debis

Services by DaimlerChrysler

Certification Report

Siemens Sign@tor Version 1.0

Siemens AG Austria

debisZERT-DSZ-ITSEC-04064-2001

debis IT Security Services

The Modern Service Provider

Preface

The product Siemens Sign@tor Version 1.0 of Siemens AG Austria has been evaluated against the *Information Technology Security Evaluation Criteria* and the *Information Technology Security Evaluation Manual*. The evaluation has been performed under the terms of the certification scheme debisZERT of debis IT Security Services. The certification procedure applied conforms to the rules of service type 4: *Certificates recognised by the BSI*.

The result is:

Security Functionality:	Product specific: secure PIN entry, preparation and final processing of digital signature, secure channel between TOE parts “Sign@tor PC” and “Sign@tor Terminal”, (secure) software update
Assurance Level:	E2
Strength of Mechanisms:	high

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

Bonn, 16.03.2001

Certifier: Head of the Certification Body:

signed by:

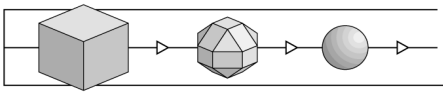
Dr. Hans-Reinhard Baader Dr. Heinrich Kersten

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

✉ debis IT Security Services, - Zertifizierungsstelle -, Rabinstr. 8, D-53111 Bonn, Germany

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

💻 Email: debiszert@itsec-debis.de, Internet: www.debiszert.de



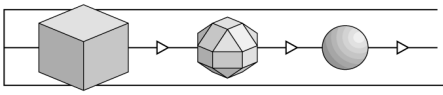
Revision List

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

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

Revision	Date	Activity
0.9	09.03.01	Preversion (based on template report 1.5) (German language)
1.0	13.03.01	Initial release (based on template report 1.5) (German language)
1.1	16.03.01	Update: Evaluation finished (German language) This version was translated into English language.

Contents



(This page is intentionally left blank.)

1 Introduction

1.1 Evaluation

1 The evaluation was sponsored by Siemens AG Austria, Siemensstr. 82, A-1210 Vienna.

2 The evaluation was carried out by the evaluation facility Prüfstelle für IT-Sicherheit der debis IT Security Services and completed on 12.03.2001

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

1.2 Certification

4 The certification was performed under the terms of the certification scheme debisZERT of debis IT Security Services. The Certification Body of debis IT Security Services complies to EN 45011 and was accredited with respect to this standard by DATech (Deutsche Akkreditierungsstelle Technik e.V.) under DAR Registration Number DIT-ZE-005/98-00.

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

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

1.3 Certification Report

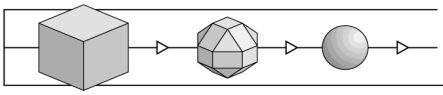
6 The certification report states the outcome of the evaluation of Siemens Sign@tor Version 1.0 - referenced as TOE = Target of Evaluation in this report.

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

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

9 The certification report is intended

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



- to assist the user of Siemens Sign@tor Version 1.0 when establishing an adequate security level.

10 The certification report contains pages 1 to 40. Copies of the certification report can be obtained from the sponsor or the Certification Body.

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

- www.debiszert.de .

1.4 Certificate

12 A survey on the outcome of the evaluation is given by the security certificate debisZERT- DSZ-ITSEC-04064-2001.

13 The contents of the certificate are published under

- www.debiszert.de .

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

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

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

1.5 Application of Results

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

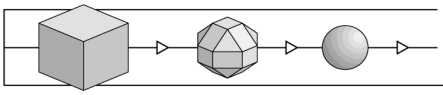
18 It is highly recommended to read the certification report carefully to benefit from the evaluation. In particular, the information provided on the intended method of use, the assumed threats, the operational environment and the evaluated configurations are essential for the user.

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

---

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

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



(This page is intentionally left blank.)

