debis

Services by DaimlerChrysler

Certification Report

SafeGuard® Sign&Crypt, Version 2.0

Utimaco Safeware AG

debisZERT-DSZ-ITSEC-04007-1999

debis IT Security Services

The Modern Service Provider

Preface

The product[1] SafeGuard® Sign&Crypt, 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:	Intended Signature Creation (including secure Viewer component), Intended Signature Verification, Symmetric Data Encryption / Decryption
Assurance Level:	**E2**
Strength of Mechanisms:	all mechanism at least: **medium** mechanisms for the Signature functions (i.e. hash functions SHA-1 und RIPEMD-160, asymmetric cryptography): **high**

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

✉	debis IT Security Services	☎	+49-228-9841-110
	- Certification Body -	Fax:	+49-228-9841-60
	Rabinstr. 8	Email:	debiszert@itsec-debis.de
	D-53111 Bonn	WWW:	www.itsec-debis.de
	Germany		

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

Bonn, 12.04.1999

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

[1] Information about the validity of the Registered Trademark can be obtained from the sponsor. In the following certification report the trademark sign is omitted.

(This page is intentionally left blank.)

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	17.02.99	Preversion (based on template report 1.4)
1.0	12.04.99	Initial release (based on template report 1.4)

Contents

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 Prüflabor für IT-Sicherheit der Industrieanlagen-Betriebsgesellschaft mbH and completed on 15.03.1999.

3 The evaluation has been performed against the Information Technology Security Evaluation Criteria (ITSEC) and 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, 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 statement 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, Version 2.0 when establishing an adequate security level.

10 The certification report contains pages 1 to 46. 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-04007-1999.

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.[2]

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.

[2] 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.

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[3] <SM1>, <SM2>, <SM3> und <SM4> are critical mechanisms.

- The mechanisms for <SM1>, <SM2>, <SM3> (and <SM5>) are of type A, the mechanism for <SM4> is of type B. The mechanisms of type A have a minimal strength given by the level *medium*. The mechanisms for the signature functions (i.e. hash functions SHA-1 and RIPEMD-160, asymmetric cryptography) have the strength *high*.

2.3 Further Remarks

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

23 The evaluation facility has formulated the following requirement to the user: The evaluation result is based on the assumption that the user strictly follows the requirements in the SafeGuard Sign&Crypt „Handbuchergänzung“ [User Manual Addendum] and operates the TOE under the restrictions formulated in the Security Target section 3.1.3.

[3] Cf. chapter 3.4 of the Security Target.

3 Security Target

24 The Security Target, version 2.2 dated 03.03.99, 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 <u>not</u> 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 Product Rationale

3.1.1 Definition of Target of Evaluation

The Target of Evaluation (TOE) is defined as the following product: SafeGuard Sign&Crypt Version 2.0.

It consists of the following product items:

- SafeGuard Sign&Crypt software,
- CardMan smartcard reading interface unit, which can be alternatively
  - CardMan smartcard reader unit for the serial port or
  - CardMan Compact smartcard reader unit for the serial port or
  - CardMan Mobile PC-Card (PCMCIA) smartcard reader or
  - CardMan Keyboard,
- SafeGuard Sign&Crypt User's Manual (printed document).

The TOE supports the following operating system platforms

- Microsoft Windows 95 and
- 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 the TOE 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.

3.1.2 Description of Target of Evaluation and Intended Method of Use

Overview

SafeGuard Sign&Crypt is a product, which allows the creation and verification of digital signatures and the generation and display of a unique document view[4]. These functions are compliant to the German Digital Signature Act and German Digital Signature Ordinance.

Additionally to the legal requirements, transferred information can be secured against access by unauthorized persons.

Thus, the TOE assures the authenticity, integrity, confidentiality and non-repudiation of signed information, which is transferred from an originator to a receiver.

The TOE reaches this goal by creating digital signatures for the information using an asymmetric key system and encrypting the information using a symmetric encryption algorithm.

General Requirements for a Signature System

A signature system achieves the electronic signature of a document.

A signature system is mainly working with a hash function in combination with an asymmetric encryption algorithm. For each member of the signature group a pair of keys is generated: a secret and a public key. The encryption algorithm works in that way, that only data signed with the secret key can be correctly verified with the according public key, while any changes to either key or data causes the signature verification to fail. Important is the fact, that the secret key can not be derived from the knowledge of the public key.

