debis

Services by DaimlerChrysler

Zertifizierungsreport

Zentrales Sicherheitsmodul (SM-Z) im
N.I.K.E. System der
Deutschen Telekom AG

Siemens AG

debisZERT-DSZ-ITSEC-04012-1998

debis IT Security Services

Die Dienstleister der Moderne

Vorwort

Das Produkt *Zentrales Sicherheitsmodul (SM-Z) im N.I.K.E. System der Deutschen Telekom AG* der Siemens AG wurde gegen die ITSEC evaluiert. Die Evaluierung wurde im Rahmen des Zertifizierungsschemas debisZERT der debis IT Security Services durchgeführt. Die Zertifizierung erfolgte im Dienstleistungsbereich 04: Zertifikate mit Anerkennung durch das BSI.

Das Ergebnis lautet:

Sicherheitsfunktionalität:	Identifikation und Authentisierung, Verschlüsselung, MAC-Sicherung, Zugriffskontrolle
Evaluationsstufe:	E3
Mechanismenstärke:	hoch

Für weitere Auskünfte und Kopien dieses Reports ist die Zertifizierungsstelle wie folgt erreichbar:

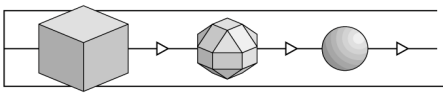
✉ debis IT Security Services	✆	0228 / 9841-110
- Zertifizierungsstelle -	Fax:	0228 / 9841-60
Rabinstr. 8	Email:	debiszert@itsec-debis.de
53111 Bonn	WWW:	www.itsec-debis.de

Die Ordnungsmäßigkeit der Evaluierung wird hiermit bestätigt.

Bonn, den 08.12.1998

Dr. Heinrich Kersten

Leiter der Zertifizierungsstelle



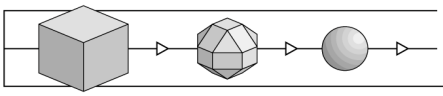
Revisionsliste

Die nachfolgende Revisionsliste gibt Auskunft über den Erstellungsprozeß für die Erstausgabe des Zertifizierungsreports.

Re-Zertifizierungen aufgrund von Produktänderungen sind in Kapitel 7 aufgeführt.

Revision	Datum	Vorgang
0.9	01.04.98	Vorversion (nach Musterreport 1.1)
1.0	07.09.98	Ersterstellung (nach Musterreport 1.3)
1.1	18.09.98	Namenskorrektur des Auftraggebers, geändertes Auslieferungsverfahren
1.2	08.12.98	Namenskorrektur des Auftraggebers, Sicherheitsvorgaben sind Bestandteil der Betriebsdokumentation (Musterreport 1.4) - veröffentlichte Fassung -

Inhalt



1 Überblick

1.1 Evaluierung

1 Die Evaluierung wurde durch die Siemens AG, Bürgermeister-Ulrich-Straße 100, 86199 Augsburg beauftragt.

2 Die Evaluierung wurde vom Prüflabor für IT-Sicherheit der debis IT Security Services durchgeführt. Die Erst-Evaluierung endete am 18.09.98. Einige prozedurale und dokumentative Änderungen wurden nachevaluiert (s. Revisionsliste); diese Prüfschritte wurden am 3.12.98 abgeschlossen.

3 Die Evaluierung wurde gegen die ITSEC und ITSEM durchgeführt. Einige Hinweise zu den Inhalten der ITSEC und ITSEM finden sich im Abschnitt 5.

1.2 Zertifizierung

4 Die Zertifizierung wurde gemäß den Regeln des Zertifizierungsschemas debis-ZERT der debis IT Security Services durchgeführt. Die Zertifizierungsstelle arbeitet im Einklang mit der DIN EN 45011 und ist im Hinblick auf diese Norm bei der Deutschen Akkreditierungsstelle für Informations- und Telekommunikationstechnik (DEKITZ) akkreditiert (DAR-Registriernummer DIT-ZE-005/98-00).

5 Die Zertifizierungsstelle der debis IT Security Services hat das Zertifizierungsverfahren nach Maßgabe folgender Dokumente durchgeführt:

/Z01/ Zertifizierungsschema

/V04/ Zertifikate mit Anerkennung durch das BSI

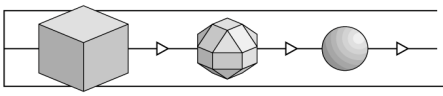
1.3 Zertifizierungsreport

6 Dieser Zertifizierungsreport gibt die Ergebnisse der Evaluierung von *Zentrales Sicherheitsmodul (SM-Z) im N.I.K.E. System der Deutschen Telekom AG* wieder - im folgenden als EVG = Evaluationsgegenstand bezeichnet.

7 Der Zertifizierungsreport gilt nur für die angegebene Version des EVG. Er kann jedoch auf neue bzw. andere Versionen ausgedehnt werden, sobald eine erfolgreiche Re-Evaluierung stattgefunden hat.

8 Der Zertifizierungsreport dient

- dem Auftraggeber als Nachweis der durchgeführten Evaluierung und
- dem Nutzer als Grundlage für den sicherheitsgerechten Einsatz von SM-Z.



9 Der Zertifizierungsreport enthält die Seiten 1 bis 50. Kopien des Zertifizierungsreports können beim Auftraggeber oder bei der Zertifizierungsstelle angefordert werden.

10 Der Zertifizierungsreport kann einerseits durch Nachweise über erfolgte Re-Zertifizierungen, andererseits durch Anhänge zu besonderen technischen Problemen ergänzt werden. Solche Nachweise bzw. Anhänge werden in folgender Druckschrift angekündigt:

/Z02/ Zertifizierte IT-Produkte, IT- Systeme und IT-Dienstleistungen

1.4 Zertifikat

11 Eine Kurzfassung der Ergebnisse enthält das Sicherheitszertifikat debisZERT-DSZ-ITSEC-04012-1998 (Ausgabedatum 1.12.1998).

12 Eine Kurzbeschreibung von *Zentrales Sicherheitsmodul (SM-Z) im N.I.K.E. System der Deutschen Telekom AG* und die Zertifizierungsergebnisse werden in der Druckschrift

/Z02/ Zertifizierte IT-Produkte, IT- Systeme und IT-Dienstleistungen

und über WWW veröffentlicht.

13 Das Zertifikat wird durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) anerkannt, das seinerseits die Gleichwertigkeit des Zertifikats zu seinen eigenen Zertifikaten im internationalen Kontext bestätigt.

14 Die Bewertung der Stärke der zur Ver- und Entschlüsselung geeigneten kryptographischen Mechanismen ist von der Anerkennung durch das BSI ausgenommen[1].

15 Das Zertifikat trägt das vom BSI genehmigte Logo. Die Tatsache der Zertifizierung wird in der Broschüre 7148 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) aufgeführt.

1.5 Anwendung der Ergebnisse

16 Die Prozesse der Evaluierung und Zertifizierung werden nach dem Stand der Technik durchgeführt, können aber keine *absolute* Garantie dafür geben, daß das zertifizierte Objekt frei von Schwachstellen ist. Mit steigender Evaluationsstufe verringert sich allerdings die Wahrscheinlichkeit erheblich, daß ausnutzbare Schwachstellen unentdeckt bleiben.

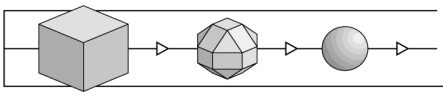
---

1 Aufgrund gesetzlicher Vorgaben /BSIG/ ist das BSI grundsätzlich gehalten, Bewertungen der genannten kryptographischen Algorithmen selbst nicht vorzunehmen und solche von anderen Zertifizierungsstellen nicht anzuerkennen.

17 Um die Ergebnisse der Evaluierung sinnvoll nutzen zu können, wird dringend empfohlen, den Zertifizierungsreport aufmerksam zu lesen. Insbesondere die Informationen zur Art der Nutzung des zertifizierten Objektes, zu den betrachteten Bedrohungen, zur Einsatzumgebung und zu den geprüften Konfigurationen sind wichtige Vorgaben für die Praxis.

18 Das Evaluierungsergebnis gilt nur unter der Voraussetzung, daß alle Vorgaben aus dem Zertifizierungsreport beachtet werden.

Sofern von diesen Vorgaben abgewichen wird, gilt das Evaluierungsergebnis nur noch bedingt. In einem solchen Fall ist eine ergänzende Analyse erforderlich, um festzustellen, ob und in welchem Umfang das zertifizierte Objekt auch unter den geänderten Bedingungen noch Sicherheit bieten kann. Die genannte Prüfstelle und die Zertifizierungsstelle können bei der Analyse unterstützen.



(Diese Seite ist beabsichtigterweise leer.)

2 Wesentliche Ergebnisse der Evaluierung

2.1 Grundlegendes

19 Das Ergebnis der Evaluierung ist im ETR (Evaluation Technical Report) dargestellt. Die Evaluierung erfolgte gegen die im Kapitel 3 dieses Zertifizierungsreports wiedergegebenen Sicherheitsvorgaben.

2.2 Ergebnis

20 Die Prüfstelle kommt zu folgendem Ergebnis:

- Der EVG genügt den Anforderungen der Evaluationsstufe **E3** gemäß ITSEC, d.h. alle Anforderungen an die Korrektheit und Wirksamkeit gemäß dieser Stufe sind erfüllt. Dies sind:

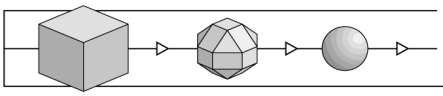
  ITSEC E3.1 bis E3.37 für die Korrektheit mit den Phasen

Konstruktion - Entwicklungsprozeß	(Anforderungen, Architekturentwurf, Feinentwurf, Implementierung),
Konstruktion - Entwicklungsumgebung	(Konfigurationskontrolle, Programmiersprachen und Compiler, Sicherheit beim Entwickler),
Betrieb - Betriebsdokumentation	(Benutzerdokumentation, Systemverwalter-Dokumentation)
Betrieb - Betriebsumgebung	(Auslieferung und Konfiguration, Anlauf und Betrieb).

  ITSEC 3.12 bis 3.37 für die Wirksamkeit mit den Aspekten

Wirksamkeitskriterien - Konstruktion	(Eignung der Funktionalität, Zusammenwirken der Funktionalität, Stärke der Mechanismen, Bewertung der Konstruktionsschwachstellen),
Wirksamkeitskriterien - Betrieb	(Benutzerfreundlichkeit, Bewertung der operationellen Schwachstellen).

- Alle Mechanismen des EVG sind kritische Mechanismen. Die Mechanismen - soweit vom Typ A - haben eine Mindeststärke gemäß der Stufe **hoch**. Der Mechanismus zu SF2 (Verschlüsselung) ist evaluiert worden, bleibt aber entsprechend den hier anzuwendenden Verfahrensvorgaben (s. Abschnitt 1.4 , Absatznummer 14) unbewertet, was die Mechanismenstärke anbetrifft.



Für die Mechanismen des Typs B ist gemäß ITSEC und ITSEM keine Mechanismenstärke anzugeben. Im Rahmen der Schwachstellenanalyse konnte jedoch festgestellt werden, daß selbst unter Zugrundelegung eines Aufwands gemäß der Stufe „hoch“ bei den angenommenen Einsatzbedingungen keine ausnutzbare Schwachstelle erkennbar ist.