2 Evaluation Findings

2.1 Introduction

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

2.2 Evaluation Results

21 The evaluation facility came to the following conclusion:

- The TOE meets the requirements of the assurance level E2 according to ITSEC, i.e. all requirements at this assurance level as to correctness and effectiveness are met:

  ITSEC E2.1 to E2.37 for the correctness phases

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

  Construction - The Development Environment (Configuration Control, Developers Security),

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

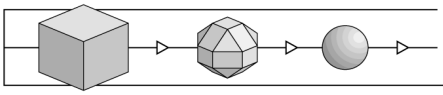
  Operation - The Operational Environment (Delivery and Configuration, Start-up and Operation).

  ITSEC 3.12 to 3.37 for the effectiveness with the aspects

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

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

- The mechanisms M1, M2, M3 and M5 for the generic headings SF1.1, SF1.2, SF2, SF3, SF4.1 and SF4.2 of the TOE are critical mechanisms; except for M1 and M2 (cryptographic mechanisms) they are of type B.



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

2.3 Further Remarks

22 The evaluation facility has formulated no further requirements to the sponsor.

23 The evaluation facility has formulated the following instructions to the user:

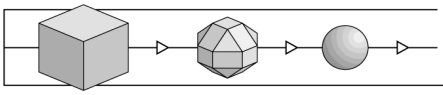
Instructions for secure use of the "signature file" functionality:

- The TOE has two operating modes. The evaluated functionality is present only in the TOE mode. This mode is indicated on the Sign@tor terminal display with "ready".
- Macros should be removed before signing.
- Documents referred to by hyperlinks are not signed.
- The indicated hash values should be compared by the user and the signature procedure should be started only when they coincide.
- The file name, file size and creation date indicated on the terminal are additional information only (and not reliable).
- The description for the procedure to be taken if the hash values are not identical (see user documentation – Sign@tor Online help) are to be followed.
- It is necessary to scroll through all four lines of the hash value on the terminal before starting the signing operation with OK.
- The card PIN has to be kept confidential.
- The signature card is disabled when the PIN is entered incorrectly three times.
- The PIN has to entered at the Sign@tor terminal only.
- The signing operation can be cancelled at the terminal with the C key.
- For security reasons, the signed file should be checked with "Check signature offline".

Instructions for secure use of the "software update Sign@tor PC and terminal":

- The original CD has to be securely stored.

- The software update should only be performed with the aid of the original CD.
- The information on possible consequences of updating with uncertified software are to be observed.



3 Security Target

24 The Security Target, version 1.7 dated 26.01.01, which was the basis for the evaluation was supplied by the sponsor in German language. It is reproduced here in English translation. In cases of doubt, the German version shall prevail.

3.1 Description of the Target of Evaluation (TOE)

3.1.1 Definition of the TOE and intended method of use

The target of evaluation (TOE) is the product Sign@tor, version 1.0. It is designated briefly as Sign@tor below.

Sign@tor serves for the creation of user signatures as well as for verification of other signatures.

It consists of the following 2 components:

1. the Sign@tor PC and

2. the Sign@tor terminal.

This results in the following compressed information on the product:

Type	Name	Version number	Delivery form
SW	SIGN@TOR PC (including installation and update program)[2]	1.0	CD
HW and SW	SIGN@TOR terminal	1.0	Hardware Device

Sign@tor provides a user interface to the signature card inserted in the terminal, belonging to the operational environment of the TOE, but not to the TOE itself (see Chapter 2). The interface is used particularly for selecting files to be used for signing or verifying signatures. Sign@tor supports selection and display of files to be signed as well as calculation of the HASH value which it then sends to the signature card.

The signature card then returns the signature generated to Sign@tor (more precisely the terminal). Sign@tor creates a signed file in the format PKCS#7, after it has taken over the file signature (created in the signature card) and the certificate of the signature card.

