Certification Report

T-Systems-DSZ-CC-04205-2007

CardOS DI V4.2B with Application for Digital Signature

Deutsches IT-Sicherheitszertifikat

anerkannt vom
Bundesamt für Sicherheit in der Informationstechnik

Deutscher
Akkreditierungs
Rat

DAT-ZE-015/98-01

CardOS DI V4.2B with Application for Digital Signature

Siemens AG

The product has been evaluated by an accredited and licensed evaluation facility against the Common Criteria for Information Technology Security Evaluation (version 2.3) and the Common Methodology for Information Technology Security Evaluation (version 2.3). The result is:

▶ Functionality	**product specific security target**	
	Common Criteria Part 2 extended	
▶ PP Conformance	**SSCD-PP Type 3 Conformant** (Version 1.05, EAL 4+, 25.07.2001, registered as BSI-PP-0006-2002)	
▶ Assurance Package	**Common Criteria Part 3 conformant**	
	EAL4 augmented by:	
	AVA_MSU.3	Vulnerability Assessment: Analysis and testing for insecure states
	AVA_VLA.4	Vulnerability Assessment: Highly resistant

This certificate is valid only for the evaluated version of the product in connection with the complete certification report and the evaluated configurations described there. Evaluation and certification have been performed in accordance with the rules of the certification scheme of T-Systems and the stipulations from BSI for the "Deutsches IT-Sicherheitszertifikat [German IT Security Certificate]". The rating of the strength of cryptographic algorithms suitable for encryption as well as decryption is excluded from the recognition by BSI.

Registration: Bonn: Nov 20, 2007

T-Systems-
DSZ-CC-04205-2007

Dr. Heinrich Kersten
Head of the Certification Body

Accredited against EN 45011 by
DATech in TGA GmbH

Preliminary Remarks

This certification report for the TOE (target of evaluation) CardOS DI V4.2B with Application for Digital Signature is intended as a formal confirmation for the sponsor concerning the performed evaluation and as a basis for the user to operate the TOE in a secure way.

Copies of this certification report may be obtained from sponsor or – if the sponsor agrees – from the certification body.

The following parts of the certification report contain important information:

- Section 1, para 3: The precise name of the TOE including its version reference: The certificate and the certification report apply only to this TOE and this specific version.
- Section 6, para 29: Specification of the delivery procedure for the TOE. Other delivery procedures may not offer the degree of security required for the assurance level EAL4.
- Section 6, para 30: Specification of the evaluated configuration(s) of the TOE. The certification of the TOE is valid only for the configuration(s) described.
- Section 6, para 31: Specification of the evaluated functionality: Only the security functions described here have been certified.
- Section 6, para 33: Information on the assurance package applied by the evaluation depending on the criteria used.
- Section 6, para 34: Stipulations for the user of the TOE. A secure usage of the TOE may not be possible if these stipulations are not met.

The security target for the TOE provides information on the intended usage of the TOE, the list of TOE components, its security objectives resp. the considered threats and the operational environment. This information should be read carefully. The security target is available as a separate document.

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. As a prerequisite for this, any requirement and stipulation described in this report, must be met. Otherwise, the evaluation results may not be fully applicable. In such a case, there is a need for 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.

When the TOE including its documentation, its delivery procedure or its operational environment is modified, the certification is no longer valid. In this case, a re-certification can be performed which will be documented in technical anneces to this certification report.

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.

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-CC-04205-2007/1, .../2,...),
- new TOE versions under evaluation or already certified.

Any warranty for the TOE by T-Systems is excluded.

The certification of the TOE is not meant to be an endorsement by T-Systems for an arbitrary usage of the TOE.

For further information, please contact the certification body:

✉ Certification Body of T-Systems
c/o T-Systems GEI GmbH, Rabinstr.8, D-53111 Bonn, Germany
☎ +49-(0)228-9841-0, FAX +49-(0)228-9841-60
💻 www.t-systems-zert.com

