debis

Services by DaimlerChrysler

Certification Report

Central Security Module (SM-Z)
in the N.I.K.E. System of
Deutsche Telekom AG

Siemens AG

debisZERT-DSZ-ITSEC-04012-1998

debis IT Security Services

The Modern Service Provider

Preface

The product *Central Security Module (SM-Z) in the N.I.K.E. System of Deutsche Telekom AG* supplied by Siemens AG has been evaluated against the ITSEC. 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:	Identification and Authentication, Encryption, MAC Security, Access Control
Assurance Level:	E3
Strength of Mechanisms:	high

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

✉ debis IT Security Services
- Certification Body -
Rabinstr. 8
D-53111 Bonn
Germany

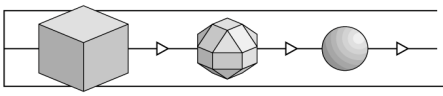
✆ +49-228-9841-110
Fax: +49-228-9841-60
Email: debiszert@itsec-debis.de
WWW: www.itsec-debis.de

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

Bonn, 8.12.1998

Dr. Heinrich Kersten

Head of the Certification Body

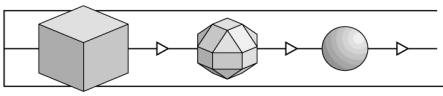


Revision List

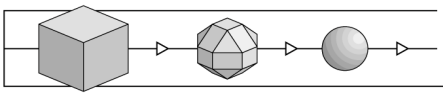
The following revision list shows the history of this certification report.

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

Revision	Date	Activity
0.9	01.04.98	Preversion (based on template report 1.1)
1.0	07.09.98	First issue (based on template report 1.3)
1.1	18.09.98	correction to the sponsor's name, modified delivery procedure
1.2	08.12.98	correction to the sponsor's name, security target is part of the operational documentation (version based on template report 1.4) - published version -



Contents



1 Introduction

1.1 Evaluation

1 The evaluation was sponsored by Siemens AG, Bürgermeister-Ulrich-Straße 100, 86199 Augsburg.

2 The evaluation was carried out by the evaluation facility Prüfstelle für IT-Sicherheit of debis IT Security Services and completed on 18.9.98. Due to modifications concerning some procedural and documentative aspects (cf. Revision List), a reevaluation as to these aspects was performed and completed on 3.12.98.

3 The evaluation has been performed against the ITSEC and 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 Telekommunikationstechnik (DEKITZ) under DAR Registration Number DIT-ZE-005/98-00.

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

/Z01/ Certification Scheme

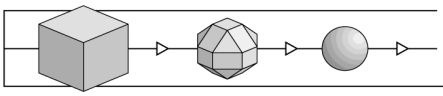
/V04/ Certificates recognised by the BSI

1.3 Certification Report

6 The certification report states the outcome of the evaluation of the *Central Security Module (SM-Z) in the N.I.K.E. System of the Deutsche Telekom AG* - referenced as TOE = Target of Evaluation in this report.

7 The certification report is only valid for the specified version 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 SM-Z when establishing an adequate security level.

10 The certification report contains pages 1 to 50. 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-04012-1998 (dated 1.12.1998).

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

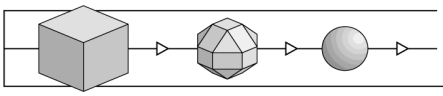
---

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

method of use, the assumed threats, the operational environment and the evaluated configurations are essential for the user.

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

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 **E3** according to ITSEC, i.e. all requirements at this assurance level as to correctness and effectiveness are met:

  ITSEC E3.1 to E3.37 for the correctness phases

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

  Construction - The Development Environment (Configuration Control, Programming Languages and Compiler, Developers Security),

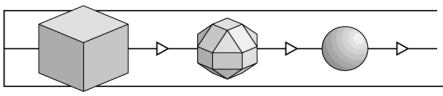
  Operation - The Operational Documentation (User Documentation, Administration Documentation)

  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).



- All mechanisms of the TOE are critical mechanisms. The minimal strength of mechanisms for mechanisms of type A is **high**. The mechanism of SF2 (encryption) was evaluated, but its strength remains unrated due to the specific conditions of this evaluation (cf. section 1.4, para 15).

  For mechanisms of type B no rating of strength is specified in accordance with ITSEM. But even if an attack potential according to level „high“ is considered in the vulnerability analysis phase, no exploitable vulnerability was detected in the assumed environment.

2.3 Further Remarks

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

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

3 Security Target

3.1 Product Description

3.1.1 General Information

The Deutsche Telekom AG intends to introduce a new system designated N.I.K.E. (New Infrastructure for Cards and Card-Related Terminal Devices) and providing electronic-cash services at public and semi-public telephones as well as generically related terminal devices (EG) using chip cards as a basis. The following security components are planned here (refer to Figure 1):

- EG with integrated IKL (intelligent card reader):
  The terminal device allows the use of the corresponding telecommunications services. Firstly, it co-ordinates and controls communications with the background system (HiGruSys); secondly, it uses the obtained IKL to read and process the user's chip card. The IKL chip card is equipped with a security module (SM-K) for storing cryptographic keys and executing cryptographic functions.

- HiGruSys with SecServ (Security Server):
  The background system realises central functions within the N.I.K.E. system. These functions include data storage, administration as well as the distribution of data to the individual terminal devices. It contains a Security Server with an integrated security module SM-Z, which is used to store sensitive data and to support cryptographically protected communications with the terminal devices.

- SD (Secure Device):
  The N.I.K.E. system plans a *Cross-Border-Use* of telephone cards (Eurochip cards) with other card providers (MoU partners). The Secure Device is employed here for a safe exchange of user keys. For the purpose of transport, the encrypted user keys are issued by the SD and written to a diskette. These user keys ultimately serve to authenticate the used chip cards and allow the safe transmission of accounting data.

- RM (Risk Management):
  The Risk Management serves to monitor the security facilities in the N.I.K.E. system. This function forwards security-related messages to a designated department or person, who can then initiate corresponding measures with the help of this function.

The *security module SM-Z* which is a component of the Security Server in the background system, represents the *target of evaluation* (TOE) and, in particular, the target of the following chapters.