Within the scope of this operational use, the terminal serves as a card reader for the user signature card and as input device for the PIN. It ensures the confidentiality of the

---

2 The CD also contains the online user documentation; note of debisZERT.

PIN in relation to the (Sign@tor and remaining) PC. Moreover, the terminal also calculates the HASH value and displays it. It is responsible for transferring it to the card for generation of the signature.

The TOE guarantees secure software updates for the PC by checking the integrity of the downloaded software for an update on the Sign@tor PC using the signature supplied.

The TOE guarantees secure software updates for the terminal by checking the integrity of the downloaded software for an update on the Sign@tor terminal using the signature.

The Sign@tor supports selection and display of files whose signature is to be checked with a viewer.

The signature check is accomplished by checking whether the signature was created with a signature key corresponding to the public key. This public key is contained in the certificate for the signed file.

The signature check is not a security function and is not an objective of evaluation.

3.1.2 Tasks of the TOE

The security relevant parts of the TOE functionality are described briefly below.

Signing file:

The Sign@tor terminal creates the HASH value for the file to be signed simultaneously with the Sign@tor PC.

The Sign@tor PC program indicates the HASH value (calculated by it) for the file to be signed. Then the HASH value (created independently) is indicated on the Sign@tor terminal.

Note: It is necessary for the user to compare the two HASH values and (when they correspond) start the signing process (transmission of HASH value to signature card) in the Sign@tor terminal.

The HASH value is encrypted in the signature card and the signature is created.

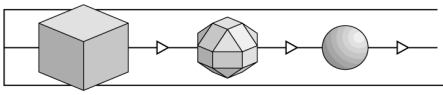
The file selected for signing is provided with the digital signature and stored in standardised format (PKCS#7).

Securing the for software updates for PC:

The integrity of the downloaded software to be used for an update on the Sign@tor PC is checked.

Securing the software updates for Terminal:

The integrity of the downloaded software to be used for an update on the Sign@tor terminal is checked.



PIN entry:

Entry of the PIN is accomplished on the Sign@tor terminal. The PIN is then transferred exclusively to the signature card. It is deleted immediately after transfer to the signature card in the Sign@tor terminal and does not leave the Sign@tor terminal in the direction of the PC.

3.1.3 Information on scope of product and delivery

In this section, particularly the information on the scope of delivery is given in detail. Here, more precise definitions are also made regarding which parts of the product are subject to evaluation (of their correctness and effectiveness) and are therefore components of the TOE in the actual sense.

The Sign@tor terminal (hardware, preinstalled software) is delivered as such and is part of the TOE in its entirety. The software for the Sign@tor terminal consists of the following components:

- Signature API,
- Update software for Sign@tor terminal

The CD delivered (part of product) contains primarily the

- Software for the Sign@tor PC
    - Signature API,
    - User interface (high level)
- and the update software Sign@tor PC.

The (installed) software for the user interface (high level) is not a part of the TOE

Following installation (of the software) on the Sign@tor PC, the following functionality is provided, which is included in the TOE (i.e. not part of the technical operational environment; see Chapter 2):

- Communication with the Sign@tor terminal via USB,
- Management of display masks,
- Polling of button keys and reaction to user entries,
- Activities in context with the signing operation.

The software for the Sign@tor terminal is all a part of the TOE (and therefore not a part of the technical operational environment, see Chapter 2): it provides primarily the following functionality:

- Communication with the Sign@tor PC via USB,
- Communication with the chipcard (T=1 protocol),
- Control of display,
- Polling of key pad and reaction to user entries,
- Activities in context with the signing operation.

In detail, the terminal software provides two terminal operating modes:

- The illustrated "TOE mode", which is relevant in context with signing files, and a
- "Pass-through mode", in which the data is exchanged only between PC and signature card without processing in the terminal.

Switch-over between the two modes requires a terminal reset. The "Pass-through" mode has no significance in terms of security aspects and will not be discussed further here.

