debis

Services by DaimlerChrysler

Certification Report

CardMan®, CardMan® Compact, CardMan® Keyboard, CardMan® Mobile with CardMan® Software Development Kit, Version 2.2

Utimaco Safeware AG

debisZERT-DSZ-ITSEC-04006-1998

debis IT Security Services

The Modern Service Provider

Preface

The product CardMan®, CardMan® Compact, CardMan® Keyboard, CardMan® Mobile with CardMan® Software Development Kit, Version 2.2 of Utimaco Safeware AG 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:	Object Reuse
Assurance Level:	E2
Strength of Mechanisms:	Type B Mechanisms: impregnable to direct attack if perfectly conceived and implemented

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

Bonn, 20.04.1998

Head of the Certification Body:

Dr. Heinrich Kersten

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

✉ debis IT Security Services, - Zertifizierungsstelle -, Rabinstr. 8, 53111 Bonn
☎ 0228 / 9841-0, Fax: 0228 / 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
1.0	13.03.98	German language: Initial Release (based on template report version 1.0).
1.1	20.04.98	Changes to German Version 1.0: 1. Product name „Cardman II“ changed by sponsor to „CardMan“; the explanatory term “(PCMCIA)” was deleted. Products have not been changed. Certification Report uses new product names. 2. Registered Trademark sign ® used on cover page and within preface. 3. Template Report version 1.1 used.
1.2E	28.01.00	Issuance of an English version of the certification report (on request of sponsor) based on German version 1.1: 1. Actual template report version 1.5 used resulting in formal changes to all chapters. 2. References to scheme documentation point to versions 1.1 of 09.01.98 used during evaluation. 3. Original Security Target (provided by sponsor in English language) re-used in this version 1.2E. 4. Old certification ID “debisZERT: BSI-ITSEC-0406-1998” changed to new style “debisZERT-DSZ-ITSEC-04006-1998”.

Contents

(This page is intentionally left blank.)

1 Introduction

1.1 Evaluation

1 The evaluation was sponsored by Utimaco Safeware AG, Dornbachstr. 30, D-61440 Oberursel, Germany.

2 The evaluation was carried out by the evaluation facility Industrieanlagen-Betriebsgesellschaft mbH (IABG) and completed on 11.03.1998.

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 the Deutsche Akkreditierungsstelle für Informations- und Telekommunikationstechnik (DEKITZ) 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, version 1.1, 09.01.98
- /V04/ Certificates recognised by the BSI, version 1.1, 09.01.98

1.3 Certification Report

6 The certification report states the outcome of the evaluation of CardMan®, CardMan® Compact, CardMan® Keyboard, CardMan® Mobile with CardMan® Software Development Kit, Version 2.2 - 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 CardMan®, CardMan® Compact, CardMan® Keyboard, CardMan® Mobile with CardMan® Software Development Kit, Version 2.2 when establishing an adequate security level.

10 The certification report contains pages 1 to 34. 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 in

- / Z02 / Certified IT Products, Systems and Services.

1.4 Certificate

12 A survey on the outcome of the evaluation is given by the security certificate debisZERT: BSI-ITSEC-0406-1998 (cf. *Revision List* on ID format).

13 The contents of the certificate are published in the document

- / Z02 / Certified IT Products, Systems and Services

and on the WWW 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 certificate carries the logo officially authorised by the BSI. The fact of certification is listed in the brochure BSI 7148.

1.5 Application of Results

16 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.

17 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.

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

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

19 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

20 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 of the TOE are critical 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

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

22 The evaluation facility has formulated the following remarks resp. requirements to the user.

1. The evaluation result is only valid if the TOE is operated under MS DOS 6.x, MS Windows 3.x, MS Windows 95 / Windows NT or OS / 2 Warp 3.0 and 4.0.

2. The TOE has to be protected against modification to or replacement of hardware components, e.g. by restricting physical TOE access to authorised individuals.

3 Security Target

23 The Security Target, version 2.5 dated 17.12.1997 was supplied by the sponsor in English language.

3.1 Product Rationale

3.1.1 Definition of Target of Evaluation

The Target of Evaluation (TOE) consists of the following product items:

- smartcard reading interface unit, which can be alternatively:
    - CardMan Compact smartcard reader unit for the serial port or
    - CardMan smartcard reader unit for the serial port or
    - CardMan Mobile PC-Card (PCMCIA) smartcard reader or
    - CardMan Keyboard.
- Software: CardMan Software Development Kit, version 2.2 for different operating system platforms,
- CardMan SDK API documentation (Programmer's Reference) (printed document in English language).