Contents

Abbreviations

AIS	Anwendungshinweise und Interpretationen zum Schema [Guidance and Interpretations of Scheme Issues] (BSI procedure)
BGBI	Bundesgesetzblatt [German Federal Gazette]
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen [(German:) Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway]
BSI	Bundesamt für Sicherheit in der Informationstechnik [(German) Federal Office for Information Security]
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CSP	Certification Service Provider
DAR	Deutscher Akkreditierungsrat [German Accreditation Council]
DATech	DATech Deutsche Akkreditierungsstelle Technik in TGA GmbH [DATech German Accreditation Body Technology in TGA GmbH]
DIN	Deutsches Institut für Normung e.V. [German Standards Institution]
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ETSI	European Telecommunications Standards Institute
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
PP	Protection Profile
SF	Security Function
SigG	German Electronic Signature Act
SigV	German Electronic Signature Ordinance

SOF	Strength of (Security) Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

References

/AISx/ Anwendungshinweise und Interpretationen zum Schema [Guidance and Interpretations of Scheme Issues], BSI, endorsed versions

/ALG/ Geeignete Kryptoalgorithmen [Approved Crypto-Algorithms], published in the Bundesanzeiger [German Federal Gazette] by the (German) Federal Network Agency, endorsed version

/CC/ Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005,
Part 1: Introduction and general model, CCMB-2005-08-001
Part 2: Security functional requirements, CCMB-2005-08-002
Part 3: Security assurance requirements, CCMB-2005-08-003

/CEM/ Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 2.3, August 2005, CCMB-2005-08-004

/ETSI/ ETSI TS 101 456: Electronic Signatures and Infrastructures (ESI): Policy requirements for certification authorities issuing qualified certificates, Version 1.3.1, 2005-05

/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

/EU-REF/ Commission Decision of 14/7/2003 on the publication of reference numbers of generally recognised standards for electronic signature products

/ISO27001/ ISO/IEC 27001:2005 Information technology. Security techniques. Information security management systems. Requirements

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

/SiGAK/ Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten: Arbeitsgrundlage für Entwickler / Hersteller und Prüf- / Bestätigungsstellen [Specification of the Operational Environment for Signature Application

Components: Basics for Developers / Manufacturers and Assessment / Certification Bodies], Federal Network Agency, version 1.4, July 19, 2005

/SigG/ Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876) [Signature Act as of May 16, 2001 (BGBl. I p. 876)], recently revised by Article 4 of the act as of February 26, 2007 (BGBl. Year 2007, Part I p. 179)

/SigV/ Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) [Ordinance on Electronic Signatures (Signature Ordinance– SigV)], recently revised by Article 2 of the first act to adapt the Signature Act (1. SigGÄndG) as of January 04, 2005 (BGBl. Year 2005, Part I, No. 1)

/SigG-A/ Austria: 190. Bundesgesetz über elektronische Signaturen [190. Federal Act on Electronic Signatures], www.a-sit.at/informationen

/SigV-A/ Austria: 30. Verordnung des Bundeskanzlers über elektronische Signaturen, [30. Ordinance of the Chancellor on Electronic Signatures], www.a-sit.at/informationen

/SigG-CH/ Switzerland: Bundesgesetz über die elektronische Signatur [Federal Act on the Electronic Signature], www.sas.ch/de/pki_isms

/SigV-CH/ Switzerland: Verordnung über die elektronische Signatur [Ordinance on the Electronic Signature], www.sas.ch/de/pki_isms

/SigR-CH/ Switzerland: Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur [Technical and Administrative Regulation on Certification Services in the Area of of Electronic Signature], www.sas.ch/de/pki_isms

/Sig-NL1/ The Netherlands: Programma van Eisen (PvE), www.pki-overheid.nl

/Sig-NL2/ The Netherlands: TTP-NL Guidance on ETSI TS 101.456, ECP.NL, CCvD-TTP.NL, May 30, 2002

Glossary

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

For criteria specific terms cf. the glossary in the relevant security criteria.

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.

Common Criteria
Security Criteria based on the former US Orange Book / Federal Criteria, the European ITSEC and the Canadian CTCPEC; a world-wide accepted security standard (ISO/IEC 15408).

Confidentiality
Classical security objective: Data should only be accessible to authorised persons.

"Confirmation Body"
A body, recognised by the BNetzA, assessing the security of technical components and of certification service providers, issuing security confirmations according to the (German) SigG and SigV.

"Confirmation Procedure"
Procedure with the objective to issue a security confirmation.

Evaluation
Assessment of an (IT) product, system or service against published IT security criteria.

Evaluation (Assurance) Level
Level of assurance gained by evaluation; level of trust that a TOE meets its security target (according to ITSEC / CC).

