debis

Services by DaimlerChrysler

Zertifizierungsreport

Hermes Online System, Version 2.0

Hermes Kreditversicherungs-AG

debisZERT-DSZ-ITSEC-04015-1999

debis IT Security Services

Die Dienstleister der Moderne

Vorwort

Das Hermes Online System, Version 2.0 der Hermes Kreditversicherungs-AG wurde gegen die *Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC)* und das *Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEM)* evaluiert. Die Evaluierung wurde im Rahmen des Zertifizierungsschemas debisZERT der debis IT Security Services durchgeführt. Die Zertifizierung erfolgte im Dienstleistungsbereich 4: *Zertifikate mit Anerkennung durch das BSI*.

Das Ergebnis lautet:

Sicherheitsfunktionalität:	Identifizierung und Authentisierung, Zugriffskontrolle, Unverfälschtheit, Übertragungssicherung
Evaluationsstufe:	E1
Mechanismenstärke:	hoch

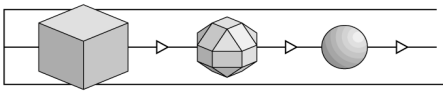
Die Ordnungsmäßigkeit der Evaluierung wird hiermit bestätigt.

Bonn, den 15.09.1999

Zertifizierer:	Leiter der Zertifizierungsstelle:
Klaus-Werner Schröder	Dr. Heinrich Kersten

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

✉ debis IT Security Services, - Zertifizierungsstelle -, Rabinstr. 8, 53111 Bonn
☎ 0228 / 9841-0, Fax: 0228 / 9841-60
💻 Email: debiszert@itsec-debis.de, Internet: www.debiszert.de



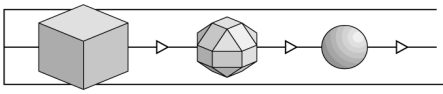
Revisionsliste

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	17.06.1999	Vorversion (nach Musterreport 1.5)
1.0	15.09.1999	Ersterstellung (nach Musterreport 1.5)

Inhalt



(Diese Seite ist beabsichtigterweise leer.)

1 Überblick

1.1 Evaluierung

1 Die Evaluierung wurde durch die Hermes Kreditversicherungs-AG, Friedensallee 254, 22763 Hamburg beauftragt.

2 Die Evaluierung wurde durchgeführt von Prüfstelle für IT-Sicherheit der debis Systemhaus Information Security Services GmbH und am 14.09.1999 beendet.

3 Die Evaluierung wurde gegen die *Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC)* und das *Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEM)* durchgeführt. Einige Hinweise zu den Inhalten der ITSEC und ITSEM finden sich im Kapitel 5.

1.2 Zertifizierung

4 Die Zertifizierung wurde gemäß den Regeln des Zertifizierungsschemas debisZERT 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 Deutsche 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

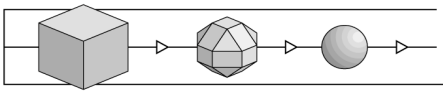
6 Dieser Zertifizierungsreport gibt die Ergebnisse der Evaluierung von Hermes Online System, Version 2.0 wieder - im folgenden als EVG = Evaluationsgegenstand bezeichnet.

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

8 Die numerierten Paragraphen in diesem Zertifizierungsreport sind formelle Aussagen der Zertifizierungsstelle. Unnumerierte Paragraphen enthalten Aussagen des Auftraggebers (Sicherheitsvorgaben) oder ergänzendes Material.

9 Der Zertifizierungsreport dient

- dem Auftraggeber als Nachweis der durchgeführten Evaluierung und



- dem Nutzer als Grundlage für den sicherheitsgerechten Einsatz von Hermes Online System, Version 2.0.

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

11 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 der Druckschrift

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

angekündigt.

1.4 Zertifikat

12 Eine Kurzfassung der Ergebnisse enthält das Sicherheitszertifikat debisZERT-DSZ-ITSEC-04015-1999.

13 Die Inhalte des Zertifikats werden in der Druckschrift

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

und über WWW veröffentlicht.

14 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.

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

16 Das Zertifikat trägt das vom BSI genehmigte Logo. Die Tatsache der Zertifizierung wird in der Broschüre 7148 des BSI aufgeführt.

1.5 Anwendung der Ergebnisse

17 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.

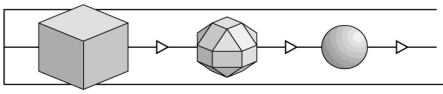
---

[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.

18 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.

19 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

20 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

21 Die Prüfstelle kommt zu folgendem Ergebnis:

- Der EVG genügt den Anforderungen der Evaluationsstufe E1 gemäß ITSEC, d.h. alle Anforderungen an die Korrektheit und Wirksamkeit gemäß dieser Stufe sind erfüllt. Dies sind:

  ITSEC E1.1 bis E1.37 für die Korrektheit mit den Phasen

Konstruktion - Entwicklungsprozeß	(Anforderungen, Architekturentwurf, Implementierung),
Konstruktion - Entwicklungsumgebung	(Konfigurationskontrolle),
Betrieb - Betriebsdokumentation	(Benutzerdokumentation, Systemverwalter-Dokumentation)
Betrieb - Betriebsumgebung	(Auslieferung und Konfiguration, Anlauf und Betrieb).

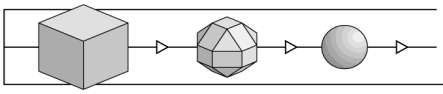
  ITSEC 3.12 bis 3.37 für die Wirksamkeit mit den Aspekten

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

- Die Mechanismen des EVG sind kritische Mechanismen; sie sind von folgendem Typ:

  Die Mechanismen des Typs A haben eine Mindeststärke gemäß der Stufe hoch.

