debis

Services by DaimlerChrysler

Certification Report

SafeGuard Sign&Crypt Software Development Kit Version 2.0

Utimaco Safeware AG

debisZERT-DSZ-ITSEC-04008-1999

debis IT Security Services

The Modern Service Provider

Preface

The product SafeGuard Sign&Crypt Software Development Kit Version 2.0 of Utimaco Safeware AG has been evaluated against the *Information Technology Security Evaluation Criteria* (ITSEC) and the *Information Technology Security Evaluation Manual* (ITSEM). 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:

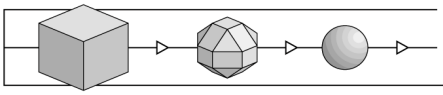
Security Functionality:	Digital Signature Creation, Digital Signature Verification, Symmetric Data Encryption / Decryption
Assurance Level:	E2
Strength of Mechanisms:	medium

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

Bonn, 21.05.1999

Certifier:	Head of the Certification Body:
Klaus-Werner Schröder	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



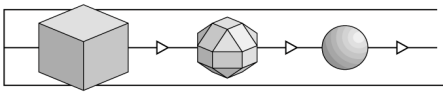
Revision List

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
0.9	10.05.1999	Preversion (based on template report 1.5)
1.0	21.05.1999	Initial release (based on template report 1.5)

Contents



(This page is intentionally left blank.)

1 Introduction

1.1 Evaluation

1 The evaluation was sponsored by Utimaco Safeware AG, Dornbachstraße 30, 61440 Oberursel.

2 The evaluation was carried out by the evaluation facility Prüflabor für IT-Sicherheit der Industrieanlagen-Betriebsgesellschaft mbH and completed on 21.05.1999.

3 The evaluation has been performed against the *Information Technology Security Evaluation Criteria* (ITSEC) and the *Information Technology Security Evaluation Manual* (ITSEM). 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 Telekommmunikationstechnik (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
- /V04/ Certificates recognised by the BSI

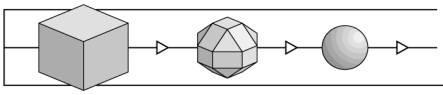
1.3 Certification Report

6 The certification report states the outcome of the evaluation of SafeGuard Sign&Crypt Software Development Kit Version 2.0 - 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 SafeGuard Sign&Crypt Software Development Kit Version 2.0 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 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- DSZ-ITSEC-04008-1999.

13 The contents of the certificate are published in the document

- /Z02/ Certified IT Products, Systems and Services

and on the WWW.

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.

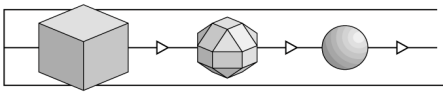
18 It is highly recommended to read the certification report carefully to benefit from the evaluation. In particular, the information provided on the intended method of use, the assumed threats, the operational environment and the evaluated configurations are essential for the user.

---

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

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.

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).

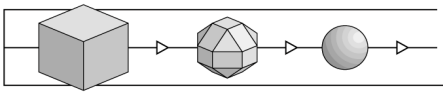
  ITSEC 3.12 to 3.37 for the effectiveness with the aspects

  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 of the TOE are critical mechanisms; they are of type A.

  The mechanisms of type A have a minimal strength of mechanism given by the level *medium*.



2.3 Further Remarks

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

23 The evaluation facility has formulated **no requirements** to the **user**.

3 Security Target

24 The Security Target, version 2.2 dated 27.04.1999, supplied by the sponsor for the evaluation is written in English language.

25 As far as the Security Target references the German Digital Signature Act and / or the German Digital Signature Ordinance and claims any conformance to these documents, the Certification Body would like to point out that such conformance declarations are not part of the certification against ITSEC / ITSEM.

26 The conformance claim is handled separately by the so called "Security Confirmation“ process (performed under debisZERT DLB 2). For the results of this process cf. the announcements of the Regulatory Authority for Telecommunications and Posts under www.regtp.de („Digitale Signaturen“).