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.
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 assessment / 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 the conformity of technical components or trust centers 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.

Sicherheit für den Mittelstand

Program of T-Systems offering service modules for enterprise IT security. The modules contain consulting, awareness, analyses, penetration tests, audits as well as procedures of registration, awarding seals and certification.

Security Function

Technical function or measure to counteract certain threats.

Security Measure

Any organisational, personal, infrastructural or technical measure contributing to achieve security objectices.

Security Objective

For the context of information security typical objectives like confidentiality, integrity, availability, authenticity as well as derived objectives like compliance (e.g. in legal context).

Security Target

Document specifying a TOE and describing its configuration and environment, security objectives and threats, met security requirements and corresponding rationale; used as a basis for the evaluation of the 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 applied criteria and ratings.

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

The defined security objectives are exposed to threats leading to attacks if unauthorised subjects try to read, modify data objects or prevent other authorised subjects to access such objects. (TOE) security functions provided by the considered TOE are intended to counter these threats.

In CC part 2, requirements to security functions are described by "functional components". The reference "CC part 2 conformant" in certification reports indicates that only functional components from CC part 2 have been selected to describe the requirements. The reference "CC part 2 extended" indicates that the requirements include functional components not in CC part 2.

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

The strength of function (SOF) expresses the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms. Three levels of SOF have been defined in the CC:

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

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

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

In the view of CC, trustworthiness of a TOE is given when there is sufficient assurance that the TOE meets its security objectives. The CC philosophy asserts that greater assurance results from the application of greater evaluation effort, and that the goal is to apply the minimum effort required to provide the necessary level of assurance. The increasing level of effort is based upon

- scope - that is, the effort is greater because a larger portion of the IT product or system is included;
- depth - that is, the effort is greater because it is deployed to a finer level of design and implementation detail;

- rigour - that is, the effort is greater because it is applied in a more structured, formal manner.

The following table gives a survey on the *assurance classes* and *assurance families* defined in CC part 3 including their abbreviated name as used in certification reports and certificates.

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

Assurance families are compiled from assurance components. From the numerous assurance components in CC part 3, seven evaluation assurance levels (EAL) have been developed defining requirements to the developer of the TOE and the evaluator. EAL1 denotes the lowest, EAL7 the highest level. Thus, trustworthiness of a product or system can be measured by an assurance level. Not all assurance components from CC part 3 have been used to define the EALs.

The following statements characterise the evaluation assurance levels.

EAL1 functionally tested

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

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

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

EAL2 structurally tested

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

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

EAL3 methodically tested and checked

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

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

EAL4 methodically designed, tested, and reviewed

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

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

EAL5 semiformally designed and tested

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

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

EAL6 semiformally verified design and tested

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

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

EAL7 formally verified design and tested

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

The following table from CC part 3 displays for each EAL its component structure. The precise definition of each component is given in CC part 3. The figures denote the component number within a family.

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

A higher level of assurance than that provided by a given EAL can be achieved by

- including additional assurance components (e.g. from other assurance families); or

- replacing an assurance component with a higher level assurance component from the same assurance family.

For a specific TOE, such extensions or replacements are reflected by the corresponding certification report: The reference "CC part 3 conformant" indicates that only assurance components from CC part 3 have been used. The reference "CC part 3 extended" indicates that the assurance requirements include assurance components not in CC part 3.

1 Sponsor and Target of Evaluation

1 Sponsor of the certification is Siemens AG, Charles-de-Gaulle-Str. 2-3, D-81737 Munich, Germany.

2 The sponsor applied for a certificate compliant with the service type 04: „Deutsches IT-Sicherheitszertifikat [German IT Security Certificate]“ by the certification body of T-Systems.

3 Target of Evaluation (TOE) is the product „CardOS DI V4.2B with Application for Digital Signature” .

4 The TOE is a SSCD (Secure Signature Creation Device).

5 The sponsor provided the security target for the TOE in English language. The security target, final version 1.0 as of November 14, 2007, is available as a separate document.

6 The security target references the Common Criteria as criteria and EAL4 as assurance level. The (minimum) strength of TOE security functions (SOF) is claimed as “high“.

2 Relevant Normative Documents for the Evaluation[1]

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

- Common Criteria for Information Technology Security Evaluation /CC/.