3.2 Description of operational environment

3.2.1 Technical operational environment

Information on the required properties in the technical operational environment is indicated in the following context.

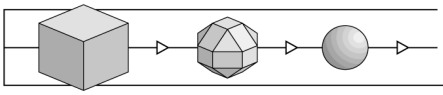
The software for the Sign@tor PC requires support by the operating systems

- Windows 98 SE,
- Windows ME or
- Windows 2000.

Note: The Sign@tor PC will be evaluated with the three operating systems listed, Windows 98, ME and Windows 2000.

The PC requires the following hardware components:

- CPU: Pentium I or higher,
- USB interface,
- Internet connection (optional),
- Hard disk: minimum 10 MB,
- Main memory: 32 MB.



There are no further requirements for the PC hardware and software on which the corresponding TOE part runs. On this PC the Sign@tor terminal is connected to the Sign@tor PC by a USB cable; for this reason, only PCs with a USB interface are supported.

There are no further interfaces to the PC.

The entire Sign@tor terminal is not part of the technical operational environment (but part of the TOE). Nevertheless, the important technical features of its hardware are listed below.

The hardware includes the following components which are not a part of the technical operational environment:

- CPU: 8051 family,
- Program memory: 64KB Flash-EPROM,
- Data memory: min. 1KByte static RAM,
- Persistent data memory: min. 2KB EEPROM,
- Chipcard interface: ISO 7816 (T1 protocol),
- Keypad: matrix 3x4 ,
- Display: not illuminated, size: 16x1,
- USB: transmission rate.

During signing, the terminal interacts with an "inserted" signature card which is a part of the technical operational environment. This is practical only with certain signature cards.

Momentarily, the following smartcards can be used.

- from the company "a-sign"
    - with Infineon processor chip
    - chipcard operating system: CardOS / M4.0 and
- from the company "A-Trust"
    - with Phillips processor chip
    - chipcard operating system: Starcos SPK 2.2 + mod.

Note: Tests were performed with the listed signature cards from the companies "a-sign (Datakom, Austria)“ and "A-Trust".

3.2.2 Assumptions on administrative operational environment

For security reasons, the following assumptions are to be met for TOE use. These assume that the user has taken the appropriate (organisational) measures.

General assumptions:

It is necessary for the user to ensure that only documents without macros are signed. Where applicable, in documents containing macros, it is necessary to remove these macros before signing, because they would otherwise also be signed.

It is necessary for the user to enter his PIN directly on the Sign@tor terminal before a signature can be generated at all.

Note: The user identifies / authenticates himself by entering the PIN and transferring it to the signature card. The card's security mechanisms ensure unique identification. It is necessary for the user to keep the PIN confidential.

Assumption in context with the Sign@tor terminal hardware:

Unauthorised persons are prevented from manipulating the hardware (TOE part) by appropriate material / physical precautions.

It is necessary for the user to check the status of the Sign@tor terminal (based on the bonded sealing points) after purchase and before initial operation. It is necessary for the terminal to remain bonded in order to prevent any possible attacks on the Sign@tor terminal during shipment to the customer.

Assumptions in context with Sign@tor terminal software:

The Sign@tor terminal software is already installed when the device is purchased.

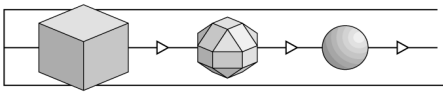
Assumptions in relation to Sign@tor PC software:

It is necessary for the user to initially install the software with the CD supplied in the SIGN@TOR package. Keep this CD in a secure place, because it is required for software updates.

Note: The user documentation is realised in the form of online documentation. Initial installation of the software can be accomplished with the CD and the Autorun feature (MS Windows). After installation of the software, the user is offered comprehensive help. The user documentation is generally realised in the form of online documentation.

It is necessary for the user to check the signature of the new software with the aid of the original CD when updating the Sign@tor PC software.