3.1 References

This Security Target bases on the evaluation documentation for SafeGuard Sign&Crypt, especially on /SIGNST/.

3.2 Product Rationale

3.2.1 Definition of Target of Evaluation

The Target of Evaluation (TOE) is defined as the following product:

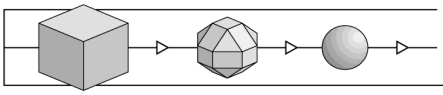
- SafeGuard Sign&Crypt Software Development Kit Version 2.0.

It consists of the following product items:

- SafeGuard Sign&Crypt Version 2.0,
- CryptWare Client Server API (CCS API) Support Software (delivered as SafeGuard Sign&Crypt SDK),
- SafeGuard Sign&Crypt User's Guide (printed document),
- SafeGuard Sign&Crypt SDK Technical Reference Manual (printed document),
- SafeGuard Sign&Crypt SDK Programmer's Guide for Secure Applications (printed document).

The TOE supports the following operating system platforms:

- Microsoft Windows 95,
- Microsoft Windows NT 4.0.



The operating system support is realised during installation of the TOE, where different components of the TOE are installed for the different operating systems.

The German and English language versions of SafeGuard Sign&Crypt are included into this definition of the TOE. They differ only in the different language of the user interface and of the user's manual of the SafeGuard Sign&Crypt Kernel.
The SafeGuard Sign&Crypt CCS API Support Software is not language dependent, but works with the kernel in each language version. The SafeGuard Sign&Crypt SDK Technical Reference Manual is only available in English version.

The TOE will be named "SafeGuard Sign&Crypt SDK" (or, for short, SDK) throughout the rest of this chapter 3.

3.2.2 Description of Target of Evaluation and Intended Method of Use

3.2.2.1 Overview

SafeGuard Sign&Crypt SDK is a toolkit for the implementation of custom-specific application programs in order to build a secure electronic messaging system. This includes the handling of digital signatures, asymmetric key systems and message encryption / decryption.

The SDK bases on the functionality of the base product SafeGuard Sign&Crypt, which is in parallel under evaluation as a system for digital signature and message encryption. For details of the functionality of SafeGuard Sign&Crypt, see /SIGNST/. The SDK enables customers to integrate the functions provided by the CryptWare Client Server API (CCS API) into their own applications. The CCS API is a part of SafeGuard Sign&Crypt.

The functions available with the help of the SDK are bound to assure the authenticity, integrity, non-repudiation and confidentiality of data, which is transferred from an originator to a receiver.

SafeGuard Sign&Crypt SDK works as a client-server system, where the SafeGuard Sign&Crypt CCS API and the SafeGuard Sign&Crypt kernel behind it work as a server and the application program, which calls the SafeGuard Sign&Crypt CCS API functions, works as a client.

SafeGuard Sign&Crypt SDK offers functions for the following tasks:

- Initialisation and shutdown of the SafeGuard Sign&Crypt CCS API communication

- Using secret keys from smartcard or from encrypted local files

- Using public keys stored in a database for document receivers

- Digital signature creation, formatting according to specific protocols and encryption of file contents

- Decryption and signature verification of file contents

For the signature creation and verification an asymmetric key system (asymmetric encryption algorithm) is used by the SDK.

For the encryption and decryption of data a symmetric encryption algorithm is used by the SDK.

The groups of functions are described more detailed in the following sections.

3.2.2.2 Lifecycle Management

The functions of this group are implemented to initiate rsp. to close the communication between the client application and the SafeGuard Sign&Crypt CCS API.

Functions for the lifecycle management include:

- Initialization of the communication between the client using the API and the SafeGuard Sign&Crypt CCS API.

- Shutdown of the communication between the client and the CCS API.

These functions have only management purpose and include no security mechanisms. They have to be called by the application program before rsp. after the use of the SDK.