  Für 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” unter den realen Einsatzbedingungen (s. Kapitel 3, Sicherheitsvorgaben) keine ausnutzbare Schwachstelle erkennbar ist.

2.3 Hinweise

22 Die Prüfstelle hat folgende Auflagen an den Auftraggeber auszusprechen.

Um die für den Brokat-Server identifizierten Schwachstellen in der Praxis wirkungsvoll abwehren zu können, muß durch die Hermes Kreditversicherungs-AG sichergestellt werden, daß der Brokat-Server aus dem Internet nur für die Dienste (Herstellen und Unterhalten einer gesicherten Kommunikationsverbindung mit dem Hermes-Applet) erreichbar ist, die für die Funktion des EVG benötigt werden. Alle eventuell weiter vorhandene Funktionalität muß vom Brokat-Server entfernt werden.

Die Hermes Kreditversicherungs-AG muß dem Benutzer für die sichere Nutzung des EVG die relevanten Informationen aus der Betriebsdokumentation zur Verfügung stellen.

23 Die Prüfstelle hat folgende Auflagen an den Benutzer auszusprechen.

Vor jeder Benutzung des von der Hermes Kreditversicherungs-AG über das Internet übertragenen Hermes-Applets muß sich der Benutzer davon überzeugen, daß er im Besitz eines authentischen und integeren Hermes-Applets ist. Um diese Prüfung zu ermöglichen, wurde das Hermes-Applet von der Hermes Kreditversicherungs-AG mit einer digitalen Signatur versehen. Ein Zertifikat, mit dem die Überprüfung dieser Signatur erfolgen kann, wurde von der Zertifizierungsstelle TC TrustCenter GmbH, Hamburg, beglaubigt. Das Zertifikat zur Überprüfung der digitalen Signatur wird ebenfalls mit dem Hermes-Applet über das Internet übertragen.

Ein Benutzer muß nun bei Erhalt des Hermes-Applets prüfen,

1. daß das Zertifikat zur Überprüfung der Signatur des Hermes-Applets authentisch ist und

2. daß die digitale Signatur des Hermes-Applets gültig ist.

Um Punkt 1. erfüllen zu können, muß der vom Kunden benutzte Internet-Browser über den entsprechenden public key der Zertifizierungsstelle TC TrustCenter GmbH authentisch verfügen. Die vom Benutzer zur Überprüfung der Punkte 1. und 2. durchzuführenden Schritte werden in der Benutzerdokumentation beschrieben und müssen dem Benutzer durch die Hermes Kreditversicherungs-AG zur Verfügung gestellt werden.

Der Benutzer darf als Internet Browser für die Kommunikation mit dem Server-Teil des EVG nur den Microsoft Internet Explorer, Version 4.0 einsetzen.

Der Benutzer muß als Betriebssystem MS Windows NT 4.0, SP3 verwenden.

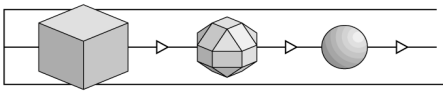
Der Benutzer muß seinen Internet-Browser für den sicheren Betrieb so konfigurieren, wie in der Benutzerdokumentation beschrieben.

Der Benutzer muß die digitale Signatur des Hermes-Applets nach jeder Übertragung des Hermes-Applets und vor jeder Benutzung prüfen.

Der Benutzer muß das vom Server während der Übertragung des Hermes-Applets mitgelieferte Zertifikat des Ausstellers mit der entsprechenden Funktion des Internet-Browsers überprüfen.

Der Benutzer darf keine Zertifikate von dem Internet-Browser unbekannten Zertifizierungsstellen akzeptieren.

Der Benutzer muß sich bewußt sein, daß das Nichtzustandekommen oder der Abbruch einer bestehenden Internetverbindung zur Hermes Kreditversicherungs-AG nicht nur auf technische Ursachen, sondern auch auf einen versuchten oder durchgeführten Angriff Dritter zurückzuführen sein kann.



(Diese Seite ist beabsichtigterweise leer.)

3 Sicherheitsvorgaben

24 Die der Evaluierung zugrunde liegenden Sicherheitsvorgaben, Version 1.14 vom 15.06.1999, sind seitens des Auftraggebers in deutscher Sprache bereitgestellt worden.

3.1 Sicherheitspolitik

3.1.1 Firmenspezifische Sicherheitspolitik

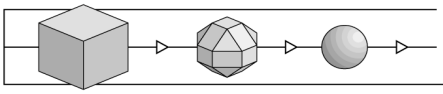
Die Hermes Kreditversicherungs-AG versichert ihre Kunden gegen Forderungsausfall bei Lieferung von Waren oder Dienstleistungen an deren Geschäftspartner. Die Kundendaten (z.B. Daten über Unternehmen, Geschäftspartner der Unternehmen, Bonitätsinformationen und weitere Daten von wirtschaftlichem Interesse) sind daher die am meisten schützenswerten Güter der Hermes Kreditversicherungs-AG.

Ihren Kunden sichert die Hermes Kreditversicherungs-AG die vertrauliche Behandlung der Details der geschäftlichen Beziehungen zu. Diese Vertraulichkeit ist Vorbedingung und Bestandteil jeder Geschäftsbeziehung der Hermes Kreditversicherungs-AG.

Ein Ziel der geschäftlichen Tätigkeit der Hermes Kreditversicherungs-AG ist es, ihre Kunden und sich selbst vor finanziellem Verlust und imagebezogenem Schaden zu schützen. Dem finanziellen Verlust wird durch Abschluß von Versicherungen vorgebeugt. Der imagebezogener Schaden wird durch vertrauliche Behandlung aller Geschäftsbeziehungen und aller im Besitz der Hermes Kreditversicherungs-AG vorhandenen wirtschaftlich relevanten Informationen verhütet.