The TOE will be named "CardMan" throughout the rest of the document.

3.1.2 Description of Target of Evaluation

3.1.2.1 Overview

CardMan is a combination of hardware and software items supporting the use of smartcards in a wide range of information security applications like

- Secure Authentication systems (PC security),
- Crypto systems (Key Management functions),
- Secure Electronic Messaging systems (Electronic Signature, Home Banking).

The CardMan smartcard reader is a small and handy interface for accessing most of ISO 7816 compatible smartcards.

The CardMan Software Development Kit includes a set of libraries and device drivers, which can be integrated into custom-specific applications. The libraries offer complex functions to realise applications for interfacing with the CardMan smartcard readers.

3.1.2.2 General Hardware Description

The CardMan reader hardware is available in four different versions (as listed in section 3.1.1 of this document). Three of the items are designated for interfacing a serial port and have identical design of the electronics, one item, the PC-Card, is designated for usage in laptops or notebooks (however it will also work in PCMCIA interface slots for desktop workstations).

The design of the different forms of smartcard reader is described below.

CardMan Compact

CardMan Compact is a smartcard reader unit in a separate case.

The reader is connected to the workstation with a fixed cable for the serial port. The power supply is taken from the serial port.

CardMan

CardMan is a special version of CardMan Compact. It is also a reader in a separate case. For CardMan, the serial cable is pluggable at the reader, where 2 connectors on different sides are available. The power supply is taken from the serial port. The reader has two LEDs (green and red) at the front side to indicate the status of the reader and the card.

CardMan Keyboard

With the CardMan Keyboard, the reader is integrated into the case of a keyboard. The card is inserted at the right back side of the keyboard. The reader electronics is functionally equivalent to that of CardMan and CardMan Compact. The reader is connected with a separate fixed cable to a serial port of the workstation.

The keyboard is available in ISO 102 key layout and ANSI 101 key layout, the ISO 102 key layout is available for a wide range of languages (German, English etc.).

CardMan Mobile

CardMan Mobile is a Type II PC-Card (PCMCIA card). It fits into any PC-Card slot for Type II cards. The smartcard is inserted from the open side of the PC-Card.

The connection is made over the PC-Card bus of the workstation, additional connections are not required. The card emulates a serial port for the workstation.

3.1.2.3 Hardware Installation

The CardMan smartcard reader is connected to a free serial port of the workstation, when using one of the serial units (CardMan, CardMan Compact or CardMan Keyboard). The serial port has to be configured with I/O address and interrupt, so that no conflicts occur.

When using the PC-Card, the card is inserted into a PCMCIA-Type II slot of the workstation. The card is emulating a serial port and must be configured as free serial port with address and I/O interrupt.

All remaining configuration is performed by the software, which is driving the smartcard reader (see below).

3.1.2.4 Software Description

The CardMan Software Development Kit (SDK) is a package of libraries and include files, which are bundled for each supported operating system and delivered on floppy disks.

The SDK consists of :

- header files (.H) for including into C source code (ANSI compatible).
- libraries, depending on the operating system:
  - static libraries (.LIB) in Microsoft linker format for static linkage under DOS version 6.0 and above,
  - 16-bit dynamic linkable libraries (.DLL) for Windows 3.1 and 3.11,
  - 32-bit dynamic linkable libraries (.DLL) for Windows 95, Windows NT 3.51 and Windows NT 4.0 (Workstation and Server),
  - 32-bit dynamic linkable libraries for OS/2 WARP Version 3.0 and 4.0.
- a device driver for processing the serial communication between the workstation and the smartcard reader, in detail:
  - a device driver (.EXE) for DOS Version 6.0 and above,
  - a VxD (.386) for Windows 3.1 and 3.11,
  - a service program for Windows 95, Windows NT 3.51 and Windows NT 4.0 (Workstation and Server),
  - a device driver for OS/2 WARP Version 3.0 and 4.0.

The software transmits the data in an encapsulated channel from the application program to the smartcard and vice versa. Only for the transmission over the serial interface the services of the operating system are used.

The communication between the library functions and the device driver is done by operating system specific measures and by using a buffer of shared memory.

All buffers used for data transmission in the software on the host side are cleared immediately after usage. All buffers used for data transmission in the firmware and hardware of the CardMan are re-used and the same information cannot be read out twice.

3.1.2.5 Scope of the API Functions

The CardMan SDK libraries contain a set of API functions for the communication of a user-specific application program with the smartcard reader and the smartcard.

The API is identical for each operating system platform. The functions are grouped in the following layers.