3.2.2.3 Session Management

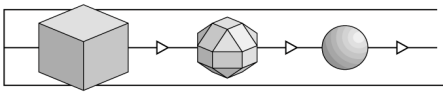
The functions of the session management handle the keys of the asymmetric key system. In this key system each user is provided with a pair of keys: a secret key (often also called private key), which is only accessible to the authorized user and a public key, which may be accessible to everybody. The function group includes:

- Functions for activating the secret key of a user; only one secret key can be activated at a time. The according functions create a handle, which describes the properties of the secret key and where it is stored.
  The secret keys can be stored in different places:

  - Secret keys on the disk: in this case each key is stored in an encrypted data file on the hard disk. The data file will be opened by a password, from which the key for the file encryption is generated.

  - Secret keys on a smartcard: the secret key is stored on a smartcard. For this case a CardMan smartcard reader has to be connected to the system. For all operations performed with the TOE the secret key is never leaving the smartcard.

- Functions for activating the public keys of so-called receivers: one or more public keys may be activated by identifying each key with a unique user identifier. The according functions create a handle, which describes the



properties of the public keys and where they are stored.
The public keys are stored as certificates in a database with internal format. In order to fill this database from different sources, a Utimaco certification authority software is available separately.

- Functions for deactivating any key handle retrieved by one of the previous functions.

When one of the key activation functions is called by the application program, the SDK function guides the user to select the desired key rsp. to insert his smartcard and PIN to activate a secret key.

3.2.2.4 File Security Functions

3.2.2.4.1 Overview

The major tasks for the file security operations are combined into four API functions. Two of these functions handle file "sealing", which includes the following operations:

- digital signature creation,
- data encryption (possibly including data compression) and
- protocol-specific data format generation.

The remaining two functions handle the reverse operations (file "unsealing"), which include:

- interpretation of protocol data,
- data decryption (including data decompression before, if required) and
- digital signature verification.

In each group one function processes a single file, whereas the second function processes multiple files one after the other within a single function call.

For the functions performing file sealing, a mode parameter provided by the calling application program indicates, what operations (digital signature creation, compression and/or encryption) should be performed by the function. Only the correct setting of this mode parameter assures the secure operation of the application which uses that function.

For the functions performing file unsealing, the contents of the affected file(s) determine the required operations.

The installation parameters of the installed SafeGuard Sign&Crypt product determine the protocol and the algorithms that will be used for the protocol-specific and cryptographic operations. For a list of the available cryptographic algorithms see /SIGNST/, Appendix A.

All functions in this function group require, that a secret key has been activated before and its handle is handed over as a parameter to the function. If encryption has been selected as a mode of file sealing, the function must also be called with a valid key handle for a set of public keys of the intended receivers of the file.

Mainly the cryptographic functions for digital signature creation, digital signature verification, data encryption and data decryption are within the scope of the security enforcing functions of the TOE.

The main actions performed by the file management functions are described in detail in the sections below.

3.2.2.4.2 Digital Signature Creation

For the creation of a digital signature, the function of the TOE calculates a hash function over the binary contents of the document. The result of the hash function is encrypted with the secret key of the originator using an asymmetric encryption algorithm. When the activated key is stored on a smartcard, this encryption is performed in the smartcard itself.

The encrypted hash value is called the digital signature, which is added to the document. Additionally a certificate identifying the originator and containing his public key, signed with a key of the certification authority, is added to the document.

The TOE then displays the correct completion of the signature process of the document to the user and the user must confirm that message to continue.

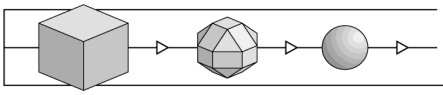
If the function is called with the compression option and the selected protocol supports compression, the compression of the document contents is performed after the signature creation.

3.2.2.4.3 Data Encryption

When encryption is selected, the document (the original or compressed document data including the digital signature) is encrypted using a symmetric encryption algorithm with a randomly generated session key. The key itself is encrypted with the public keys of the receiver(s) and the encrypted key(s) together with the identifier(s) of the receiver(s) is / are added to the encrypted document. For this step, the file sealing function must be called with a valid key handle of a set of public keys identifying the receiver(s).

After processing the mechanisms of signature creation and / or data encryption described above, the TOE function returns to the application program, handing over the correctness or the failure of the process as a result.

