certifier)	(Head of the Certification Body)



(This page is intentionally left blank.)

5 Summary of Results

24 The following configurations of the TOE were evaluated:

The evaluators found four relevant parameters governing different configurations of the TOE. Those parameters are stated and allowed ranges of their values given.

1. The following two main configurations of the TOE are distinguished by the sponsor:

- **Conf_CERT**[1] and
- **Conf_GerLaw**[2].

The only difference between them is using of PUK as showed in following:

Configuration	Total number of PUK usage for the entire life of the TOE
Conf_CERT	≤ 14
Conf_GerLaw	= 0

Table 1: Configurations of the TOE for PUK usage

The PUK can never be used, if **Conf_GerLaw** was chosen.

Each of those two main configurations can be furthermore configured according to one of the following sixteen sub-configurations.

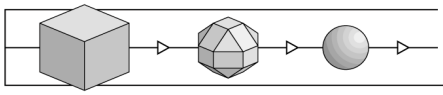
2. The Security Target [see Appendix, SRE8 – authentication expiration] describes the set {1} = {1a,1b,1c}. In case 1a cardholder can generate exactly one signature after successful authentication, while in case 1b cardholder may generate *n* of digital signatures after successful authentication. In case 1c authentication does not expire as a result of signature generation.

The set {1} is steered by the value of the parameter wear_cycles stored during personalisation.

---

1 A general configuration (personalization of the signature application) that is valid under the ITSEC scheme and universally applicable. This configuration is not intended to gain a confirmation after the German signature law.

2 A specific configuration that is ITSEC certified and accommodates the German signature law requirements concerning the PUK management.



Configuration[3]	Amount of signatures that can be generated with a single PIN verification, bits [b4-b1]
WearCycle_single	= 1
WearCycle_policy	≥ 2 and ≤ 6 or unlimited[4]

Table 2: Configurations of the TOE
for authentication expiration after signing

Only the configuration **WearCycle_single** (1a) is allowed to be used, if the TOE has to be personalised for normal signature generation by cardholder (a personal signature card). The configuration **WearCycle_policy** (1b and 1c) is permitted to be used, only if the TOE has to be personalised to be running under an appropriate external security policy (e.g. for time stamp services as a signature generation module within a Trust Centre).

3. The Security Target [see Appendix, SRE8 – authentication expiration] describes the set {2} = {2a,2b}. In case 2a user is authenticated, but his authentication expires automatically after unblocking the SigG cardholder reference data (PIN), before any signatures can be generated. In case 2b the authentication remains valid also after unblocking the SigG cardholder reference data.

The set {2} is steered by the value of the parameter authenticated_by_ unblocking stored during personalisation.

Configuration[4]	Does the authentication remain valid after unblocking the PIN (bit b8)?
Authenticated_by_unblocking_no	= 0 (no)
Authenticated_by_unblocking_yes	= 1 (yes)

Table 3: Configurations of the TOE
for authentication expiration after PIN unblocking

Only the configuration Authenticated_by_unblocking_no is allowed to be used.

4. The Security Target [see Appendix, SRE8 – authentication expiration] describes the set {3} = {3a,3b}. In case 3a user is authenticated, but his authentication expires automatically after changing the SigG cardholder reference data (PIN), before any signatures can be generated. In case 3b the authentication remains valid also after changing the SigG cardholder reference data.

The set {3} is steered by the value of the parameter authenticated_by_changing stored during personalisation.

[3] The naming is given by the evaluators for the sake of clearness.

[4] wear_cycles = 0

Configuration[4]	Does the authentication remain valid after changing the PIN (bit b7)?
Authenticated_by_changing_no	= 0 (no)
Authenticated_by_changing_yes	= 1 (yes)

Table 4: Configurations of the TOE
for authentication expiration after PIN changing

Only the configuration Authenticated_by_changing_no is allowed to be used.

Each of those configurations has been evaluated. The configuration {Conf_GerLaw, WearCycle_single, Authenticated_by_unblocking_no, Authenticated_by_changing_no}[5] is the intended TOE configuration, if TOE has to be configured for normal signature generation by cardholder according to the German Electronic Signatures Act. This configuration is used in the "hardest" operational environment[6] of the TOE. Due to these facts it is the most important configuration of the TOE. The configuration {Conf_Cert, WearCycle_single, Authenticated_by_unblocking_no, Authenticated_by_changing_no} is also appropriate for normal signature generation by cardholder.

25 The evaluation result is only valid for the configurations of the TOE described above.

26 Based on the security target and the outcome of the evaluation, the TOE has the following **security functionality**:

Identification and Authentication, Access Control, Audit, Object Reuse, Data Exchange

27 The evaluation facility came to the conclusion that the TOE meets all correctness and effectiveness requirements for the **assurance level** E3 of the ITSEC:

- ITSEC E3.1 to E3.37 for correctness phases

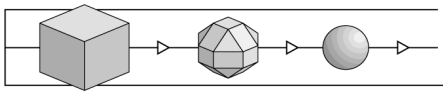
Construction - Development Process :
Requirements, Architectural Design, Detailed Design, Implementation

Construction - Development Environment:
Configuration Control, Programming Languages and Compilers,
Developers Security

Operation - Operational Documentation:

5 {Conf_GerLaw,1a,2a,3a}

6 The "hardest" environment is the operational environment with the minimal security requirements.



User Documentation, Administration Documentation

Operation - Betriebsumgebung:
*D*elivery and Configuration, Start-up and Operation

ITSEC 3.12 to 3.37 for the effectiveness aspects

Effectiveness Criteria - Construction:
Suitability of Functionality, Binding of Functionality, Strength of Mechanisms, Construction Vulnerability Assessment

Effectiveness Criteria - Operation:
Ease of Use, Operational Vulnerability Assessment

29 As to the **security mechanisms** the evaluation provided the following result (cf. Security Target for abbreviations):

These mechanisms of the TOE are **critical**: M1, M2, M3, M4, M5, M6.1, M6.2, M7, M9, M10, M11.1, M11.2.

These mechanisms are of **type A** and have a minimum strength of level **high**: M1, M2, M4, M5, M10, M11.1, M11.2.

These mechanisms are of **type B**: M3, M6.1, M6.2, M7, M9.
For mechanisms of type B no rating of the strength is specified in accordance with the criteria. But even if an attack potential according to level **high** was considered in the vulnerability assessment phase, no exploitable vulnerability could be detected in the assumed environment.

30 The **delivery procedure** for the TOE is described by the sponsor as follows:

Details of the procedure are described in the document „Setec Signature Card SetEID v1.0, Delivery and Configuration, Version 0.31 as of 26.05.2003".

The procedure of delivery comprises three steps of delivery:
a) the card manufacturer's delivery to the chip producer
b) the chip producer's delivery back to the card manufacturer, and
c) the card manufacturer's delivery to the trust centre.

The procedure of delivery guarantees the authenticity of the delivered TOE.

This delivery procedure meets the requirements of the national certification body for the assurance level E3 of ITSEC.

31 The following stipulations are to be met by the sponsor:

1. The appropriate cryptographic algorithms for the applications being conform with the German Signature Legislative are published in the Bundesanzeiger (cf. /SigV/, Annex 1, section 2). The current valid publication is /ALG/. The TOE implements the RSA algorithms for signature generation with the length of the key modulus of 1024 bits. According to /ALG/, sec. 3.1 this minimal length is valid up to end of 2007. The recommended length is 2048 bits.
   The validity of the hash function SHA-1 is defined up to the end of 2008 (see sec. 2 of /ALG/). The padding after PKCS #1, v1.5 BT1 is not confined by time.
   Due to this fact the results of the current assessment of the strength of mechanisms for the RSA algorithm are also valid up to the end of 2007. They shall be revised then.

32 The following stipulations for the secure usage of the TOE have to be met:

1. Only the configuration **WearCycle_single** (cardholder can generate exactly one signature after successful authentication) is allowed be used, if the TOE has to be personalised for normal signature generation by cardholder (a personal signature card). The configuration **WearCycle_policy** (cardholder may generate *n* of digital signatures after successful authentication or authentication does not expire as a result of signature generation) is permitted to be used, only if the TOE has to be personalised to be running under an appropriate external security policy (e.g. for time stamp services as a signature generation module within a Trust Centre).

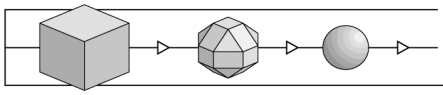
2. Only the configurations **Authenticated_by_unblocking_no** and **Authenticated_by_changing_no** (cardholder's authentication expires automatically after unblocking and changing the SigG cardholder reference data (PIN), respectively, before any signatures can be generated) are allowed to be used.