3.1.2 System-Sicherheitspolitik

Die System-Sicherheitspolitik für das Hermes Online System der Hermes Kreditversicherungs-AG ergibt sich aus der Anwendung der Firmen-Sicherheitspolitik der Hermes Kreditversicherungs-AG auf das Hermes Online System der Hermes Kreditversicherungs-AG. Die System-Sicherheitspolitik beschreibt die Gesetze, Regeln und Praktiken, die festlegen, wie sensitive Informationen und andere Betriebsmittel im Hermes Online System der Hermes Kreditversicherungs-AG verwaltet, geschützt und verteilt werden. Sie zeigt die Sicherheitsziele des Systems und die Bedrohungen gegen das System auf. Diese Sicherheitsziele werden sowohl durch eine Kombination von sicherheitsspezifischen Funktionen im System (implementiert im EVG), als auch durch zugehörige materielle, personelle und organisatorische Maßnahmen erfüllt. Die System-Sicherheitspolitik beleuchtet alle Aspekte der Sicherheit, die das System betreffen, einschließlich der zugehörigen materiellen, organisatorischen und personellen Sicherheitsmaßnahmen. Nachfolgend werden die materiellen, organisatorischen und personellen Sicherheitsmaßnahmen beschrieben. Ab Kapitel 3.2 werden die Bestandteile der technischen Sicherheitspolitik beschrieben, ohne daß darauf noch einmal verwiesen wird.



3.1.2.1 Materielle Sicherheitsmaßnahmen

Vertrauliche Unterlagen werden ständig in einem verschlossenen Schreibtisch unter Verschluß gehalten und nur für Zwecke der Bearbeitung entnommen. Nach der Beendigung der Bearbeitung werden die vertrauliche Unterlagen wieder in den Schreibtisch eingeschlossen.

Der Schreibtisch befindet sich in einem verschlossenen Raum innerhalb einer Sicherheitszone des Rechenzentrums. Diese besteht aus einem abgetrennten Bereich des Rechenzentrums, der mit einer elektronischen Zutrittskontrolle überwacht wird. Zutritt erlangt nur derjenige, der mit einem entsprechend freigegebenen Firmenausweis das elektronische Schloß der Sicherheitszone öffnet.

In dieser Sicherheitszone ist auch die Hardware installiert, auf der das Hermes Online System der Hermes Kreditversicherungs-AG betrieben wird.

3.1.2.2 Organisatorische Sicherheitsmaßnahmen

Für jeden Mitarbeiter der Hermes Kreditversicherungs-AG sind seine Zuständigkeiten geregelt. Insbesondere haben nur bestimmte Mitarbeiter Zutritt zur Sicherheitszone des Rechenzentrums. Die Zuständigkeitsregelung umfaßt auch die Regelung der Stellvertretung.

Jeder Kunde hat ein für die Bearbeitung zuständiges Team. Kundenkontakte werden innerhalb des Teams durch den zuständigen Mitarbeiter oder einen Stellvertreter wahrgenommen.

3.1.2.3 Personelle Sicherheitsmaßnahmen

Bei Abschluß des Arbeitsvertrages werden die Mitarbeiter der Hermes Kreditversicherungs-AG auf ihre Pflicht zur vertraulichen Behandlung aller dienstlichen Angelegenheiten hingewiesen; eine entsprechende Vertraulichkeitserklärung ist Bestandteil aller Arbeitsverträge. Die Mitarbeiter werden zur Einhaltung der betrieblichen Regelungen zur Wahrung der Vertraulichkeit verpflichtet. Diese Verpflichtung gilt über das Ende der Arbeitsverhältnisses hinaus. Die Führungskräfte stellen die Einhaltung der Verpflichtungserklärung sicher und belehren ggf. neu.

3.1.2.4 Aufteilung der Verantwortlichkeit

Die nachfolgend zu beschreibende technische Sicherheitspolitik wird durch sicherheitsspezifische Funktionen umgesetzt, die bisher beschriebenen Maßnahmen (vgl. Abschnitte 3.1.2.1 bis 3.1.2.3) setzen die anderen Aspekte der System-Sicherheitspolitik um. Es ist daher nötig, die Aufteilung der Verantwortlichkeit zu erläutern.

In Umsetzung der Firmen-Sicherheitspolitik hat die System-Sicherheitspolitik die Aufgabe zu beschreiben, auf welche Weise das Hermes Online System der Hermes Kreditversicherungs-AG die Vertraulichkeit der o. g. Kundeninformationen schützt. Die in den Abschnitten 3.1.2.1 bis 3.1.2.3 beschriebenen Maßnahmen schützen dabei den

konventionellen Weg des Kundenkontaktes (zur Unterscheidung vgl. Abschnitt 3.3.2.1), die sicherheitsspezifischen Funktionen sind für die Absicherung des Internetzugangs zum Hermes Online System der Hermes Kreditversicherungs-AG verantwortlich.

3.2 Zu zertifizierendes Objekt

3.2.1 Genaue Bezeichnung

Das zu zertifizierende Objekt ist das

Hermes Online System der Hermes Kreditversicherungs-AG, Version 2.0.

Das Hermes Online System der Hermes Kreditversicherungs-AG, Version 2.0 (nachfolgend der Evaluationsgegenstand, EVG, genannt) ist ein System im Sinne der ITSEC [1]. Dies bedeutet, daß der EVG eine spezielle IT-Installation (vgl. Abschnitt 3.2.2) mit einem definierten Zweck (vgl. Abschnitt 3.2.5) und einer realen Einsatzumgebung (vgl. Abschnitte 3.2.3 und 3.2.4) ist.