The document is now ready for transfer to the receiver(s). Transferring the document is not within the scope of the TOE.



3.2.2.4.4 Data Decryption

When a received document is processed by one of the file unsealing functions, it is checked, whether it is encrypted. In this case it has to be decrypted first. For this task, the session key must be decrypted from the header entry corresponding to the actual receiver. This is done by using the secret key, which is actually activated and whose handle has been handed over as a parameter to the unsealing function. For this task, the asymmetric encryption algorithm is used. The decrypted session key is then used to decrypt the data part of the document (including the signature(s)) with the symmetric encryption algorithm.

If the document is compressed, it will be decompressed after the decryption.

3.2.2.4.5 Digital Signature Verification

After decryption (if the document is encrypted) the digital signature is going to be verified in the unsealing function.

The certificate of the originator is extracted from the document and is first going to be verified with the key of the certification authority. Then the public key is retrieved from the certificate. The signed hash value from the document's signature is verified with the public key. On the other hand, a hash value is calculated over the raw data of the document using the same hash function. The decrypted received hash value and the locally calculated hash value are compared. If they are identical, the signature is verified correctly; otherwise the failure of the verification is indicated.

The result of this operation is displayed to the user and the user must confirm this message to continue.

After processing the mechanisms of data decryption and/or signature verification described above, the TOE function returns to the application program, handing over the correctness or the failure of the process as a result.

3.2.2.5 Product Installation and Usage

SafeGuard Sign&Crypt SDK is intended to be installed first in an application development environment, where the applications using the API functions are developed.

For the usage of SafeGuard Sign&Crypt SDK the product SafeGuard Sign&Crypt has to be installed first. This is done with an installation program from floppy disks. A description of SafeGuard Sign&Crypt and its installation can be found in /SIGNST/. Then the specific contents of the SafeGuard Sign&Crypt CCS API Support Software have to be installed from a separate floppy disk. This part includes:

- Header file (.H) and a static linkable libarary (*.LIB) for C code,
- Description file (.BAS) for VisualBasic code,

- Description file (.PAS) for Pascal code,

- Sample programs (C, BASIC, PASCAL) for the usage of the API.

The header files rsp. description files can be included into the C, VisualBasic or Pascal source code of the custom-specific application program.

To execute any application program, which has been built with the help of the SDK, the following must be present on the target system:

- SafeGuard Sign&Crypt Kernel and CCS API, the major component of the product SafeGuard Sign&Crypt,

- the application program built with the help of the SDK.

3.2.3 Intended Environment

3.2.3.1 Hardware Requirements

The TOE and, as a consequence, application programs built with the help of the TOE run on standard personal computers with a microprocessor compatible to Intel Pentium and above.

There are no special hardware requirements for the remaining parts like fixed disk equipment and others (besides enough free space for the installation of the TOE).

When smartcards will be used, the personal computer requires one free serial port for the connection of the CardMan / CardMan Compact smartcard reader. The CardMan keyboard also requires a serial port for the connection of the reader. When using CardMan Mobile no free serial port is required, but one of the four available serial port connections should be free.
The TOE requires one of the following types of smartcards for secure operation:

- SLE CR80S with T-COS operating system and 768-bit RSA on card,

- SLE 44CR80S with CardOS operating system and 1024-bit RSA on card.

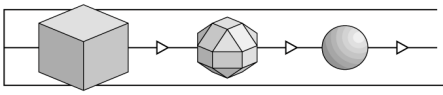
(The TOE will support more smartcards, but certified operation is restricted to the listed smartcard types).

3.2.3.2 Software Requirements

SafeGuard Sign&Crypt SDK is available for the support of the following operating systems:

- Windows 95,

- Windows NT 4.0 Workstation and Server.



SafeGuard Sign&Crypt SDK supports the following platforms for the development of application programs:

- all ANSI compatible C compilers for the listed operating system platforms,
- Microsoft VisualBasic,
- Borland (Inprise) DELPHI Pascal development environment.