3. Generation of the signature key pair must be performed by the personalising Trust Centre operating under an appropriate security policy.

6 Application of Results

33 The processes of evaluation and certification are carried out with state-of-the-art expertise, but cannot give an absolute guarantee that the TOE is free of vulnerabilities. With increasing evaluation level however, the probability of undiscovered *exploitable* vulnerabilities decreases significantly.

34 The certification report is intended as a formal confirmation for the sponsor concerning the evaluation performed and as a basis for the user to operate the TOE in a secure way.



35 For the secure usage of the TOE, the following parts of the certification report contain important information:

- Chapter 1: the precise product name and version.
  The certificate and the certification report apply only to this TOE and its specific version.

- Chapter 5: specification of the delivery procedure for the TOE.
  Other delivery procedures may not offer the degree of security required for the assurance level E3.

- Chapter 5: specification of the evaluated configuration(s) of the TOE.
  The certification of the TOE is valid only for the configuration(s) described.

- Chapter 5: stipulations for the user of the TOE.
  A secure usage of the TOE may not be possible if these stipulations are not met.

- Annex: security target for the TOE.
  In particular, the information provided on the intended usage of the TOE, the list of TOE components, its security objectives resp. the considered threats and the operational environment should be read carefully.

36 If any requirement described in this report is not met, the evaluation results may not be fully applicable. In this case, there is a need of an additional analysis whether and to which degree the TOE may offer security under the modified conditions. The evaluation facility and the certification body can give support to perform this analysis.

37 When the TOE, its delivery procedure or its operational environment is modified, a **re-certification** can be performed in accordance with the rules of the certification body. The results of such a re-certification will be documented in technical anneces to this certification report.

38 If current findings in the field of IT security affect the security of the TOE, technical anneces to this certification report may be issued as well.

39 The web pages of the certification body (www.t-systems-zert.com) will provide information on

- the issuance of technical anneces to this certification report (technical anneces are numbered consecutively: T-Systems-DSZ-ITSEC-04016-2003**/1**, ...**/2**,...),

- new TOE versions under evaluation or already certified.

End of the Certification Report for T-Systems-DSZ-ITSEC-04016-2003.

Annex.

Security Target for

„Setec Signature Card SetEID v1.0“

Setec Signature Card SetEID v1.0

Security Target

Compliant with SigG, SigV and DIN 66391-1

Document version 1.2

9.7.2003

Jussipekka Leiwo

SETEC

P.O. Box 31
FIN-01741 Vantaa
FINLAND

Telephone +358 9 89411
Fax +358 9 878 6133
Internet http://www.setec.fi

Version History

Version	Date	Description	Editor
1.0	11.05.2001	ITSEC deliverable	JLe
1.1	4.7.2003	Finalized for ETR: 1. Table 1 (Sect. 2.2) converted into text, updated to reflect the final versions of documents. 2. Updated reference to RMS+ (Sect. 2.2)	JLe
1.2	8.7.2003	Returned Table 1	JLe

Contents

1. Evaluation scope

1.1. Evaluation Scheme

Based on this Security Target an evaluation shall be carried out in Germany on the basis of the „Information Technology Security Evaluation Criteria (ITSEC)“.

According to the German security evaluation scheme, the Evaluation Facility must be accredited by the Accreditation Body of „Bundesamt für Sicherheit in der Informationstechnik (BSI)“ in accordance with EN 45001 and must be licensed after having shown to the satisfaction of the Certification Body of the „Bundesamt für Sicherheit in der Informationstechnik (BSI)“ that it is technically competent in the specific field of IT security evaluation and that it is in the position to comply in full with the rules of the Scheme concerned.

For common evaluations the Evaluation Facility shall also be licensed by the respective Certification Body which monitors the evaluation process and which certifies the result. But this is not required here. Nevertheless, a special confirmation is required according to §17 (4) in [4].

1.2. Developer and Sponsor

The evaluated product has been developed and produced by

Setec Oy
Suometsäntie 1
FIN-01740 Vantaa
Finland
☎ +358 9 89411
+ 358 9 878 6133

Setec Oy is also the sponsor of the evaluation according to ITSEC.

1.3. Evaluation Target

TOE’s critical security mechanisms of ITSEM type A are expected to provide a strength of mechanisms, which is HIGH.

TOE will be evaluated using level E3 (”E Three”).

2. Product Rationale

2.1. Product Overview

The product, Setec Signature Card SetEID v1.0, is a combination of software and application data, both stored and operated in an ICC. This combination provides a digital signature application according to the "Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG)" [4].

Software of the product (SetCOS 4.4.1 rev A.2) is a multi-application operating system with a hierarchical file system. It supports dynamic file system

management, symmetric and asymmetric cryptographic operations, user authentication, and flexible access control for the files. Interface to the smart card follows ISO standards 7816-3, 7816-4, 7816-5, 7816-6 and 7816-8, and the DIN standard DIN 66391-1.

Intended use of SetCOS 4.4.1 rev A.2 is for applications employing public key cryptography, e.g. digital signatures. In particular, it can be used as a basis for a Signature Component according to the abovementioned SigG. It supports the asymmetric RSA cryptographic algorithm with up to 1024-bit key lengths, and the symmetric DES-3 (triple-DES) cryptographic algorithm utilising 128-bit keys (112 bits effective).

The application on top of SetCOS 4.4.1 rev A.2, herein called "SigG signature application", follows the file structure described in the DIN 66391-1 standard. It provides a card holder PIN value and card holder's private key for signature function. Mutual authentication with a SigG-accredited terminal (Public IFD) is not supported.

2.2. Identification of TOE

The integrated circuit card (ICC) contains

(1) target of evaluation (TOE), and

(2) data of other applications.

The TOE consists of

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

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

The TOE provides functions

(3) for creating the signature application (including the data being specific for the cardholder) within the card during the initialisation, pre-personalisation, and personalisation phases in the ICC life cycle,

(4) for generating key pairs on the ICC,

(5) for providing security for the key pair generation,

(6) for generating digital signatures, and

(7) for providing security for the digital signature generation.

Other parts of the TOE software are needed

(8) for using the SigG signature application with additional functions,

(9) for providing specific functions for non-SigG applications which may also reside on the card and are different from SigG signature application, and

(10) for providing other ICC functions for 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 data of the SigG application is defined in [2] and [18]. The former is a more generic specification while the latter presents several precise configurations where the subjects to changes are (i) cardholder identification configuration, (ii) sizes of mandatory files, (iii) amount and characteristics of additional files, and (iv) access condition options for files.

TOE is a product.

The complete software on the ICC is named "SetCOS 4.4.1 rev A.2". Part of that software is hardwired into the ROM of the ICC and part is loaded into the ICC during initialisation process. Further revisions may emerge in future, but they are not part of this evaluation. All such revisions are based on the same operating system platform in ROM (SetCOS 4.4.1), differing only in some details.

The ICC in which the TOE is implemented is the "SLE 66CX320P", produced by Infineon Technologies AG [12]. It contains also a firmware component "Resource Management System" (RMS+ v0.6 [22]) which is part of the TOE. The TOE also uses resources of the ICC (e.g. Special Function Registers) directly when no mandatory firmware interface for the access exists. The resources available to and used by the TOE are described in [19]. Both the ICC and part of the firmware have been evaluated in accordance with ITSEC level E4 with strength of mechanisms high (see [19]). All firmware and hardware of the ICC is excluded from this evaluation, only the software using them (i.e. the TOE) is in the scope of the evaluation.

The TOE can be accessed only by an Interface Device (IFD) via a serial interface circuitry in accordance with [8], provided by the ICC. The serial interface circuitry of the ICC is controlled by the TOE. The ICC provides adequate protection to prevent direct access to the TOE (i.e. to ICC memory cells). The ICC also provides protection against covert channel information flow from TOE to external world, part of which are activated and operated by the TOE.

Table 1 identifies items which formally constitute the TOE.

Table 1 Identification of delivered TOE.