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

- Common Methodology for Information Technology Security Evaluation /CEM/,
- Anwendungshinweise und Interpretationen zum Schema [Guidance and Interpretations of Scheme Issues], BSI /AIS/,
- Internal Work instruction „Verfahrenstyp 04: Deutsches IT-Sicherheitszertifikat [German IT Security Certificate]“ by T-Systems (endorsed version).

[1] The precise bibliographical data for these documents can be found in the section "References" in this certification report.

3 Evaluation

9 The evaluation of the TOE by the Prüfstelle für IT-Sicherheit of T-Systems GEI GmbH was sponsored by Siemens AG.

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

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

12 The Evaluation Technical Report (ETR), version 1.10 and dated November 14, 2007, provided by the evaluation facility, contains the outcome of the evaluation.

13 The evaluation was completed on November 16, 2007.

4 Certification

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

15 The certification body of T-Systems operates in compliance with EN 45011 and has a corresponding accreditation by DATech in TGA GmbH for certifications against IT-SEC and Common Criteria (DAR registration code DAT-ZE-015/98-01).

16 The certification of the TOE was carried out under registration code T-Systems-DSZ-CC-04205-2007.

17 In compliance with the criteria, the evaluation performed by the Prüfstelle für IT-Sicherheit of T-Systems GEI GmbH was monitored by the certification body.

18 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.

19 The certification of the TOE may be subject to stipulations and further guidelines, cf. section 6 for details.

20 A summary of the results is given by the security certificate T-Systems-DSZ-CC-04205-2007 as of Nov 20, 2007 reproduced on page 2 in this report.

21 The status of the TOE being certified is published on the web pages of the certification body (www.t-systems-zert.com).

22 The certification report is available for download under www.t-systems-zert.com.

5 National and international acceptance

23 The certificate T-Systems-DSZ-CC-04205-2007 as a "Deutsches IT-Sicherheitszertifikat [German IT Security Certificate]" carries the logo officially approved by the (German) Federal Office for Information Security (BSI).

24 The status of the TOE being certified will be published in the broschures BSI 7148 / 7149 of the BSI.

25 The certificate is recognised by the BSI as equal to their own certificates.

26 As contractually agreed, the BSI explicitly confirms this equivalence in the international context.

27 A further international acceptance of the certification results is achieved through the multi-lateral mutual recognition agreement of EA, ILAC and IAF signed by the accreditor DATech in TGA GmbH (cf. www.datech.de for details).

6 Summary of Results

28 Remark: In the sense of /SigG/ the certification authority (CA) mentioned in several documents of the sponsor, is part of the certification service provider (CSP) under which all roles acting under an appropriate security policy of the CSP are subsumed, e. g. the card manufacturer (CM). The notation CSP is used in the sequel in this sense.

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

The different steps and ways of delivering the TOE as well as the procedures for initialization and personalisation have been described in detail in “Delivery and Operation, CardOS DI V4.2B, Edition 10/2007”, version 1.20 as of October 08, 2007 by Siemens AG. This document describes the delivery to the chip manufacturer, the certification authority, the card holder and to terminal developers as well as the procedures of initialization, key generation, personalization and installation of certificates.

The delivery procedure described meets the requirements of the national certification body for the assurance level EAL4 of the CC.

30 The following configurations of the TOE were evaluated:

The TOE may be configured and operated with different values of the ARA-Counter of the PIN_DS object, i. e. the number of signatures that can be created after one successful PIN authentication depends on the configured value for the ARA-Counter: 1-254 (ARA-Counter 01h-FEh) or infinite (ARA-Counter 00h or FFh)[2].

Cf. para [34], no. 7, for further information on the use of the ARA counter.
The evaluation result is only valid for the configurations of the TOE described above.

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

- SF1 User Identification and Authentication
- SF2 Access Control
- SF3 SCD/SVD Pair Generation
- SF4 Signature Creation
- SF5 Protection
- SF6 Secure Messaging
- SF7 SVD Transfer

32 As to the strength of the TOE security functions, the evaluation provided the following result (cf. the Security Target for details):

The TOE security functions SF1, SF3, SF4, SF6, SF7 have a minimum strength of SOF-high.

33 The evaluation provided the following results:

The security target meets the requirements of the corresponding class ASE (Security Target Evaluation) of the Common Criteria.

The functional requirements are CC Part 2 extended.

The assurance package is CC Part 3 conformant.