Furthermore, the functions of the API can be called from every application program, which is able to call 32-bit Windows DLL functions.

3.2.3.3 Secure Configuration

In order to build a secure application, the functions of the API have to be used according to the instructions in the Programmer's Guide for Secure Applications. This assures, that the functions are used in a way, that the security mechanisms do not deactivate, bypass or circumvent each other. The instructions are:

- For each call of a SDK function (except CCSClose) the return code of the call has to be checked.
- If the return code of a SDK function indicates any problem, the user should be informed about the problem and the application should close the connection to the SafeGuard Sign&Crypt Kernel and return into idle state.
- The secret key handle intended to be used as a parameter for one of the file security functions has to be retrieved from the SDK immediately before the call and has to be checked on validity. The function shall not be called if the handle is not valid.
- The public key handle intended to be used as a parameter for one of the file security functions has to be retrieved from the SDK immediately before the call and has to be checked on validity. The function shall not be called if the handle is not valid.
- Especially the mode parameter of the major digital signature creation / verification functions (see section 3.2.2.4) must be set correctly to get a secure digital signature creation and verification of documents.

The parameter must include the characters "S" and "E" for generating digital signatures and encrypting the document.

3.2.4 Subjects, Objects and Actions

3.2.4.1 General

"Document" in the definitions below means a file, which is transferred from an originator to one or more receiver(s).

Signature is a set of data, which is added to the document by the originator and which can be verified by any receiver.

3.2.4.2 Subjects

<S1> Originator of a document.

<S2> Authorised receiver of a document (one who is intended to be a receiver by the originator).

<S3> Unauthorised person (either trying to get notice of the contents of a document or trying to change the contents of a signed document).

<S4> Person, whose identity is claimed (either intentionally or unintentionally) by the real originator of a document.

3.2.4.3 Objects

<O1> Contents of a document, i.e. the binary data ("raw data" without added certificates and signatures) which is transferred from the originator to the receiver(s).

3.2.4.4 Actions

<A1> Signing a document.

<A2> Verifying a document's signature.

<A3> Modifying a document's contents.

<A4> Getting knowledge of a document's contents.

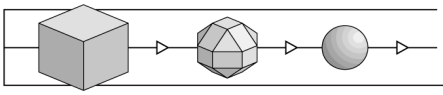
3.2.5 Security Objective and Assumed Threats

3.2.5.1 Security Objective

The TOE is designed to build application programs for a secure electronic messaging system including digital signature creation, verification and data encryption / decryption.

Those applications achieve the non-repudiation of a document, which is signed by its originator. The authenticity of the originator and the integrity of the document can both be proved by using the signature functions of the TOE. All cryptographic mechanisms and key selection operations required for that tasks are provided by the functions of the TOE.

This is claimed under the assumption, that the certification authority which is responsible for providing the user certificates and the public and secret keys is working in a secure manner.



When using the TOE under that assumption, the originator of a document can be sure, that only he is able to sign documents with his signature and he can be sure, that only the exact contents of the document, which he has signed, is verified correctly at the receiver's side.

The receiver of the document can be sure, that the given originator has signed exactly that contents of the document, which is indicated to him as correctly verified by that originator.

Additionally the TOE provides functions for achieving the confidentiality of a document between signing and verification by using symmetric encryption mechanisms.

Regarding the given assumptions, applications built with the usage of the TOE are able to avert the assumed threats listed below.

3.2.5.2 Assumed Threats

<T1> Attack against Data Integrity

The document <O1> which has been signed <A1> by the originator <S1> is manipulated <A3> by an unauthorised person <S3> and is indicated as correctly verified <A2> to the receiver <S2>, however.

<T2> Attack against Originator Authenticity

An originator <S4>, who is not the real originator <S1> of the document <O1> is displayed <A2> to the receiver <S2>. This may be the case, when the person <S1> is issuing a document, claiming to be person <S4> (intentionally or unintentionally).

<T3> Attack against Data Confidentiality

Document contents <O1> can be read <A4> by an unauthorised user <S3> during transfer of the data between <S1> and any <S2>.