TOE item name	Type	Version	Date	ROM release
SetCOS 4.4.1	SW (in ICC ROM)	1.1	3.12.2002	
rev A.2 extension for SetCOS 4.4.1	SW (in ICC EEPROM)	A2	12.11.2002	-
SigG signature application	ICC application data (in ICC EEPROM)	1.1	24.6.2003	-
Infineon RMS+ Resource management system	Firmware component	0.6	04/2000	
Setec Signature Card SetEID v1.0, Signature application	Document	1.1	24.6.2003	-
SetCOS 4.4.1, Initialisation details	Document	1.0	8.4.2003	-
Setec Signature Card SetEID v1.0, Personalisation of the signature application	Document	1.2	1.7.2003	-
Setec Signature Card SetEID v1.0, Guidance documentation	Document	0.35	1.7.2003	-
SetCOS User's Guide Part 1, Overview	Document	1.2	15.10.1999	-
SetCOS User's Guide Part 2, SetCOS 4.x series	Document	1.3	28.4.2003	-
SetCOS User's Guide Part 3, SetCOS 4.4.1	Document	1.5	11.11.2002	-

2.3. Intended method of use

TOE is intended to provide a digital signature function to the legitimate cardholder acting as the owner of an individual ICC equipped with the signature key of the cardholder in accordance with the SigG legislative [4] and [21], and standard [2].

Development and manufacturing of the ICC's software and hardware leads to the ICC being ready for use in a specific application. ICC will be loaded with the SigG application, including data specific to the cardholder, in the pre-personalisation and personalisation phases of the ICC. TOE implements security features to ensure secure personalisation of the ICC.

TOE supports (i) generation of the signing key pairs on the ICC, (ii) loading of PIN/PUK information securely from outside of the TOE, (iii) extraction of the public key information together with a cryptographic checksum, (iv) loading of other SigG (as well as non-SigG) data from outside of the TOE, and (v) specific access conditions for the personalisation phase, as described in [16]. Initialisation and pre-personalisation of ICC shall be performed in a secure environment. Loading key pairs from outside the ICC is not supported.

In the operational use phase of the ICC, TOE is used by the cardholder by providing it to some IT system containing a message for which the cardholder wishes to generate a digital signature. The TOE and the IT system

communicate through the interface device (IFD). Moreover the IFD is the human interface to the ICC.

TOE may only be used with an office IFD, not with a Public IFD.

Cardholder has to authenticate himself to the TOE prior to the signature generation. IFD presents TOE with the verification data of the cardholder. After a successful authentication, TOE allows (i) generation of an unlimited number of digital signatures within the current session, or (ii) generation of a limited number of digital signatures within the current session (see [2], section 8). The digital signature is created from a hash-value of the message text. The IT system (i) transforms the message text into the has-value and transmits the hash-value to the TOE, (ii) calculates an intermediate hash-value of the message text and transmits the remaining message text to the TOE, or (iii) transmits the complete message text to by hashed by the TOE. TOE calculates the digital signature of the hash-value with the SigG private signature key of the cardholder, stored in the TOE. TOE returns the digital signature to the IFD. Cardholder's SigG private signature key never leaves the ICC.

The ICC may be used as a multi-application smart card. In this case, applications may be loaded on the ICC in the operational usage phase, but TOE prevents execution of any executable data in this application.

2.4. Assumptions about the environment

Assumptions are made regarding conditions external to the TOE to ensure the effectiveness of TOE's security functions. The assumptions are summarized in Table 2.

Table 2 Assumptions about the environment

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

2.4.1. AE1: Life cycle security

The main purpose of the TOE is to enforce security objectives described in section 2.6 within the operational use phase. To effectively fulfil TOE's security objectives in the operational use phase, security of earlier life cycle stages shall be relied upon. Assumptions AE1 about the security of the ICC life cycle are made (see also Assumptions AE2 in section 2.4.2):

(AE1.1) Security of procedures in (i) the manufacturing phase, (ii) the initialisation phase, (iii) pre-personalisation phase, and (iv) the personalisation phase of the ICC life cycle are assured.

(AE1.2) Personalisation facility and certification authority preserve the confidentiality of the authentication information of TOE users.

(AE1.3) Key generation environment provides measures for preventing the analysis of physical observables representing covert channel information flow. Recording of the physical observables shall be prevented during key generation.

Descriptions of procedures for secure manufacturing, initialisation, pre-personalisation and personalisation of ICC are available in [12], [17], and [18]. Measures to prevent analysis of key generation concern either pre-personalisation or personalisation phase and can be found in [17].

2.4.2. AE2: Integrity and quality of key material

TOE is used in a public key infrastructure for SigG digital signatures. Assumptions AE2 about the public key infrastructure are made:

(AE2.1) The environment ensures the following properties for the SigG signing key pair of the root certification authority:

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

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

(3) authenticity (especially origin) of the public key (see PK.DEPCA.DS in [2], sections 9).

(AE2.2) The environment ensures the following properties for the SigG signing key pair of the certification authorities for SigG signing keys:

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

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

(3) authenticity (especially origin) of the public key (see PK.CA.DS in [2], sections 9 and 18.3.2) in the certificate C.CA.DS.

(AE2.3) The environment ensures authenticity (especially origin) of the public key (see PK.CH.DS in [2], annex D) in the certificate C.CH.DS, generated by the certification authority for SigG digital signatures.

2.4.3. AE3: SigG compliant use of the TOE

Assumptions AE3 about the SigG compliant use of the TOE are made:

(AE3.1) Cardholder uses the TOE in accordance with the SigG legislative. According to the regulations, the cardholder must at least:

(1) ensure secure storage and handling of the ICC to prevent misuse and manipulation of the ICC,

(2) use the TOE SigG signature generation function only for generating signature for data of which integrity or authenticity are assured,

(3) preserve the confidentiality of the PIN, PUK or password[1]

(4) change the PIN, PUK or password regularly,

(5) know whether the used IFD is (i) a public IFD or (ii) an office IFD, and

(6) only use the TOE SigG application with an office IFD.

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

2.4.4. AE4: Use with SigG compliant IFD

SigG regulations require that the TOE is only used with SigG compliant technical components. Bodies operating the technical components are responsible for setting up and maintaining appropriate security for the SigG compliant technical components. Assumptions AE4 about the use with SigG compliant IFD are made:

(AE4.1) Cardholder uses the TOE SigG application only with a SigG compliant office IFD.

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

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

(2) the office IFD preserves the confidentiality of the cardholder's authentication information,

(3) the environment preserves the confidentiality and integrity of the data transmitted between the office IFD and the ICC.,

(4) the IFD appropriately informs the cardholder about the current state of the TOE if (i) the TOE is in the secure blocking state, or (ii) a PIN or a PKU is in the blocked state.

2.4.5. AE5: Security assumption about the ICC hardware

Assumptions AE5 about the ICC hardware are made:

(AE5.1) ICC hardware is tamper resistant, in a manner that it

[1] PIN and PUK are different representations of the string put into the IFD by the cardholder. The IFD transforms the input string into the reference data as a string transmitted to the ICC. Thus the TOE does not care about the different presentation of the reference data (PIN or PUK) by the cardholder.

(1) protects the TOE against modification, and

(2) protects the confidentiality of the cardholder's SigG private signature key, stored on the ICC, against physical attacks.

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

(AE5.3) ICC hardware implements security mechanisms

(1) to detect potential security violations by physical tampering,

(2) to signal the TOE to react,

(3) and to prevent the execution of TOE.

ICC hardware mechanisms can detect and directly react to abnormal environmental conditions. Alternatively, the ICC hardware may signal TOE of abnormal environmental conditions detected, or the TOE may detect the abnormal environmental conditions by monitoring the values of various environmental registers set by the ICC hardware.

Detection of abnormal environmental conditions immediately ceases the operation of the TOE and triggers a reset on the ICC, restarting the TOE in a controlled way when (a) the conditions are normal, and (b) an external reset signal is applied to the ICC. The cardholder can detect this from the response of the TOE to external events: the TOE becomes non-responsive until it has been reset under normal conditions. This reaction is separate from TOE and hence does not lead to a permanent blocking state of the TOE.

The ICC hardware mechanisms can also detect physical tampering of the ICC. Upon occurence of such an event the ICC may (i) trigger a reset on the ICC, (ii) signal the TOE to react on it, or (iii) set the values of various registers to allow TOE to detect the physical tampering and take appropriate action.

2.5. Assumed Threats

Assumed threats for the TOE are a consequence of the method of use, the environment of the TOE, and the overall security policy, derived from the TOE's overall purpose of being a technical component for generating digital signatures compliant with SigG legislative and [2]. The fundamental threat is cardholder's signature being generated for a data item the cardholder does not want to be signed (by himself).

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 the subsection. Figure 1 illustrates the threat scenario assumed for the TOE. Items with dotted borderline are forged or otherwise potentially malicious. Items with solid borderline are ”authentic”. Table 3 summarizes the assumed threats.