Protocol Layer

This layer includes functions for interfacing with the smartcard reader and perform generic smartcard functions:

- connect and disconnect reader,
- reading reader status,
- controlling reader LEDs (CardMan only),
- locking and unlocking the reader interface.
- Power On and Power Off to smartcard,
- forcing reader protocol to smartcard (transmission rate etc.),
- protocol adjust and
- communicate with smartcard.

The communication functions are available for each supported protocol (T=0, T=1, T=14, Synchronous).

Smartcard Layer

For each supported family of smartcards a set of smartcard-specific functions is available. The families supported in the TOE are:

- BULL CP8 SCOT
- Siemens SLE 4428,
- Siemens SLE 4442,
- Siemens SLE 44C200,
- GEMPLUS MCOS.

The set of functions contained in each library is dependent on the smartcard operating system, they mirror the major functions of the Smartcard OS, for example:

- initialise card,
- present PIN,
- read data (word, directory, record etc.),
- write data (word, directory, record etc.),
- read status,
- perform card specific encryption algorithms (RSA, DES etc.).

All functions of the CardMan SDK use only functions of the lower layers of the SDK itself, or the device driver of the CardMan SDK, respectively.

A detailed printed documentation delivered with the TOE describes the interfaces and the use of all interface functions.

3.1.2.6 Software Installation and Usage

CardMan SDK is installed with an installation program from floppy disks; only for DOS, the installation must be performed manually by executing a self-extracting compressed file. The installation program prompts for the installation paths. The rest of the installation is fully automatic.

CardMan SDK is installed in an application development environment, where the applications using the API functions are developed.

When using the dynamic linkable libraries, they have to be copied to a directory, where the application can load them when it is running.

When using the device driver, it has to be installed correctly, depending on the operating system of the target workstation:

- with an entry in CONFIG.SYS for DOS Version 6.0 and above,
- with an entry in SYSTEM.INI for Windows 3.1 and 3.11,
- using the system configuration under Windows 95, Windows NT and OS/2 WARP.

When a custom-specific application, which is build using the CardMan SDK, is delivered, the required libraries and the appropriate device driver of the CardMan SDK have to be added to the application executables.

On the target workstation, where the application is installed, the libraries have to be copied to a path, where the application can load them when it is running. The device driver has to be installed correctly.

3.1.3 Intended Environment

3.1.3.1 Hardware Requirements

The TOE runs on standard personal computers with a microprocessor compatible to Intel 80386 and above. The personal computer requires one free serial port for the connection of the CardMan smartcard reader. The CardMan Keyboard with integrated smartcard reader also requires a serial port for the connection of the reader. When using the CardMan Mobile no free serial port is required, but one of the four available serial port connections must not be equipped by a physical serial port.

There are no special hardware requirements for the remaining parts like fixed disk equipment and others.

The TOE supports smartcards compliant with ISO 7816, using one of the protocols T=0, T=1, T=14 or certain synchronous communication. The operating current must be no more than 10 mA, when using the CardMan in CardMan Keyboard, the operating current may be up to 50 mA.

3.1.3.2 Software Requirements

The CardMan software API supports the following operating systems:

- MS-DOS Version 6.0 and above,
- Windows 3.1, Windows for Workgroups 3.11,
- Windows 95,
- Windows NT 3.51 Workstation and Server, Windows NT 4.0 Workstation and Server,
- OS / 2 WARP Version 3.0 and Version 4.0.

The CardMan software API is supplied for the following compilers:

- Microsoft C (Version 6.0 and above) and VisualC (Version 1.0 and above) and object format compatible ANSI C compilers,
- OS / 2 Visual Age C compiler.

3.1.3.3 Special Measures

The following special measures have to be taken to assure the secure functionality of the system:

Building Secure Applications

In order to build a secure application, the functions of the API have to be used according to the instructions in the documentation (Programmer's Manual). This assures, that the functions are used in a way, that the security mechanisms do not deactivate, bypass or circumvent each other.

3.1.4 Subjects, Objects and Actions

3.1.4.1 Subjects

(S1) Any process running on the target system, which is not part of the TOE.

(S2) Any person having access to the smartcard reader hardware device.

3.1.4.2 Objects

(O1) Communication data from communication with the smartcard stored in main memory.

(O2) Communication data stored in memory on the hardware device (smartcard reader).

3.1.4.3 Actions

(A1) Access to communication data in main memory (O1) by any process (S1) after the completion of a data transmission by the TOE.

(A2) Access to communication data in hardware device memory (O2) by any measure by any person (S2) after completion of a data transmission by the TOE.