The TOE meets the requirements of the evaluation assurance level EAL4 of the Common Criteria. The assurance components for this level are given in the section Security Criteria Background starting at page 11 in this report.

Augmentation is described as follows:

[2] There may national restrictions governing the use of this feature.

AVA_MSU.3	Vulnerability Assessment: Analysis and testing for insecure states
AVA_VLA.4	Vulnerability Assessment: Highly resistant

The TOE is SSCD-PP Type 3[3] conformant.

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

1. If a CSP decides to employ a personalisation procedure in which correspondence verification is performed during the personalisation without the Signatory being present, then this certification service provider will have to use either the organizational SSCR package or the technical SSCR package. In this case it is recommended that the organisational SSCR package should not be used, if the SSCR technical package can be used instead. For details see the Administrator Guidance.

2. It is recommended to the CSP to choose the ICCSN (16 byte unique Integrated Circuit Card Serial Number) in such a way that both 8 Byte Strings will differ for different cards. At best, the ICCSNs of each arbitrary couple of cards have different first and different last 8 bytes.

3. The TOE uses RSA key pairs with a modulus length of 1024 bits. It has to be observed whether the key length of only 1024 bits will become a vulnerability some day. Depending on the national framework on electronic signatures there may be restrictions on the use of this modulus length. (For Germany: The modulus length of 1024 Bit must not be used beyond end of 2007 if signatures created should comply to /SigG/.)

4. The number of TOE devices (i.e. smart cards) in operational use must not exceed 83 million examples.

5. The CSP issuing the TOE smart cards has to ensure that except for the well-defined software defined in the Security Target (Table 1) no other executable code is loaded onto the smart card. It is especially not allowed to load any other packages than those listed in the Security Target (Table 1), i.e. the Command Set Extension Package, the CNS Package, the SISS Package and the MOC Package. Temporarily during personalisation, also the SSCR Technical Package and the SSCR Organizational Package can be loaded as well. The CSP has to ensure that misuse of the functionality to load packages is effectively prevented.

6. The TOE may be configured such that the ARA counter of the PIN is set to a value greater than 1, i.e. it is possible to generate more than one signature after the PIN has been entered once. If such configurations are distributed to end

[3] Version 1.05, EAL 4+, 25.07.2001, registered as BSI-PP-0006-2002

users, special warnings on that functionality must be given to those end users. Depending on national legislation additional requirements or further restrictions may apply.

7. The CM/CA should be aware of the problem that a signatory having received his smartcard might already create signatures, although his certificate has not been published yet in the CA's Directory Service. This situation may arise especially when a written receipt is required to be sent by the Signatory confirming the reception of the smartcard. It depends on the legal framework if signatures created before the certificate was published are legally binding or not.
   A solution could be to store a certificate for the signature public key on the smartcard which is distinguishable from the relevant certificate published by the CA's Directory Service. It depends on the national legislation if such a solution is acceptable.

8. The CSP shall use cryptographically strong random number generators for key generation and other aspects (including the challenge-response-authentication).

9. For the DS application the mandatory extensive AIS31 RNG test of the chip's Random Number Generator must definitely not be suppressed by an FRN (Fast Random Numbers, ID = 0xC7) object. Therefore the administrator has to take special care that an FRN object is not installed in the MF, the DF_DS and all DF_DS child DFs. Any administrator has to ensure that no FRN object is introduced that allows a faster generation of random numbers for the digital signature application. The CSP has to use the appropriate scripts and has to deliver the respective scripts and guidance to the according facilities.

35 For the validity of the certification, the following stipulations have to be met by the sponsor:

1. The developer shall inform the administrative user of the TOE (CM / CA) about the need of a cryptographically strong random number generator for the generation of keys used e.g. for secure messaging and authentication.

2. The software developer (Siemens AG) and the chip manufacturer (Infineon Technologies AG) are responsible to prevent misuse of the PackageLoadKey; especially they have to ensure the confidentiality of this key.

End of Certification Report T-Systems-DSZ-CC-04205-2007.

Certification Report:
T-Systems-DSZ-CC-04205-2007

Editor:	T-Systems GEI GmbH
Address:	Rabinstr.8, D-53111 Bonn, Germany
Phone:	+49-(0)228-9841-0
Fax:	+49-(0)228-9841-60
Web:	www.t-systems.com/ict-security www.t-systems-zert.com