2.3 Hinweise

21 Die Prüfstelle hat keine Auflagen an den Hersteller ausgesprochen.

22 Die Prüfstelle hat keine Auflagen an den Anwender auszusprechen.

3 Sicherheitsvorgaben

3.1 Produktbeschreibung

3.1.1 Allgemeines

Die Deutsche Telekom AG beabsichtigt, ein neues System N.I.K.E. (Neue Infrastruktur für Karten und kartenbezogene Endeinrichtungen) zur Nutzung bargeldloser Dienste an öffentlichen und halböffentlichen Telefonen bzw. artverwandten Endgeräten (EG) auf Chipkartenbasis einzuführen. Vorgesehen ist dabei die Verwendung der folgenden Sicherheitskomponenten (vgl. Abbildung 1):

- EG mit integriertem IKL (intelligenter Kartenleser):
  Das Endgerät ermöglicht einem Benutzer die Nutzung der entsprechenden Telekommunikationsdienste. Es koordiniert und steuert dabei einerseits die Kommunikation mit dem Hintergrundsystem (HiGruSys), andererseits liest und bearbeitet es über den enthaltenen IKL die vom Benutzer verwendete Chipkarte. Der IKL besitzt zur Speicherung kryptographischer Schlüssel und zur Ausführung kryptographischer Funktionen ein Sicherheitsmodul (SM-K).

- HiGruSys mit SecServ (Security Server):
  Innerhalb des N.I.K.E. Systems realisiert das Hintergrundsystem die Zentrale. Hier erfolgt die Datenhaltung, Administration sowie die Datenverteilung an die einzelnen EGs. Es enthält einen Security Server mit dem integriertem Sicherheitsmodul SM-Z, der zur Speicherung sensitiver Daten und zur Unterstützung der kryptographisch abgesicherten Kommunikation mit den EGs eingesetzt wird.

- SD (Secure Device):
  Das N.I.K.E. System sieht einen *Cross-Border-Use* von Telefonkarten (Eurochipkarten) mit anderen Kartenausgebern vor (MoU Partner). Das Secure Device wird dabei zum sicheren Schlüsselaustausch der Anwenderschlüssel verwendet. Zum Transport werden die verschlüsselten Anwenderschlüssel vom SD ausgegeben und auf Diskette geschrieben. Diese Anwendungsschlüssel dienen letztlich zur Authentisierung der verwendeten Chipkarten und zur sicheren Übertragung von Abrechnungsdaten.

- RM (Risk Management):
  Das Risk Management dient zur Überwachung der Sicherheitseinrichtungen im N.I.K.E. System. Sicherheitsrelevante Meldungen werden von ihm an eine ausgezeichnete Stelle bzw. Person weitergeleitet, die mit seiner Hilfe entsprechende Maßnahmen einleiten kann.

Das *Sicherheitsmodul SM-Z* welches ein Bestandteil des Security Server im Hintergrundsystem ist, stellt den *Evaluationsgegenstand* (EVG) und insbesondere den Gegenstand der nachfolgenden Kapitel dar.

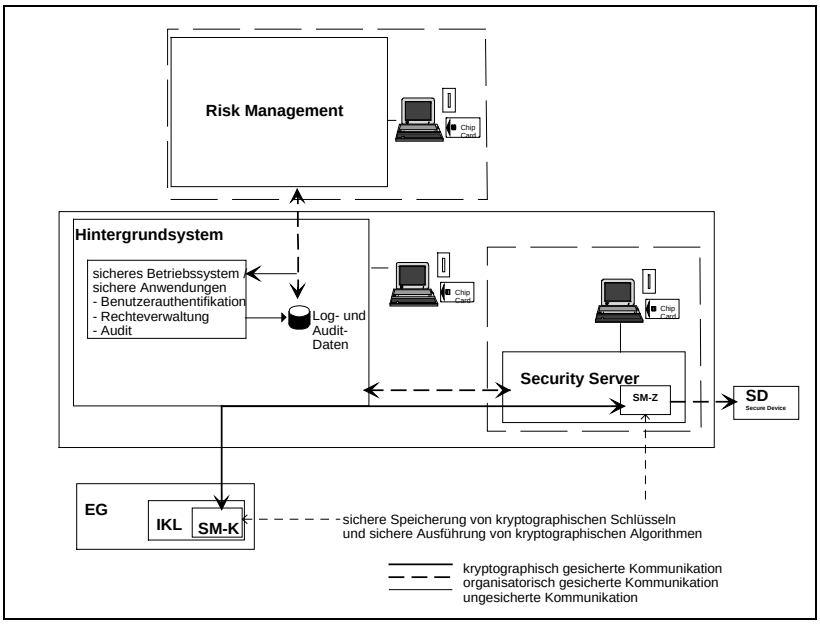


Abbildung 1: Schematische Darstellung des N.I.K.E. Systems

3.1.2 Produktdefinition und Art der Nutzung

Definition des EVG

Der EVG, im folgenden mit SM-Z bezeichnet, ist die Firmware (FW) des Sicherheitsmoduls SM-Z inklusive der für den Anwendungsprogrammierer bestimmten Dokumentation (siehe Tabelle1).

Die wesentlichen Komponenten der FW sind:

– Basis-FW: Maskenprogramm des PROVE (Prozessor zur Ver- und Entschlüsselung)

– Standard-FW: Implementierung der allgemeinen Funktionalität

– FW für das Schlüsselsystem ADMIN: Implementierung der Funktionen, die vom SKM genutzt werden.

– FW für das Schlüsselsystem ISO7816: Implementierung der Funktionen, die vom Hintergrundsystem (HiGruSys) genutzt werden.

Typ	Bezeichnung	Version
Hardware-Modul: Basis-FW & Standard-FW & Schlüsselsystem ADMIN & Schlüsselsystem ISO7816	SICRYPT Security Modul 7, Typ SM-Z	NIK 11.1 A vom 27.04.98
Dokumentation für den Anwendungsprogrammierer 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

Tabelle 1: Komponenten des EVG (Produktumfang)

Die Abbildung 2 zeigt die komplette Konfiguration des SM-Z sowohl zur Administration als auch zum operativen Betrieb.

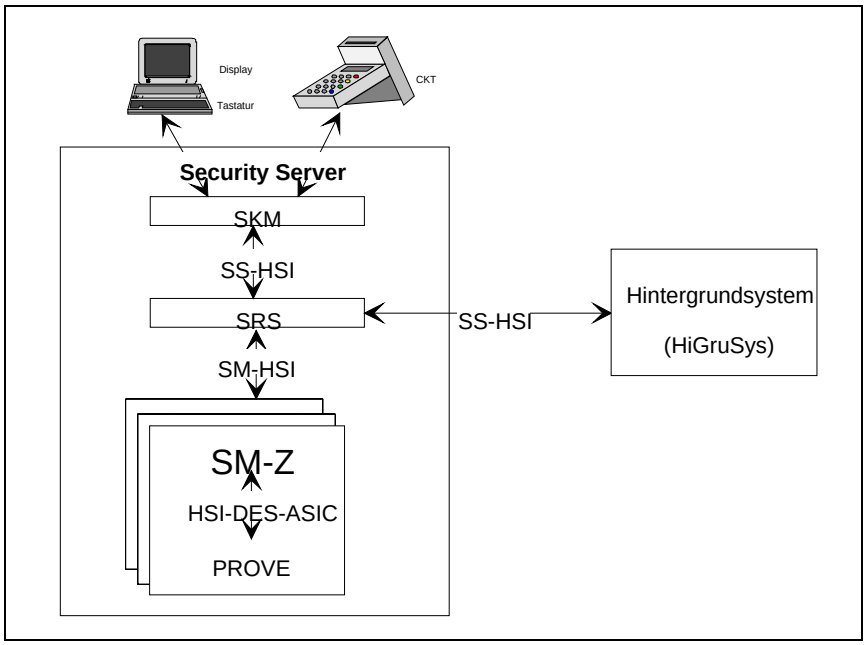
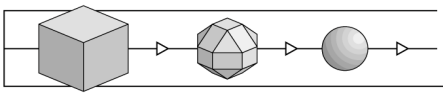


Abbildung 2: Schematische Darstellung der Gesamtkonfiguration des SM-Z

Art der Nutzung

Das SM-Z wird zur vertraulichen Speicherung und Verwaltung von schützenswerten Datenobjekten (z.B. Schlüssel) sowie zur Ausführung von auf Kryptographie basierenden



Aktionen, die vertrauliche Informationen verwenden, im Hintergrundsystem genutzt. Hierunter fallen

– Identifikation und Authentisierung von

  1. dezentralen Sicherheitsmodulen (SM-K)

  2. Personen (Administratoren), die zur Administration des SM-Z berechtigt sind

– Speichern und Verwalten von

  3. kryptographischen Schlüsseln,

  4. vertraulichen Datenobjekten und

  5. Firmware der dezentralen Sicherheitsmodule (SM-K).

– sowie

  6. Unterstützung des vertraulichen und integritätsgeschützten Austauschs schützenswerter Datenobjekte zwischen HiGruSys und EG oder SM-K.

  7. Generierung von Daten zur erstmaligen Personalisierung oder zum Download der dezentralen Sicherheitsmodule (SM-K).

Der Netzbetreiber nutzt die Aktionen 1-7.

Der Benutzerkarten-Herausgeber Telekom nutzt die Aktionen 3 und 6.

Der Benutzerkarten-Herausgeber MoU-Partner nutzt die Aktionen 3 und 6.

Zur Nutzung der im SM-Z enthaltenen Kryptofunktionen müssen zuvor spezielle Informationen in die Hardware des Sicherheitsmodul SM-Z geladen werden:

– FW (wird beim SM-Hersteller geladen),

– Basisschlüssel (werden beim SM-Hersteller geladen),

– Betriebsschlüssel (KSMctl; wird bei der Deutschen Telekom AG generiert oder geladen) und

– Anwendungsschlüssel (KAc1 & KAc2; werden bei der Deutschen Telekom AG generiert oder geladen).

Das Prozedere des Erzeugens, Einbringens und des Verwaltens von integeren Schlüsseln für das SM-Z geschieht

– in der durch organisatorische und bauliche Maßnahmen gesicherten Produktionsumgebung des Herstellers oder

– in der durch organisatorische und bauliche Maßnahmen gesicherten Produktionsumgebung der Deutschen Telekom AG.

Die Basistechnologie der Kryptofunktionen und des Schlüsselmanagements des SM-Z ist der Prozessor zur Ver- und Entschlüsselung (PROVE) des Sicherheitsmoduls und die als Masken-ROM-Code im PROVE integrierte Basis Firmware.

3.1.3 Einsatzumgebung

Technische Einsatzumgebung

Die technischen Voraussetzungen zum Betreiben eines SM-Z sind:

– Standard PC mit Pentium-Prozessor und mindesten 16 MB Hauptspeicher / 500 MB Festplatte.

– Betriebssystem Windows NT ab Release 3.50.
Das SS-HSI (vgl. Abbildung 2) wird am *'NT-TDI (transport driver interface)'* bereitgestellt.
Das SM-HSI (vgl. Abbildung 2) wird am *'NT-SCSI-Port driver interface'* bereitgestellt.
Die Softwarekomponente SICRYPT Server Runtime Software (SRS) in der Variante N.I.K.E..
Die Softwarekomponente SICRYPT Key Management (SKM) in der Variante N.I.K.E..

– Sicherheitsmodul-HW (SM-Z)- als 'Tamper Resistant Device' (vgl. [WD13491]).