3.2.5.3 Compliance with German Digital Signature Act

Averting <T1> and <T2> together covers the non-repudiation of the document, i.e. the originator can not deny to have signed the document exactly with the transferred contents.

The threats listed above are not identical to the threats, which should be averted by a product claiming to be compliant to the German Digital Signature Act.

However, when fulfilling the following additional restrictions for the application program and requirements for the environment also the threats defined for the German Digital Signature Act will be averted by the application program constructed with the help of the TOE.

- The application program uses a display component, which is compliant to the requirements of the German Digital Signature Act.

- The certification authority operates in a way compliant to the claims of the German Digital Signature Act and is approved for that process by the root instance (RegTP).

- The used smartcards are compliant to the requirements of the German Digital Signature Act and a security confirmation ("Sicherheitsbestätigung") has been issued to confirm that.

- The application program with the TOE is operated in a non-public enviroment, e.g. at home, in an authority or in a company office.

- The TOE is operated under one of the following configurations: MailTrusT V. 1.0 protocol with SHA-1 or RIPEMD-160 for hash value generation or S/MIME protocol with SHA-1 for hash value generation.

- The TOE is configured to use only secret keys from smartcards and thus to use the RSA on smartcard with a minimum of 768 bit key length for signature generation.

This claim is not part of the ITSEC certificate but will be confirmed separately (by the so called security confirmation ("Sicherheitsbestätigung")).

3.3 Security Enforcing and Security Relevant Functions

3.3.1 <SF1> Digital Signature Creation

The digital signature is created over the binary contents of a file ("raw data").

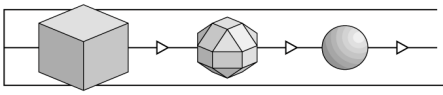
Signatures are created by calculating a hash value over the data and signing the hash value with the secret key of the originator stored on a smartcard or in the local database by using an asymmetric encryption algorithm.

In addition to the document signature a certificate of the certification authority is added to the document to prove the identity of the signature originator. This certificate also contains the public key of the originator. The identity of the originator is proved by his authorisation at the smartcard or by his knowledge of the password for the secret key in the database.

The user is informed about the correct signature of the data and must confirm that information.

3.3.2 <SF2> Digital Signature Verification

A document including a digital signature, which is created by <SF1>, is verified by



decrypting the hash value of the received signature with the public key of the originator and calculating a new hash value over the received document. The comparison of the hash values belonging together will decide whether the document is authentic and unchanged (hash values are identical).

The correct verification of a received document is displayed to the user and the user must confirm that information.

The identity of the originator of a document and his public key are retrieved from the certificate included in the document, which is verified using a key of the certification authority (either stored in the smartcard or in the local database).

3.3.3 <SF3> Symmetric Data Encryption / Decryption

The data of the document together with the signature is encrypted after signing using a symmetric encryption algorithm.

The data is decrypted before the signature is verified by the receiver.

The key used for the encryption is randomly generated ("session key") and sent to the receiver as a part of the document, encrypted by the public key of the receiver. Only the receiver is able to decrypt the session key with his secret key and then to decrypt the document and signature. Multiple receivers are possible by adding a set of encrypted public key fields to the document.

3.3.4 Effectiveness of Security Functions

The following table gives an overview, which security enforcing functions, shown under "<SFx>" avert which assumed threats, shown under "<Tx>".
Where more than one function is listed for a threat, all functions together counter the threat.

	<T1>	<T2>	<T3>
<SF1>			
<SF2>			
<SF3>			

The security mechanisms, which implement the security functions are listed in Appendix A of /SIGNST/.

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

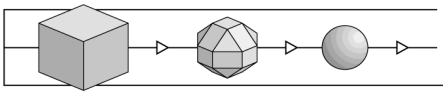
All listed product arrangements of the TOE (German and English version) are identical in their security enforcing and security relevant parts, functions and mechanisms.

3.4.1 Claimed Rating of Minimum Strength of Mechanisms

The claimed rating of the minimum strength of mechanisms for the configuration of the TOE mentioned in chapter 2.3 is **medium**.