3.2.2 Auflistung der Komponenten

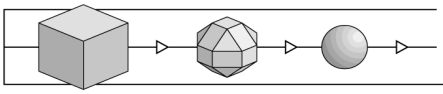
Der EVG besteht aus zwei Teilen, die in einer Client-Server-Beziehung zueinander stehen. Auf der Client-Seite befindet sich das Hermes-Applet, ein JAVA-Applet, das seinerseits aus Anwendungsklassen und Brokat-Klassen besteht. Die Anwendungsklassen werden von Hermes entwickelt und implementieren eine Bedieneroberfläche für das Hermes-Applet. Die Brokat-Klassen implementieren zusammen mit einem Brokat-Server ein kryptographisch gesichertes Übertragungsprotokoll für eine Kommunikationsverbindung über das Internet und werden von der Fa. Brokat als Teil des Produkts „X♦PRESSO Security Package 1.3“ ausgeliefert.

Auf der Server-Seite befinden sich die restlichen Komponenten des EVG. Hierzu zählen ein Webserver, ein Brokat-Server, ein CGI-Skript, verschiedene Transaktionsprozesse und das Betriebssystemmodul TopSecret.

Der Webserver wird vom Browser des Kunden kontaktiert und überträgt das Hermes-Applet auf dessen PC. Das Hermes-Applet seinerseits baut eine kryptographisch gesicherte Kommunikationsverbindung über das Internet mit dem Brokat-Server unter Nutzung der Brokat-Klassen auf. Über diese gesicherte Verbindung werden schließlich die Nutzdaten des Kunden über das Internet transportiert.

Der Brokat-Server entschlüsselt die Nutzdaten des Kunden und leitet sie an den Webserver weiter. Andererseits empfängt der Brokat-Server Nutzdaten des Kunden vom Webserver, verschlüsselt sie und sendet sie über die gesicherte Verbindung via Internet an das Hermes-Applet.

Der Webserver startet das CGI-Skript, wenn er vom Brokat-Server Nutzdaten des Kunden empfängt und leitet die für den Kunden bestimmten Ausgaben des CGI-Skripts an den Brokat-Server zurück.



Das CGI-Skript leitet die Nutzdaten vom Webserver an die Transaktionsprozesse weiter bzw. leitet Nutzdaten von den Transaktionsprozessen an den Webserver weiter. Die Transaktionsprozesse stellen die Schnittstelle zum Hermes-Kundensystem dar und führen auf der DB2-Datenbank des Hermes-Kundensystems SQL-Abfragen durch.

Die Ausführung der Transaktionsprozesse wird durch das Betriebssystemmodul TopSecret über eine Zugriffskontrolle überwacht. Dabei stellt TopSecret sicher, daß nur autorisierte Benutzer die Transaktionsprozesse starten. Außerdem führt TopSecret eine Identifikation und Authentikation der Kunden durch, indem es kundenspezifische Kennungen und Paßwörter überprüft.

Die folgende tabellarische Zusammenstellung enthält alle Bestandteile, aus denen der EVG besteht und die ihn als spezielle IT-Installation charakterisieren. Diese Darstellung ist insofern vollständig, als alle hier nicht aufgeführten, technischen Bestandteile, die eventuell benötigt werden, um die Funktionsweise, den Ablauf oder die Sicherheitseigenschaften des EVG zu verstehen, der technischen Einsatzumgebung angehören.

Nr	Typ	Bezeichnung	Version
1	SW	Hermes-Applet bestehend aus: - Brokat-Klassen[2] - Anwendungsklassen	2.0
2	SW	X♦PRESSO Security Package 1.3, bestehend aus: - X♦PRESSO Java Security Classes (Brokat-Klassen) - X♦PRESSO Security Server (Brokat-Server)	1.3.7
3	DK	X♦PRESSO Security Package 1.3	5
4	SW	Lotus Domino Webserver	4.6.1
5	SW	TopSecret	5.0
6	SW	CGI-Skript	1.1

2 Die Brokatklassen sind Bestandteil des Lieferumfanges des X♦PRESSO Security Package 1.3 und werden in das Hermes-Applet mit eingebunden. Sie stellen die gesicherte Kommunikationsverbindung mit dem Brokat-Server her. Sie werden von den Anwendungsklassen des Hermes-Applets aufgerufen.

Nr	Typ	Bezeichnung	Version
7	SW	Transaktionsprozesse	
		- Kundendatenbank – O43I2000	1.07
		- Antragsbearbeitung – O43I0100	1.16
		- Vorauswahl / Benutzerdatenpflege – O43I0200	1.03
		- Adreßsuche – O43I1100	1.06
		- KZÜ - Meldung – O43I4100	1.07
		- Negativmeldung – O43I4800	1.06
		- Schadenanzeige – O43I4700	1.07
		- Überblick KZÜ – Meldung O4344100	1.96
		- Überblick Negativ Info – O4344850	1.13
		- Überblick Schadenmeldung – O4344600	1.37
		- Delkreda Inkasso – O43I0300	1.04
		- Überblick Bestandsliste Delkreda – O43I4700	1.07
		- Adreßänderung – O43I4900	1.05

Tabelle 1: Bestandteile des Hermes Online Systems der Hermes Kreditversicherungs-AG, Version 2.0

3.2.3 Technische Einsatzumgebung

Der EVG stellt den Versicherungsnehmern der Hermes Kreditversicherungs-AG (Hermes) einen Internetzugang zum Hermes-Kundensystem zur Verfügung. Mit diesem Zugang können die Versicherungsnehmer u. a. Anträge für Kreditversicherungen stellen, die Antragssummen erhöhen, Kreditanträge streichen und Informationen zu bestehenden Kreditanträgen abrufen.