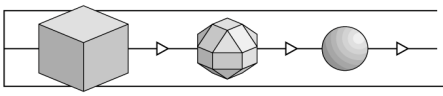
– Chipkarten Terminal (CKT) mit PIN-Tastatur und Display (PNr. CT220 / ab FW-Version 48), welches an einer seriellen Schnittstelle, z.B. COM2 des PC, angeschlossen wird.

Administrative Einsatzumgebung

Nach der Produktion des Sicherheitsmoduls muß zunächst eine Personalisierung des Schlüsselsystems, des individuellen HW-Schlüssels, des Produktionsschlüssels (PER), des Kommunikationsschlüssels (COM), der Firmware und der Sicherheitsmodulidentifikation (SID) erfolgen, damit das Sicherheitsmodul für den Einsatz als SM-Z im Security Server vorbereitet ist. Das SM-Z wird in einer organisatorisch gesicherten Umgebung betrieben.

Dazu ist die Realisierung folgender Ziele in der Organisation notwendig:

ORG1: Vertrauenswürdige (personelle, materielle, organisatorische) und unveränderbare (im Sinne einer gezielten Manipulation) Einbringung der Schlüssel in das SM-Z. Die **Personalisierung** wird in einem zugangsgeschützten Raum in einer sicheren Umgebung betrieben.



ORG2: Vertrauenswürdiges (personell, materiell, organisatorisch) Schlüsselhandling außerhalb des Sicherheitsmoduls.

Die Benutzer- und Dateneingaben zum Schlüsselmanagement des SM-Z erfolgt durch die Eingabemedien Chipkarte, Diskette, Netzwerk und Tastatur des Chipkartenterminals (CKT) .

Schlüssel-BackUp

Ein Schlüssel-BackUp der im SM-Z gespeicherten Schlüssel wird auf die folgende Art durchgeführt:

Ein Schlüssel-BackUp der Basisschlüssel COM und PER, welche durch den SM-Hersteller in das SM-Z geladen werden, ist beim SM-Hersteller vorhanden. Ein Schlüssel-BackUp des Basisschlüssels HW´ ist nicht erforderlich, da der Schlüssel HW´ bei der Erstpersonalisierung für jedes SM-Z individuell erzeugt wird (siehe [PER-DEV] Kapitel 5.6).

Ein Schlüssel-BackUp der im SM-Z gespeicherten Betriebs- und Anwenderschlüssel wird durch die im Kapitel 3.1.4.3 definierten Aktionen Act1 (Lesen) und Act2 (Schreiben) durchgeführt. Die Schüssel werden durch das SM-Z aus seinem internen Schlüsselspeicher gelesen und verschlüsselt ausgegeben. Sie können nun auf einem beliebigen Speichermedium gespeichert werden. Beim Einspielen des Schlüssel-BackUp in das SM-Z werden die Schlüssel verschlüsselt in das SM-Z geladen, durch das SM-Z entschlüsselt und in den internen Schlüsselspeicher geschrieben.

3.1.4 Subjekte, Objekte und Aktionen

Subjekte

In der Abbildung 3 werden die Subjekte, die aus Sicht des SM-Z (EVG) relevant sind, schematisch dargestellt. Die dort dargestellten Subjekte HW-Hersteller, Chip-Hersteller, Software-Hersteller (Sub2) und Security Server (Sub10) sind nicht Gegenstand der Betrachtungen dieses Dokuments.

Sub1: Firmware-Hersteller
Sub2: Software-Hersteller
Sub3: Personalisierer - SM-Hersteller
Sub4: Administrator - Identifikation und Authentisierung erfolgt durch Präsentation einer PIN
Sub5: Netzbetreiber - Deutsche Telekom
Sub6: Hintergrundsystem (HiGruSys)
Sub7: Benutzerkarten-Herausgeber - MoU-Partner
Sub8: Benutzerkarten-Herausgeber - Telekom
Sub9: SM-K
Sub10: Security Server

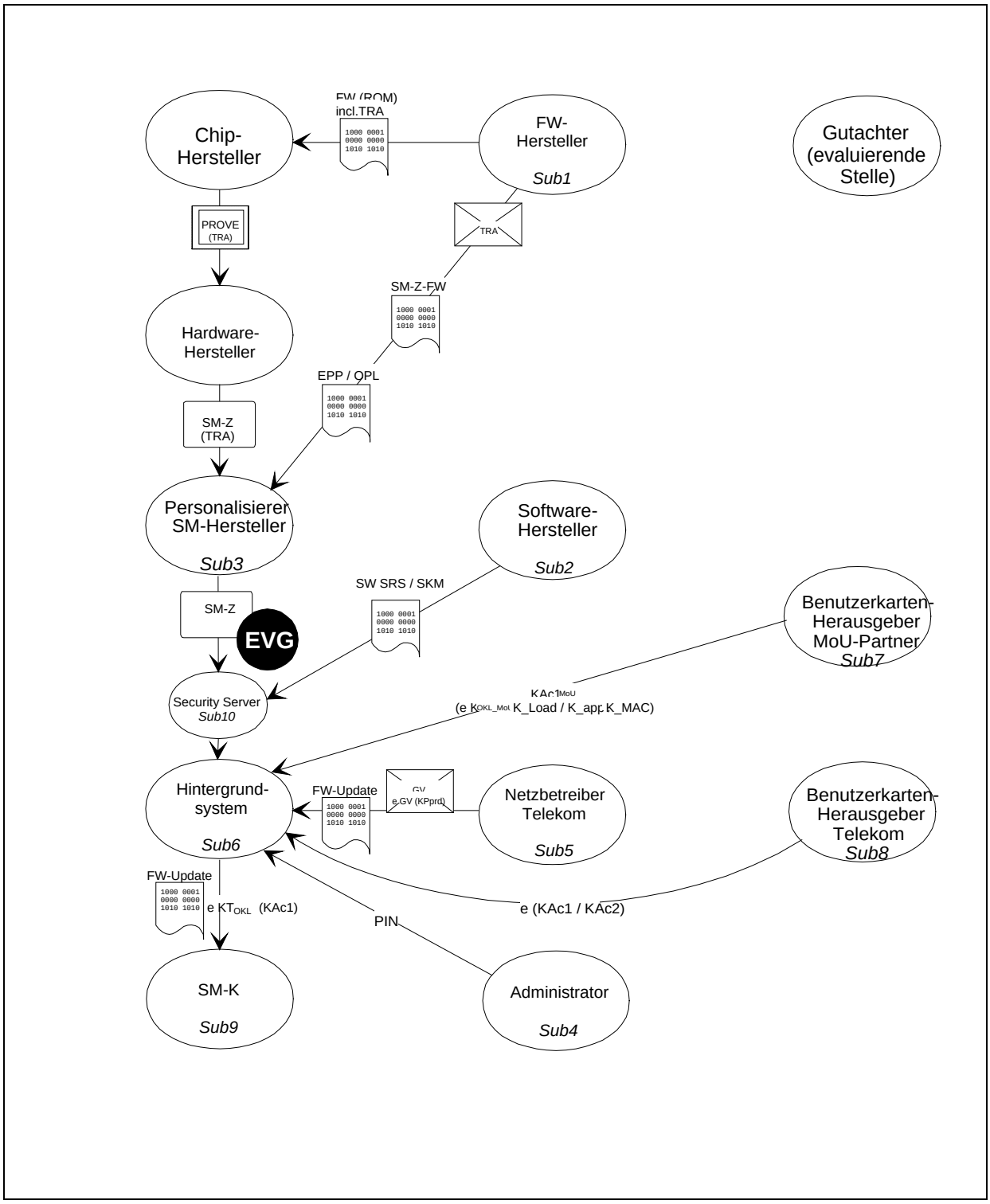
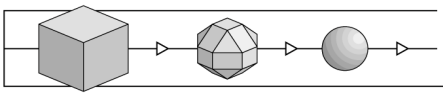


Abbildung 3: Schematische Darstellung der Subjekte



Der Entwicklungs- und Fertigungsprozeß eines SM-Z hat folgenden Ablauf:

1. Der FW-Hersteller entwickelt die Basis-FW (ROM-Code des PROVE) das Erstpersonalisierungsprogramm (EPP), das Programm zum Laden der SM-Z-FW (OPL) und die SM-Z-FW. Er übergibt den ROM-Code für den PROVE an den Chip-Hersteller. Der Maskenschlüssel TRA ist Bestandteil des ROM-Code.

2. Der Chip-Hersteller produziert den PROVE mit der Maske (Programm im ROM), die dem übergebenen ROM-Code entspricht.

3. Der FW-Hersteller übergibt dem Personalisierer des SM Herstellers den Maskenschlüssel (TRA), das signierte EPP, das OPL und die SM-Z-FW.

4. Der Personalisierer des SM-Herstellers generiert den Produktionsschlüssel PER.

5. Der Personalisierer des SM Herstellers lädt das Erstpersonalisierungsprogramm (EPP), unter Verwendung der Laderoutine des PROVE, in den RAM des SM-Z. Der PROVE überprüft die Integrität des EPP unter Verwendung des Maskenschlüssels (TRA). Ist der MAC über das EPP korrekt, wird das EPP vom PROVE ausgeführt. Unter Kontrolle des EPP werden nacheinander der Produktionsschlüssel (PER), der Kommunikationsschlüssel (COM) der individuelle HW-Schlüssel (HW') und die Referenztabelle zur Definition des Schlüsselsystems geladen. Dieser Produktionsschritt wird in der gesicherten Produktionsumgebung des SM-Herstellers durchgeführt.

6. Der Personalisierer des SM-Herstellers lädt das Programm zum Laden der SM-Z-FW (OPL), unter Verwendung der Laderoutine des PROVE, in den RAM des SM-Z. Der PROVE überprüft die Integrität des OPL unter Verwendung des Produktionsschlüssels (PER). Ist der MAC über das OPL korrekt, wird das OPL vom PROVE ausgeführt. Unter Kontrolle des OPL wird die FW des SM-Z geladen und die Integrität überprüft. Dieser Produktionsschritt ist nicht an eine gesicherte Produktionsumgebung gebunden.
   Ab diesem Zeitpunkt repräsentiert das SM-Z den EVG.

7. Der SW-Hersteller entwickelt die Programme SRS und SKM und übergibt diese dem SM-Hersteller.

8. Anschließend wird der Security Server aus den Komponenten Standard-PC, SM-Z, CKT, SRS, SKM und der Benutzerdokumentation zusammengestellt und an den Endnutzer, hier die Deutsche Telekom AG, ausgeliefert.

Objekte

Schutzwürdige *Objekte* sind:

Obj1: Datenelemente, deren Inhalt durch einen Administrator verwaltet wird. (z.B. Datum / Uhrzeit, Profile, ...)

Obj2: Datenelemente für Abrechnungsdaten, die vom SM-K zum HiGruSys gesichert übertragen werden.

Obj3: Datenelemente, die vom HiGruSys zum SM-K vertraulich übertragen werden.