3.4.2 Target Evaluation Level

The desired evaluation level for the TOE is **E2**.

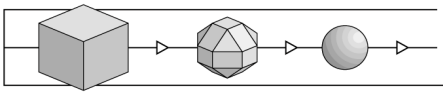


(This page is intentionally left blank.)

4 Remarks and Recommendations concerning the Certified Object

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

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



(This page is intentionally left blank.)

5 Security Criteria Background

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

5.1 Fundamentals

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

31 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.

32 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.

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

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

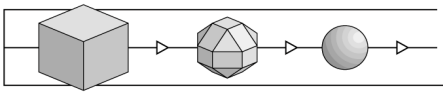
35 There are two basic questions:

- 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

36 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.



37 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.

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

39 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.

40 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."

41 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

42 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.

43 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.

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

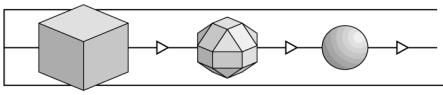
Example: The function *Identification and Authentication* can be realised by a password procedure, usage of chipcards with a challenge response scheme or by biometrical algorithms.

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

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

47 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.“

48 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.“

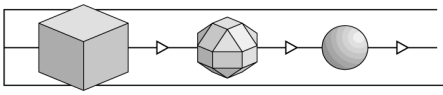
high: „For the minimum strength of a critical mechanism to be rated *high* it shall be evident that it could only be defeated by attackers possessing a high level of expertise, opportunity and resources, successful attack being judged to be beyond normal practicability."

6 Annex

6.1 Glossary

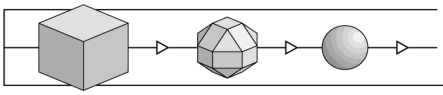
This glossary provides descriptions of the expressions used in this brochure, but does not guarantee their completeness or general validity. The term *security* here is always used in the context of information technology.

Accreditation	A process to confirm that an evaluation facility complies with the requirements stipulated by the DIN EN 45001 standard. Accreditation is performed by an *accreditation body.* Accreditations from bodies represented in the German Accreditation Council (DAR) are generally recognised.
Availability	Classical security objective: Data should always be available to authorised persons, i.e. this data should neither be made inaccessible by unauthorised persons nor be rendered unavailable due to technical defects.
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 (see also „Trust Centre“ for a second meaning).
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.
Confidentiality	Classical security objective: Data should only be accessible to authorised persons.



Confirmation Body	Body that issues security confirmations in accordance with SiG and SigV for technical components (suitability) and trust centres (implementation of security concepts)
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.
Evaluation	Assessment of an (IT) product, system or service against published IT security criteria or IT security standards.
Evaluation facility	The organisational unit which performs evaluations.
Evaluation level	Refer to „Security level“.
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	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 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).
Licence agreement	An agreement between an evaluation facility and a certification body specifying procedures and responsibilities for evaluation and certification.
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 ID	ID designating a certification or confirmation process within debisZERT.
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	Many security criteria (e.g. ITSEC, CC) define a metric 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 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.
Trust centre	A centre which confirms the relationship between signature keys and persons by means of electronic certificates - such a centre is termed „certification body“ in the Digital Signature Act.
ZKA criteria	Security criteria used by the central credit committee (ZKA) in Germany

6.2 References

/ A00 / Lizenzierungsschema, debisZERT, Version 1.1, 16.12.98

[Licensing Scheme]

/ ALG / Anhang zu „Bekanntmachung zur digitalen Signatur nach Signaturgesetz und Signaturverordnung vom 09.02.98 im Bundesanzeiger Nr. 31 v. 14.02.98“, http: / / www.regtp.de / Fachinfo / Digitalsign / start.htm

[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“]

/ BSIG / Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz - BSIG), BGBl. I. vom 17. Dezember 1990, Seite 2834 ff.