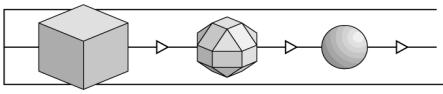
Entsprechend der Aufgabenstellung des EVG sind als technische Einsatzumgebung drei Schnittstellen (EVG / Hermes-Kundensystem, Serverteil des EVG / Internet und EVG / Browser) sowie die bestehende Plattform zu betrachten.

3.2.3.1 Schnittstelle des EVG zum Hermes-Kundensystem

Der EVG liefert Nutzdaten der Kunden in das Hermes-Kundensystem ein und transportiert Nutzdaten der Kunden zu deren Rechner zurück. Zur Kommunikation mit dem Hermes-Kundensystem dienen die Transaktionsprozesse. Sie setzen Kundenanfragen in SQL-Statements der Datenbank DB2 um und veranlassen deren Ausführung. Sie nehmen die Resultate auf und leiten sie an das CGI-Skript weiter.

3.2.3.2 Schnittstelle des Serverteils des EVG zum Internet

Die Schnittstelle des Serverteils des EVG zum Internet besteht aus zwei Teilen. Der erste Teil besteht aus der Schnittstelle zwischen Internet und Webserver. Über diese Schnittstelle kontaktiert ein Browser des Kunden den EVG. Über diese Schnittstelle wird anschließend das Hermes-Applet auf den Kundenrechner übertragen.



Den zweiten Teil der Schnittstelle zwischen EVG und Internet bildet die Schnittstelle zwischen Internet und Brokat-Server. Über diese Schnittstelle baut das Hermes-Applet eine kryptographisch gesicherte Kommunikationsverbindung zum Brokat-Server auf. Die Nutzdaten des Kunden werden ausschließlich über diese gesicherte Kommunikationsverbindung übertragen.

3.2.3.3 Schnittstelle des EVG zum Browser

Das Hermes-Applet wird auf den PC des Kunden geladen und dort innerhalb der JAVA-Umgebung eines Browsers ausgeführt. Es besteht aus Anwendungsklassen, die eine Bedieneroberfläche für die Kundeneingaben implementieren sowie den Brokat-Klassen aus dem X♦PRESSO Security Package 1.3, die zusammen mit dem Brokat-Server für die sichere Übertragung der Nutzdaten des Kunden über das Internet sorgen. Der HTML-Browser sowie die Schnittstelle des Browsers zum Hermes-Applet gehören zur technischen Einsatzumgebung des EVG.

3.2.3.4 Bestandteile des IBM Großrechners

Das Hermes-Kundensystem wird auf einem IBM Großrechner betrieben. Dieser Rechner ist in zwei logische Maschinen aufgeteilt, die vom Betriebssystem OS/390 kontrolliert werden.

Die erste logische Maschine wird als Produktionsmaschine bezeichnet. Auf ihr ist das Hermes-Kundensystem installiert. Die Kundendaten werden über die Datenbank DB2 verwaltet. Der EVG greift über die Schnittstelle EVG/Hermes-Kundensystem auf diese Daten zu.

Die zweite logische Maschine wird als Webgate bezeichnet. Auf ihr ist der Webserver (Domino-Webserver) zusammen mit dem CGI-Skript installiert.

Beide logische Maschinen, also Webgate und Produktionsmaschine, können ausschließlich über einen SNA-Kanal auf Basis von Lichtwellenleitern miteinander kommunizieren.

3.2.3.5 Anforderungen auf Kundenseite

Damit ein Kunde der Hermes Kreditversicherungs-AG den EVG benutzen kann, muß er über bestimmte technische Ausrüstung und Programme verfügen. Er benötigt einen Rechner mit Internet-Anschluß und Browser-Software. Der Browser muß die Java Applet API Versionen 1.0 oder 1.1 und RSA-Schlüsselzertifikate unterstützen. Weiterhin muß der verwendete Browser des Kunden den öffentlichen Schlüssel der CA (Certification Authority) TC TrustCenter GmbH enthalten, damit der Kunde die Zertifikate dieser CA prüfen kann. Fehlt dieser öffentliche Schlüssel, muß er vor der Nutzung des EVG in den Browser geladen werden.

Der Browser ist so zu konfigurieren, daß Zertifikate nur manuell geprüft werden können. Die Schlüsselzertifikate sind in jeder Sitzung einzeln zu prüfen, und es ist jeweils zu entscheiden, ob ein Schlüsselzertifikat zugelassen wird.

Nach dem Verbindungsaufbau des Browsers auf dem Kundenrechner mit dem Webserver des EVG überträgt dieser ein signiertes JAVA-Applet (Hermes-Applet) auf den Kundenrechner. Vor der Nutzung des Hermes-Applets muß der Kunde mit Hilfe des öffentlichen Schlüssels der CA TC TrustCenter GmbH und der vom Browser zur Verfügung gestellten Funktionalität manuell überprüfen, daß die Signatur des Hermes-Applets von der Hermes Kreditversicherungs AG geleistet wurde und damit das Applet authentisch bei ihm vorliegt. Mit dieser externen Sicherheitsmaßnahme „Signaturprüfung“ und den im Applet fest kodierten Informationen (URL und öffentlicher Schlüssel des Brokat-Servers) hat er dann die Möglichkeit, eine authentische Verbindung mit dem EVG herstellen zu können.