Obj4: Basisschlüssel (TRA, PER, COM, HW')

Obj5: BackUp-Schlüssel (UR, ZSTR)

Obj6: Betriebsschlüssel (KSMctl, KPprd)

Obj7: Schlüssel des Benutzerkarten-Herausgeber - Telekom (Sub8; Anwendungsschlüssel)

Obj8: Schlüssel des Benutzerkarten-Herausgeber - MoU-Partner (Sub7; Anwendungsschlüssel)

Obj9: Programmcode (FW) / SM-Z-Funktionen

Obj10: Zufallszahlen

Aktionen

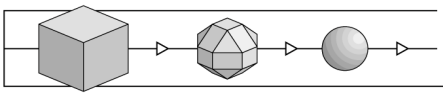
Nachfolgende Aktionen sind für die definierten Subjekte an den schutzwürdigen Objekten möglich:

Act1: Lesen (R)

Act2: Schreiben, Löschen (W)

Act3: Ausführen / Benutzen (E)

Act4 Generieren (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-Basis)	G / W	-	G / W	E	-	-	-	-	-
Obj5 (K-BackUp)	-	-	-	R[1&2&4] / W[1&2&4] / G / E	-	-	-	-	-
Obj6 (K-Betrieb)	-	-	-	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	-	-	-

Tabelle 2: Zugelassene Aktionen von Subjekten an Objekten

Einschränkungen:

[1] verschlüsselt gemäß Referenztabelle (Export / Import)
[2] unverschlüsselt gemäß Referenztabelle (Export / Import)
[3] verschlüsselt
[4] nur ZSTR

Zur Administration des SM-Z sind im Subjekt 4 die folgenden drei Rollen definiert:

1. der netzweite Administrator (ADMIN-Net),

2. der zweite netzweite Administratoren (ADMIN-Net_x_2) zur Durchsetzung des Vier-Augen-Prinzips,

3. der lokale Administrator (ADMIN-Local).

Der ***ADMIN-Net*** hat das Recht, die BackUp-Schlüssel zu generieren und zu laden. Diese sind die kryptographische Basis zur Erstellung des BackUp der Betriebs- und Anwendungsschlüssel, zu deren Erstellung und Einspielung er ebenfalls das Recht hat. Außerdem hat er das Recht das SM-Z zu initialisieren und zu konfigurieren.

Bei dem ***ADMIN-Net_x_2*** handelt es sich um einen netzweiten Administrator ***ADMIN-Net,*** welcher sich zur Durchsetzung des Vier-Augen-Prinzips nach dem ***ADMIN-Net*** mit der Eingabe seiner PIN authentisiert, so daß die beiden Administratoren ***ADMIN-Net*** die zusätzlichen Rechte zum Export und Import von Klartextschlüsseln erhalten, die ggf. die Basis zur kryptographischen Kommunikation mit Kooperationspartnern sind.

Der ***ADMIN-Local*** hat das Recht, ein Schlüssel-BackUp zu erstellen und gegebenenfalls wieder einzuspielen.

Die Tabelle 3 definiert die weiteren Rechte der drei Administratorrollen (Fußnoten s. Seite 20) .

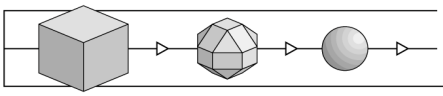
	Sub4.1 (ADMIN-Net)	**Sub4.2** (ADMIN-Net_x_2)	**Sub4.3** (ADMIN-Local)
Obj1.1 (Datum / Uhrzeit)	R / W	R / W	R
Obj1.2 (Profile)	R / W	R / W	R
Obj4 (K-Basis)	E	E	E
Obj5 (K-BackUp)	R[1)] / W[1)] / E / G	R[1 & 2)] / W[1 & 2)] / E / G	R[1 & 4)] / W[1 & 4)] E
Obj6 (K-Betrieb)	R[1)] / W[1)] / E	R[1 & 2)] / 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)	-	-	-

Tabelle 3 Zugelassene Aktionen von Administratoren an Objekten

Die Administration der drei Rollen im SM-Z erfolgt durch die Identifizierungsmerkmale Funktionsgruppe (z.B. ADMIN-Net, ADMIN-Local) und der zugehörige(n) PIN(s).

– Der netzweite Administrator (ADMIN-Net) identifiziert sich durch die Funktionsgruppe ADMIN-Net und die Eingabe der zugehörigen PIN.

– Der zweite netzweite Administrator (ADMIN-Net_x_2) identifiziert sich durch die Eingabe der Funktionsgruppe ADMIN-Net und durch die Eingabe seiner PIN. Erst nach Eingabe der zweiten PIN sind die zusätzlichen Rechte der ADMIN-Net_x_2 verfügbar.



– Der lokale Administrator (ADMIN-Local) identifiziert sich durch die Funktionsgruppe ADMIN-Local und die Eingabe der zugehörigen PIN.

3.1.5 Bedrohungen

Die im folgenden angeführten angenommenen Bedrohungen ergeben sich letztlich aus den zwei Grundbedrohungen von IT-Produkten: dem Verlust der Vertraulichkeit und dem Verlust der Integrität von Informationen, die durch dieses Produkt "verwaltet" werden.

Es werden die folgenden Bedrohungen (Threats) angenommen:

Thr1: Unberechtigter Zugriff auf die im SM-Z abgelegten Daten.
Hinweis: Ein Zugriff ist unberechtigt, wenn die entsprechende Zuordnung Subjekt / Objekt / Aktion in der Tabelle 2 nicht markiert ist.

Thr2: Unerkannte Manipulation zu schützender Daten (Obj1 und Obj2) und Offenlegung von vertraulichen Daten (Obj3), die auf dem Übertragungsweg zum / vom HiGruSys gelangen.

Thr3: Vortäuschen der falschen Identität durch einen "Kommunikationspartner" (Sub4 und Sub9).

3.1.6 Sicherheitsziele

Das SM-Z dient der Wahrung der Vertraulichkeit und der Wahrung der Integrität durch Erreichung der folgenden Sicherheitsziele:

STar1: Integere und vertrauliche Speicherung von kryptographischen Schlüsseln (Obj4-7) und vertrauliche Speicherung von vertraulichen Daten (Obj8, die Daten werden im SM-Z in verschlüsselter Form gespeichert).

STar2: Integerer Export und Import von kryptographischen Schlüsseln (Obj5-7). Der Schlüsselimport mittels dem Chipkartenterminal CKT erfolgt in verschlüsselter Form auf der Basis eines dynamischen Transportschlüssels (ZST). Der Transportschlüssel wird mittels dem Schlüssel COM verschlüsselt zwischen dem SM-Z und dem CKT ausgetauscht. Der Schlüssel COM wird, wie in [PER-DEV] Kapitel 5.6 und 5.7 beschrieben, ausschließlich während des Erstpersonalierungsvorganges in das SM-Z geladen.

STar3: Unterstützung eines vertraulichen und integeren Datenaustauschs zwischen dem HiGruSys (Sub6) und dem EG oder SM-K (Sub9) (Manipulationen während einer Datenübertragung können nicht verhindert werden, müssen aber zuverlässig als solche erkannt werden).

STar4: Unterstützung eines kryptographisch gesicherten Transfers von Gebühren (Obj2) aus dem SM-K (Sub9) in das HiGruSys (Sub6)

STar5: Kryptographisch relevante Kommunikation des HiGruSys (Sub6) nur mit authentischen Partnern (Sub4 und Sub9)

3.2 Sicherheitsfunktionen

Keine der in den ITSEC angebotenen Funktionalitätsklassen deckt die Sicherheitsfunktionen des SM-Zs ab. Um den unter 3.1.5 genannten Bedrohungen wirkungsvoll zu begegnen, verfügt das SM-Z über die folgenden Sicherheitsfunktionen, die in den nachfolgenden Kapiteln näher erläutert werden:

SF1: Identifikation und Authentisierung (I&A)

SF2: Verschlüsselung (ENC)

SF3: MAC-Sicherung (INT)

SF4: Zugriffsschutz (AC)

3.2.1 SF1: Identifikation und Authentisierung (I&A)

Das SM-Z hat die Aufgabe, das HiGruSys (Sub6) bei der Identifikation von bzw. gegenüber dezentralen Sicherheitsmodulen SM-K (Sub9; vgl. Kapitel 0) zu unterstützen, indem es die dafür notwendigen kryptographischen Aufgaben übernimmt. Zusätzlich identifiziert das SM-Z das zu seiner Administration zugelassene Personal (Sub4).

Die Authentisierung erfolgt durch Zurverfügungstellung und Prüfung einer dem jeweiligen Subjekt zugeordneten Authentisierungsinformation durch ein zugehöriges Authentisierungsverfahren (Challenge and Response oder Präsentation einer persönlichen Identifikationsnummer -PIN-). Die Authentisierungsinformationen sind dabei gegen unbefugten Zugriff geschützt im SM-Z abgelegt. Die Authentisierungsverfahren unterscheiden sich nach einseitiger und zweiseitiger Authentikation.

Das Ergebnis einer Authentisierung wird vom SM-Z oder HiGruSys (Sub6) derart ausgewertet, daß mehrere aufeinander folgende erfolglose Authentisierungsversuche erkannt und weitere verhindern werden.

I&A SM-K / SM-Z

Gegenüber dem dezentralen Sicherheitsmodul SM-K (Sub9) erfolgt eine zweiseitige Authentisierung. Sie dient als Grundlage zum Aufbau einer gesicherten Verbindung zwischen SM-K (Sub9) und dem HiGruSys (Sub6). Die erfolgreiche Authentisierung des SM-K (Sub9) durch das SM-Z ist zusätzlich die zwingende Voraussetzung zur Freigabe der kryptographisch gesicherten Download Funktionen (Schlüssel, Parameter, SW und FW) zum SM-K (Sub9) oder zum EG durch das HiGruSys (Sub6).

Bei der einseitigen Authentisierung identifiziert und authentisiert sich das zur Administration des SM-Z zugelassene Personal des Netzbetreibers (Sub4) mittels den im Kapitel 3.1.2.1 definierten Rollen gegenüber dem SM-Z. In jedem Fall ist die erfolgreiche Authentisierung die zwingende Voraussetzung für die Administration des SM-Z. Die Firmware des SM-Z stellt sicher, daß die Eingabe der zur Authentisierung erforderlichen PINs nur in verschlüsselter Form erfolgt.

Unter Administration verstehen wir hier die folgenden Funktionen:

– Ändern von Benutzungsprofilen (Obj1.2) der Schnittstelle zum HiGruSys (Sub6) oder zum SKM (SS / SM-HSI),

– Generieren von Schlüsseln,

– Importieren von Schlüsseln und

– Exportieren von Schlüsseln (ohne die Funktionen, die vom HiGruSys (Sub6) ausgeführt werden)

3.2.2 SF2: Verschlüsselung (ENC)

Das SM-Z kann vom HiGruSys (Sub6) erhaltene Datenelemente (Obj3) zum vertraulichen Transport zum SM-K (Sub9) verschlüsseln. Die verwendeten Schlüssel werden vom Netzbetreiber (Sub5) generiert und vom SM-Z für jedes SM-K (Sub9) individuell abgeleitet. Zusätzlich geht eine Sequenznummer zum Schutz gegen Replay-Attacken in die Verschlüsselung der Daten ein. Die Schlüssel sind in einer Weise geschützt, daß kein Unbefugter Zugang erlangen kann.

Die Firmware des SM-Z stellt sicher, daß der Import und Export von Schlüsseln in / aus das / dem SM-Z nur in verschlüsselter Form erfolgt.

3.2.3 SF3: MAC-Sicherung (INT)

Das SM-Z kann schützenswerte Datenobjekte (Obj2) zwecks integerer Übertragung von und zum HiGruSys (Sub6) zur Erkennung von Manipulationen MAC-prüfen bzw. MAC-sichern.