The signature system uses the secret key to sign a significant hash value over the document and adds this signed value to the document. Any receiver with the knowledge of the public key of the document's originator is able to verify the hash value and to compare it with the contents of the received document. Thus he is able to verify the integrity and the authenticity of the document, while the originator can not deny that he signed the document (non-repudiation of the origin).

Key Management

For the use of SafeGuard Sign&Crypt, it is supposed that the key management for the asymmetric encryption is performed by a certification authority (CA), also called a

[4] Viewer Component of SafeGuard Sign&Crypt: International patent pending.

"Trust Center". Each member of a signature group is assigned with a unique identifier. The certification authority distributes to each member of the signature group an individual secret key. The key is stored on a smartcard to reduce the possibilities of misuse to a minimum. The owner of the smartcard uses a PIN for authenticating himself to the smartcard. The secret key is written to the smartcard by the certification authority and is never leaving this smartcard.

The smartcard also contains keys of the certification authority itself, which are used to create certificates which prove, that the originator of a signature has been authorized by that special certification authority. Such a certificate is added to a signed document and can be verified with the certification authority keys at the receiver's side.

The members' identifiers and their public keys are distributed by the Trust Center by means of data transfer (by download, floppy disks etc.). These keys are used for the encryption of session keys, when transferred documents are additionally encrypted.

Using the administration component of SafeGuard Sign&Crypt, these keys and identifiers can be imported into a local database of SafeGuard Sign&Crypt, where they can be looked up during the operation of SafeGuard Sign&Crypt.

Message Protocols

The output data created by SafeGuard Sign&Crypt after signing any information has the format of a message defined by a selected transmission protocol. SafeGuard Sign&Crypt currently supports three protocols:

- CMT Version 1.4 (a proprietary Utimaco procotol),
- S / MIME and
- MailTrusT (MTT) Version 1.0.

All these protocols define clearly the format of the output message and they support message fields where the digital signature value can be stored.

Data Formats Supported by the TOE

The TOE offers two front-ends for the document management. On the one end an originator is supported with the functions for signing and encrypting of a document. On the other hand the receiver is provided with means for the decryption and verification of a received document.

The TOE accepts two different types of input data for digital signature:

<IN1> Data File
The input is any data file, which can be opened and displayed by any application program supported by the TOE.

<IN2> Open Document
The contents of an actual document, which is open in one of the application programs supported by the TOE.

The TOE supports two formats of output data after signature of a document:

<OUT1> Signed Viewer Representation
The output data is the binary data of the displayed representation of the document generated by a special viewer. The output data is extended by the digital signature over the viewer data, by a certificate of the originator and by additional information according to the selected protocol.

<OUT2> Signed Original File and Viewer Representation
When the input data is a file (<IN1>), the output data can consist of two parts: one is the same output as generated by <OUT1>, the other is the original file contents, extended by a digital signature, a certificate of the originator and additional information according to the selected protocol. At the receiver's site the additional information including the signature can be removed after the verification of the document, so that the original file contents can be restored.

In both cases in a second step the output data can be compressed and / or encrypted. After this processing the data is stored as one or two files on the file system or forwarded by a mail system to the receiver. For that combination of signing, optional compressing and optional encrypting, the term "sealing" is used throughout this document ("unsealing" is used for the reverse process).

Method <OUT2> can only be combined with input type <IN1>, whereas method <OUT1> can be used with <IN1> and <IN2>. For each single case the user can select, if he wants to use method <OUT1> or <OUT2> (if applicable).

Method <OUT2> has the advantage, that the data can be electronically processed by a receiver; method <OUT1> has the advantage, that the application program, which generated the document, must not necessarily be installed at the receiver's site.

However, all combinations are identical in their security enforcing functions.

General Description of Data Flow

To process a document by the TOE, it has to go through the following steps:

1. The document is created with one of the application programs supported by SafeGuard Sign&Crypt.
   Either it is stored as a file on the file system and SafeGuard Sign&Crypt is called with the help of the file manager (Explorer) or Safe Guard Sign&Crypt is directly started from within the application program (only for <OUT1>).

2. The document is displayed using the viewer of SafeGuard Sign&Crypt. The output of the viewer is a bitmap image.

3. The digital signature is created. For this task, the personal smartcard of the originator has to be inserted into the smartcard reader and the PIN of the card has to be entered by the user.
   For method <OUT1> one signature over the binary data of the viewer output is created.
   For method <OUT2> additionally a signature over the binary contents of the original file is created.
   The signature, a certificate with an identifier and the public key of the originator and different other information according to the selected protocol are added to the input data (the file rsp. the viewer output).
   In the following the term "document" is used for the original file (for <IN1>) or the binary data created and displayed by the viewer (for <IN2>).