It is necessary for the user to ensure that an up-to-date virus scanner is always installed on the Sign@tor PC with the installed software and that it is activated at regular intervals.



It is necessary for the user to ensure that only trustworthy software is used.

Assumptions on physical operational environment:

The Sign@tor terminal and Sign@tor PC must be located in the same room and, during use, directly in front of the user for the following reasons:

- validation of the data as well as the HASH value must be possible,
- it is necessary to avoid anyone hearing or changing the document contents during data transfer between the Sign@tor PC and Sign@tor terminal.

3.2.3 Definition of objects, subjects and types of access

In this chapter, all subjects, objects and types of access are defined which are required for analysis of the security characteristics of the TOE and by consequence for definition of the security objectives (Chapter 3.3.1, Threats, Chapter 3.3.2 and Security Functions, Chapter 3.4).

Subjects

Subjects are persons or processes who have access to objects, particularly information.

Subjects within the context of Sign@tor are:

- TOE-specific processes which run on the PC and terminal (especially signing processes).
- Processes or applications which run on the PC and are not a part of the TOE.
- Processes which run in the signature card and therefore in the TOE environment.
- Persons who have access to the Sign@tor PC software and/or terminal (authorised or unauthorised).
- Service companies which provide the associated software as well as the software updates for the Sign@tor (PC and terminal).

Objects

Objects are primarily passive information units to be protected.

Such objects in context with Sign@tor are:

- files to be signed,
- Sign@tor terminal software not being executed (located in the internal memory),
- Sign@tor PC software on the CD or on the PC harddisk,

- the user PIN.

Types of access

Data objects can be read, received, written / modified, transmitted and executed by subjects (where applicable with malicious intent). For Sign@tor, particularly manipulative (malicious modification) or spying (malicious reading) access to data are significant before, after and during transfer.

The above listed (classic) types of access are already linked with additional information (regarding objects, times) in the following list:

- Loading of incorrect / manipulated (update) software into the Sign@tor PC or Sign@tor terminal,

- manipulation of the data (file to be signed, terminal update software) during transfer from the Sign@tor PC to the Sign@tor terminal,

- spying out the entered PIN (before transfer to the signature card),

- modification of data (signature card certificate, signature) during and after transfer from the Sign@tor terminal to the Sign@tor PC,

- modification of data (already signed file in PKCS#7 format) before, during and after storage.

Note: The last two changes cannot be prevented by the TOE itself. However, they can be discovered by checking the file signature. Consequently, definition of the corresponding threat and security objective is not accomplished in the following chapter.

3.3 Security objectives and threats

3.3.1 Security objectives

The objective is to generate an electronic signature with the greatest possible security for the user. For this purpose, the following sub-objectives are defined:

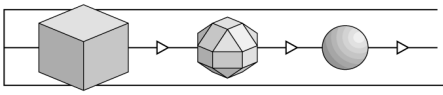
SZ1: The confidentiality of the PIN must be ensured in terms of processes on the PC.

SZ2: The integrity of the file transmitted from the Sign@tor PC to the Sign@tor terminal must be capable of being checked by the user.

SZ3: The authenticity of the files intended for updating the Sign@tor PC or Sign@tor terminal must be capable of being checked by the user.

3.3.2 Threats

Since Sign@tor will be offered on the free market, a potential attacker would have the possibility after procurement of manipulating the complete terminal (hardware, stored



software) and contents of the CD (of the product purchased) or obtaining knowledge for such manipulation. The Sign@tor terminal hardware consists otherwise of standard modules freely available on the market.

The following threats are assumed for the TOE in the intended operational environment:

B1: Spying out PIN

The PIN intended for authentication of the user with the signature chipcard can be spied out.

B2: Forging file during signature

The file to be signed can be forged after selection of the file on the way between the Sign@tor PC and Sign@tor terminal.

B3: Forging update software

The software intended for updating the TOE (PC and Terminal) can be forged or substituted unnoticed on the way between the vendor and user.