3.2.4 Administrative Einsatzumgebung

Für den Betrieb des EVG gelten folgende Regelungen (Auflagen), die von den Mitarbeitern der Hermes beachtet werden:

3.2.4.1 Unterscheidung zwischen Kunden und (potentiellen) Nutzern

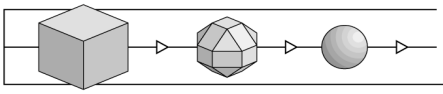
Jeder Nutzer des Internets kann das Informationsangebot der Hermes über das Internet nutzen. Dazu stellt er eine HTTP-Verbindung zum Webserver des EVG her. Anhand einer für alle Kunden der Hermes gleichen Identifikation und eines dazugehörigen, ebenfalls für alle Kunden der Hermes gleichen Paßwortes ist der Webserver des EVG in der Lage, zwischen Kunden des EVG und sonstigen Internet-Benutzern zu unterscheiden (Hermes-Kennung). Die Hermes-Kennung wird allen Kunden des EVG mit folgender Auflage übermittelt:

R1 Die Hermes-Kennung soll nur zur Herstellung einer Internet-Verbindung mit dem Hermes Online System der Hermes Kreditversicherungs-AG verwendet werden. Hermes-Mitarbeiter dürfen die Hermes-Kennung nur an Kunden der Hermes weitergeben. Wird die Hermes-Kennung geändert, so werden alle Hermes-Kunden über die bevorstehende Änderung und das Datum ihrer Wirksamkeit informiert.

3.2.4.2 Hermes-Applet

Die Sicherheit einer bestehenden, kryptographisch gesicherten Internet-Verbindung zwischen den beiden Teilen des EVG hängt u.a. davon ab, daß das Hermes-Applet korrekt programmiert ist. Dies wird im Rahmen dieser System-Zertifizierung geprüft. Es ist daher unverzichtbar, daß der Kunde eine Kopie des authentischen und gegenüber dem geprüften unveränderten Hermes-Applet besitzt. Für die Bereitstellung des Hermes-Applets besteht daher folgende Regelung:

R2 Das im Rahmen dieser System-Zertifizierung geprüfte Hermes-Applet wird mit einer digitalen Signatur versehen, die Integritätsverletzungen erkennbar werden läßt. Das zur Signaturprüfung notwendige Schlüsselzertifikat wird von Hermes bereitgestellt. Das signierte Hermes-Applet wird ausschließlich von einer dazu autorisierten Person in das Hermes Online System der Hermes Kreditversicherungs-AG eingespielt.



3.2.4.3 Zuordnung von Daten zu Kunden

Die vom EVG vermittelten Aktionen der Hermes-Kunden beziehen sich auf Daten, die in einer DB2-Datenbank unter MVS auf einem IBM Großrechner gehalten werden. Da diese Daten sich auf einzelne Kunden beziehen, gilt für die Datenpflege folgende Regelung:

R3 Alle Datensätze der DB2-Datenbank, auf die über das Hermes Online System der Hermes Kreditversicherungs-AG zugegriffen werden kann, verfügen über eine eindeutige Kennzeichnung, welche die Entscheidung erlaubt, ob ein bestimmter, aber beliebiger Kunde den Zugriff ausüben darf. Für mittels des EVG neu generierte Datensätze wird eine solche eindeutige Kennzeichnung (kundenspezifische Kennung) automatisch erzeugt, die den neu generierten Datensatz genau dem zugreifenden Kunden zuordnet.

3.2.4.4 Internet-Zugang

Der EVG ermöglicht den sicheren Zugang zum Hermes-Kundensystem unter Nutzung des (unsicheren) Internets. Indem das Hermes-Kundensystem mit dem Internet verbunden ist, werden auch die potentiellen Mißbrauchsmöglichkeiten aus dem Internet relevant. Daher wird der (offene) Internet-Zugang durch ein System von Firewalls (Sunscreen EFS und Firewall One) für Angriffe aus dem Internet verschlossen. Da jede Internet-Firewall gewartet werden muß, gilt folgende Regelung:

R4 Die Internet-Firewalls werden in regelmäßigen Abständen gewartet. Die vom Hersteller ggf. bereitgestellten Patches zur Verbesserung des Sicherheitswertes der Firewalls werden unverzüglich nach Erscheinen eingespielt. Die Konfiguration der Firewalls wird in Übereinstimmung mit der System-Sicherheitspolitik (s. o.) vorgenommen. Die Log-Dateien der Firewalls werden routinemäßig auf mögliche Sicherheitsvorkommnisse hin überprüft.

3.2.4.5 Kundenspezifische Kennung

Das Sicherheitsziel (vgl. Abschnitt 3.3.2.1) kann nur erreicht werden, wenn die den Daten zugeordnete kundenspezifische Kennung für verschiedene Kunden unterschiedlich ist. Daher gilt folgende Regelung:

R5 Jeder von der Hermes Kreditversicherungs-AG vergebenen kundenspezifischen Kennung ist genau ein Kunde der Hermes zugeordnet. Die kundenspezifische Kennung wird von Hermes unter Beachtung der Empfehlungen des BSI-Grundschutzhandbuches erzeugt und dem betreffenden Kunden auf sicherem Wege (brieflich oder fernmündlich) mitgeteilt. Der Kunde wird darüber informiert, daß er nur solchen Personen diese Information zugänglich machen soll, die berechtigt sind, seine bei der Hermes gespeicherten Daten einzusehen, zu verändern oder zu erzeugen.

3.2.4.6 Information der Hermes-Kunden

Die kundenspezifische Kennung wird vom Hermes-Applet unter Benutzung des Internets an den Serverteil des EVG gesandt, nachdem das Hermes-Applets einen sicheren Kanal (bzgl. Vertraulichkeit und Integrität) zum Serverteil des EVG aufgebaut hat. Damit dieser sichere Kanal aufgebaut werden kann, sind die in Abschnitt 3.2.3.5 genannten Anforderungen durch den Kunden zu realisieren. Daher gilt folgende Regelung:

R6 Alle Hermes-Kunden, denen eine kundenspezifische Kennung mitgeteilt wird, werden über die notwendigen Schritte zum Aufbau einer gesicherten Verbindung zwischen den beiden Teilen des EVG und über die sichere Anwendung des Hermes-Applets informiert.