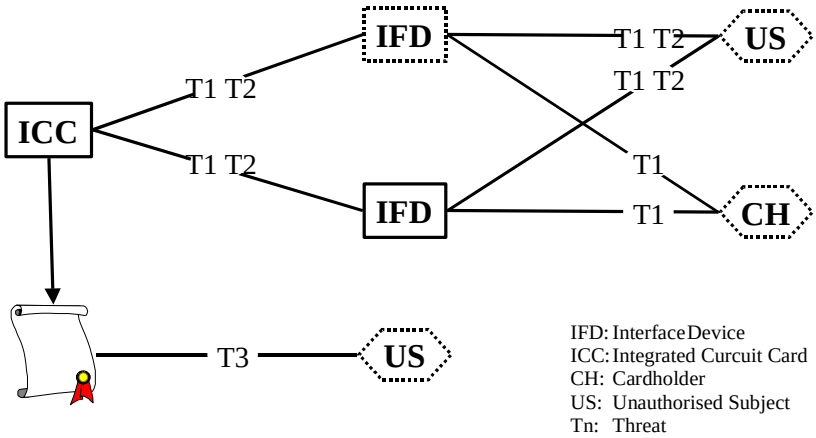


Figure 1: Threat Scenario

Table 3 Security Threats

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

2.5.1. T1: Extraction of the cardholder's secret key

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

(T1.1) User may try to extract from the ICC the SigG signing key owned by the cardholder and used for digital signatures.

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

(T1.2) User may try to modify the secret key stored in the ICC.

Modification of the secret key may result in a digital signature generated by the TOE no longer regarded as compliant to the SigG legislative.

2.5.2. T2: Misuse of the signature function

TOE generates digital signatures for the cardholder.

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

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

2.5.3. T3: Forged data ascribed to the cardholder

A message is characterised by (i) the sender, (ii) the designated receiver, and (iii) the message text. Hash-value is an image of the message text.

(T3.1) An unauthorised subject may succeed in modifying, undetected to the recipient, of the message text originating from the cardholder.

Message text originating from the cardholder is exposed to modifications not authorised by the cardholder. Modification of the message text cannot be adverted but may be detected by the recipient of the message.

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

The message will be ascribed to the originator notified within the message. If the message text 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.

2.6. Security Objectives

Table 4 summarises the security objectives, 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. Security objective are described in corresponding subsections by (i) stating the security objective, (ii) giving rationales and explaining the relationship to assumed security threats previously presented, and (iii) indicating the security functionality used to achieve the security objective.

Table 4 Security objectives [2]

Id	Security Objective
SO1	Prevent extraction and modification of the cardholder's SigG private signature key
SO2	Prevent unauthorised use of the SigG digital signature function
SO6	Quality of key generation
SO7	Generate secure digital signature
SO8	React to potential security violations

2.6.1. SO1: Prevent extraction and modification of the cardholder's SigG private signature key

TOE ensures confidentiality and integrity of the cardholder's SigG private signature key stored in the TOE by two means:

(SO1.1) by preventing any kind of extraction of the cardholder’s secret key from the ICC, and

[2] The numbering is not sequential. The used numbering aims to provide consistency with [3].

(SO1.2) by preventing any kind of modification of the cardholder's secret key in the ICC.

Cardholder intends to protect the integrity of his messages while in transit (either over space or time) to the intended recipient. It is the TOE's principal function to generate digital signatures for data related to the message text as provided by the IFD. The signature enables recipient to verify origin and integrity of the message text. The effectiveness of digital signature mechanism is based on confidentiality and integrity of the cardholder's secret key. TOE is intended to be used within the context of SigG legislative, which is strict about the confidentiality: the key may never leave the signature device and may not be disclosed when used (see [21] §15 (1)).

These security objectives cover threats T1.1 and T1.2 defined in section 2.5.1.

TOE implements security enforcing functions SEF AC1 and SEF AC2 described in section 3.5 to fulfil security objective SO1. Security enforcing function SEF OR1 described in section 3.5.5 prevents illicit information flow between the SigG application and other applications embedded in the ICC through temporarily used storage areas. Security enforcing functions SEF DX1 and SEF DX2 described in section 3.6 prevent disclosure of cardholder's SigG private signature key in digital signatures generated by the TOE. Secure blocking state of TOE ensure security of cardholder's SigG private signature key if a potential attack is detected (see security enforcing functions SEF AC3 and SEF AU1 in sections 3.5 and 3.5.4.)

2.6.2. SO2: Prevent unauthorised use of the SigG digital signature function

TOE allows use of the digital signature function only to the cardholder. This security objective has the following aspects:

(SO2.1) TOE allows use of the digital signature function only to the cardholder after successful authentication by knowledge,

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

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

Security objectives SO2 correspond to [21] §15 (1) Sentence 1 requiring authentication of the cardholder for access to functions using the SigG private signature key of the cardholder.

Security objectives SO2 counter threat T2 (section 2.5.2).

TOE implements security enforcing functions SEF IA1, SEF IA2, SEF IA3, SEF IA4 and SEF AC1 described in sections 3.4, and 3.5 to fulfil security objectives SO2. Secure blocking state of TOE ensures security of the SigG signature function if a potential attack is detected (see security enforcing functions SEF AC3 and SEF AU1 in sections 3.5 and 3.5.4.)

2.6.3. SO6: Quality of key generation

Any key material generated by TOE bears strong cryptographic quality. Cryptographic quality of secret keys is characterised as follows:

(SO6.1) if generated in the pre-personalisation or in the personalisation phase, the generation of keys preserves their confidentiality,

(SO6.2) if generated by TOE, they shall be unique with a very high probability and cryptographically strong, and

(SO6.3) they can not be calculated from the corresponding public keys.

Security objectives SO6 fulfil the requirement of [21] §15 (1) for the SigG signature key pair of the cardholder.

Security objectives SO6 counter threat T3 ensuring a precondition for the cryptographic strength of the digital signature (see also [1]).

TOE implements security enforcing function SEF DX1 described in section 3.6 to fulfil security objectives SO6 by the means of generation of secure SigG signature key pairs. Secure blocking state of the TOE prevents misuse of SEF DX1 if a potential attack is detected (see SEF AC3 and SEF AU1 in sections 3.5 and 3.5.4.)

2.6.4. SO7: Generate secure digital signature

The principal security objective of TOE is SO7 the generation of secure SigG digital signatures:

(SO7.1) TOE provides a function for generating SigG digital signatures for data presented by the IFD. The signature is generated using the cardholder's SigG private signature key stored in the TOE.

(SO7.2) Function for generating SigG digital signatures works in a manner that prevents other individuals, i.e. those not possessing cardholder's SigG private signature key, from generating valid signatures.

Security objectives SO7 are drawn from [21] §15 (1). The requirement of [21] §15 (1) stating that cardholder’s secret key can not be derived from the signature is a sub-case of security objective SO1.1 because signature is a part of the TOE’s output. Security objective SO7.2 relates to a cryptanalytical attack against a signed message independently of the TOE and addresses the cryptographic strength of the signing function of the TOE (see [1]).

Data presented by the IFD to be signed is (i) a hash-value of the message text, (ii) an intermediate has-value of the message text and the remaining message to be hashed, or (iii) the complete message text to be hashed by the TOE (see [2], section 14).

Security objectives SO7 are the principal objectives of TOE, directly countering threat T3.

TOE implements security enforcing function SEF DX2 described in section 3.6 to fulfil security objective SO7. Secure blocking state of TOE ensures security of the SigG signature generation if a potential attack is detected (see SEF AC3 and SEF AU1 in sections 3.5 and 3.5.4.)

2.6.5. SO8: React to potential security violations

TOE fulfils security objectives SO8 in agreement with assumptions AE5.3:

(SO8.1) TOE reacts to potential security violations which are (i) recognized and signalled to the TOE by the underlying ICC hardware, or (ii) detected by the TOE itself.

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

(1) TOE reaches a secure blocking state disabling at least the SigG application of the ICC, and

(2) the blocking state is made apparent to the user.

In case ICC hardware detecting a potential security violation and preventing the execution of TOE (see assumption AE5.3(2)), security objectives SO8 are fulfilled since this is a secure state of ICC discernible by the cardholder.

Security objectives SO8 are drawn from [21] §15 (4).

Security objectives SO8 are related to all threats T1, T2 and T3.

TOE implements security enforcing functions SEF IA1.3, SEF AC3 and SEF AU1 described in sections 3.4, 3.5, and 3.5.4 to fulfil security objectives SO8.