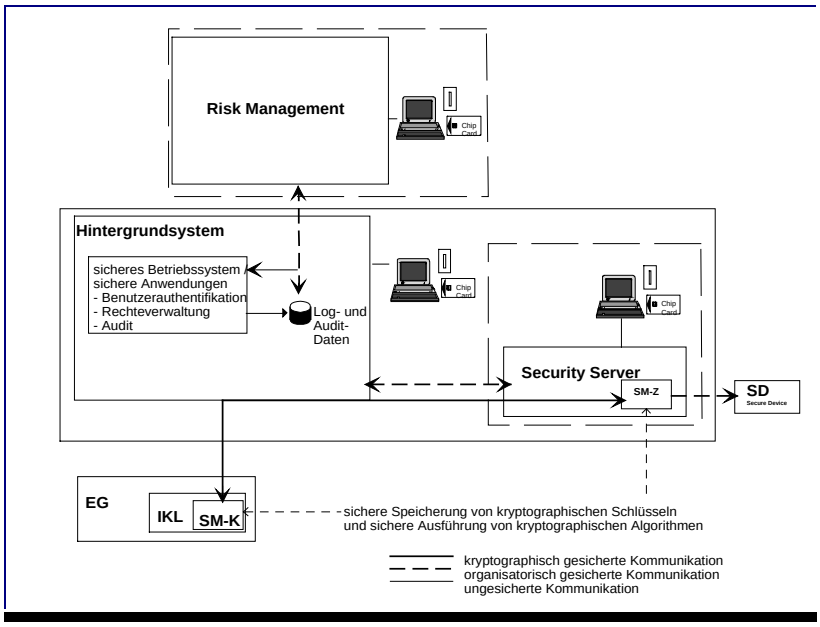


Figure 1: Schematic representation of the N.I.K.E. system[2]

3.1.2 Product Definition and Method of Use

Definition of the TOE

The TOE, designated SM-Z in the following, is the Firmware (FW) of the security module SM-Z, including the documentation intended for application programming (refer to Table 1).

The essential components of the FW are:

– Basic-FW: Mask program of the PROVE (processor for encryption and decryption)

– Standard-FW: Implementation of general functionality

– FW for the ADMIN key system: Implementation of functions used by SKM.

– FW for the ISO7816 key system: Implementation of functions used by the background system (HiGruSys).

---

2 Hintergrundsystem = Background System; sicheres Betriebssystem= secure Operating System; sichere Anwendungen = secure applications; Benutzerauthentifikation = user authentication; Rechteverwaltung = administration of rights; sichere Speicherung .... = secure storage of cryptographic keys and secure exeecution of cryptographic algorithms; kryptographisch gesicherte Kommunikation = cryptographically protected communication; organisatorisch gesicherte Kommunikation = communication protected by organisational measures; ungesicherte Kommunikation = unprotected communication

Type	Designation	Version
Hardware-Modul: Basis-FW & Standard-FW & Schlüsselsystem ADMIN & Schlüsselsystem ISO7816 [Hardware module: Basic-FW & Standard-FW & key system ADMIN & key system ISO7816]	SICRYPT Security Modul 7, Typ SM-Z	NIK 11.1 A vom 27.04.98
Dokumentation für den Anwendungsprogrammierer [Documentation for application programming] SICRYPT Hardware Software Interface [SS-HSI]	SS-HSI Allgemeiner Teil SS-HSI Anhang A SS-HSI Anhang D	V2.4 vom 11.06.96 V1.4 vom 26.11.97 V1.3 vom 26.11.97

Table 1: Components of the TOE (product scope)

Figure 2 shows the complete configuration of the SM-Z both for administrative and operative functions.

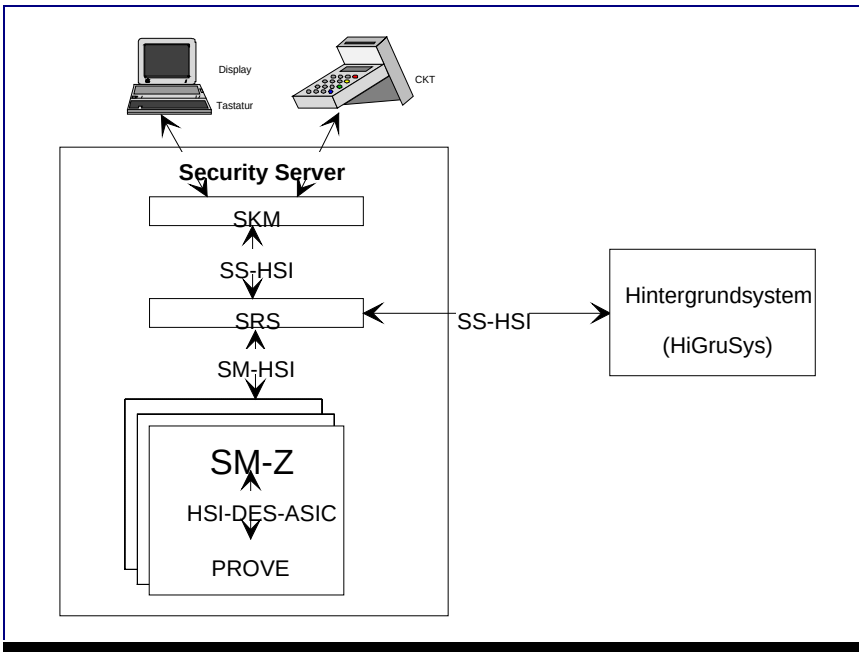
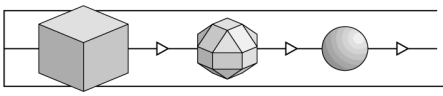


Figure 2: Schematic representation of the complete configuration of the SM-Z



Method of Use

The SM-Z is used in the background system for the confidential storage and management of data objects requiring protection (for example, keys) as well as executing actions which are based on cryptography and which make use of confidential information. This includes

– Identification and authentication of

  1. Decentral security modules (SM-K)

  2. Persons (administrators) authorised to administer the SM-Z

– Storage and management of

  3. Cryptographic keys

  4. Confidential data objects and

  5. Firmware of the decentral security modules (SM-K).

– as well as

  6. Support of confidential and integral exchange of data objects requiring protection between HiGruSys and EG or SM-K.

  7. Generation of data for initial personalization and downloading decentral security modules (SM-K).

The network operator makes use of actions 1-7.

The provider of user cards (Telekom) makes use of actions 3 and 6.

The provider of user cards (MoU-Partner) makes use of actions 3 and 6.

To allow the use of the cryptographic functions contained in SM-Z, special information must first be loaded into the hardware of the security module SM-Z:

– FW (loaded at the SM manufacturer),

– Basic keys (loaded at the SM manufacturer),

– Operating keys (KSMctl; generated or loaded at Deutsche Telekom AG)

– Application keys (KAc1 & KAc2; generated or loaded at Deutsche Telekom AG).

The generation, introduction and management of integer keys for the SM-Z takes place

– In the production environment of the manufacturer protected by organisational and construction-related measures or

– In the production environment of the Deutsche Telekom AG protected by organisational and construction-related measures.