Note: This threat is aimed at a part of the TOE (software for update). This part is threatened during transfer via a public media.

3.4 Security functions of the TOE

Some of the following security functions have no relationship to the generic ITSEC headings. Where applicable; their definitions are supplemented by notes on the technical, organisational measures relevant in their environment.

SF1 – Secure PIN entry

SF1.1: Entry of the PIN for user authentication with the signature chipcard is accomplished on the Sign@tor terminal keypad. The Sign@tor terminal transfers the entered PIN exclusively to the signature chipcard.

SF1.2: After the PIN has been transferred to the signature chipcard, it is deleted.

SF2 - Secure channel between Sign@tor PC and Sign@tor terminal

The Sign@tor terminal and Sign@tor PC both display a self-calculated HASH value for the file to be signed. It is necessary for the user to compare the two HASH values before the actual signing process (transfer of HASH value to signature chipcard) can be started.

SF3 - Preparation and final processing of digital signature

The Sign@tor terminal transmits the HASH value described in SF2 to the signature chipcard and receives the signature back from it.

In addition, the TOE encodes the result (file, signature and associated certificate) in PKCS#7 format.

SF4 – Software update

SF4.1:The integrity of the software intended for updating the Sign@tor PC is checked with a program on the original CD which can be started by the user after downloading the software. (The CD contains the integer and authentic public key for verification of the signature). The software components for the Sign@tor PC intended for updating the Sign@tor PC have been provided with a digital signature by Siemens.

SF4.2:The software intended for updating the Sign@tor terminal is checked for integrity and authenticity before installation on the Sign@tor terminal. For this purpose, the update software has a digital signature provided by Siemens and the Sign@tor terminal has a corresponding public key.

3.5 Appropriateness of the security functions

Comparison of security functions with: Type of use - Threat – Security objectives.

1. Signature card on Sign@tor terminal / Spying out PIN.

   The PIN could be spied out by an attacker (B1). To counteract this, the PIN is entered on the terminal (SF1.1). The PIN is transferred exclusively to the card and then deleted immediately (SF1.2).

   This averts threat B1.

2. Manipulation / Forging of file selected for signing

   Manipulations can be recognised by the user, because the Sign@tor PC as well as the Sign@tor terminal calculate a HASH value for the file and indicate it to the user. Differences in these two values indicate manipulation.

   The signature process is then started and the result stored by the TOE coded in PKCS#7 format.

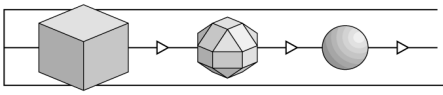
   This averts threat B2.

3. Forging of the software for updating (Sign@tor PC and terminal) on the way between vendor and user

   The update software for the TOE is provided with a digital signature.

   The digital signature on the PC software is checked by an authentic and integer software on the original CD.

   The digital signature on the terminal software is checked at the Sign@tor terminal.



3.6 Evaluation assurance level and minimum strength of mechanisms

The target evaluation level for the TOE is E2, the claimed minimum strength of mechanisms is high.

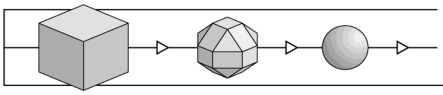
3.7 Terms

The basic procedures and definitions for generation of electronic signatures are presumed to be known. As a supplement, the following terms are defined here and used subsequently:

Application	Independent part of program which can be loaded into the memory of a PC (with the Sign@tor PC) or the terminal, can perform certain, independent operations and thereby has access to functions of the operating system. Note: According to this general definition, the Sign@tor PC and Sign@tor terminal themselves are applications. The term is used specifically in context with external applications on the PC where Sign@tor PC is running.
User	User
File information	File information consists of: File name, file length and creation date of file.
Document	A document present in file form.
HASH value	Checksum calculated for a document. Characteristic for a document, however not necessarily unique.
PKCS#7	General syntax for encrypting and decrypting data
Private Key	Confidential part of RSA key pair
Public Key	Public part of RSA key pair
Signature	File with following contents: Data on user, HASH value for the document, electronic signature (generated from HASH value).
Signature card	Chipcard on which the required keys are stored. Calculation of the signature from the HASH value is also accomplished on the signature card.
Signature	Signature
Certificate	File transferred by the trust centre. It contains data on the user as well as his public key. A certificate is signed by the trust centre with its private key. If this document speaks of a certificate, the certificate of the sender is meant unless otherwise specified.