3. Security Enforcing Functions

Informal descriptions, as required by ITSEC level E3, are given on security enforcing functions the TOE implements to counter the assumed threats. Subjects, Objects, and security relevant events are also introduced to aid in understanding descriptions of security enforcing functions. Definitions and terms used are also collected in a glossary in section 7.

3.1. Subjects

IFD presents as technical process the outside world beyond the interface of the ICC and thus the TOE. 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 the body running the IT-system as a service provider to the human user. In the point of view of the TOE security policy, outside world is a combination of two types of subjects: (i) the human users, and (ii) the IT-systems. Subjects S1, S2 and S7 represent human users. Subject S3 represents an IT-systems. Subjects are also listed in Table 5. Term “Anybody” is introduced for the set of subjects S1 and S2 to make some descriptions easy.

Table 5 Subjects [3]

Id	Subject
S1	Cardholder
S2	Somebody
S3	IFD
S7	Potential attacker

3.1.1. S1: Cardholder

In the operational phase, subject S1 is a human user for which the SigG application of TOE is personalised: cardholder is the only person in a 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 assumption AE3.1).

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

3.1.2. S2: Somebody

Subject S2 is a human user of the ICC different from subjects S1 and S7, i. e. (i) a party not in a legitimate possession of the verification data defined for the cardholder, and (ii) a party using TOE that is not in the secure blocking state. Subject S2 may be in a legitimate possession of the verification data for a non-SigG application on the ICC.

3.1.3. S3: IFD

Subject S3 is an interface device connected to the ICC which is not a SigG accredited IFD, i.e. it is an office IFD (see assumption AE3.1(6) for reasons).

3.1.4. S7: Potential attacker

Subject S7 is an arbitrary subject trying to use TOE in the secure blocking state (e. g. after a potential attack is detected, see Security Relevant event SRE10 and security objectives SO8 for details).

3.2. Security relevant events

Security-relevant-events depend on (i) the commands presented by the IFD to the TOE, (ii) command data presented by the IFD to the TOE, (iii) data about security relevant events persistently stored in the TOE, and (iv) events signalled by the ICC hardware to the TOE (see assumption AE5).

Security-relevant-events listed in Table 6 are recognised by the TOE.

[3] The numbering is not sequential. The used numbering aims to provide consistency with [3].

Table 6 Security-relevant-events [4]

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

3.2.1. SRE1: Resetting of the ICC

Security relevant event SRE1 occurs if (i) the ICC is powered up by inserting the ICC into a suitable IFD (”activation”) or a hardware reset signal is given to the ICC, and (ii) the TOE detects that the Potential security violation flag is not set. TOE performs a well-defined initialisation procedure (”card reset”) without intervention of the user or the IFD.

3.2.2. SRE2: Deactivation of the ICC

Security relevant event SRE2 occurs if (i) the power supply of the ICC is down like by removal from the IFD. After SRE2, all information of the TOE associated with the run-time session is lost.

3.2.3. SRE3: Opening of the SigG application

Security relevant event SRE3 occurs if (i) no file of the SigG application is currently selected, and (ii) a file in the SigG application directory is selected.

Note: if the SigG application is still open, the selection of a file in the SigG application will not cause the security relevant event SRE3.

3.2.4. SRE4: Closing of the SigG application

Security relevant event SRE4 occurs if (i) a file of the SigG application is currently selected, and (ii) a file outside the SigG application directory is selected.

[4] The numbering is not sequential. The used numbering aims to provide consistency with [3].

3.2.5. SRE5: Successful cardholder authentication

Security relevant event SRE5 occurs if (i) the authentication of a human user for the SigG application with the verification data is attempted, (ii) the number of consecutive failed authentication attempts with reference data does not exceed the maximum number of allowed failed authentication attempts, and (iii) the verification data presented for human user authentication matches object O3 (see Section 3.3) stored for the SigG application of the TOE. As the TOE supports only the user authentication by knowledge for the SigG application, (ii) is fulfilled if and only if the verification data presented matches the reference data for knowledge based authentication. Upon occurrence of SRE5, the number of consecutive failed authentication attempts with reference data is set to zero.

3.2.6. SRE6: Cardholder authentication failure

Security relevant event SRE6 occurs if (i) the authentication of a human user for the SigG application with the verification data is attempted, (ii) SRE5 does not occur, and (iii) the maximum number of allowed consecutive failed authentication attempts with reference data is not exceeded. Upon occurrence of SRE6, the number of consecutive failed authentication attempts with reference data is incremented by one.

3.2.7. SRE7: Repeated authentication failure

Security relevant event SRE7 occurs if (i) the authentication of a human user for the SigG application with verification data is attempted, and (ii) SRE5 does not occur and (iii) the maximum number of allowed consecutive failed authentication attempts with reference data is exceeded.

3.2.8. SRE8: Authentication expiration

Security relevant event SRE8

(case 1a) occurs if a digital signature was generated (not configurable by the cardholder),

(case 1b) occurs if one of the following events occurs according to the configuration selected by the cardholder

(1) a digital signature was generated, or

(2) after n digital signatures,

(case 1c) does not occur after any number of digital signatures,

(case 2a) occurs after unblocking the SigG cardholder reference data,

(case 2b) does not occur after unblocking the SigG cardholder reference data,

(case 3a) occurs after changing the SigG cardholder reference data,

(case 3b) does not occur after changing the SigG cardholder reference data,

depending on the personalised configuration. TOE can be configured to any combination of cases {1a,1b,1c}, {2a,2b} and {3a,3b} during personalisation[5].

In the case 1a, cardholder has no control over the amount of signatures that can be generated after successful authentication, while in the case 1b, cardholder may define the number *n* of digital signatures, but only once and only before the personalisation of the ICC. In the case 1c, authentication does not expire as a result of signature generation [6].

In cases 2a and 3a, user is authenticated but this authentication expires automatically before any signatures can be generated. In cases 2b and 3b, authentication remains valid also after unblocking or changing the SigG cardholder reference data. This configuration must be made during personalisation.

3.2.9. SRE10: Potential security violation occurred

Security relevant event SRE10 occurs if:

(1) (i) underlying hardware signals a failure or other event deemed as a potential security violation, or (ii) an event detected by the TOE deemed as a potential security violation occurs, or

(2) TOE detects that after the ICC is powered up or a hardware reset signal is given to the ICC.

In both cases, the Potential security flag is set. Conditions which lead to the Potential security violation flag being set have been described in section 2.6.5.

3.2.10. SRE11: Cardholder authenticated by reset code

Security relevant event SRE11 occurs if (i) authentication by reset code of the SigG application was attempted, (ii) the human user authentication for the SigG application by presenting the reset code is allowed[7], and (iii) the reset code presented matches object *O4* (Section 3.3) of the SigG application of TOE.

SRE11 may automatically trigger security relevant event SRE8 in some TOE configurations.

[5] To cater for a number of application scenarios, different authentication expiration thresholds are required. For example, an end-user card could be configured to require reauthentication prior to any signature creation. A frequently used card, e.g. one used for providing a time stamping service, could only require reauthentication after a reasonably large number of signatures being generated.

[6] This configuration can be used when TOE has been configured e.g. for time stamp services. It is not intended to be used when TOE has been configured for normal signature generation by cardholder.

[7] This is allowed if the maximum number of consecutive failed authentication attempts with reference data has been exceeded and if the maximum number of consecutive failed authentication attempts with reset code has not been exceeded.

3.2.11. SRE12: Cardholder authentication by reset code failed

Security relevant event SRE12 occurs if (i) authentication with SigG cardholder reset code is attempted, and (ii) the presented code does not match object *O4* (Section 3.3) stored in the TOE.

If retry of the human user authentication for the SigG application by presenting the reset code is no longer allowed (due to the repeated occurrence of SRE12), occurrence of security relevant events SRE11 and SRE12 becomes impossible (requirement (ii) of SRE11 cannot be fulfilled). As (in particular a repeated occurrence of) SRE12 is possible only when security relevant event SRE7 has occurred, human user authentication for the SigG application becomes irreversibly and ultimately inhibited.

3.3. Objects and Access-types

Objects and related access-types identified by the TOE are listed in Table 7, and used for replacing the placeholders in the following text.

Table 7 Objects and related access-types [9]

Id	Object	Access-types
O1	SigG application	open, close
O2	SigG private signature key of the cardholder	generate, use for signature generation, extract
O3	SigG cardholder reference data	use for cardholder authentication, modify, block, unblock
O4	SigG cardholder reference reset code	use for authentication, block
O5	SigG signature key certificate of the cardholder	read, modify
O6	SigG public key of the root certification authority	read, modify
O7	Other credentials for signature verification	read, modify
O12	SigG public key of the cardholder	read, generate

3.3.1. O1: SigG application

Object O1 includes SigG related data objects and functions and methods to access or use that data.