The basic technology of the cryptographic functions and the key management of the SM-Z is supplied by the processor for encryption and decryption (PROVE) of the security module and the basic Firmware integrated as mask-ROM-Code in PROVE.

3.1.3 Operational Environment

Technical Operational Environment

The technical prerequisites for operating an SM-Z are:

– Standard PC with Pentium processor and at least 16 MB main memory / 500 MB hard disk.

– Windows NT operating system from Release 3.50 onwards.
The SS-HSI (refer to Figure 2) is supplied on the *'NT-TDI (transport driver interface)'*.
The SM-HSI (refer to Figure 2) is supplied on the *'NT-SCSI-Port driver interface'*.
The software component SICRYPT Server Runtime Software (SRS) in the variant N.I.K.E.
The software component SICRYPT Key Management (SKM) in the variant N.I.K.E.

– Security module-HW (SM-Z)- as a 'Tamper Resistant Device' (refer to [WD13491]).

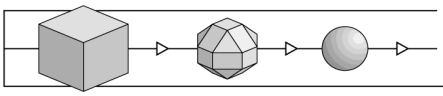
– Chip card terminal (CKT) with PIN keyboard and display (PNr. CT220 / from FW-Version 48 onwards), which is connected to a serial interface, for example, COM2 of the PC.

Administrative Operational Environment

After the security module has been produced, it is first necessary to personalise the key system, the individual HW-key, the production key (PER), the communications key (COM), the Firmware and the security module identification (SID), in order to prepare the security module for use as SM-Z in the Security Server. The SM-Z is operated in an organisationally secure environment.

For this purpose, the following organisational objectives need to be met:

ORG1: Trustworthy (personal, material, organisational) and unalterable (in the sense of an intentional manipulation) integration of the keys into the SM-Z. The **personalization** is operated in a safe environment in a room with protected access.



ORG2: Trustworthy (personal, material, organisational) key handling outside the security module.

The user and data specifications for key management of the SM-Z are performed via the following input media: Chip card, diskette, network and keyboard of the chip-card terminal (CKT).

Key BackUp

The keys stored in the SM-Z are backed up using the following technique:

A key back-up of the basic keys COM and PER, which are loaded by the SM manufacturer in the SM-Z, is present at the SM manufacturer. A back-up of the basic key HW´ is not required, as this key is generated individually during initial personalization for each SM-Z (refer to [PER-DEV] Chapter 5.6).

A key back-up of the operating and application keys stored in the SM-Z is performed with actions Act1 (read) and Act2 (write) defined in Chapter 3.1.4.3. The keys are read out of the internal key memory of the SM-Z and output in encrypted form. After that, they can be saved on any type of storage medium. When the key BackUp is read into the SM-Z, the keys are loaded in encrypted form into the SM-Z, decrypted by the SM-Z and written to the internal key memory.

3.1.4 Subjects, Objects and Actions

Subjects

Figure 3 provides a schematic representation of the subjects which are of relevance for the SM-Z (TOE). The subjects represented here, i.e. HW manufacturer, chip manufacturer, software manufacturer (Sub2) and Security Server (Sub10) are not considered in this document.

Sub1: Firmware manufacturer

Sub2: Software manufacturer

Sub3: Personalization - SM manufacturer

Sub4: Administrator – identification and authentication are performed through the presentation of a PIN

Sub5: Network operator - Deutsche Telekom

Sub6: Background system (HiGruSys)

Sub7: Provider of user cards - MoU-Partner

Sub8: Provider of user cards - Telekom

Sub9: SM-K

Sub10: Security Server

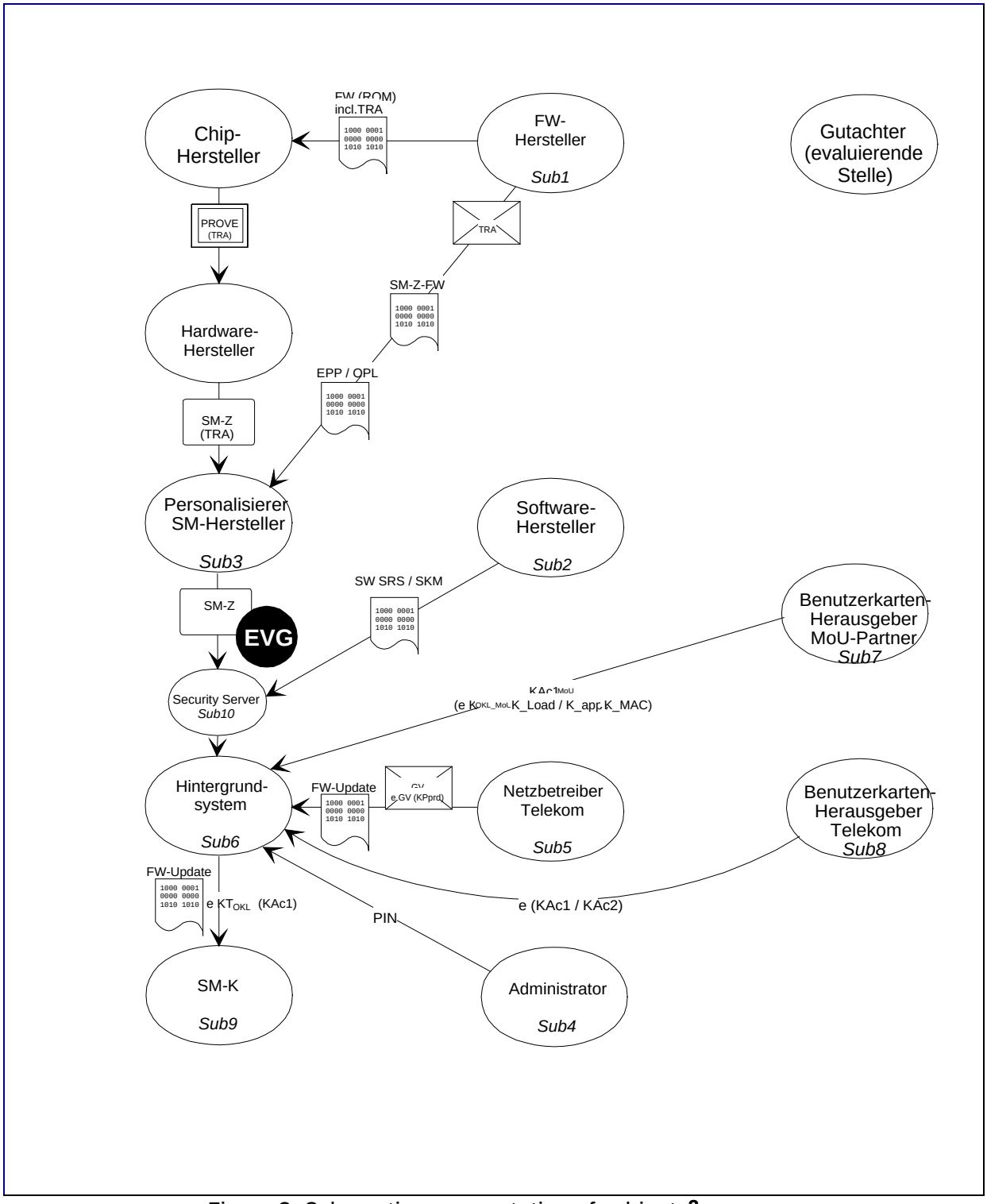
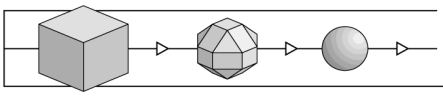