[Act on the Establishment of the German Information Security Agency, BGBl. I. from 17th December 1990, Page 2834]

/ CC / Common Criteria for Information Technology Security Evaluation, CCIB-98-026, CCIB-98-027, CCIB-98-027A, CCIB-98-028, Version 2.0, Mai 1998

/ EBA / Kriterien für die sicherheitstechnische Bewertung und Konstruktion von CIR-Netzkomponenten, Eisenbahn-Bundesamt, Version 1.0 vom 8.2.94

[Criteria for Security-Related Evaluation and Construction of CIR Network Components, Federal Railway Office, version 1.0 from 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

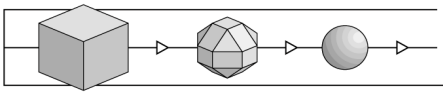
/ IuKDG / Gesetz zur Regelung der Rahmenbedingungen für Informations- and Kommunikationsdienste (Informations- and Kommunikationsdienste-Gesetz - IuKDG), BGBl. I. vom 28. Juli 1997, Seite 1872 ff.

[Information and Communication Services Act, BGBl. I. from 28th July 1997, Page 1872]

/ JIL / Joint Interpretation Library, Version 1.04, December 1997

/ Mkat12 / Maßnahmenkatalog nach §12 Abs. 2, Regulierungsbehörde für Telekommunikation und Post,
http: / / www.RegTp.de / Fachinfo / Digitalsign / start.htm

[Catalogue of Security Measures in accordance with §12 Abs. 2, Regulatory Authority for Telecommunications and Posts]



/Mkat16/ Maßnahmenkatalog nach §16 Abs. 6, Regulierungsbehörde für Telekommunikation und Post, http://www.RegTp.de/Fachinfo/Digitalsign/start.htm

[Catalogue of Security Measures in accordance with §16 Abs. 6, Regulatory Authority for Telecommunications and Posts]

/SigG/ Article 3 of /IuKDG/

/SIGNST/ SafeGuard Sign&Crypt Evaluation Documentation / SafeGuard Sign&Crypt / Security Target, debisZERT-DSZ-ITSEC-04007, Utimaco Safeware AG, Version 2.2, 03-03-1999.

/SIGV/ Verordnung zur digitalen Signatur (Signaturverordnung - SigV), BGBl. I. vom 27.10.1997, Seite 2498 ff.

[Digital Signature Ordinance, BGBl. I. from 27th October 1997, Page 2498 ff.]

/TKG/ Telekommunikationsgesetz (TKG), BGBl. I. vom 25.7.1996, Seite 1120

[Telecommunications Act, BGBl. I. from 25.7.1996, Page 1120]

/V01/ Certificates in accordance with ITSEC/CC, Service type 1, debisZERT, Version 1.4E, 16.12.98

/V02/ Confirmations for Products in accordance with the German Digital Signature Act, Service type 2, debisZERT, Version 1.4E, 16.12.98

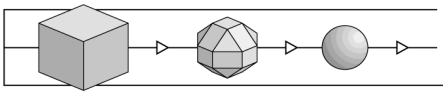
/V04/ Certificates recognised by the BSI, Service type 4, debisZERT, Version 1.4E, 16.12.98

/Z01/ Certification Scheme, debis IT Security Services, Version 1.4E, 16.12.98

/Z02/ Certified IT Products, Systems and Services, debisZERT, Version 1.1E dated 16.12.98 (consecutively numbered issues)

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
CLEF	Commercially licenced evaluation facility (under debisZERT) (cf. ITSEF)
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 Telekommmunikationstechnik [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	IT Security Evaluation Criteria
ITSEF	IT Security Evaluation Facility
ITSEM	IT Security Evaluation Manual
IuKDG	German Information and Communication Services Act
LG	Management Board
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]
ZL	Head of the Certification Body
ZZ	Person in charge of a certification procedure (responsible certifier)



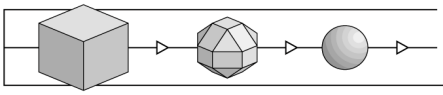
7 Re-Certification

49 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.

50 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.

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

52 The annexes are numbered consecutively.



End of initial version of the certification report.