3.8 Abbreviations

Bx	Threat, x= Sequential number
CPU	Central Processing Unit
TOE	Target of Evaluation
HW	Hardware
ISO	International Standardisation Organisation
OS	Operating system
PC	Personal Computer
PIN	Personal Identification Number
RSA	Rivest Shamir Adleman
SFx	Security function, x= Sequential number
SW	Software
SZx	Security objective, x= Sequential number
USB	Universal Serial Bus

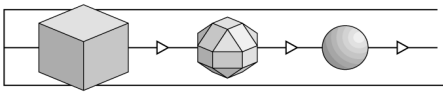


(This page is intentionally left blank.)

4 Remarks and Recommendations concerning the Certified Object

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

26 The Certification Body has no further information or recommendations for the user.



(This page is intentionally left blank.)

5 Security Criteria Background

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

5.1 Fundamentals

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

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

- confidentiality
- availability
- integrity

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

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

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

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

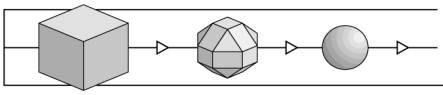
33 There are two basic questions:

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

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

5.2 Assurance level

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.3 Security Functions and Security Mechanisms

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

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

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

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

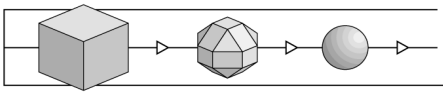
Example: The function *Identification and Authentication* can be realised by a password procedure, usage of chipcards with a challenge response scheme or by biometrical algorithms.

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

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

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

Type B „A *type B mechanism* is a security mechanism which, if perfectly conceived and implemented, will have no weaknesses. A type B



mechanism can be considered to be impregnable to direct attack regardless of the level of resources, expertise and opportunity deployed. A potential example of a type B mechanism would be access control based on access control lists: if perfectly conceived and implemented, this type B mechanism cannot be defeated by direct attack. However, these type B mechanisms can be defeated by indirect attacks which are the subject of other effectiveness analyses."

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

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

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

46 How is the strength for type A mechanisms defined?

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

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

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

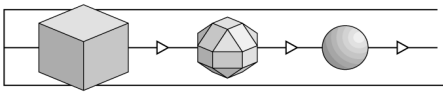
high: „For the minimum strength of a critical mechanism to be rated *high* it shall be evident that it could only be defeated by attackers possessing a high level of expertise, opportunity and resources, successful attack being judged to be beyond normal practicability."

6 Annex

6.1 Glossary

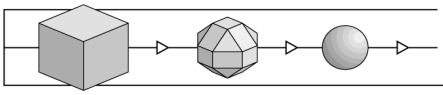
This glossary provides descriptions of the expressions used in this brochure, but does not guarantee their completeness or general validity. The term *security* here is always used in the context of information technology.