Figure 3: Schematic representation of subjects[3]

[3] Chip-/ FW-/Hardware/SM-/ Software Hersteller = Chip /FW/ Hardware/ SM / Software manufacturer; Gutachter (evaluierende Stelle) = evaluator (evaluation facility); Hintergrundsystem = Background System;



The development and production processes for an SM-Z are structured as follows:

1. The FW manufacturer develops the basic FW (ROM-Code of the PROVE), the initial personalization program (EPP), the program for loading the SM-Z-FW (OPL) and the SM-Z-FW. It transfers the ROM-Code for the PROVE to the chip manufacturer. The TRA mask key is a component of the ROM-Code.

2. The chip manufacturer produces the PROVE with the mask (program in the ROM), which corresponds to the transferred ROM-Code.

3. The FW manufacturer transfers the mask key (TRA), the signed EPP, the OPL and the SM-Z-FW to the personalization function of the SM manufacturer.

4. The personalization function of the SM manufacturer generates the PER production key.

5. The personalization function of the SM manufacturer loads the initial personalization program (EPP), using the loading routine of the PROVE, into the RAM of the SM-Z. The PROVE checks the integrity of the EPP using the mask key (TRA). If the MAC on the EPP is correct, the EPP is executed by the PROVE. Under the control of the EPP, the production key (PER), communications key (COM), individual HW-key (HW') and reference table for defining the key system are loaded consecutively. This production step is executed in the secure production environment of the SM manufacturer.

6. The personalization function of the SM manufacturer loads the program for loading the SM-Z-FW (OPL), using the loading routine of the PROVE, into the RAM of the SM-Z. The PROVE checks the integrity of the OPL using the production key (PER). If the MAC on the OPL is correct, the OPL is executed by PROVE. Under the control of the OPL, the FW of the SM-Z is loaded and its integrity is checked. This production step does not require a secure production environment. From this point in time onwards, the SM-Z represents the TOE.

7. The SW manufacturer develops the programs named SRS and SKM, and supplies them to the SM manufacturer.

8. After that, the Security Server is put together using the components designated Standard-PC, SM-Z, CKT, SRS, SKM as well as the user documentation, and supplied to the end user (in this case, Deutsche Telekom AG).

Objects

Objects requiring protection are:

Obj1: Data elements whose contents are managed by an administrator (e.g. date / time, profile, ...)

Netzbetreiber = Network Operator; Benutzerkarten-Herausgeber = Provider of User Cards

Obj2: Data elements for accounting data which are transferred securely from the SM-K to the HiGruSys.

Obj3: Data elements which are transferred confidentially from the HiGruSys to the SM-K.

Obj4: Basic keys (TRA, PER, COM, HW')

Obj5: BackUp keys (UR, ZSTR)

Obj6: Operating keys (KSMctl, KPprd)

Obj7: Keys of the provider of the user cards - Telekom (Sub8; application keys)

Obj8: Keys of the provider of the user cards - MoU-Partner (Sub7; application keys)

Obj9: Program code (FW) / SM-Z functions

Obj10: Random numbers

Actions

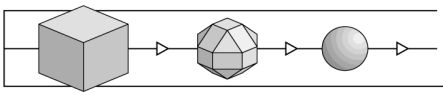
The following actions can be performed by the defined subjects on the objects requiring protection:

Act1: Read (R)

Act2: Write, delete (W)

Act3: Execute / use (E)

Act4 Generate (G)



	Sub1 (H-FW)	Sub2 / Sub 10	Sub3 (SM-Pers.)	Sub4 (Admin)	Sub5 (N-Telekom)	Sub6 (HiGruSys)	Sub7 (B-MoU)	Sub8 (B-Telekom)	Sub9 (SM-K)
Obj1 (D-Admin)	-	-	-	R / W / G	-	R	-	-	-
Obj2 (D-INT)	-	-	-	-	-	R	-	-	G
Obj3 (D-CONF)	-	-	-	-	-	G	-	-	R
Obj4 (K-Basic)	G / W	-	G / W	E	-	-	-	-	-
Obj5 (K-BackUp)	-	-	-	R[1&2&4] / W[1&2&4] / G / E	-	-	-	-	-
Obj6 (K-Operation)	-	-	-	R[1&2] / W[1&2] / E	G	E	-	-	-
Obj7 (K-Telekom)	-	-	-	R[1&2] / W[1&2]	-	R[1]	-	G	-
Obj8 (K-MoU)	-	-	-	R[1&3] / W[3]	-	R[1]	G	-	-
Obj9 (P-FW)	G	-	W / E	E	-	E	-	-	-
Obj10 (Random-N)	-	-	-	-	-	R / G	-	-	-

Table 2: Permissible actions by subjects on objects

Restrictions:

[1] encrypted in accordance with the reference table (Export / Import)
[2] unencrypted in accordance with the reference table (Export / Import)
[3] encrypted
[4] only ZSTR

For administration of the SM-Z, the following three roles are defined in subject 4:

1. The network-wide administrator (ADMIN-Net)

2. The second network-wide administrator (ADMIN-Net_x_2) for enforcing the two-person control principle

3. The local administrator (ADMIN-Local).

The ***ADMIN-Net*** has the right to generate and load the BackUp keys. These form the cryptographic basis for generating the BackUps of the operating and application keys, for whose generation and loading this administrator also possesses the rights. In addition, this administrator has the right to initialise and configure the SM-Z.

The ***ADMIN-Net_x_2*** is a network-wide administrator ***ADMIN-Net,*** who authenticates himself with his PIN after the ***ADMIN-Net*** in order to implement the two-person control principle, so that both administrators ***ADMIN-Net*** additionally receive the rights to export and import plain-text keys, which can form the basis for cryptographic communications with cooperation partners.

The ***ADMIN-Local*** has the right to generate a key BackUp key and load it again when required.

Table 3 defines additional rights for the three administrators roles (for footnotes, refer to Page 22).