3.2.4.7 IT-Sicherheit beim Kunden

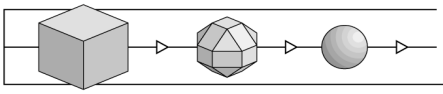
Die in diesem Abschnitt niedergelegten Informationen sind nicht Bestandteil der System-Sicherheitspolitik. Sie sind als zusätzliche Informationen zu betrachten und dienen der Darstellung des Sicherheitsbewußtseins, mit dem diese Sicherheitsvorgaben geschrieben wurden. Die vom EVG zur Verfügung gestellte sicherheitsspezifische Funktionalität hängt nicht von der Beachtung oder Mißachtung der hier niedergelegten Information ab.

Um das Hermes Online System der Hermes Kreditversicherungs-AG benutzen zu können, muß der Hermes-Kunde mit dem Internet verbunden sein. Daher ist seine Informationstechnik (IT), die mit dem Internet verbunden ist, ebenfalls offen für Angriffe aus dem Internet. Hermes empfiehlt ihren Kunden daher den Einsatz einer geeigneten Sicherungseinrichtung (z. B. einer Firewall).

Die vorstehend genannten Regelungen R1, R2, R5 und R6 beziehen sich zum Teil auf Informationen (z. B. die kundenspezifische Kennung) oder Vorgänge, die nicht nur Hermes bekannt sind bzw. die nicht allein von Hermes durchgeführt werden können (z. B. Authentizitätsnachweis des Hermes-Applets). Hermes empfiehlt ihren Kunden daher,

- die ihnen zur Verfügung gestellte Hermes-Kennung und die kundenspezifischen Kennungen geheimzuhalten,
- die Integrität und Authentizität des Hermes-Applets vor jedem Aufbau einer gesicherten Verbindung zum EVG zu prüfen,
- die Benutzungshinweise zum Hermes-Applet zu befolgen,
- allgemein anerkannte Grundregeln zum Schutz der IT zu beachten und
- eine System-Sicherheitspolitik für ihr IT-System aufzustellen.

Ungeachtet dieser Empfehlungen bleiben die Hermes-Kunden für die Sicherheit ihrer IT eigenverantwortlich. Der EVG schützt die Kundendaten nur auf der Kommunikationsstrecke zwischen Clientteil des EVG und Brokat-Server im Serverteil



des EVG, d. h. nur im (offenen) Internet gegen den Verlust der Vertraulichkeit und Integrität.

3.2.5 Art der Nutzung

Zum Verständnis der Art der Nutzung des EVG ist es hilfreich, sieben Phasen der Nutzung zu unterscheiden. Bei jeder Kontaktaufnahme eines Hermes-Kunden mit dem EVG wiederholen sich diese Phasen.

3.2.5.1 Phase 1: Nutzung der Website der Hermes Kreditversicherungs-AG

Ein Hermes-Kunde tritt in Kontakt mit dem EVG , wenn er eine Verbindung zum Webserver des EVG herstellt. Dies geschieht, indem er in seinem Webbrowser die URL der Hermes als Zieladresse angibt (http://hermes-online.hermes-kredit.com). Der Webbrowser des Kunden stellt dann eine Verbindung zum Domino Webserver des EVG her. Die kryptographischen Eigenschaften dieser Verbindung sind für die Evaluation ohne Bedeutung, da für derartige Verbindungen seitens des EVG kein Sicherheitsziel besteht. Das Hermes Online System der Hermes Kreditversicherungs-AG geht davon aus, daß die in Phase 1 aufgebaute Verbindung zwischen Kunden und Hermes nicht ausreichend gegen Ausforschung gesichert ist. Ferner ist aus dem Bestehen der Verbindung kein Rückschluß auf die Identität der Partner der Verbindung möglich. Damit gilt für den Kunden:

- der Kunde hat noch keine verläßliche Information über die Identität des Partners, mit dem die Verbindung besteht und

- Hermes hat noch keine verläßliche Information über die Identität des Partners, mit dem die Verbindung besteht.

3.2.5.2 Phase 2: Übertragung des Hermes-Applets

Wenn der Kunde eine bestimmte Seite der Hermes-Website ausgewählt hat, kann er das Hermes-Applet herunterladen. Dazu muß er die Hermes-Kennung angeben. Die angegebene Kennung wird vom Domino Webserver geprüft, und bei Übereinstimmung mit der Hermes-Kennung wird das Hermes-Applet an den Verbindungspartner versandt. Auch in dieser Phase besteht seitens des EVG kein Sicherheitsziel, und ein Rückschluß auf die Identität der Partner ist unzuverlässig.

3.2.5.3 Phase 3: Integritätsprüfung des Hermes-Applets

Das Hermes-Applet repräsentiert den Clientteil des EVG und stellt eine besonders gesicherte Verbindung zum Brokat-Server im Serverteil des EVG her. Das Hermes-Applet stellt die Mittel (Signatur und Zertifikat) bereit, die es einem Kunden ermöglichen, seine Identität und Integrität zweifelsfrei festzustellen. Der dazu notwendige öffentliche Schlüssel einer Certification Authority (CA) muß hierfür im Browser vorhanden sein.

Neben den Anforderungen an die Sicherheitsfunktion, die das Hermes-Applet implementiert und die durch diese Evaluation geprüft werden, besteht daher die

Anforderung, das in Phase 2 erhaltene Applet auf authentische Herkunft und Integrität zu prüfen. Die Funktionalität (Prüfung des Zertifikates) dazu stellt der Webbrowser beim Kunden zur Verfügung, die Daten (hier: digitale Signatur und zugehöriges Zertifikat) werden dem Kunden in Phase 2 jedoch übermittelt. Bezüglich der Phase 3 besteht das Ziel festzustellen, daß der Kunde genau das Hermes-Applet in Phase 2 geladen hat, das als Objekt zum EVG gehört.