So werden beispielsweise Kommandos, die vom HiGruSys (Sub6) generiert und anschließend vom SM-K (Sub9) ausgeführt werden, mittels Kryptogramm (MAC über Kommando und Daten) gegen Manipulationen geschützt. Solch ein Kommando wird vom SM-K (Sub9) erst dann ausgeführt, wenn die Prüfung des Kryptogramms positiv verlaufen ist.

Datenelemente werden vor der Übertragung zum HiGruSys (Sub6) vom SM-K (Sub9) mit einem MAC versehen. Dieser MAC kann dann vom SM-Z auf Korrektheit überprüft werden.

Die Firmware des SM-Z stellt sicher, daß der Import und Export von Schlüsseln in/aus das/dem SM-Z nur in verschlüsselter Form erfolgt.

3.2.4 SF4: Zugriffskontrolle (AC)

Das SM-Z kann schützenswerte Datenobjekte (Obj1) mit Zugriffsbedingungen versehen. So können beispielsweise für Schreib- oder Lesezugriffe unterschiedliche Zugriffsbedingungen zugeordnet werden. Es ist möglich das Lesen eines Datenobjekts immer zuzulassen und gleichzeitig das Schreiben nur nach vorheriger Authentisierung eines Administrators (Sub4) zuzulassen. Außerdem kann der Zugriff auf Datenobjekte ausschließlich durch interne Funktionen, beispielsweise integriert in die Ausführung eines Kommandos, zugelassen sein.

Um die mißbräuchliche Verwendung von kryptographischen Schlüsseln (Obj4-8) zu verhindern, ist deren Funktion und Verwendung, ggf. auf bestimmte Objekte, festgelegt. Somit kann beispielsweise ein Schlüssel zum Integritätsschutz (MAC-Berechnung) nicht zur Sicherung der Vertraulichkeit (Ver- oder Entschlüsselung) verwendet werden. Insbesondere darf ein Schlüssel zur Verschlüsselung von Schlüsseln (KEK; Key Enciphering Key) nicht zur Entschlüsselung von Daten verwendet werden.

Die Zugriffsbedingungen werden vom FW-Hersteller bei der Kodierung oder vom Administrator entsprechend den Tabellen 2 und 3 festgelegt.

3.2.5 Zweckmäßigkeit und Wirksamkeit

Im Kapitel 0 wird die vorgesehene Art der Nutzung des SM-Zs beschrieben. Zusammenfassend ist dies der Einsatz zur

Anwendung 1 (App1): Identifikation und Authentisierung von dezentralen Sicherheitsmodulen (SM-K)

Anwendung 2 (App2): Identifikation und Authentisierung von Administratoren

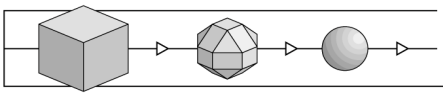
Anwendung 3 (App3): Unterstützung des Austauschs von vertraulichen Informationen mit dem SM-K

Anwendung 4 (App4): Unterstützung des Austauschs von integritätsgeschützten Informationen mit dem SM-K

Anwendung 5 (App5): Speichern und Führen von kryptographischen Schlüsseln und vertraulichen Datenobjekten.

Anwendung 6 (App6): Generierung von Daten zur erstmaligen Personalisierung oder zum Download für das SM-K.

Anwendung 7 (App7): Import und Export von kryptographischen Schlüsseln.



Die Funktionalität ist für die geplante Art der Nutzung sowohl geeignet als auch zweckmäßig, da sie alle dazu zitierten Sicherheitsfunktionen zur Verfügung stellt und zum Erreichen der Sicherheitsziele erforderlich ist und auch sämtlichen aus der geplanten Einsatzumgebung erwachsenden Bedrohungen entgegenwirkt.

Im einzelnen gilt dabei folgendes:

- SF1 (I&A) ist zweckmäßig für die Anwendungen 1 und 2. Diese Funktion prüft die ihr zur Verfügung gestellten (Authentisierungs-) Informationen auf "Korrektheit" und stellt seinerseits bei einer zweiseitigen Authentisierung die notwendigen (Authentisierungs-) Informationen für den Partner zur Verfügung, die dieser wiederum auf "Korrektheit" prüfen kann.

- SF2 (ENC) ist zweckmäßig für die Anwendungen 3 und 6 - 7. Diese Funktion verschlüsselt vom Hintergrundsystem erhaltene Informationen (App3) oder im SM-Z gespeicherte Informationen (App6), damit diese vertraulich zum SM-K übertragen werden können. Diese können dann im SM-K entschlüsselt und anschließend gespeichert oder ausgewertet werden.

- SF3 (INT) ist zweckmäßig für die Anwendungen 4 und 7. Diese Funktion erzeugt oder prüft den MAC von Informationen, die integer vom und zum Hintergrundsystem übertragen werden. Vom HiGruSys werden nur dann Daten als integer akzeptiert, wenn die Prüfung des MAC positiv war.

- SF4 (AC) ist zweckmäßig für die Anwendung 5. Diese Funktion verhindert unzulässige Zugriffe auf schützenswerte Daten, die im SM-Z gespeichert sind.

	SF1	SF2	SF3	SF4
App1				
App2				
App3				
App4				
App5				
App6				
App7				

Tabelle 4: Zweckmäßigkeit Funktionalität

Eine detailliertere Analyse dieser Funktionalitätseigenschaften folgt später bei der Betrachtung der Wirksamkeitsaspekte.

Die Sicherheitsfunktionen sind als Schutz gegen die identifizierten Bedrohungen sowohl geeignet als auch zweckmäßig, weil jeder Bedrohung mindestens eine Sicherheitsfunktion entgegenwirkt.

Im einzelnen gilt dabei folgendes:

– SF1 wirkt Thr3 entgegen. Diese Funktion prüft die Identität eines Kommunikationspartners auf Basis geheimer Informationen und ggf. kryptographischer Algorithmen. Somit wird dem Vortäuschen einer falschen Identität entgegengewirkt.

– SF2 wirkt Thr2 entgegen. Diese Funktion verschlüsselt vertrauliche Daten auf Basis geheimer Informationen und kryptographischer Algorithmen. Somit wird der Offenlegung vertraulicher Daten entgegengewirkt.

– SF3 wirkt Thr2 entgegen. Diese Funktion berechnet oder prüft einen MAC über zu schützende Daten auf Basis geheimer Informationen und kryptographischer Algorithmen. Somit wird der unentdeckten Manipulation geschützter Daten entgegengewirkt.

– SF4 wirkt Thr1 entgegen. Diese Funktion überprüft, ob für die gewünschte Aktion auf ein Datenobjekt die Zugriffsberechtigungen erfüllt sind. Somit ist ein unberechtigter Zugriff auf Daten im SM-Z nicht möglich.

Die Tabelle 5 zeigt welchen Bedrohungen welche Sicherheitsfunktionen entgegen wirken.

	SF1	SF2	SF3	SF4
Thr1				
Thr2				
Thr3				

Tabelle 5: Entgegenwirken Sicherheitsfunktionen / Bedrohungen

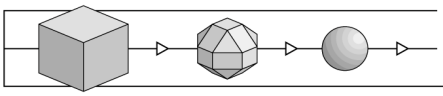
Die Sicherheitsfunktionen sind zur Erreichung der Sicherheitsziele sowohl geeignet als auch zweckmäßig, weil jede Sicherheitsfunktion mindestens zur Erreichung eines Sicherheitsziels beiträgt.

Im einzelnen gilt dabei folgendes:

– SF1 trägt zur Erreichung von STar3 und STar5 bei. Diese Funktion prüft die Authentizität eines Kommunikationspartners auf Basis geheimer Informationen und kryptographischer Algorithmen. Somit ist einerseits sichergestellt, daß eine kryptographisch relevante Kommunikation nur mit authentischen Partnern (STar5) erfolgen kann, was andererseits Voraussetzung für einen vertraulichen und integeren Datenaustausch beispielsweise mit dem HiGruSys (STar3) ist.

– SF2 trägt zur Erreichung von STar2 und STar3 bei. Diese Funktion verschlüsselt vertrauliche Daten auf Basis geheimer Informationen und kryptographischer Algorithmen. Somit ist sichergestellt, daß ein vertraulicher Datenaustausch mit dem HiGruSys erfolgen kann.

– SF3 trägt zur Erreichung von STar2, STar3 und STar4 bei. Diese Funktion berechnet oder prüft einen MAC über geschützte Daten auf Basis geheimer Informationen und



kryptographischer Algorithmen. Somit ist sichergestellt, daß ein integerer Datenaustausch (STar2 und STar3) mit dem HiGruSys und ein kryptographisch gesicherter Transfer von Gebühren (STar4) aus dem SM-K in das HiGruSys erfolgen kann. Hierbei ist zu beachten, daß Manipulationen an den Daten nicht verhindert, jedoch erkannt werden können.

– SF4 trägt zur Erreichung von STar1 bei. Diese Funktion überprüft ob für die gewünschte Aktion auf ein Datenobjekt die Zugriffsberechtigungen erfüllt sind. Somit ist, wenn die in Tabelle 2 definierten Zugriffsbedingungen korrekt implementiert sind, die sichere und vertrauliche Speicherung von kryptographischen Schlüsseln und vertraulichen Daten gewährleistet.

Die Tabelle 6 zeigt, welcher Bezug zwischen den Sicherheitsfunktionen und den geforderten Sicherheitszielen existiert.

	SF1	SF2	SF3	SF4
STar1				
STar2				
STar3				
STar4				
STar5				

Tabelle 6: Bezug Sicherheitsfunktionen / Sicherheitsziele

3.3 Mechanismen

Die folgenden Abschnitte legen die geplanten Realisierungen der in Kapitel 3.2 spezifizierten Sicherheitsfunktionen dar. Da sich das Produkt noch im Entwicklungsstadium befindet und Änderungen an den vorgesehen Mechanismen eintreten können, wird an dieser Stelle nur eine zusammenfassende Beschreibung gegeben. Die Identifizierung der einzelnen Sicherheitsmechanismen erfolgt später im Feinentwurf.

3.3.1 SF1: Identifikation und Authentisierung (I&A)

Zur Identifikation und Authentisierung werden abhängig davon, welche Partner aktiv sind, unterschiedliche Verfahren verwendet. Grundsätzlich gilt jedoch im Falle einer Authentisierung nach dem ' Challenge and Response '-Prinzip, daß immer der Challenger als jeweilige authentisierende Komponente die Challenge in Form einer Zufallszahl generiert und die Response, die der Responder unter Verwendung eines gemeinsamen Geheimnisses berechnet, prüft. Ist die Prüfung der Response positiv, ist der Responder authentisch.

I&A SM-Z ⇔ SM-K

Bei der Authentisierung SM-Z ⇔ SM-K handelt es sich um eine gegenseitige Authentisierung.

Zuerst generiert das SM-K eine Zufallszahl (RND_1), diese wird vom SM-Z mit dem Authentisierungsschlüssel K_{Auth} des SM-K verschlüsselt und als Signatur (SIG_1) an das SM-K übergeben. Die Verschlüsselung erfolgt mit dem Double (Triple) DES-Algorithmus.

Im Gegenzug wird vom SM-Z eine Zufallszahl (RND_2) generiert, diese wird vom SM-K mit seinem Authentisierungsschlüssel K_{Auth} verschlüsselt und als Signatur (SIG_2) an das SM-Z zurückgeschickt. Die Verschlüsselung erfolgt mit dem Double (Triple) DES-Algorithmus.