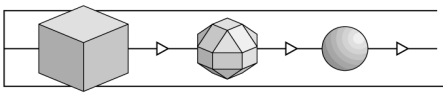
	Sub4.1 (ADMIN-Net)	**Sub4.2** (ADMIN-Net_x_2)	**Sub4.3** (ADMIN-Local)
Obj1.1 (Date / time)	R / W	R / W	R
Obj1.2 (Profile)	R / W	R / W	R
Obj4 (K-Basic)	E	E	E
Obj5 (K-BackUp)	R[1)] / W[1)] / E / G	R[1 & 2)] / W[1 & 2)] / E / G	R[1 & 4)] / W[1 & 4)] E
Obj6 (K-Operation)	R[1)] / W[1)] / E	R[1 & 2)] / W[1 & 2)] / E	R[1)] / W[1)] / E
Obj7 (K-Telekom)	R[1)] / W[1)]	R[1 & 2)] / W[1 & 2)]	R[1)] / W[1)]
Obj8 (K-MoU)	R[1)] / W[1)]	R[1 & 3)] / W[1 & 3)]	R[1)] / W[1)]
Obj9 (P-FW)	E	E	E
Obj10 (P-SW)	-	-	-

Table 3: Permissible actions by administrators on objects

Administration of the three roles in the SM-Z is performed by the identification-features function group (e.g. ADMIN-Net, ADMIN-Local) and the corresponding PIN(s).

– The network-wide administrator (ADMIN-Net) identifies himself via the function group designated ADMIN-Net and by specifying the corresponding PIN.

– The second network-wide administrator (ADMIN-Net_x_2) identifies himself by specifying the function group designated ADMIN-Net and by specifying his PIN. It is only after the entry of the second PIN that the additional rights pertaining to ADMIN-Net_x_2 become available.



– The local administrator (ADMIN-Local) identifies himself via the function group designated ADMIN-Local and by specifying the corresponding PIN.

3.1.5 Threats

The assumed threats stated in the following ultimately result from the two basic threats which IT products face: Loss of confidentiality and loss of integrity of information "managed" by this product.

The following threats are assumed:

Thr1: Unauthorised access to the data stored in the SM-Z.
Note: Access is unauthorised if the corresponding assignment designated Subject / Object / Action in Table 2 is not marked.

Thr2: Unrecognised manipulation of data requiring protection (Obj1 and Obj2) and disclosure of confidential data (Obj3) on the transmission route to/from HiGruSys.

Thr3: Feigning of false identity by a "communications partner" (Sub4 and Sub9).

3.1.6 Security objectives

The SM-Z is meant to ensure confidentiality and integrity by achieving the following security objectives:

STar1: Integral and confidential storage of cryptographic keys (Obj4-7), and confidential storage of confidential data (Obj8, the data are stored in encrypted form in SM-Z).

STar2: Integral export and import of cryptographic keys (Obj5-7). The import of keys via the chip-card terminal CKT takes place in encrypted form on the basis of a dynamic transport key (ZST). Using the COM key, the transport key is exchanged in encrypted form between the SM-Z and the CKT. As described in [PER-DEV] Chapters 5.6 and 5.7, the COM key is loaded into the SM-Z exclusively during the initial personalization procedure.

STar3: Support of a confidential and integral data exchange between the HiGruSys (Sub6) and the EG or SM-K (Sub9) (manipulations during data transmission cannot be prevented, but must be reliably detected).

STar4 Support of a cryptographically secure transfer of charges (Obj2) from the SM-K (Sub9) to the HiGruSys (Sub6).

STar5: Cryptographically relevant communications by the HiGruSys (Sub6) only with authentic partners (Sub4 and Sub9)

3.2 Security functions

None of the functionality classes offered in the ITSEC covers the security functions of the SM-Z. In order to effectively counteract the threats mentioned under 3.1.5, the SM-Z is equipped with the following security functions which are described more closely in the subsequent chapters:

SF1: Identification and authentication (I&A)

SF2: Encryption (ENC)

SF3: MAC safeguarding (INT)

SF4: Access control (AC)

3.2.1 SF1: Identification and authentication (I&A)

The SM-Z is intended to support the HiGruSys (Sub6) during identification wiht respect to the decentral security modules SM-K (Sub9; refer to Chapter 0), by performing the cryptographic tasks required for this purpose. In addition, the SM-Z identifies the personnel approved for its administration (Sub4).

Authentication is performed by supplying and checking an item of information assigned to the respective subject using a corresponding authentication procedure (Challenge and Response or presentation of a personal identification number -PIN-). The authentication information is stored in the SM-Z and protected against unauthorised access. There are two types of authentication procedures – two-sided and one-sided.

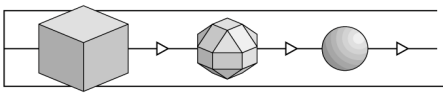
The result of an authentication is evaluated by the SM-Z or HiGruSys (Sub6) such that several consecutive, unsuccessful attempts at authentication are detected and further attempts are prevented.

I&A SM-K / SM-Z

Two-sided authentication takes place with respect to the decentral security module SM-K (Sub9). It serves as a basis for establishing a secure link between the SM-K (Sub9) and the HiGruSys (Sub6). Additionally, successful authentication of the SM-K (Sub9) by the SM-Z is a mandatory prerequisite for releasing the cryptographically secured Download Functions (keys, parameters, SW and FW) for the SM-K (Sub9) or the EG by the HiGruSys (Sub6).

I&A Administrator / SM-Z

During one-sided authentication, the personnel of the network operator (Sub4) authorised to administer the SM-Z identifies and authenticates itself with respect to the SM-Z using the roles defined in Chapter 3.1.2.1. In any case, successful authentication is a mandatory prerequisite for the administration of the SM-Z.



The firmware of the SM-Z ensures that the PINs required for authentication are only entered in encrypted form.

Administration involves the following functions here:

– Modification of user profiles (Obj1.2) for the interface to the HiGruSys (Sub6) or the SKM (SS / SM-HSI),

– Generation of keys

– Import of keys and

– Export of keys (without the functions which are executed by the HiGruSys (Sub6))

3.2.2 SF2: Encryption (ENC)

The SM-Z can encrypt data elements (Obj3) obtained from the HiGruSys (Sub6) for the purpose of confidential transfer to the SM-K (Sub9). The used keys are generated by the network operator (Sub5) and derived by the SM-Z for each individual SM-K (Sub9). In addition, the sequential number is included in the data encryption for protection against Replay-Attacks. The keys are protected such that unauthorised parties cannot gain access to them.

The Firmware of the SM-Z ensures that the import and export of keys to and from the SM-Z only takes place in encrypted form.