3.1.5 Security Objectives and Assumed Threats

3.1.5.1 Security Objectives

The TOE is designed to prevent access to the transmitted data from or to the smartcard by any measure after the data transmission has been completed. This is done for data stored in main memory as well as for data stored in the smartcard reader hardware device. All memory objects used by the TOE for transmission data are cleared before they can be used by other processes or read out from hardware.

3.1.5.2 Assumed Threats

The TOE is able to cover the assumed threat listed below:

(T1) Any process outside the TOE (S1) getting knowledge of the transmission data stored in main memory (O1) by reading the memory (A1).

(T2) Any person (S2) getting knowledge of transmission data stored in the hardware device (O2) after completion of the transmission by reading out the memory contents (A2) of the hardware device.

3.2 Security Functions

3.2.1 (F1) Clearing Main Memory Buffers

The TOE provides a function, which clears the allocated buffers of main memory, which may contain transmission data. The buffers are cleared immediately after the completion of the data transmission.

3.2.2 (F2) Object Reuse of Hardware Device Buffers

The TOE assures, that the information in the buffers in the hardware device (any version of the smartcard reader), which contain transmission data, can only be read out once, i.e. the information can not be read out any more after the TOE has read out the data.

3.2.3 Effectiveness of the Security Functions

The security function (F1) covers the threat (T1), the security function (F2) covers the threat (T2)[1].

3.3 Claimed Rating of Minimum Strength of Mechanisms and Target Evaluation Level

All listed product arrangements of the TOE are identical as to their security functions and their security enforcing and security relevant parts.

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

[1] This scenario is essential to meet the requirements of the German Digital Signature Act and the German Digital Signature Ordinance.

4 Remarks and Recommendations concerning the Certified Object

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

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

(This page is intentionally left blank.)

5 Security Criteria Background

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

5.1 Fundamentals

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

28 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.

29 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.

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

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

32 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

33 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.

34 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.

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

36 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.

37 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."

38 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

39 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.

40 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.

41 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.

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

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

44 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.“

45 How is the strength for type A mechanisms defined?

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

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

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

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

6 Annex

6.1 Glossary

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

Accreditation

A process to confirm that an evaluation facility complies with the requirements stipulated by the EN 45001 standard. Accreditation is performed by an *accreditation body.* Accreditations from bodies represented in the German Accreditation Council (DAR) are generally recognised.

Associated Laboratory

A development laboratory co-operating with debisZERT under a contract, using optimised procedures to prepare for an evaluation.

Availability

Classical security objective: Data should always be available to authorised persons, i.e. this data should neither be made inaccessible by unauthorised persons nor be rendered unavailable due to technical defects.

Certificate

Summary representation of a certification result, issued by the certification body.

Certification

Independent confirmation of the correctness of an evaluation. This term is also used to describe the overall process consisting of evaluation, monitoring and subsequent issue of certificates and certification reports.

Certification Body

An organisation which performs certifications.

Certification ID

Code designating a certification process.

Certification Report

Report on the object, procedures and results of certification; this report is issued by the certification body.

Certification Scheme

A summary of all principles, regulations and procedures applied by a certification body.

Certifier

Employee at a certification body authorised to carry out certification and to monitor evaluations.

Common Criteria

Security criteria derived from the US Orange Book / Federal Criteria, European ITSEC and Canadian CTCPEC, and intended to form an internationally accepted security evaluation standard.

Component According to SigG

A logical unit in an IT system performing a task defined in SigG / SigV (display component, component for key generation, etc.).

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

IT Service
A service depending on the support by IT products and / or IT systems.

IT System
An inherently functional combination of IT products. (ITSEC:) A real installation of IT products with a known operational environment.

ITSEC
Information Technology Security Evaluation Criteria: European de facto standard for the evaluation of IT products and IT systems.

ITSEM
Information Technology Security Evaluation Manual. This manual on ITSEC applies in particular to evaluation processes.

Licence (personal)
Confirmation of a personal qualification (in the context of debisZERT here, cf. licenced engineer).

Licence Agreement
An agreement between an evaluation facility and a certification body specifying procedures and responsibilities for evaluation and certification.

Licenced Engineer
A person with qualifications in the context of evaluation approved by debisZERT.

Licensing
Evaluation of organisation and qualification of an evaluation facility with respect to an intended licence agreement (to become a CLEF).

Manufacturer's Laboratory
An organisational unit belonging to the manufacturer of a product /system or the supplier of a service, charged with performing evaluation of that product, system or service.