4. If it is supported by the selected protocol and if it is desired, the document data (without the signature and the certificate) can be compressed.

5. If desired, the document can be encrypted. For this task, the public keys of the receivers must be known by SafeGuard Sign&Crypt. The receivers of the document can be selected by the user. The document will then be encrypted and the encryption key will be added to the document, encrypted with the public key of each receiver.

6. The document is transferred to the receiver(s) by any means of data exchange (electronic mail, file upload, on data media etc.).

7. The receiver can decrypt, decompress and verify the document. If the document is encrypted and the receiver is one of the intended receivers, the document can be decrypted by using his secret key. For that task, the receiver has to use his personal smartcard and to enter the PIN of the card.

8. The document can be verified by the receiver. The TOE on the receiver side proves the certificate in the document against a key stored on the smartcard of the receiver and gets the public key of the originator. With the knowledge of the public key, the receiver can verify the signature of the document.
   When using method <OUT1>, the bitmap image can be displayed using the SafeGuard Sign&Crypt viewer and the signature over the image data can be verified.
   When using method <OUT2>, the bitmap image can be displayed using the SafeGuard Sign&Crypt viewer and additionally the sealed original file can be verified and extracted by the receiver.

The following sections describe in detail the single steps of this process and give additional information on each step.

Document Viewing

Input (in the format <IN1>) for SafeGuard Sign&Crypt can be all files, which are created by a supported application program or which are in the format of a data file of these application programs. The supported application programs are

- Microsoft Word 95 (= Word for Windows 7.0), Word 97,
- Microsoft Exchange and
- Microsoft Outlook.

Another input (in the format <IN2>) can be the actual contents of a document loaded within one of the application programs listed above or within

- any application program, which supports the standard Windows print interface.

Such files or actual data contents will be called "documents" throughout the following sections, "contents" always means the binary contents of these files or data.

The SafeGuard Sign&Crypt viewer is a method to generate and display a unique bitmap image of each document. The viewer consists of two sub-components: a printer driver and a display component.

In a first step, the document is converted into a unique pixel-oriented bitmap image. This is done by the special printer driver which is part of the viewer.

The image created by the printer driver depends on

- the contents of the original document (text, numbers, graphics),
- the display options of the original document (font size, colors) and
- the fonts installed on the system (font images).

In a second step the resulting bitmap image is displayed by the display component on the user's screen. The display component allows zooming and scrolling the entire document, but not modifying the bitmap image contents.

Different instances of the display component are working on the originator's side, when displaying a document for signing, and on the receiver's side, when displaying a correctly verified document.

Document Signing

When the originator is ready to sign a document, he opens the document in the viewer. This can be done by explicitly opening the viewer or, when using a supported application program, by pressing a special button for the activation of the viewer. These buttons are added to the application programs during installation of SafeGuard Sign&Crypt. In the viewer the user can determine whether to use output method <OUT1> or <OUT2> (if applicable) and whether to send the signed document concurrently with electronic mail. To start the process of signature, a special button must be pressed. Then the originator is prompted to insert his smartcard containing his secret key into the smartcard reader and he is prompted to enter his PIN for the smartcard. The PIN is verified on the smartcard.

If the PIN is correct, SafeGuard Sign&Crypt calculates a hash value over the binary contents of the document and over the viewer output data (method <OUT2>) or only on the viewer output data (method <OUT1>). The result(s) of the hash function is / are encrypted with the secret key of the originator. This encryption is performed in the smartcard.

The encrypted hash values are called the signatures; for method <OUT2> two signatures, for method <OUT1> only one signature is created. Also a certificate identifying the originator and containing his public key is added to the document encrypted by a key of the certification authority.

SafeGuard Sign&Crypt then displays the correct completion of the signature process of the document to the user.

If the selected protocol supports compression, the user can select to compress the document for lower transmission costs. In this case the compression of the document contents is performed after the signature. The option for compression has to be selected before the sealing process has been started (compression is only supported under CMT Version 1.4 protocol).