3.2.3 SF3: MAC safeguarding (INT)

To ensure integral transmission to and from HiGruSys (Sub6), the SM-Z can MAC-check and MAC-secure data objects requiring protection (Obj2) in order to detect any manipulation.

For example, this protects commands generated by the HiGruSys (Sub6) and subsequently executed by the SM-K (Sub9) against manipulation using a cryptogram (MAC via command and data). This type of command is only executed by the SM-K (Sub9) once the check of the cryptogram has provided a positive result.

Before transmission to the HiGruSys (Sub6), data elements are equipped with a MAC by the SM-K (Sub9). This MAC can then be checked for correctness by the SM-Z.

The Firmware of the SM-Z ensures that the import and export of keys to and from the SM-Z only takes place in encrypted form.

3.2.4 SF4: Access control (AC)

The SM-Z can furnish data objects requiring protection (Obj1) with access conditions. For example, different access conditions can be assigned to write and read access. It is possible to allow permanent read access to a data object but only allow write access to it following authentication by an administrator (Sub4). Furthermore, access to data ob-

jects can be allowed exclusively via internal functions which, for example, are integrated into the execution of a command.

To prevent a misuse of cryptographic keys (Obj4-8), their function and usage can be restricted to certain objects, if required. For example, a key intended for integrity protection (MAC calculation) can be barred against use for confidentiality protection (encryption or decryption). In particular, a key for encrypting keys (KEK; Key Enciphering Key) must not be used for decrypting data.

The access conditions are specified by the FW manufacturer during coding or by the administrator in accordance with Tables 2 and 3.

3.2.5 Appropriateness and Effectiveness

Chapter 0 describes the intended type of usage of the SM-Zs. In summary, the intended usage involves:

Application 1 (App1): Identification and authentication of decentral security modules (SM-K)

Application 2 (App2): Identification and authentication of administrators

Application 3 (App3): Support of the exchange of confidential information with the SM-K

Application 4 (App4): Support of the exchange of integrity-protected information with the SM-K

Application 5 (App5): Storage and management of cryptographic keys and confidential data objects.

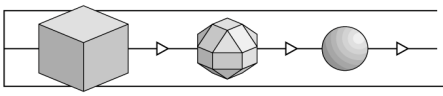
Application 6 (App6): Generation of data for initial personalization or Download for the SM-K.

Application 7 (App7): Import and export of cryptographic keys.

The functionality is useful as well as appropriate for the intended type of usage, as it supplies all the security functions specified for this purpose, is necessary for achieving the security objectives, and counteracts all threats emerging from the planned operational environment.

The following individual details apply here:

– SF1 (I&A) is appropriate for applications 1 and 2. This function checks the correctness of the (authentication) information supplied to it, and provides the required (authentication) information during two-sided authentication to the partner, who can then check this information for "correctness".



– SF2 (ENC) is appropriate for applications 3 and 6 - 7. This function encrypts information obtained from the background system (App3) or information stored in the SM-Z (App6), so that it can be transferred confidentially to the SM-K. This information can then be decrypted in the SM-K, and subsequently be stored or evaluated.

– SF3 (INT) is appropriate for applications 4 and 7. This function generates or checks the MAC from information which is transmitted integrally to and from the background system. The HiGruSys only accepts data as integral if the MAC-check was positive.

– SF4 (AC) is appropriate for application 5. This function prevents unauthorised access to data which require protection and are stored in the SM-Z.

	SF1	SF2	SF3	SF4
App1				
App2				
App3				
App4				
App5				
App6				
App7				

Table 4: Appropriateness of functionality

A more detailed analysis of these functionality attributes is provided later during a consideration of the effectiveness criteria.

The security functions are useful as well as appropriate for protection against the identified threats, because each threat is countered by at least one of these security functions.

The following individual details apply here:

– SF1 counters Thr3. This function checks the identity of a communications partner on the basis of secret information and, if necessary, cryptographic algorithms. This counters attempts at impersonation under a false identity.

– SF2 counters Thr2. This function encrypts confidential data on the basis of secret information and cryptographic algorithms. This counters the disclosure of confidential data.

– SF3 counters Thr2. This function calculates and checks MACs on data requiring protection on the basis of secret information and cryptographic algorithms. This counters the undetected manipulation of protected data.

– SF4 counters Thr1. This function checks for compliance with the access authorisation for an action to be performed on a data object. This prevents unauthorised access to data in SM-Z.

Table 5 shows which security functions counter which threats.

	SF1	SF2	SF3	SF4
Thr1				
Thr2				
Thr3				

Table 5: Counteracting security functions / threats

The security functions are useful as well as appropriate for attaining the security objectives, because each security function contributes toward the attainment of at least one security objective.

The following individual details apply here:

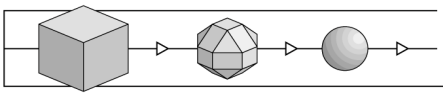
– SF1 contributes toward the attainment of STar3 and STar5. This function checks the authenticity of a communications partner on the basis of secret information and cryptographic algorithms. This ensures that cryptographically relevant information is only exchanged with the authentic partners (STar5), which, in turn, is a prerequisite for the confidential and integral exchange of data, for example, with the HiGruSys (STar3).

– SF2 contributes toward the attainment of STar2 and STar3. This function encrypts confidential data on the basis of secret information and cryptographic algorithms. This ensures a confidential exchange of data with the HiGruSys.

– SF3 contributes toward the attainment of STar2, STar3 and STar4. This function calculates and checks MACs on protected data on the basis of secret information and cryptographic algorithms. This ensures an integral exchange of data (STar2 and STar3) with the HiGruSys and a cryptographically secure transfer of charges (STar4) from the SM-K to the HiGruSys. Here, it must be noted that manipulations of data cannot be prevented, although they can be detected.

– SF4 contributes toward the attainment of STar1. This function checks for compliance with the access authorisation for a required action on a data object. If the access conditions defined in Table 2 are correctly implemented, this ensures a safe and confidential storage of cryptographic keys and confidential data.

Table 6 shows the relationships existing between the security functions and the required security objectives.



	SF1	SF2	SF3	SF4
STar1				
STar2				
STar3				
STar4				
STar5				

Table 6: Relationships between security functions / security objectives

3.3 Mechanisms

The following sections describe the planned implementation of the security functions specified in Chapter 3.2. As the product is still in the development phase, and changes to the planned mechanisms could still be performed, only a brief description is provided here. The individual security mechanisms will be identified later in a fine draft.

3.3.1 SF1: Identification and authentication (I&A)

Different procedures are used for identification and authentication, depending on which partners are active. Basically, however, the 'Challenge and Response' principle applies in the case of authentication, i.e. the challenger - as the authenticating component – always generates the challenge in the form of a random number and checks the response which the responder calculates using a joint secret. If the response check provides a positive result, the responder is authentic.