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



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

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



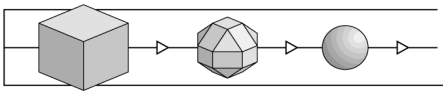
Product Certification	Certification of an IT product.
Re-Certification	Renewed certification of a previously certified object due to a new version following modification; re-certification might also be required after a change of tools, production / delivery processes and security criteria.
Recognition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

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

6.2 References[3]

/A00/	Lizenzierungsschema [Licensing Scheme], debisZERT, version 1.6, 31.03.2000, http://www.debiszert.de/
/ALG/	Geeignete Kryptoalgorithmen gemäß § 17 (2) SigV [Approved Crypto-Algorithms according to § 17 (2) SigV], published in Bundesanzeiger [Federal Gazette] No. 230 – page 22.946 as of December 7, 2000
/BSIG/	Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz - BSIG) [Act on the Establishment of the German Information Security Agency], BGBl. I. of 17.12.1990, page 2834 ff.
/CC/	Common Criteria for Information Technology Security Evaluation, version 2.1, Part 1 (Introduction and general model), Part 2 (Security functional requirements), Part 2 : Annexes, Part 3 (Security assurance requirements) , August 1999
/CEM/	Common Methodology for Information Technology Security Evaluation, Part 1 (Introduction and general model), version 0.6, January 1997, Part 2 (Evaluation Methodology), version 1.0, August 1999
/ITSEC/	Information Technology Security Evaluation Criteria (ITSEC), version 1.2 (1991), ISBN 92-826-3004-8
/ITSEM/	Information Technology Security Evaluation Manual (ITSEM), version 1.0 (1993), ISBN 92-826-7087-2
/IuKDG/	Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz - IuKDG) [Information and Communication Services Act], BGBl. I. of 28.07.1997, page 1872 ff.
/JIL/	Joint Interpretation Library, version 2.0, November 1998

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



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

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

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

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

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

/V01/ Certificates according to ITSEC/CC, service type 1 of debisZERT, version 1.5E, 30.06.1999, http://www.debiszert.de/

/V02/ Security Confirmations for Components according to the German Digital Signature Act, service type 2 of debisZERT, version 1.5E, 30.06.1999, http://www.debiszert.de/

/V03/ Sicherheitsbestätigungen für Zertifizierungsstellen gemäß dem Signaturgesetz [Security Confirmations for Trust Centres according to the German Digital Signature Act], service type 3 of debisZERT, version 1.0, 29.10.1999, http://www.debiszert.de/

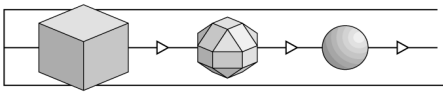
/V04/ Certificates recognised by the BSI, service type 4 of debisZERT, version 1.5E, 30.06.1999, http://www.debiszert.de/

/Z01/ Certification Scheme, debisZERT, version 1.5E, 30.06.1999, http://www.debiszert.de/

6.3 Abbreviations

AA	Work instructions
AIS	Request for an interpretation of security criteria
BSI	Bundesamt für Sicherheit in der Informationstechnik [German Information Security Agency]
BSIG	Act on the Establishment of the BSI
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CTCPEC	Canadian Trusted Computer Products Evaluation Criteria
DAR	Deutscher Akkreditierungsrat [German Accreditation Council]
DBAG	Deutsche Bahn AG [German Railways AG]
debisZERT	Certification Scheme of debis IT Security Services
DATech	Deutsche Akkreditierungsstelle Technik e.V. [German Accreditation Body Technology]

DLB	service type
EBA	Eisenbahn-Bundesamt [Federal German Railway Office]
ETR	Evaluation Technical Report
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	IT Security Evaluation Facility
ITSEM	Information Technology Security Evaluation Manual
IuKDG	German Information and Communication Services Act
RegTP	Regulierungsbehörde für Telekommunikation und Post [Regulatory Authority for Telecommunications and Posts]
SigG	German Digital Signature Act
SigV	German Digital Signature Ordinance
TKG	German Telecommunications Act
TOE	Target of Evaluation



(This page is intentionally left blank.)

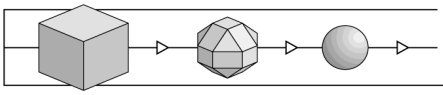
7 Re-Certification

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

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

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

50 The annexes are numbered consecutively.



End of initial version of the certification report.