Document Encryption

If the originator wants to keep the document confidential, he can direct SafeGuard Sign&Crypt to encrypt the document. This option has to be selected before the sealing process has been started. For the encryption function the name(s) of the receiver(s) has / have to be selected. His / her (their) public key(s) must be present in a local database.

When encryption is selected the document is encrypted using a symmetrical 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, certificate(s) of the receiver(s) must be present in the database of the originator's system, from which the public keys can be retrieved. The validity of the certificates is checked against the key of the CA on the smartcard and, if any of the certificates is not valid, the encryption is not performed.

The document is now ready for transfer to the receiver(s). Transferring the document is not within the scope of SafeGuard Sign&Crypt.

Document Decryption

When the document is received and it is encrypted, it has to be decrypted first. For this task, the receiver has to provide his secret key on his smartcard (using the same procedure as described in section "Document Signing"). The encrypted session key is taken from the document and decrypted on the smartcard. This key is then used to decrypt the data part of the document (including the signature(s)).

If the document is compressed, it has to be decompressed afterwards.

This works identically for viewer outputs as well as for signed original files.

Document Verification

After decryption (if the document is encrypted) the signature is going to be verified.

To verify a received document, the receiver is first requested to insert his smartcard into the reader and to enter his PIN for the smartcard before the operation is continued. This is required to verify the certificate of the originator contained in the document. With this step the public key of the originator is retrieved from the certificate.

When the certificate has been proved, the signed hash value is verified with the public key. On the other hand, a hash value is calculated over the binary contents of the received document using the same hash function. The decrypted received hash value and the locally calculated hash value are compared.

If the values are identical, SafeGuard Sign&Crypt informs the user with a message on the screen about the originator of the document and about the correct signature in the document.

This works identically for viewer outputs as well as for signed original files.

When the received document is a viewer output bitmap data, the viewer displays that data on the screen. The indication of the correct signature is done with the document display in the background.

When the received document is a signed original file, only the verification window is displayed. Then the original file contents can be extracted from the received data and stored as an application data file at the receiver's site.

If the certificate of the originator can not be verified or if the hash values are not identical, the user is informed about that fact and the viewer does not display the contents of the document.

Product Installation and Usage

SafeGuard Sign&Crypt is installed with an installation program from floppy disks. The installation program prompts for different options like

- Program binaries' path,
- Key database path,
- Selected transmission protocol,
- Application programs, where SafeGuard Sign&Crypt should be integrated, and
- Smartcard reader type.

The rest of the installation is fully automatic.

The usage of SafeGuard Sign&Crypt is intuitive. The sealing or unsealing of documents can be started in different ways:

- Selecting the file to be signed or verified and opening it with the "Digital Signature" icon on the desktop (e.g. by dragging the file there or sending it there using the context menu of "Explorer"). This works only for specially supported application programs.
- Calling SafeGuard Sign&Crypt from one of the supported application programs (Word, Exchange, Outlook) and signing the actually open document or opening a received document. This start is done by an additional menu item or button, which has been added to the application program during installation.
- Starting the SafeGuard Sign&Crypt application program from the start menu of the operating system. The application program enables to sign more than one document after authenticating once at the smartcard.
- Calling SafeGuard Sign&Crypt by printing the document to the printer driver "Digital Signature". This works for all application programs which support the standard Windows print interface.

For the signature of a document, the options for compression and encryption can be selected. The user can also decide, if to use method <OUT1> or method <OUT2> (if applicable) and if to seal a document only as a file on disk or concurrently to send it by electronic mail.

A tool is included into the TOE, which can be used to check the integrity of the binary files of the installed TOE at any time.

Administration Functions

The administration of SafeGuard Sign&Crypt mainly comprises the following functions:

- a function to change the user's PIN of the smartcard and
- a function to add or delete identifiers and corresponding certificates (with public keys) in the internal database of the system.

The selection of algorithms and protocols can be changed by modifying a configuration file for the TOE. This shall be done only by selected administrators.

3.1.3 Intended Environment

Hardware Requirements

The TOE runs on standard personal computers with a microprocessor compatible to Intel Pentium (60 MHz) and above. 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 Mobild no free serial port is required, but one of the four available serial port connections should be free.

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

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 or
- 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)

Software Requirements

The TOE is proved to work under the following operating systems:

- Windows 95 and
- Windows NT 4.0 Workstation and Server.