I&A SM-Z ⇔ SM-K

SM-Z ⇔ SM-K authentication involves mutual authentication.

First of all, the SM-K generates a random number (RND_1); the SM-Z encrypts this number using the authentication key K_{Auth} of the SM-K, and transfers it as a signature (SIG_1) to the SM-K. Encryption is performed with the Double (Triple) DES algorithm.

In response, the SM-Z generates a random number (RND_2); the SM-K encrypts this number using its authentication key K_{Auth} and returns it as a signature (SIG_2) to the SM-Z. Encryption is performed with the Double (Triple) DES algorithm.

The general form of calculating the signature is:

$$SIG_i = e_{dDES}\ K_{Auth}\ (RND_i) \quad | \ i = 1\ldots2$$

In this manner, every authentication partner can check whether the other partner is in possession of the joint secret (K_{Auth}).

I&A Administrator

Administrator ⇒ SM-Z authentication involves one-sided authentication.

The administrator enters his personal identification number (PIN) via the keyboard of the chip-card terminal (CKT). The entered PIN is encrypted in the chip-card terminal using a Session Key and then transmitted in encrypted form to the SM-Z (transport security). The SM-Z decrypts the received PIN and – by performing a simple comparison of the presented, decrypted PIN with the confidential, stored PIN which is assigned the required administrator role – checks whether the administrator is in possession of the joint secret (PIN). If the comparison yields a positive result, the counter of incorrect attempts is set to its initialisation value. The PIN has a length of 6-14 numeric digits.

3.3.2 SF2: Encryption (ENC)

The DES algorithm is used in various modes for the encryption of confidentially transmitted information.

For encryption of

– the FW of the SM-K, the DES is used in the CBC-Mode

– the keys, the DES is used in the Triple DES variant in the ECB-Mode

– parameters, the DES is used in the ECB-Mode.

3.3.3 SF3: MAC security (INT)

To calculate and check MACs, the DES algorithm is used in the CBC-Mode.

3.3.4 SF4: Access control (AC)

In the SM-Z, access conditions are assigned for various actions on data (Act1-4). The following access conditions are provided for the data objects of the SM-Z:

– *anyone* – anyone can gain access

– *authentic* – only an authentic partner (administrator) can gain access

– *enciphered* – the data used at the SS / SM-HSI interface are encrypted

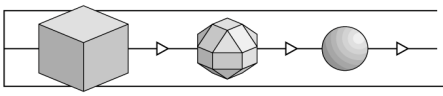
– *authentic & enciphered* - combination of the two conditions

– *internal*

The *internal* access condition is assigned to every data object, if at least one SW / FW function has implicit access to the corresponding data.

3.4 Minimal Strength of Mechanisms and Assurance Level

The mechanisms used for the SM-Z are to achieve the minimal strength designated *high*. Assurance level *E3* is specified for the SM-Z.



3.5 Appendix of security specifications

3.5.1 References

[WD13491] Banking - Secure Cryptographic Devices (Retail)
Part 1: Concepts, Characteristics, Management & Compliance

[SS-HSI] SICRYPT® Hardware Software Interface Security Server / Security Modul
- Allgemeiner Teil,
- Anhang A SICRYPT Server Projekt N.I.K.E. Schlüsselsystem ADMIN,
- Anhang D SICRYPT Server Projekt N.I.K.E. Schlüsselsystem ISO7816,
[Module
– General section,
- Appendix A SICRYPT Server Project N.I.K.E. key system ADMIN,
- Appendix D SICRYPT Server Project N.I.K.E. key system ISO7816]
Siemens Nixdorf Informationssysteme AG

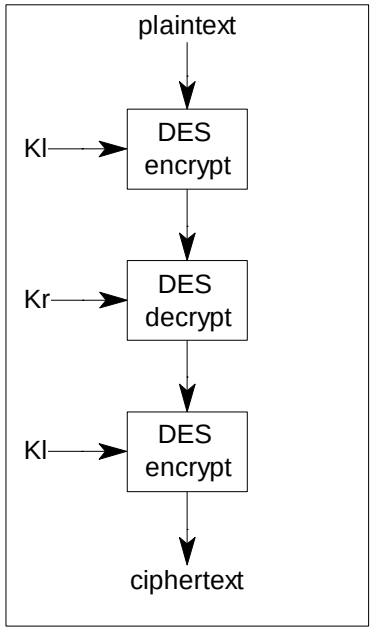
[PER-DEV] Spezifikation Personalisierung ladbarer Geräte [Specification of the personalization of loadable devices], Version V 3.1c, Siemens Nixdorf Informationssysteme AG

3.5.2 Terms and abbreviations

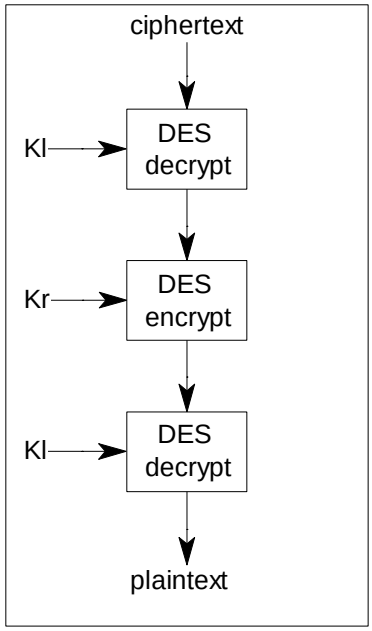
DES key A distinction is made between two types of DES key: sDES key (single-DES or single long key) and dDES key (double-DES or double long key). sDES keys consist of one key component (**K**) and dDES keys consist of two key components (**K = Kl || Kr**).
Every key component has a length of 8 bytes; 7 bits per byte comprise the key for encryption / decryption, while bit 2^0 is used as the parity bit (odd). The 56 bits of a key component are to be selected randomly during generation. If a dDES key is used as an sDES key, its first key component (**K = Kl**) is used.

Double (Triple) DES

This algorithm is based on the DES algorithm. It is a double long key **K= Kl || Kr** (dDES key).