Milestone Plan
A project schedule for the implementation of evaluation and certification processes.

Monitoring
Procedure implemented by the certification body in order to check whether an evaluation is performed correctly (compliance with criteria, use of standard processes and appraisal techniques etc.).

Pre-Certification
Confirmation of the results of a preliminary investigation of a product-specific or process-specific security standard or a security-related tool (with a view to later certification).

Problem Report
Report sent by an evaluation facility to the certification body and concerning special problems during evaluation, e. g. concerning the interpretation of IT security criteria.

Process (Enterprise~)
Sequence of linked activities (prozess elements) performed within a given environment – with the objective to provide a certain service.

Process ID
ID designating a certification or confirmation process within debisZERT.

Product Certification
Certification of an IT product.

Re-Certification
Renewed certification of a previously certified object due to a new version following modification; re-certification might also be required after a change of tools, production / delivery processes and security criteria.

Recognition (Agreement)
Declaration and confirmation (of the equivalence of certificates and licences).

Regulatory Authority for Telecommunications and Posts
The authority responsible in accordance with §66 of the German Telecommunications Act (TKG).

Right of Disposal
In this case: Authorisation to allow all inspections of a product, system or service as part of evaluation and certification.

Security Certificate
Refer to „Certificate".

Security Confirmation
In debisZERT: A legally binding confirmation of security features extending beyond the scope of a certificate,
e. g. a confirmation according to SigG / SigV.

Security Criteria
Normative document that may contain technical requirements for products, systems and services, but at least describes the evaluation of such requirements.

Security Function
Function of an IT product or IT system for counteracting certain threats.

Security Level
A metric defined in security criteria to indicate various levels of security relating to different requirements for the object to be certified and the degree of detail needed during evaluation.

Security Specification
Security-related functional requirements for products, systems and services.

Security Standards
A joint expression encompassing security criteria and security specifications.

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

Service Type
Particular type of service (DLB) offered by debisZERT.

Sponsor
A natural or legal person who (in this case) issues an order for certification or evaluation, and who must possess a sufficient right of disposal for the object to be certified or evaluated, respectively.

System Accreditation
Procedure of accepting an IT system or IT service for usage (considered here from the perspective of adequate security) in a specific environment and / or application.

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

6.2 References[2]

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

/ALG/ Anhang zu „Bekanntmachung zur digitalen Signatur nach Signaturgesetz und Signaturverordnung vom 09.02.98 im Bundesanzeiger Nr. 31 v. 14.02.98“ [Annex to „Official Announcement concerning the Digital Signature according to the Digital Signature Act and Signature Ordinance by February 9, 1998 published in Bundesanzeiger No. 31, February 14, 1998“], http://www.regtp.de/Fachinfo/Digitalsign/start.htm

/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 2.0, Part 1 (Introduction and general model), Part 2 (Security functional requirements), Part 2 : Annexes, Part 3 (Security assurance requirements) , November 1998, http://csrc.nist.gov/cc/info/infolist.htm

/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, http://csrc.nist.gov/cc/info/infolist.htm

/EBA/ Kriterien für die sicherheitstechnische Bewertung und Konstruktion von CIR-Netzkomponenten [Criteria for Security-Related Evaluation and Construction of CIR Network Components], Eisenbahn-Bundesamt, version 1.0 of 8.2.94

/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

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

/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

/Mkat12/ Maßnahmenkatalog nach §12 Abs. 2 [Catalogue of Security Measures in accordance with §12 Sec. 2], Regulierungsbehörde für Telekommunikation und Post, http://www.RegTp.de/Fachinfo/Digitalsign/start.htm

/Mkat16/ Maßnahmenkatalog nach §16 Abs. 6 [Catalogue of Security Measures in accordance with §16 Sec. 6], Regulierungsbehörde für Telekommunikation und Post, http://www.RegTp.de/Fachinfo/Digitalsign/start.htm

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

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

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

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

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

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

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

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

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

/Z02/ Certified IT Products, Systems and Services, debisZERT, version 1.4E, consecutively numbered issues, 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 Informa-

	tion 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
DEKITZ	Deutsche Akkreditierungsstelle für Informations- und Telekommunikationstechnik [German Accreditation Body for Information and Telecommunication 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
ZKA	Zentraler Kreditausschuß [German Central Credit Committee]

(This page is intentionally left blank.)

7 Re-Certification

46 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.

47 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.

48 Re-certification and new technical annexes will be announced in the brochure /Z02/, also published on WWW.

49 The annexes are numbered consecutively.

End of initial version of the certification report.