Term "**open**" of O1 means enabling 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.

Term "**close**" of O1 means disabling of these access-types and giving way to other not SigG related activities.

Object O1 is always implicitly closed immediately after resetting the TOE.

[9] The numbering is not sequential. The used numbering aims to provide consistency with [3].

3.3.2. O2: SigG private signature key of the cardholder

Object O2 is part of object O1 and is used by TOE for generating a digital signature on behalf of the cardholder. This object is named SK.CH.DS in [2].

Term "**generate**" of O2 means generation of a SigG key pair for the cardholder on the ICC and storing cardholder's SigG private signature key in the TOE.

Term "**use for signature generation**" of O2 means calling and performing of respective commands to generate a digital signature.

Term "**extract**" of O2 means (i) using the key for any other function beside signature generation (in sense of referral), and (ii) gathering of any information about the O2 by observing the TOE's external behaviour during the computation of a digital signature (e.g. electromagnetic emanation, power consumption and timing, in sense of inferring).

3.3.3. O3: SigG cardholder reference data

Object O3 is the data permanently stored in the TOE to verify the verification data provided for the cardholder authentication.

Term "**use for cardholder authentication**" of O3 means calling services that provide human user authentication by comparing object O3 with the verification data presented (see security enforcing function SEF IA1 described in section 3.4.)

Term "**modify**" of O3 means (i) using O3 for cardholder authentication, and (ii) if this cardholder authentication is successful, then replacing the value of O3 with the presented value.

Term "**block**" of O3 means deactivating O3 for being used for cardholder authentication as a consequence of a repeated authentication failure (see security relevant event SRE7 in section 3.2).

Term "**unblock**" of O3 means (i) using object O4 for cardholder authentication, and (ii) if this cardholder authentication is successful, then replacing the value of O3 with the presented value if such a value is presented.

3.3.4. O4: SigG cardholder reference reset code

Object O4 is the data permanently stored in TOE to verify the reset code provided to unblock and to change values of object O3.

Term "**use for authentication**" of O4 means calling services which (i) compare the value of O4 with the reset code presented (see security enforcing function SEF IA1 in section 3.4), and (ii) allow unblocking and changing of object O3 if the presented reset code matches the value of O4 (see SEF IA4 in section 3.4.).

Term "**block**" of O4 means deactivating O4 for being used for cardholder authentication as a consequence of a repeated authentication failure (see security relevant event SRE12 in section 3.2.11).

3.3.5. O5: SigG signature key certificate of the cardholder

Object O5 is the certificate of the SigG public key of the cardholder. The certified public key corresponds to the secret key used for the signing algorithm by the TOE, and is stored in the TOE and may be extracted and used by external parties to verify the cardholder's signatures. This object is named C.CH.DS in [2].

Term "**read**" of O5 means exporting the object O5 to the IFD.

Term "**modify**" of O5 means changing the stored value of O5.

3.3.6. O6: SigG public key of the root certification authority

Object O6 is the public key of the root certification authority, used by the signing algorithm supported by the TOE. It is stored in the TOE and may be extracted and used by an external party to verify the certificate stored as object O5. O6 is named PK.RCA.DS in [2].

Term "**read**" of O6 means exporting the object O6 to the IFD.

Term "**modify**" of O6 means changing the stored value of O6.

3.3.7. O7: Other credentials for signature verification

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

Term "**read**" means exporting the object O7 to the IFD.

Term "**modify**" means changing the stored value of O7.

Term "**supplement**" means adding data (public keys or certificates) to O7.

3.3.8. O12: SigG public key of the cardholder

Object O12 is part of object O1 and is used by the TOE to verify the digital signature of the cardholder. Object O12 is named PK.CH.DS in [2].

Term "**read**" of O12 means using of the respective command of TOE to transmit object O12 to the IFD.

Term "**generate**" of O12 means 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.

3.4. Identification and Authentication functions

3.4.1. SEF IA1:Authentication of human user

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

(1) SEF IA1.1 authenticates subject S1

(2) SEF IA1.2 assumes the default identity S2,

(3) SEF IA1.3 detects subject S7.

TOE contains an authentication function SEF IA1.1 that detects subject S1 in two different ways:

(1) SEF IA1.1.1 allows subjects S1 to authenticate themselves for the SigG application by presenting the verification data, provided that the SEF IA3 does not prevent usage of SEF IA1.1.1. If the presented data matches object O3, this is interpreted as security relevant event SRE5. If the presented data does not match object O3, then this will be interpreted either (i) as security relevant event SRE6 (if the maximum number of allowed consecutive failed authentication attempts with reference data is not exceeded, see security enforcing function SEF IA3), or (ii) as security relevant event SRE7 (if the maximum number of allowed consecutive failed authentication attempts with reference data is exceeded, see security enforcing function SEF IA3).

(2) SEF IA1.1.2 allows subjects S1 to authenticate themselves for the SigG application presenting data as reset code, provided that the amounts of retries of authentication by presenting the verification data or reset code do not prevent it (see below). The presented data is with respect to object O4. If the presented data matches object O4, this is interpreted as security relevant event SRE11. If the presented data does not match object O4 then this will be interpreted as security relevant event SRE12. If (i) the retry of authentication by presenting the reset code is not allowed, or (ii) the retry of authentication by presenting the verification data is still allowed, then all further attempts to authenticate by presenting the reset code will be prevented and fail independently of whether the presented data matches object O4.

TOE assumes for the SigG application the default identity of the human user S2 after security relevant events SRE1, SRE2, SRE3, SRE4, SRE6, SRE7, SRE8, and SRE12.

If security relevant event SRE10 occurs, TOE will assume subject S7 as the human user of the ICC.

3.4.2. SEF IA2: Changing reference data

TOE contains an authentication function SEF IA2 that permits subject S1, successfully authenticated with object O3, to change the value of object O3.

Cardholder changes the reference data using SEF IA2 (i) by presenting verification data matching object O3, and (ii) by defining a new value for object O3.

SEF IA2 permits the change of SigG cardholder reference data only after successful authentication of the cardholder, defined as security relevant event SRE5. SEF IA2 requires that security enforcing function SEF IA1.1.1 has been successfully executed to detect the identity of subject S1, thereby requiring

also that security enforcing function SEF IA3 has not prevented usage of object O3 for authentication.

3.4.3. SEF IA3: Blocking the reference data

SEF IA3 counts the consecutive failed authentication attempts with the verification data and prevents subjects S1 and S2 from using object O3 if the maximum number of allowed consecutive failed authentication attempts with reference data is exceeded (e.g. security relevant event SRE7 has occurred).

If security relevant event SRE7 occurred, SEF IA3 prevents authentication attempts independently of whether the presented data matches O3.

3.4.4. SEF IA4: Unblocking and changing the reference data

SEF IA4 permits subjects S1, when successfully authenticated with object O4, (i) to unblock object O3, and (ii) to modify the value of object O3.

SEF IA4 permits unblocking and modification of the SigG cardholder reference data only after successful authentication of the cardholder defined as security relevant event SRE11 (see also security enforcing function SEF IA1.1.2).

As a result of unblocking or changing the reference data, security relevant event SRE8 may occur, depending on the configuration of the TOE.

3.5. Access Control functions

3.5.1. SEF AC1: Access control of commands

SEF AC1 controls access of subjects S1, S2 and S7 representing a human user.

SEF AC1 permits subjects *s* to access objects *o* by the access-type acy(*s,o*) as defined in Table 8. SEF AC1 prevents subjects *s* from accessing objects *o* by the access-type acn(*s,o*) as defined in Table 9.

Access-sets *acy* and *acn* do not guarantee the possibility of an access request. This does not contradict the security policy because reliability of service is not a security objective of the TOE.

Access-sets *acy* and *acn* are defined for the operational phase only. TOE will detect subjects S7 if the TOE is in the blocking state of the TOE. Access-type “extract” is prevented partially by security enforcing function SEF AC1 and partially by SEF AC2 for all subjects. This security target does not cover the privileged IFD authenticated with RoleID=02 defined in [2], annex C. Therefore the TOE does not allow modification or supplementing of objects O5, O6, O7.

Access-sets *acy(s,o)* and *acn(s,o)* are applied in the operational phase only, i.e. for the time after objects O2 and O12 are generated and objects O3, O5, O6 and O7 loaded into the ICC. Additional measures are used to prevent signature generation during pre-personalisation and personalisation, as defined in [17].