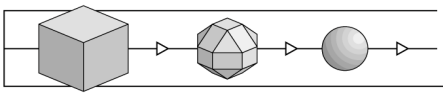


Verschlüsselung



Entschlüsselung

$d_{dDES}K(x)$	Indicates a decryption of the plain text x with the K key using the 'Double (Triple) DES' algorithm
$d_{sDES}K(x)$	Indicates a decryption of the plain text x with the K key using the 'DES' algorithm
$e_{dDES}K(x)$	Indicates an encryption of the plain text x with the K key using the 'Double (Triple) DES' algorithm
$e_{sDES}K(x)$	Indicates an encryption of the plain text x with the K key using the 'DES' algorithm
EG	Terminal Device
HiGruSys	Background System
IKL	Intelligent Card Reader
N.I.K.E.	New Infrastructure for Cards and Card-related Terminal Devices of Deutsche Telekom AG
RM	**R**isk **M**anagement
SecServ	**Sec**urity **Serv**er
SD	**S**ecure **D**evice
SM-K	Security Module in the Card Reader

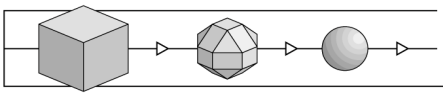


SM-Z	Central Security Module
SKM	**S**ICRYPT **K**ey **M**anagement
SRS	**S**ICRYPT Server **R**untime **S**oftware

4 Remarks and Recommendations concerning the Certified Object

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

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



2

(This page is intentionally left blank.)

5 Security Criteria Background

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

5.1 Fundamentals

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

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

- confidentiality
- availability
- integrity

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

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

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

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

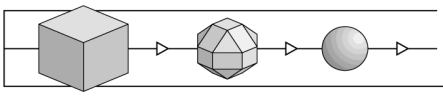
32 There are two basic questions:

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

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

5.2 Assurance level

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.3 Security Functions and Security Mechanisms

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

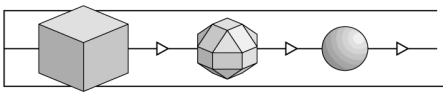
40 Functionality classes are formed by grouping a reasonable set of security functions.

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

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

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

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



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

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

Type B „A *type B mechanism* is a security mechanism which, if perfectly conceived and implemented, will have no weaknesses. A type B mechanism can be considered to be impregnable to direct attack regardless of the level of resources, expertise and opportunity deployed. A potential example of a type B mechanism would be access control based on access control lists: if perfectly conceived and implemented, this type B mechanism cannot be defeated by direct attack. However, these type B mechanisms can be defeated by indirect attacks which are the subject of other effectiveness analyses."

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

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

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

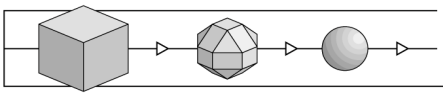
45 How is the strength for type A mechanisms defined?

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

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

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

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



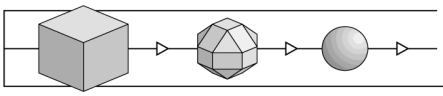
6 Annex

6.1 Glossary

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

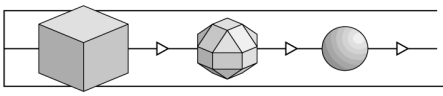
Accreditation	– A process to confirm that an evaluation facility complies with the requirements stipulated by the DIN EN 45001 standard. Accreditation is performed by an *accreditation body.* Accreditations from bodies represented in the German Accreditation Council (DAR) are generally recognised. – Result of an accreditation procedure.
Availability	Classical security objective: Data should always be available to authorised persons, i.e. this data should not be made inaccessible by unauthorised persons and should not 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 (s. 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 at 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 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 Ordinance – SigV	Official regulations concerning the implementation of the German Signature Law.
EN 45000	A series of European standards applicable, in particular, to evaluation facilities and certification bodies.
Evaluation	Assessment of a product, system or service against defined security criteria and security standards.
Evaluation facility	The organisational unit which performs evaluations.
Evaluation level	Refer to „Security level“.
Evaluation report	Individual evaluation report or evaluation technical report.
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	Initial certification of a 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.
IT product	Software and / or hardware which can be procured from a supplier (manufacturer, distributor).
IT service	A service related to the support of IT products and IT systems.
IT system	– A 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).
Licensing	Evaluation of organisation and qualification of an evaluation facility with respect to an intended licence agreement.
Licence agreement	An agreement between an evaluation facility and a certification body specifying procedures and responsibilities for evaluation and certification.
Manufacturers' 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.
Process ID	ID designating a certification or confirmation process within debisZERT.
Re-certification	Renewed certification of a new version following modification of a previously certified object; 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).
Regulation Authority (for Telecommunications and Post)	The authority responsible in accordance with §66 of the German Telecommunications Law (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.
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	Functions of an IT product or IT system for counter-acting particular threats.
Security level	Many criteria sets (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.
Signature Law - SigG	§3 of legislation on Information and Communications Services Act (IuKDG).
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 requiring certification.
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 German Signature Law.
ZKA criteria	Security criteria used by the central credit committee (ZKA) in Germany



6.2 References

/A00/ Lizenzierungsschema (Licensing Scheme), debisZERT, Version 1.0, 7.8.98

/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/Digitale%20Signatur/start.htm

[Annex to „Official Announcement concerning the Digital Signature according to the German Signature Law 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.

[Law 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 97

/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, Regulation Authority for Telecommunications and Post]

/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, Regulation Authority for Telecommunications and Post]

/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, Version 1.3E, September 17, 1998

/V02/ Confirmations for IT Products in accordance with the German Signature Law, Service type 2, Version 1.3E, September 10,1998

/V04/ Certificates recognised by the BSI, Service type 4, debisZERT, Version 1.3E, 5.8.98

/Z01/ Certification Scheme, debis IT Security Services, Version 1.3E, 5.8.98

/Z02/ Certified IT Products, Systems and Services, debisZERT, Release 2, October 1998]

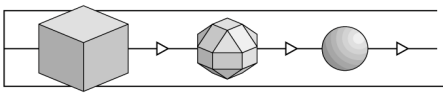
6.3 Abbreviations

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



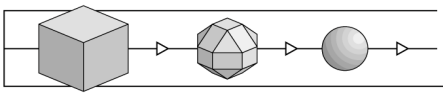
CC	Common Criteria for Information Technology Security Evaluation
CTCPEC	Canadian Trusted Computer Products Evaluation Criteria
DAR	Deutscher Akkreditierungsrat (the German Accreditation Council)
DBAG	Deutsche Bahn AG (the Federal German Railways Inc.)
debisZERT	The debis IT Security Services Certification Scheme
DEKITZ	Deutsche Akkreditierungsstelle für Informations- und Kommunikationstechnik (the German Accreditation Body for Information and Telecommunication Technology)
DLB	Service type
EBA	Eisenbahn-Bundesamt (the Federal German Railway Office)
ETR	Evaluation Technical Report
IT	Information technology
ITSEC	IT Security Evaluation Criteria
ITSEM	IT Security Evaluation Manual
IuKDG	German Information and Communication Services Act
LG	Management Board
SigG	German Digital Signature Act
SigV	German 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

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

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

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



End of initial version of the certification report.