Die allgemeine Form zur Berechnung der Signatur ist:

$$SIG_i = e_{dDES}\, K_{Auth}(RND_i) \quad | \; i = 1 \ldots 2$$

Auf diese Weise kann jeder Authentisierungspartner prüfen, ob der jeweils andere im Besitz des gemeinsamen Geheimnisses (K_{Auth}) ist.

I&A Administrator

Bei der Authentisierung Administrator $\Rightarrow$ SM-Z handelt es sich um eine einseitige Authentisierung.

Der Administrator gibt über die Tastatur des Chipkartenterminals (CKT) seine persönliche Identifikationsnummer (PIN) ein. Die eingegebene PIN wird im Chipkartenterminal mittels eines Session Keys verschlüsselt und anschließend verschlüsselt zum SM-Z übertragen (Transportsicherung). Das SM-Z entschlüsselt die empfangene PIN und überprüft durch einen einfachen Vergleich der präsentierten entschlüsselten PIN mit der vertraulich gespeicherten PIN, die der gewünschten Administrationsrolle zugeordnet ist, ob der Administrator im Besitz des gemeinsamen Geheimnisses (PIN) ist. Bei positivem Vergleich wird der Fehlversuchszähler auf seinen Initialisierungswert gesetzt. Die PIN hat eine Länge von 6-14 numerischen Stellen.

3.3.2 SF2: Verschlüsselung (ENC)

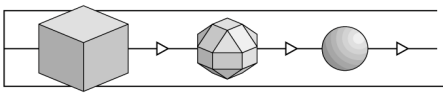
Zur Verschlüsselung von vertraulich übertragenen Informationen wird der DES-Algorithmus in verschiedenen Modi verwendet.

Zur Verschlüsselung

- der FW des SM-K wird der DES im CBC-Mode,
- der Schlüssel wird der DES in der Variante Triple DES im ECB-Mode,
- von Parametern wird der DES im ECB-Mode verwendet.

3.3.3 SF3: MAC-Sicherung (INT)

Zur Berechnung und Prüfung von MACs wird der DES-Algorithmus im CBC-Mode verwendet.



3.3.4 SF4: Zugriffskontrolle (AC)

Im SM-Z sind für verschiedene Aktionen auf Datenobjekten (Act1-4) Zugriffsbedingungen zugeordnet. Die vorgesehenen Zugriffsbedingungen sind für die Datenobjekte des SM-Z:

– *anyone* - jeder darf zugreifen -,

– *authentic* - nur ein authentischer Partner (Administrator) darf zugreifen -,

– *enciphered* - die Daten, die an der Schnittstelle SS / SM-HSI verwendet werden sind verschlüsselt -,

– *authentic & enciphered* - Kombination aus *authentic* und *enciphered* und

– *internal.*

Die Zugriffsbedingung *internal* ist jedem Datenobjekt zugeordnet, wenn mindestens eine SW- / FW-Funktion implizit auf dessen Daten zugreift.

3.4 Mindeststärke der Mechanismen und Evaluationsstufe

Für das SM-Z sollen die verwendeten Mechanismen die Mindeststärke *hoch* erreichen.

Für das SM-Z wird die Evaluationsstufe mit *E3* festgelegt.

3.5 Anhang zu den Sicherheitsvorgaben

3.5.1 Referenzen

[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,
Siemens Nixdorf Informationssysteme AG

[PER-DEV] Spezifikation Personalisierung ladbarer Geräte, Version V 3.1c, Siemens Nixdorf Informationssysteme AG

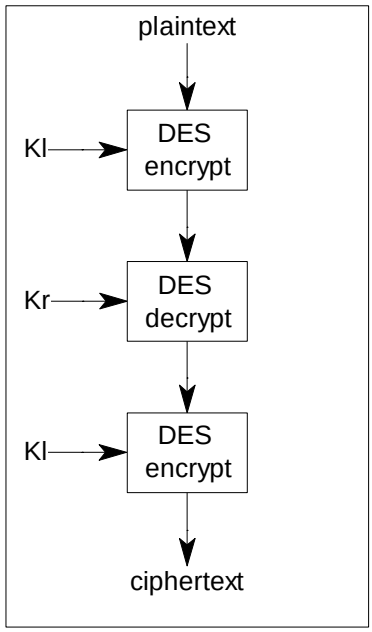
3.5.2 Begriffe und Abkürzungen

DES-Schlüssel

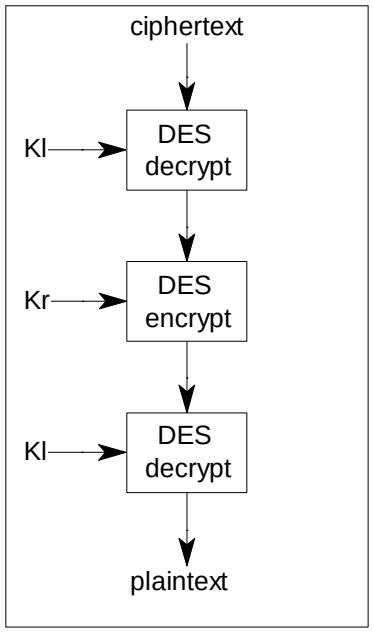
Es werden zwei Typen von DES-Schlüsseln, nämlich sDES-Schlüssel (single-DES oder auch einfach lange DES-Schlüssel) und dDES-Schlüssel (double-DES oder doppelt lange Schlüssel), unterschieden. sDES-Schlüssel bestehen aus einer Schlüsselkomponente (**K**) und dDES-Schlüssel bestehen aus zwei Schlüsselkomponenten (**K = Kl || Kr**).
Jede Schlüsselkomponente hat eine Länge von 8 Byte, wovon 7 Bit je Byte als Schlüssel in die Ver-/ Entschlüsselung eingehen und das Bit 2^0 als Paritäts-Bit (odd) verwendet wird. Die 56 Bit einer Schlüsselkomponente sollen bei der Generierung zufällig gewählt werden. Bei Verwendung eines dDES-Schlüssels als sDES-Schlüssel wird dessen erste Schlüsselkomponente (**K = Kl**) verwendet.

Double (Triple) DES

Dieser Algorithmus basiert auf dem DES-Algorithmus. Es wird ein doppelt langer Schlüssel **K= Kl || Kr** (dDES-Schlüssel).



Verschlüsselung



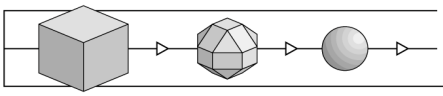
Entschlüsselung

$d_{dDES}K(x)$ kennzeichnet eine Entschlüsselung des Klartextes x mit dem Schlüssel K unter Verwendung des 'Double (Triple) DES'-Algorithmus

$d_{sDES}K(x)$ kennzeichnet eine Entschlüsselung des Klartextes x mit dem Schlüssel K unter Verwendung des 'DES'-Algorithmus

$e_{dDES}K(x)$ kennzeichnet eine Verschlüsselung des Klartextes x mit dem Schlüssel K unter Verwendung des 'Double (Triple) DES'-Algorithmus

$e_{sDES}K(x)$ kennzeichnet eine Verschlüsselung des Klartextes x mit dem Schlüssel K unter Verwendung des 'DES'-Algorithmus

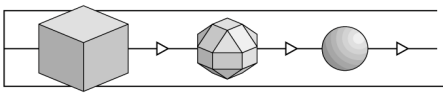


EG	**E**nd**g**erät
HiGruSys	**Hi**nter**gru**nd**sys**tem
IKL	**I**ntelligenter **K**arten**l**eser
N.I.K.E.	**N**eue **I**nfrastruktur für **K**arten und kartenbezogene **E**ndeinrichtungen der Deutschen Telekom AG
RM	**R**isk **M**anagement
SecServ	**Sec**urity **Serv**er
SD	**S**ecure **D**evice
SM-K	**S**icherheits**m**odul im **K**artenleser
SM-Z	**S**icherheits**m**odul **z**entral
SKM	**S**ICRYPT **K**ey **M**anagement
SRS	**S**ICRYPT Server **R**untime **S**oftware

4 Hinweise und Empfehlungen zum zertifizierten Objekt

23 Die Ausführungen in Kapitel 2 sind als Ergebnis der Evaluierung zu beachten.

24 Bei der Zertifizierung haben sich keine weitergehenden Hinweise oder Empfehlungen für den Anwender ergeben.



5 Hinweise zu den Vorgaben und Kriterien

25 Dieser Abschnitt soll einen Überblick über die Vorgaben und Kriterien geben, die bei der Evaluierung zugrunde lagen, und deren Bewertungsmaßstäbe erläutern.

5.1 Grundbegriffe

26 *Sicherheit* ist nach dem Verständnis der ITSEC dann gegeben, wenn ausreichendes Vertrauen darin besteht, daß das Produkt oder System seine *Sicherheitsziele* erfüllt.

27 *Sicherheitsziele* setzen sich in der Regel aus Forderungen nach

- Vertraulichkeit
- Verfügbarkeit
- Integrität

von bestimmten Datenobjekten zusammen. Solche Sicherheitsziele werden bei einem Produkt durch den Hersteller oder Anbieter, bei einem System durch den Anwender festgelegt.

28 Den festgelegten Sicherheitszielen stehen *Bedrohungen* gegenüber, nämlich der Verlust der Vertraulichkeit, der Verlust der Verfügbarkeit, der Verlust der Integrität bestimmter Datenobjekte.

29 Solche Bedrohungen werden Realität, wenn Subjekte unerlaubt Daten mitlesen oder abhören, Dritten vorenthalten oder unbefugt ändern können.

30 *Sicherheitsfunktionen* in dem betrachteten Produkt oder System sollen solche *Angriffe* abwehren.

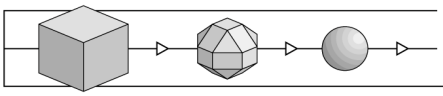
31 Es stellen sich dabei zwei Grundfragen:

- Funktionieren die Sicherheitsfunktionen korrekt?
- Sind sie wirksam?

Vertrauen in die Erfüllung der Sicherheitsziele kann man also dann haben, wenn *Korrektheit* und *Wirksamkeit* geprüft (*evaluiert*) worden sind.

5.2 Evaluationsstufen

32 Eine Evaluierung kann nur mit begrenztem Aufwand und in begrenzter Zeit durchgeführt werden. Die mögliche Tiefe einer Evaluierung ist also stets be-



grenzt. Das Angemessenheitsprinzip verbietet es andererseits, bei geringem Sicherheitsbedarf eine extrem aufwendige Prüfung durchzuführen; ebenso unangemessen wäre es, bei höchstem Sicherheitsbedarf nur „oberflächlich“ zu prüfen.

33 Es ist deshalb sinnvoll, unterschiedliche Prüftiefen (und damit Prüfaufwände) festzulegen: In den ITSEC werden 6 Evaluationsstufen zur Prüfung von Korrektheit und Wirksamkeit definiert. E1 bezeichnet die niedrigste, E6 die höchste Stufe.

34 Die Vertrauenswürdigkeit eines Produktes oder Systems kann also nach diesen Stufen „gemessen“ werden.

35 Die folgenden Auszüge aus den ITSEC lassen erkennen, welche Prüfaspekte im Rahmen einer Evaluierung behandelt werden und welche Prüftiefe welcher E-Stufe entspricht.