The TOE supports documents created by the following application programs:

- Microsoft Word 95 (=Word for Windows Version 7.0) and Microsoft Word 97,
- Microsoft Exchange Version 4.0 for Windows 95 and Windows NT,
- Microsoft Outlook for Windows 95 and Windows NT and
- all application programs with a standard Windows print interface.

Environment Assumptions

For the secure operation of the TOE, the security of the environment responsible for key generation and storage is assumed. This includes the following assumptions:

- The certification authority guarantees the confidentiality of the secret keys during generation and distribution and is certified for that process.
- The used smartcard and its operating system are certified for keeping the stored keys secret.
- The secret keys shall not be subject to disclosure in any environment.
- The operating system of the used smartcard is certified for processing the asymmectric encryption algorithms (RSA) correctly.

- The length of the smartcard PIN is defined appropriately (6 digits or more).
- The smartcard is locked for the user after an applicable amount of erraneous entries of the PIN (suggested: 3 entries)

The fulfillment of these requirements is within the responsibility of the certification authority.

For the certified use of the TOE, the user shall not trust a certification authority, which does not fulfill the above requirements.

Special Measures

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

Secure Environment

The workstation has to be secured against access of unauthorised users by

- separating the workstation into a room, where only authorised users have access to
  and / or
- using a secure environment, where a security functionality comprising secure user identification and authentication is provided by a certified security system. (Examples for such an environment are Windows 95 together with SafeGuard Easy for Windows 95 resp. Windows NT Workstation 4.0 together with SafeGuard Easy for Windows NT).
  In that environment, the usage of the TOE has to be restricted to those users who are designated to be originators or receivers of signed documents in the scope of the TOE.

Secure Operation

The TOE has to be installed and operated in a way, that the following options and parameters are selected:

- Hash generation with MD5, RIPEMD-160 or SHA-1 (depending on the selected protocol),

Note: MD5 is not a valid selection for the requirements of the German Digital Signature Act (see section 1261896.1259320.108850540).

- Encryption with DES, Triple DES or IDEA (depending on the selected protocol),
- CardMan support selected,
- secret keys only provided on smartcards,

- Document encryption selected for each document.

User Advices

When the TOE is installed on a workstation, which is connected to an external network (e.g. Internet), the users have to be advised

- to pay attention to the integrity of the TOE and its environment, especially:

- not to run network applications (Internet browser etc.) simultaneously with the TOE and

- to check the integrity of the TOE (with the provided integrity check tool), when one of the components of the TOE is intended to be used after any connection to external networks had been established between now and the last integrity check.

Additionally the users of the TOE have to be advised

- not to install untrustworthy software on the workstation where the TOE is installed,

- to keep their smartcard PIN secret,

- not to trust a certificate, if it cannot be verified by the TOE with the use of the CA's public key on the smartcard,

- not to change the configuration of the TOE and

- to keep the option "Encrypt" on during the operation of the TOE.

Organisational Measures

The persons, which are authorised to install and administer SafeGuard Sign&Crypt shall be selected carefully and shall be highly trustable.

3.1.4 Subjects, Objects and Actions

General

In the definitions below, "document" is a set of connected data, normally a file, which is transferred from an originator to one or more receiver(s).

Two forms of the document, the original data and the visualisation generated by the viewer are considered herein.

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

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.

Objects

<O1> Visualisation of a document. The original document is a data file generated by one of the supported application programs or a document loaded in the memory of one of the supported application programs, the visualisation is the binary image of this document, generated by the TOE's viewer.

Actions

<A1> Viewing and signing a document.

<A2> Viewing a document and verifying the document's signature.

<A3> Modifying a document's contents.

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

3.1.5 Security Objective and Assumed Threats

Security Objective

The TOE is designed to 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.

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 view 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 view of the document, which is viewed to him and which is indicated to contain a correctly verified signature of that originator.

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

With the given assumptions the TOE is able to avert the assumed threats listed below:

Assumed Threats

<T1> Attack against Data Integrity

The document <O1> which has been viewed and 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>.

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 in the displayed version.

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, the threats listed above together with the correct implementation of the viewer and with the Ease of Use implementation of the TOE avert the threats to be considered by the German Digital Signature Act.

To operate the TOE in compliance with the German Digital Signature Act the following additional restrictions for the use of the TOE and additional requirements for the environment have to be fulfilled:

- The certification authority operates in a way compliant to the claims of the German Digital Signature Act and has an operational licence by the Regulatory Authority for Telecommunications and Posts.
- The used smartcards are compliant to the requirements of the German Digital Signature Act and a corresponding security confirmation has been issued.
- 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 uses the RSA on smartcard with a minimum of 768 bit key length for signature generation.