Table 8 Access-set acy(*s,o*) of SEF AC1

Object	S1	S2	S7
O1	open, close	open, close	
O2	use for signature generation		
O3	use for cardholder authentication, modify, block, unblock	use for cardholder authentication, block	
O4	use for authentication, block	use for authentication, block	
O5	read		
O6	read	read	
O7	read	read	
O12	read	read	

Table 9 Access-set acn(o,s) of SEF AC1

Object	S1	S2	S7
O1			open, close
O2	extract [10], generate	extract [10], generate, use for signature generation	extract [10], generate, use for signature generation
O3		modify, unblock	use for cardholder authentication, modify, block, unblock
O4			use for authentication, block
O5	modify	read, modify	read, modify
O6	modify	modify	read, modify
O7	modify	modify	read, modify
O12	generate	generate	generate, read

3.5.2. SEF AC2: Access control of extration

SEF AC2 prevents extraction – in the sense of inferring – of the cardholder's SigG private signature key.

Extraction in the sense of inferring concerns any kind of gathering information about object O2 by observing the TOE's external behaviour during the computation of a digital signature (electromagnetic emanation, power consumption, fault effects and timing). Prevention of inference during key generation relies on measures provided by the environment (see assumption AE1.3 in section 2.4.1).

AC2 is closely related to and partly dependent of functions and mechanisms provided by the ICC: assumption AE5.1 protects object O2 against direct physical attacks and assumption AE5.2 supports prevention of inference via normal ICC interface.

[10] Extract is prevented here only in the sense of refer, not infer.

3.5.3. SEF AC3: Secure blocking state

SEF AC3 prevents subject S7 from opening the SigG application.

Secure blocking state achieved by SEF AC3 is similar to the situation where a command TERMINATE CARD USAGE has been applied: no external requests are processed by the TOE except error signalling and functionality of security enforcing function SEF AU1. Secure blocking state is permanent.

SEF AC3 operates partially independently of the security mechanisms of the ICC hardware to detect potential security violations (see assumptions AE5.3 in section 2.4.5). ICC security mechanisms may, however, detect and independently react to potential security violations. Alternatively, the ICC hardware mechanisms may detect potential security violations and signal them to the TOE.

SEF AC3 is related to the tamper resistance of the ICC (assumptions AE5.1 in section 2.4.5), as it is able to detect modifications caused by tampering but is not sufficient without assumptions AE5.1 (section 2.4.5). In other words, SEF AC3 enhances security provided by AE5.1.

3.5.4. SEF AU1: Audit

SEF AU1 informs the human user about the secure blocking state of the TOE by means of a blocking information that the SigG application is disabled.

TOE only sends information about its (secure blocking) state during start-up. The state information is provided in the Answer-to-Reset (ATR) sequence. Additionally, the TOE will not process any further external requests, apart from signalling an error.

3.5.5. SEF OR1: Object Reuse

SEF OR1 clears from temporarily used storage areas (volatile memory in case of TOE) all data related to signature generation used by the SigG application before the action of closing the SigG application caused by security relevant event SRE4 is finished. SEF OR1 also concerns PIN and PUK codes: they shall be erased, too, before the SigG application will be closed.

3.6. Data Exchange functions

3.6.1. SEF DX1: Key Generation

SEF DX1 generates the cardholder's signature key pair on the ICC [11]. Cardholder's signature key pair consists of objects O2 and O12. SEF DX1 is used only in pre-personalisation or personalisation phase. SEF DX1 uses mechanism M10 defined in paragraph 4.1.

[11] In fact the DX1 could also be used for generation of other key pairs on the ICC.

3.6.2. SEF DX2: Digital signature generation

Cardholder generates signatures for data transmitted to the TOE using SigG private signature key by means of SEF DX2. Only the cardholder is allowed to execute SEF DX2 [12]. SEF DX2 uses mechanism M11 defined in section 4.2.

As a result of the generation of a digital signature, security relevant event SRE8 may occur.

4. Security mechanisms

Security functions specified in chapter 3 are partially implemented using security mechanisms summarized in Table 10.

Table 10 Security mechanisms[13]

ID	Mechanism
M10	Signature key pair generation
M11	Signature generation

4.1. M10: Signature key pair generation

TOE implements security mechanisms M10 as required for security enforcing function SEF DX1 in accordance with [1]. Mechanism M10 generates primes *p* and *q* for the formation of a key pair, and comprises of

(1) Random number generation: utilising the random number generator of ICC (see [19] and security enforcing function SEF SF7) and implementing verification of its correct operation.

(2) Post-processing of random numbers: performing post-processing for the generated random numbers.

(3) Prime number testing: implementing statistical tests (e.g. Miller-Rabin test) to diminish the probability of a generated random number to be a non-prime number.

(4) Computation of the key components from the generated prime numbers. The key components are used later by M11 in digital signature generation.

In general, it must hold that for the generated p and q, log2(p)+log2(q)>1023 and that approximately 0.5 < |log2(p)-log2(q)|. For the public exponent to be valid, it must be that GCD(e,(p-1)(q-1))=1 and for the secret exponent to be valid, it must hold that ed≡1 mod (p-1)(q-1).

[12] This is valid for the personalisation phase also when supported by the procedural security measures described in [17].

[13] The numbering is not sequential. The used numbering aims to provide consistency with [3].

4.2. M11: Signature generation

TOE implements security mechanisms M11 as required for security enforcing function SEF DX2. M11 comprises of RSA algorithm with 1024 bit key length (length of the basic module $n = pq$), according to [1]. M11 can generate the hash value of a message with SHA-1 algorithm, and it computes the DSI according to PKCS#1v1.5 standard.

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 mapping between threats, security objectives and security enforcing functions is given in Table 11.

Table 11 Mapping between threats, security objectives and security enforcing functions

	SO1	SO2	SO6	SO7	SO8
T1	SEF AC1, SEF AC2, SEF OR1			SEF DX1, SEF DX2	SEF AC3, SEF AU1
T2		SEF IA1, SEF IA2, SEF IA3, SEF IA4, SEF AC1			SEF AC3, SEF AU1
T3			SEF DX1	SEF DX2	SEF AC3, SEF AU1

5.1. Threat T1

Threats T1 are countered by security objectives SO1, SO7 and SO8, and by the assumed environmental measures AE1.1, AE1.3, AE5.1, AE5.2 and AE5.3.

TOE implements security enforcing functions SEF AC1 and SEF AC2, described in section 3.5 to prevent misuse of ICC commands implemented by the TOE and the extraction of the SigG private signature key. Security enforcing function SEF OR1, described in section 3.5.5, prevents illicit information flows between the SigG application, including the SigG private signature key, and other applications embedded on the ICC through the temporary used storage areas. Together they fulfil the security objectives SO1.

Security enforcing functions SEF DX1 and SEF DX2, described in section 3.6, prevent disclosure of the SigG private signature key of the cardholder by cryptanalytic attacks against digital signatures generated by the TOE to fulfil security objective SO7.

Secure blocking state of TOE ensures the security of cardholder's SigG private signature key if a potential attack is detected (see security enforcing functions SEF AC3 and SEF AU1 in sections 3.5 and 3.5.4) to fulfil security objectives SO8.

Assumption AE1.1 ensures secure manufacturing, initialisation, pre-personalisation and personalisation of the ICC. Assumption AE1.3 ensures protection against inference during key generation.

Assumption AE5.1 ensures protection against physical attacks by ICC. Assumption AE5.2 supports prevention of inference (together with AC2). Assumption AE5.3 supports detection of security violations.

5.2. Threat T2

Threats T2 are countered by security objectives SO2 and SO8, and by the assumed environmental measure AE4.2(3).

TOE implements security enforcing functions SEF IA1, SEF IA2, SEF IA3, and SEF IA4 (described in section 3.4) for cardholder authentication, and SEF AC1 (described in section 3.5) for access control over the usage of the cardholder's SigG signature key to fulfil security objectives SO2.

Secure blocking state of TOE ensures the security of the SigG signature function if a potential attack is detected (see security enforcing functions SEF AC3 and SEF AU1 in sections 3.5 and 3.5.4) to fulfil security objectives SO8.

Assumption AE4.2(3) ensure that the environment preserves confidentiality and integrity of the data translated between the office IFD and the ICC.

5.3. Threat T3

Threats T3 are countered by security objectives SO6, SO7 and SO8, and by the assumed environmental measure AE4.2(3).