36 Die Aufzählung beinhaltet zunächst gewisse Anforderungen an die Korrektheit und läßt die Tiefe der Prüfung erkennen („EVG“ meint das zu prüfende Produkt oder System):

E1 „Auf dieser Stufe müssen für den EVG die Sicherheitsvorgaben und eine informelle Beschreibung des Architekturentwurfs vorliegen. Durch funktionale Tests muß nachgewiesen werden, daß der EVG die Anforderungen der Sicherheitsvorgaben erfüllt.“

E2 „Zusätzlich zu den Anforderungen für die Stufe E1 muß hier eine informelle Beschreibung des Feinentwurfs vorliegen. Die Aussagekraft der funktionalen Tests muß bewertet werden. Ein Konfigurationskontrollsystem und ein genehmigtes Distributionsverfahren müssen vorhanden sein.“

E3 „Zusätzlich zu den Anforderungen für die Stufe E2 müssen der Quellcode bzw. die Hardware-Konstruktionszeichnungen, die den Sicherheitsmechanismen entsprechen, bewertet werden. Die Aussagekraft der Tests dieser Mechanismen muß bewertet werden.“

E4 „Zusätzlich zu den Anforderungen für die Stufe E3 muß ein formales Sicherheitsmodell Teil der Sicherheitsvorgaben sein. Die sicherheitsspezifischen Funktionen, der Architekturentwurf und der Feinentwurf müssen in semiformaler Notation vorliegen.“

E5 „Zusätzlich zu den Anforderungen für die Stufe E4 muß ein enger Zusammenhang zwischen dem Feinentwurf und dem Quellcode bzw. den Hardware-Konstruktionszeichnungen bestehen.“

E6 „Zusätzlich zu den Anforderungen für die Stufe E5 müssen die sicherheitsspezifischen Funktionen und der Architekturentwurf in einer for-

malen Notation vorliegen, die konsistent mit dem zugrundeliegenden formalen Sicherheitsmodell ist."

37 In jeder der Stufen E1 bis E6 müssen darüber hinaus Wirksamkeitsaspekte nach folgendem Schema untersucht werden:

Alle E-Stufen

"Die Bewertung der Wirksamkeit erfordert die Betrachtung der folgenden Aspekte des EVG:

a) die Eignung der sicherheitsspezifischen Funktionen des EVG, den in den Sicherheitsvorgaben aufgezählten Bedrohungen zu widerstehen;

b) die Fähigkeit der sicherheitsspezifischen Funktionen und Mechanismen des EVG, in einer Weise zusammenzuwirken, daß sie sich gegenseitig unterstützen und ein integriertes, wirksames Ganzes bilden;

c) die Fähigkeit der Sicherheitsmechanismen des EVG, einem direkten Angriff zu widerstehen;

d) ob bekannte Sicherheitsschwachstellen in der Konstruktion des EVG in der Praxis die Sicherheit des EVG kompromittieren können;

e) daß der EVG nicht in einer Weise konfiguriert werden kann, die unsicher ist, aber von der ein Systemverwalter oder ein Endnutzer vernünftigerweise glauben könnte, daß sie sicher ist;

f) ob bekannte Sicherheitsschwachstellen beim Betrieb des EVG in der Praxis die Sicherheit des EVG kompromittieren können."

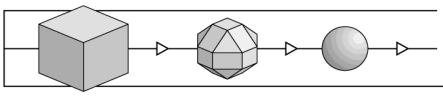
5.3 Sicherheitsfunktion und Sicherheitsmechanismen

38 Typische Beispiele für Sicherheitsfunktionen sind die *Identifikation und Authentisierung* (von Subjekten), die *Zugriffskontrolle*, die *Beweissicherung* (Protokollierung), die *Protokollauswertung*, die *Übertragungssicherung*. Ein Produkt oder System kann solche Sicherheitsfunktionen beinhalten.

39 Meist kommen solche Sicherheitsfunktionen in einer typischen Kombination („Funktionalitätsklasse“) vor.

Beispiel: Die Funktionalitätsklasse F-C2 setzt sich aus den Funktionen *Identifikation und Authentisierung*, *Zugriffskontrolle*, *Beweissicherung*, *Protokollauswertung* und *Wiederaufbereitung* zusammen. Diese Klasse ist bei vielen kommerziellen Betriebssystemen gegeben.

40 Jede Sicherheitsfunktion kann auf unterschiedlichste Weise realisiert werden.



Beispiel: Die Funktion *Identifikation und Authentisierung* kann unter anderem durch ein Paßwort-Verfahren, durch Verwendung von Chipkarten mit Challenge-Response Verfahren oder durch biometrische Verfahren realisiert sein.

41 Jede Realisierung dieser Art heißt *(Sicherheits-)Mechanismus* der Sicherheitsfunktion *Identifikation und Authentisierung*.
Für andere Sicherheitsfunktionen gilt sinngemäß das gleiche.

42 Die Wiederstandskraft eines Sicherheitsmechanismus gegenüber direkten Angriffen wird als *Stärke* des Mechanismus bezeichnet.

43 In den ITSEM werden zwei Arten von Mechanismen unterschieden: Typ B und Typ A.

Typ B „Ein Mechanismus vom Typ B ist ein Sicherheitsmechanismus, der bei perfekter Konzipierung und Implementierung keine Schwächen aufweist. Ein Mechanismus vom Typ B kann als nicht durch einen direkten Angriff überwindbar betrachtet werden, gleichgültig, wie groß der Aufwand an Ressourcen, Fachkenntnissen und entsprechenden Gelegenheiten ist. Ein mögliches Beispiel für einen Mechanismus vom Typ B wäre die Zugangskontrolle auf der Basis von Zugangskontrollisten: Bei perfekter Konzipierung und Implementierung kann dieser Mechanismus vom Typ B nicht durch einen direkten Angriff überwunden werden. Mechanismen vom Typ B können jedoch durch indirekte Angriffe überwunden werden, mit denen sich andere Wirksamkeitsanalysen befassen."

Typ B Mechanismen sind in diesem Sinne unüberwindbar.

Typ A „Ein Mechanismus vom Typ A ist ein Sicherheitsmechanismus mit einer potentiellen Schwachstelle in seinem Algorithmus, seinen Prinzipien oder seinen Eigenschaften, aufgrund derer er durch Einsatz ausreichender Ressourcen, Fachkenntnisse und entsprechender Gelegenheiten mit einem direkten Angriff überwunden werden kann. Ein Beispiel für einen Mechanismus vom Typ A ist ein Authentisierungsprogramm, bei dem ein Paßwort verwendet wird; wenn das Paßwort erraten werden kann, indem nacheinander alle möglichen Paßwörter ausprobiert werden, handelt es sich um einen Authentisierungsmechanismus vom Typ A. Mechanismen vom Typ A bedienen sich häufig eines "Geheimnisses" wie etwa eines Paßwortes oder eines kryptographischen Schlüssels.“

„Alle Mechanismen vom Typ A ... haben eine Stärke, die dem Aufwand an Ressourcen, Fachkenntnissen und Gelegenheiten, zur Gefährdung der Sicherheit durch einen direkten Angriff auf den Mechanismus entspricht.“

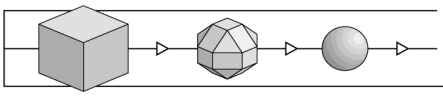
44 Wie wird nun bei Typ A Mechanismen die Stärke definiert?

„Alle kritischen Sicherheitsmechanismen (d.h. diejenigen, deren Versagen eine Sicherheitslücke hervorrufen würde), werden hinsichtlich ihrer Fähigkeit bewertet, einem direkten Angriff zu widerstehen. Die Mindeststärke jedes kritischen Mechanismus wird entweder als niedrig, mittel oder hoch bewertet.

niedrig „Damit die Mindeststärke eines kritischen Mechanismus als niedrig eingestuft werden kann, muß erkennbar sein, daß er Schutz gegen zufälliges unbeabsichtigtes Eindringen bietet, während er durch sachkundige Angreifer überwunden werden kann.“

mittel „Damit die Mindeststärke eines kritischen Mechanismus als mittel eingestuft werden kann, muß erkennbar sein, daß er Schutz gegen Angreifer mit beschränkten Gelegenheiten oder Betriebsmitteln bietet.“

hoch „Damit die Mindeststärke eines kritischen Mechanismus als hoch eingestuft werden kann, muß erkennbar sein, daß er nur von Angreifern überwunden werden kann, die über sehr gute Fachkenntnisse, Gelegenheiten und Betriebsmittel verfügen, wobei ein solcher erfolgreicher Angriff als normalerweise nicht durchführbar beurteilt wird."



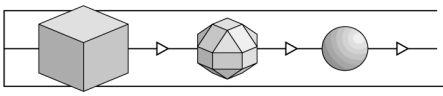
(Diese Seite ist beabsichtigterweise leer.)

6 Anhänge

6.1 Glossar

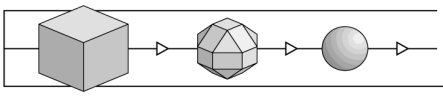
Das Glossar erläutert die in dieser Broschüre verwendeten Begriffe, erhebt allerdings keinerlei Anspruch auf Vollständigkeit oder Allgemeingültigkeit. Der Begriff *Sicherheit* meint hier stets Sicherheit im Kontext der Informationstechnik.

Akkreditierung	– Prozeß mit dem Ziel der Bestätigung, daß eine Prüfstelle den Anforderungen der Norm DIN EN 45001 entspricht. Eine Akkreditierung wird durch eine *Akkreditierungsstelle* durchgeführt. Allgemein anerkannt sind Akkreditierungen von Akkreditierungsstellen, die im Deutschen Akkreditierungsrat (DAR) vertreten sind. – Ergebnis eines Akkreditierungsverfahrens
Anerkennung	Ausdruck und Bestätigung der Gleichwertigkeit (von Zertifikaten und Lizenzen).
Auftraggeber	Eine natürliche oder juristische Person, die einen Auftrag (hier:) zur Zertifizierung oder Evaluierung erteilt; sie muß eine ausreichende Verfügungsberechtigung über das zu zertifizierende Objekt besitzen.
Common Criteria	Sicherheitskriterien, die aus dem amerikanischen Orange Book / den Federal Criteria, den europäischen ITSEC und den kanadischen CTCPEC hervorgegangen sind und ein weltweit akzeptierter Sicherheitsstandard werden sollen.
Bestätigungsstelle	Stelle, die im Einklang mit SigG und SigV Sicherheitsbestätigungen für technische Komponenten und für die Umsetzung von Sicherheitskonzepten bei Trust Centern herausgibt.
DebisZERT	Name des Zertifizierungsschemas von debis IT Security Services.
Dienstleistungsbereich	Bezeichnung für einen bestimmten Typ von Verfahren innerhalb von debisZERT.
DIN EN 45000	Normen-Reihe, die einschlägige Standards insbesondere für Prüf- und Zertifizierungsstellen enthält.
Einzelbericht	Bericht einer Prüfstelle zu einzelnen Prüfaspekten bei



	einer Evaluierung
Erst-Zertifizierung	Erstmalige Zertifizierung eines Produkts, Systems oder einer Dienstleistung.
Evaluationsstufen	s. Sicherheitsstufen.
Evaluator	Prüfer / in in einer Prüfstelle.
Evaluierung	Prüfung eines Produktes, Systems oder einer Dienstleistung auf der Basis von Sicherheitskriterien oder einer Sicherheitsnorm.
Evaluierungsbericht	Abschlußbericht einer Prüfstelle über Ablauf und Ergebnis einer Evaluierung. (Name „ETR“ im ITSEC-Kontext)
Hersteller-Laboratorium	Bei dem Hersteller eines Produkts / Systems oder bei dem Anbieter von Dienstleistungen angesiedelte Organisationseinheit, die Evaluierungen durchführt.
Integrität	Klassisches Sicherheitsziel: Daten sollen nur von Befugten geändert werden können.
IT-Dienstleistung	Dienstleistung, die sich bei ihrer Erbringung auf IT-Produkte und IT-Systeme abstützt.
IT-Komponente	Abgrenzbarer Teil eines IT-Produkts oder eines IT-Systems.
IT-Produkt	Software und / oder Hardware, die bei einem Anbieter (Hersteller, Vertreiber) erworben werden kann.
ITSEC	Information Technology Security Evaluation Criteria: Europäischer de facto Standard für die Evaluierung von IT-Produkten und IT-Systemen.
ITSEM	Information Technology Security Evaluation Manual: Handbuch zu den ITSEC, das vor allem die Durchführung von Evaluierungen betrifft.
IT-System	– Eine in sich funktionsfähige Kombination von IT-Produkten. – (ITSEC:) Eine reale Installation von IT-Produkten mit einer bekannten Einsatzumgebung.
Lizenz (persönliche)	Bestätigung einer persönlichen Qualifikation (hier im Kontext von debisZERT).
Lizenzierung	Verfahren der Überprüfung von Organisation und Qualifikation einer Prüfstelle im Hinblick auf den möglichen Abschluß einer Lizenzvereinbarung.
Lizenzvereinbarung	Vereinbarung zwischen einer Prüfstelle und einer Zertifizierungsstelle - den Ablauf und die Verantwortlichkeiten bei einer Evaluierung und Zertifizierung betreffend.