- The user is instructed to use the viewer whenever creating a digital signature.

3.2 Security Enforcing and Security Relevant Functions

3.2.1 <SF1> Intended Signature Creation

The signature is created over the binary contents of a document.

Two basic methods of document transfer imply signature generation over different data:

- Method <OUT1>
  A signature is only created for the binary image data generated by the viewer out of the document contents.

- Method <OUT2>
  A signature is created for the binary contents of the document and another signature is created for the binary image data generated by the viewer out of the document contents.

Signatures are always created by calculating a hash value over the according data and signing the hash value with the secret key of the originator stored on a smartcard 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.

The creation of the signature(s) is an explicit act of will: the user must explicitly start the creation of the signature(s).

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

3.2.2 <SF2> Intended Signature Verification

A document including a 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 if the document is authentic and unchanged (hash values are identical).

The verification is only performed with the explicit confirmation of the user.

The correct verification of a received document is displayed simultaneously with the display of the contents of the document by the viewer.

The identity of the originator of a document and his public key are retrieved from the certificate included in the document.

3.2.3 <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.

3.2.4 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>			

3.3 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.

3.3.1 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 3.1.3 is **medium**.

The claimed rating of the strength of the major mechanisms <SM1> and <SM2> (see Appendix A) is **high**. This claim is required for the compliance to the German Digital Signature Act.

3.3.2 Target Evaluation Level

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

3.4 Appendix A: Security Mechanisms

The following sections give an overview on the security mechanisms for SafeGuard Sign&Crypt. A detailed description of the security mechanisms will be part of the Architectural and Detailed Design document.

3.4.1 A.1 <SM1> Hash Function

For the generation of a hash value over the contents or / and the binary image of a document, the following algorithms are implemented:

- SHA-1,
- MD-5 (default for S / MIME and MailTrusT) and
- RIPEMD-160 (with ISO 9796 padding).

For information only: additional algorithms are implemented, but their use is not within the scope of certified operation:

- DESMAC,
- NVB and
- MDC2.

3.4.2 A.2 <SM2> Asymmetric Encryption Algorithm

For the asymmetric encryption tasks (encrypting with secret key, decrypting with public key, encrypting with public key, decrypting with secret key) the standard RSA algorithm with a minimum of 768 bit key length is used.

The asymmetric encryption algorithm implemented in the TOE is only applied, when a public key is involved. When a secret key is involved, the implementation of the asymmetric encryption algorithm on the smartcard is used by the TOE.

3.4.3 A.3 <SM3> Symmetric Encryption Algorithm

For the symmetric encryption / decryption of the document the following standard algorithms are implemented in the TOE:

- DES (CBC, 16 rounds, key size 56 bits),

- TRIPLE DES (3x16 rounds CBC with 2 different keys where Key1 = Key3) and
- IDEA (CBC, key size 128 bits)

For information only: an additional algorithm is implemented, but its use is not within the scope of the certified operation:

- SAFER.

3.4.4 A.4 <SM4> Document Generation Protocol

The finally transferred and received document consists of the raw data and of additional information.

This additional information includes

- a certificate of the originator,
- the document signature (encrypted hash value),
- the session key for the document encryption encrypted for each receiver and
- additional protocol-specific data.

For the data compression/decompression (CMT 1.4 protocol only) the following algorithms may be used:

- LZSS and
- ZLIB.

3.4.5 A.5 <SM5> Program Integrity Check

The integrity of the program files can be checked at any time with a separate tool. This tool calculates a hash value over the installed binary files of SafeGuard Sign&Crypt and compares it to a reference hash value, which is calculated after the installation of SafeGuard Sign&Crypt and stored in the Windows registry. For the calculation of the hash value the SHA-1 algorithm is used.

3.4.6 A.6 Relation between Security Functions and Security Mechanisms

The following table gives an overview, which security functions "<SFx>" are implemented by which security mechanisms "<SMx>".

Where more than one mechanism is listed for a function, all mechanisms together implement the function.

	<SF1>	<SF2>	<SF3>

<SM1>			
<SM2>			
<SM3>			
<SM4>			
<SM5>	u		

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 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.
- Result of an accreditation procedure.

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/

/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)

(This page is intentionally left blank.)

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.