TOE implements security enforcing function SEF DX1 described in section 3.6 to fulfil security objectives SO6 by the means of generation of secure SigG signature key pairs.

TOE implements security enforcing function SEF DX2 described in section 3.6 to fulfil security objectives SO7 by the means of usage of secure algorithms for generating SigG signatures.

Secure blocking state of TOE prevents misuse of this SEF if a potential attack is detected (see security enforcing functions SEF AC3 and SEF AU1 in sections 3.5 and 3.5.4) to fulfil security objectives SO8.

Assumption AE4.2(3) ensures that the environment preserves confidentiality and particularly integrity of the data translated between the office IFD and the ICC.

6. List of abbreviations

AC	Access Control
AE1	Assumption about environment: Life cycle security
AE2	Assumption about environment: Integrity and quality of key material
AE3	Assumption about environment: SigG compliant use of the TOE
AE4	Assumption about environment: Use with SigG accredited IFD
AE5	Assumption about environment: Assumptions about the ICC hardware
AEn.m	Assumption about the Environment (No. n)
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	Security mechanism: Human user authentication
M10	Security mechanism: Signature key pair generation
M11	Security mechanism: Signature generation
M2	Security mechanism: Change the unblocked reference data
M3	Security mechanism: Locking of the reference data
M4	Security mechanism: Unblock and change of the reference data
M5	Security mechanism: Extraction resistance
M6	Security mechanism: Access control for command execution
M7	Security mechanism: Secure blocking state
M9	Security mechanism: Clearing of memory
Mn	Security mechanism Nr. n
O1	Object: SigG application
O2	Object: SigG private signature key of the cardholder
O3	Object: SigG cardholder reference data
O4	Object: SigG cardholder reference reset code
O5	Object: SigG signature key certificate of the cardholder
O6	Object: SigG public key of the root certification authority
O7	Object: Other credentials for signature verification
O12	Object: SigG public key of the cardholder
On	Object (No. n)
OR	Object Reuse

PIN	Personal identification number
PUK	Personal unblocking key, PIN unblocking key
S1	Subject: Cardholder
S2	Subject: Somebody
S3	Subject: IFD
S7	Subject: Potential attacker
SigG	Signaturgesetz
SigV	Signaturverordnung
SO1	Security objective: Prevent extraction and modification of cardholder's SigG private signature key
SO2	Security objective: Prevent unauthorised use of the SigG digital signature function
SO6	Security objective: Quality of key generation
SO7	Security objective: Provide secure digital signature
SO8	Security objective: React to potential security violations
SOn.m	Security Objective (No. n)
SRE1	Security relevant event:: Resetting of the ICC
SRE10	Security relevant event:: Potential security violation occurred
SRE11	Security relevant event: Cardholder authenticated by reset code
SRE12	Security relevant event: Cardholder authentication by reset code failed
SRE2	Security relevant event: Deactivation of the ICC
SRE3	Security relevant event: Opening of the SigG application
SRE4	Security relevant event: Closing of the SigG application
SRE5	Security relevant event: Successful cardholder authentication
SRE6	Security relevant event: Cardholder authentication failure
SRE7	Security relevant event: Repeated authentication failure
SRE8	Security relevant event: Authentication expiration
SREn	Security Relevant Event (No. n)
T1	Assumed threat: Extraction of the cardholder’s secret key
T2	Assumed threat: Misuse of the signature function
T3	Assumed threat: Forged data ascribed to the cardholder
Tn.m	Threat (No. n)
TOE	Target of Evaluation

7. Glossary

Anybody: The set of subjects S1:Cardholder and S2:Somebody.

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

Authentication information: Information used to prove or to verify the identity of a subject by means of authentication. The user authentication information are the verification data provided by the cardholder to prove her or his identity and the reference data used by the TOE to verify this identity.

Blocking state of the TOE: Secure State of the ICC disabling all applications of the ICC. This state shall be apparent to the cardholder.

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.

Certificate: A digital certificate bearing a digital signature and pertaining to the assignment of a public signature key to a natural person (signature key certificate) or a separate digital certificate containing further information and clearly referring to a specific signature key certificate (attribute certificate) (see §2 SigG [4]).

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 § 4 of the SigG [4].

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.

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.

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

Infer: Any form of determination of 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: An 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 is personalised for the cardholder and (ii) the SigG private signature key of the cardholder is stored in the TOE). It will be transferred to the cardholder typically involving some „smart card issuer“.

Personalisation phase: The life cycle phase, when the SigG application equipped ICC is equipped with 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 (PIN and PUK) given to the cardholder as the legitimate person in the operational phase). The TOE may be used to generate the cardholder's signature key pair on the ICC or the already generated key pair is dedicated to the cardholder.

Potential security violation flag: A flag set by the TOE indicating that a potential security violation is detected. This flag is persistently set and cannot be reset.

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

Pre-personalisation phase: The life cycle phase, when the ICC is equipped with SigG application related data, but no data related to a specific cardholder. The TOE may be used to generate the signature key pair on the ICC which is then later dedicated to a specific cardholder (in personalisation phase).

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 to 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 usual in form of a certificate to keep its authenticity and integrity.

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 for the authentication of the cardholder.

Reset retry counter: The retry counter of the reset code (i) stores the number of 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 of allowed number of 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.

Retry counter for the reference data: The retry counter for the reference data (i) stores the number of 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 of allowed number of failed authentication attempts with the verification data.

SigG accredited IFD: Public IFD (i) being a SigG accredited technical component and (ii) acting as customer IFD according to [2], section 18, and (iii) supporting the mutual device authentication and secure messaging according to [2], annex D).

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

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

SigG cardholder reference data: Data permanently stored in the TOE to verify the cardholder authentication.

SigG cardholder verification data: Data provided by the user to authenticate himself as cardholder by knowledge.

SigG compliance of technical component: A property of technical components to adhere the given SigG legislative with respect to its implementation and configuration. The SigG compliance of a technical component shall be evaluated and conformed according to [4] §17 (1). The SigG compliance of a technical component is usually not directly apparent to the user or to an other technical component. Note that a SigG compliant technical component is not necessary a SigG accredited technical component.

SigG compliant digital signature: A digital signature compliant with the German digital signature legislative [1], [4] and [19]. It shall be generated by SigG compliant technical components.

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 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.

Verification data: Data presented by a human user for authentication as cardholder and corresponding to the reference data stored in the TOE

8. References

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

[2] DIN: Spezifikation der Schnittstelle zu Chipkarten mit Digitaler Signatur-Anwendung / Funktion nach SigG und SigV. V 1.0 (Draft), 17.11.98, 1998 (DIN NI-17.4) – Entwurf (use the current version “Vornorm DIN 66391-1”)

[3] Generic Security Target for ICC Embedded Software Compliant with SigG, SigV and DIN V 66391-1, version 1.0.

[4] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) (in Kraft getr. am 22.05.2001)

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

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

[7] 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)

[8] 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)

[9] 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)

[10] 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 (1999)

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

[12] Operational document SLE66CX320P, v1.0. Infineon Technologies AG, July 10,2000.

[13] SetCOS 4.4.0, Initialisation, Version 1.1, Setec Oy (TBD).

[14] SetCOS User's Guide Part 1, Overview, Version 1.2, Setec Oy (15.10.1999)

[15] SetCOS User's Guide Part 2, SetCOS 4.x series, Version 1.4, Setec Oy.

[16] SetCOS User's Guide Part 3, SetCOS 4.4.0, Version 1.4, Setec Oy .

[17] Setec Signature Card SetEID v1.0, Personalisation, Setec Oy

[18] Setec Signature Card SetEID v1.0, SigG application, Setec Oy

[19] Sicherheitsuntersuchung des Chipkartenprozessors SLE66CX320P mit der STS-Version 41.06.06 für die Chipkarte des deutschen Kreditgewerbes, v1.0. Infineon Technologies AG, April 19, 2000.

[20] Smart Card IC SLE 66CX320P, version m1421b14, Certification report. Aug 04, 2000.

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

[22] Resource Management System, RMS+ v0.6. Confidential Data Sheet 04.00. Infineon Technologies AG 04/2000.

End of the Security Target for
„Setec Signature Card SetEID v1.0“.

Certification Report T-Systems-DSZ-ITSEC-04016-2003

Editor:	T-Systems GEI GmbH, BU ITC Security
Address:	Rabinstr.8, D-53111 Bonn, Germany
Phone:	+49-228-9841-0
Fax:	+49-228-9841-60
Web:	www.t-systems-itc-security.com www.t-systems-zert.com