Meilensteinplan	Projekt- / Terminplan für die Durchführung einer Evaluierung und Zertifizierung
Problembericht	Bericht einer Prüfstelle an die Zertifizierungsstelle über besondere Probleme bei einer Evaluierung
Prüfbegleiter	Mitarbeiter / in der Zertifizierungsstelle, führt die Prüfbegleitung durch.
Prüfbegleitung	Verfahren der Zertifizierungsstelle, um die Ordnungsmäßigkeit (Kriterienkonformität, einheitliche Vorgehensweise und Bewertungen, etc.) einer Evaluierung zu überprüfen.
Prüfbericht	Einzelbericht oder Evaluierungsbericht
Prüfstelle	Stelle, die Evaluierungen durchführt.
Regulierungsbehörde	die nach §66 Telekommunikationsgesetz (TKG) zuständige Regulierungsbehörde für Telekommunikation und Post
Re-Zertifizierung	Nach Änderungen am zertifizierten Objekt notwendig werdende Zertifizierung der geänderten Version; kann auch bei Wechsel von Werkzeugen, Produktions- und Auslieferungsprozessen, Sicherheitskriterien erforderlich werden.
Sicherheitsbestätigung	In debisZERT eine juristisch verbindliche Bestätigung von Sicherheitseigenschaften; z.B. eine Bescheinigung, die die Erfüllung der Anforderungen des Signaturgesetzes bestätigt.
Sicherheitsfunktion	Funktionen eines IT-Produktes oder IT-Systems zur Abwehr bestimmter Bedrohungen.
Sicherheitskriterien	Dokument, das technische Anforderungen an Produkte, Systeme und / oder Dienstleistungen enthalten kann, zumindest aber die Evaluierung solcher Anforderungen beschreibt.
Sicherheitsnorm	Anforderungen an Produkte, Systeme oder Dienstleistungen die Sicherheit betreffend.
Sicherheitsstandard	Zusammenfassender Begriff für Sicherheitskriterien und Sicherheitsnormen.
Sicherheitsstufen	In manchen Kriterienwerken (z.B. ITSEC, CC) definierte Stufen, die aufgrund unterschiedlicher Anforderungen an das zu zertifizierende Objekt und an die Tiefe der Prüfung eine unterschiedlich hohe Sicherheit ausdrücken.
Sicherheitszertifikat	s. Zertifikat



Signaturgesetz - SigG	§3 des Informations- und Kommunikationsdienstegesetzes (IuKDG), in Deutschland gültig seit 1.8.1997.
Signaturverordnung - SigV	Amtliche Ausführungsbestimmungen zum Signaturgesetz.
System-Akkreditierung	Freigabe eines IT-Systems oder einer IT-Dienstleistung zur Nutzung (hier unter dem Blickwinkel ausreichender Sicherheit).
Trust Center	Stelle, die die Zugehörigkeit von Signaturschlüsseln zu einer Person durch ein (elektronisches) Zertifikat bestätigt - im Signaturgesetz als „Zertifizierungsstelle“ bezeichnet.
Verfahrenskennung	Code-Bezeichnung für ein Bestätigungsverfahren
Verfügbarkeit	Klassisches Sicherheitsziel: Daten sollen Befugten stets zur Verfügung stehen, d.h. nicht von Unbefugten vorenthalten werden können oder aufgrund technischer Defekte nicht verfügbar sein.
Verfügungsberechtigung	hier: Berechtigung, alle mit einer Evaluierung und Zertifizierung verbundenen Inspektionen an einem Produkt, System oder einer Dienstleistung zulassen zu können.
Vertraulichkeit	Klassisches Sicherheitsziel: Daten sollen nur durch Befugte zur Kenntnis genommen werden können.
Vor-Zertifizierung	Bestätigung der Ergebnisse einer Voruntersuchung einer produkt- bzw. prozeßspezifischen Sicherheitsnorm oder eines sicherheitsrelevanten Werkzeugs (im Hinblick auf spätere Zertifizierungen).
Zertifikat	Zusammenfassende (Kurz-)Darstellung eines Zertifizierungsergebnisses; wird durch die Zertifizierungsstelle ausgestellt.
Zertifizierer	Mitarbeiter / in einer Zertifizierungsstelle, die eine Zertifizierung durchführt.
Zertifizierung	Unabhängige Bestätigung der Ordnungsmäßigkeit einer Evaluierung. Auch Bezeichnung für das Gesamtverfahren bestehend aus Evaluierung, Prüfbegleitung und Ausstellung von Zertifikaten und Zertifizierungsreports.
Zertifizierungskennung	Code-Bezeichnung für ein Zertifizierungsverfahren.
Zertifizierungsreport	Bericht über Gegenstand, Ablauf und Ergebnis eines Zertifizierungsverfahrens; wird durch die Zertifizierungsstelle ausgestellt.
Zertifizierungsschema	Zusammenfassung aller Grundsätze, Regeln und Verfahren einer Zertifizierungsstelle.

Zertifizierungsstelle	Stelle, die Zertifizierungen durchführt. (s. auch *Trust Center* für eine zweite Bedeutung.)
ZKA-Kriterien	Sicherheitskriterien des Zentralen Kreditausschusses.

6.2 Referenzen

/ A00 / Lizenzierungsschema, 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)

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

/ 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

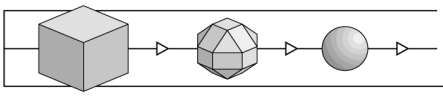
/ ITSEC / Information Technology Security Evaluation Criteria (ITSEC), Version 1.2 (1991), ISBN 92-826-3004-8

(deutsche Übersetzung:) Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC), Version 1.2 (1991), Bundesanzeiger-Verlag Köln, ISBN 92-826-3003-X

(französische Übersetzung:) Critères d'Évaluation de la Sécurité des Systèmes Informatiques (ITSEC), Version 1.2 (1991), ISBN 92-826-3005-6

/ ITSEM / Information Technology Security Evaluation Manual (ITSEM), Version 1.0 (1993), ISBN 92-826-7087-2

(deutsche Übersetzung:) Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEM), Version 1.0 (1993), Bundesanzeiger Verlag Köln, ISBN 92-826-7078-2



/ IuKDG / Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz - IuKDG), BGBl. I. vom 28. Juli 1997, Seite 1870 ff.

/ JIL / Joint Interpretation Library, Version 1.04, Dez 97

/ Mkat12 / Maßnahmenkatalog nach §12 Abs. 2, RegTP, http: / / www.RegTp.de / Fachinfo / DigitalSign / start.htm

/ Mkat16 / Maßnahmenkatalog nach §16 Abs. 6, RegTP, http: / / www.RegTp.de / Fachinfo / DigitalSign / start.htm

/ SigG / Artikel 3 von / IuKDG /

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

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

/ V01 / Zertifikate gemäß ITSEC / CC, Dienstleistungsbereich 1, debisZERT, Version 1.3, 5.8.98

/ V02 / Bestätigungen für Produkte gemäß Signaturgesetz, Dienstleistungsbereich 2, debisZERT, Version 1.3, 5.8.98

/ V04 / Zertifikate mit Anerkennung durch das BSI, Dienstleistungsbereich 4, debisZERT, Version 1.3, 5.8.98

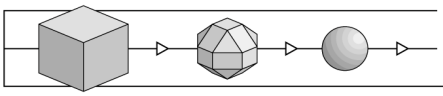
/ Z01 / Zertifizierungsschema, debis IT Security Services, Version 1.3, 5.8.98

/ Z02 / Zertifizierte IT-Produkte, IT- Systeme und IT-Dienstleistungen, debisZERT, Version 1.0, Stand: 5.8.98

6.3 Abkürzungen

AA	Arbeitsanweisungen
AIS	Anforderung einer Interpretation von Sicherheitskriterien
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI-Errichtungsgesetz
CC	Common Criteria
CTCPEC	Canadian Trusted Computer Products Evaluation Criteria
DAR	Deutscher Akkreditierungsrat

DBAG	Deutsche Bahn AG
DebisZERT	Zertifizierungsschema der debis IT Security Services
DEKITZ	Deutsche Akkreditierungsstelle für Informations- und Telekommunikationstechnik
DLB	Dienstleistungsbereich
EBA	Eisenbahn-Bundesamt
ETR	Evaluation Technical Report (Evaluierungsbericht)
EVG	Evaluationsgegenstand
IT	Informationstechnik
ITSEC	IT Security Evaluation Criteria
ITSEM	IT Security Evaluation Manual
IuKDG	Informations- und Kommunikationsdienstegesetz
LG	Lenkungsgremium
SigG	Signaturgesetz
SigV	Signaturverordnung
TKG	Telekommunikationsgesetz
ZKA	Zentraler Kreditausschuß
ZL	Leiter der Zertifizierungsstelle
ZZ	(für ein Verfahren) zuständiger Zertifizierer



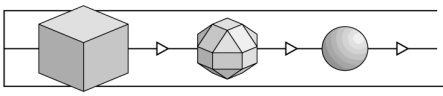
(Diese Seite ist beabsichtigterweise leer.)

7 Re-Zertifizierungen

Bei Änderungen an dem zertifizierten Objekt kann nach Maßgabe der Verfahrensregeln von debisZERT eine Re-Zertifizierung erfolgen. Die hier in zeitlicher Reihenfolge erscheinenden Anhänge beschreiben die Art der Änderungen, die neue Produktversion und den Zertifizierungsstatus.

Bei neuen Erkenntnissen über die Sicherheit des zertifizierten Objektes kann ein technischer Anhang zum Zertifizierungsreport herausgegeben werden.

Re-Zertifizierungen und neue technische Anhänge werden in der Druckschrift /Z02/ (s. Kapitel 1) und über WWW angekündigt.



Ende der Erstausgabe des Zertifizierungsreports.