Als externe Sicherheitsmaßnahme wird die digitale Signatur verwendet. Einzelheiten der Funktionsweise sind z. B. in [4] nachzulesen. Durch Verwendung der digitalen Signatur werden zwei Aussagen ermöglicht:

1. Die Verifizierung der digitalen Signatur zeigt an, daß die Kopie des Hermes-Applets auf dem Kundenrechner mit dem Applet übereinstimmt, das mit dem zugehörigen geheimen Signaturschlüssel digital signiert wurde.

2. Die Prüfung des mitgelieferten Zertifikates (bis zum Root-Zertifikat) zeigt an, daß das betreffende Applet von Hermes signiert wurde.

Am Ende der Phase 3 verfügt der Kunde über die Gewißheit, eine Kopie des im Rahmen der System-Zertifizierung des EVG geprüften Hermes-Applets geladen zu haben. Ein Rückschluß auf die Identität der Partner ist noch immer unzuverlässig.

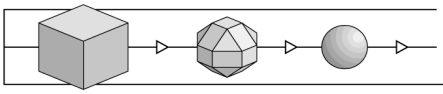
3.2.5.4 Phase 4: Server-Authentisierung

Das Hermes-Applet (genauer: die Kopie des Hermes-Applets beim Kunden) erfüllt zwei Aufgaben, die für die Sicherheit Bedeutung haben. Das Hermes-Applet nimmt Verbindung zum Brokat-Server auf. Über ein Handshake-Verfahren wird der Brokat-Server authentisiert (vgl. [5], Seite B-4). Der hierzu benötigte öffentliche Schlüssel des Brokat-Servers ist im Hermes-Applet fest kodiert. Im Anschluß an die Authentisierung des Brokat-Servers wird zwischen Hermes-Applet (Clientseite des EVG) und Brokat-Server auf der Serverseite des EVG eine kryptographisch gesicherte Verbindung aufgebaut. Jeder weitere Datenverkehr wird innerhalb dieser gesicherten Verbindung abgewickelt, wobei die einzelnen Datenpakete selbst noch gegen den Verlust der Integrität gesichert werden.

Ziel der Phase 4 ist die Feststellung des Kunden, daß sein Verbindungspartner genau der Serverteil des EVG ist. Dazu werden zwei sicherheitsspezifische Funktionen eingesetzt, die Server-Authentisierung und die Verschlüsselung. Ferner besteht das Ziel, innerhalb der gesicherten Verbindung Daten integer und vertraulich auszutauschen.

Am Ende der Phase 4 weiß der Kunde, daß er mit dem Serverteil des EVG verbunden ist. Beide Verbindungspartner wissen, daß die Daten integritätsgesichert ausgetauscht werden. Über die Identität des Kunden liegen noch immer keine gesicherten Informationen vor.

Die folgenden Phasen 5 und 6 werden bei jeder Kundenanfrage durchlaufen. Die Kundenanfragen werden im Hermes-Kundensystem transaktionsorientiert abgearbeitet, wobei jede Kundenanfrage in einer separaten Transaktion läuft. Der Serverteil des EVG speichert die geprüfte Identität des Kunden nicht. Das bedeutet auch, daß vor jeder



Ausführung einer Kundenabfrage eine erneute Client-Authentisierung (siehe Phase 5) durch den Serverteil des EVG durchgeführt wird.

3.2.5.5 Phase 5: Client-Authentisierung

Ziel der Verbindung des Kunden mit dem EVG ist die Nutzung spezieller Dienste der Hermes auf schnelle, unkomplizierte Weise. Nach dem Aufbau der gesicherten Verbindung zwischen Clientteil und Serverteil des EVG muß der Kunde, der z. B. seine Vertragsdaten lesen will, sich gegenüber dem Serverteil des EVG als Kunde der Hermes authentisieren. Dazu gibt er auf entsprechende Aufforderung hin seine kundenspezifische Kennung an. Obwohl die kundenspezifische Kennung über ein offenes Netz (Internet) übertragen wird, ist sie gegen Ausforschung durch die in Phase 4 aufgebaute sichere Verbindung geschützt. Eine Maskerade des Serverteils des EVG ist ebenfalls in Phase 4 gescheitert. Die kundenspezifische Kennung wird vom Serverteil des EVG geprüft (Client-Authentisierung).

Bezüglich der Phase 5 besteht das Ziel, daß der Serverteil des EVG feststellt, daß sein Kommunikationspartner ein Kunde der Hermes ist. Ferner wird festgestellt, um welchen Kunden es sich handelt.

Am Ende der Phase 5 kennt der EVG die Identität des Kunden. Damit sind alle Voraussetzungen geschaffen, die für eine vertrauenswürdige Kommunikation zwischen zwei einander bekannten Partnern sorgen.

Die folgende Phase 6 ”Nutzphase” wird nur dann ausgeführt, wenn der Kunde richtig authentisiert wurde.

3.2.5.6 Phase 6: Nutzphase

Alle in dieser Phase zwischen Clientteil und Serverteil des EVG ausgetauschten Nutzdaten sind gegen den Verlust der Vertraulichkeit und der Integrität während der Übertragung über das Internet gesichert. Auf der Grundlage der in Phase 5 festgestellten Identität des Nutzers entscheidet der Serverteil des EVG darüber, ob der betreffende Nutzer die gewollte Interaktion (z. B. Lesen von Vertragsdaten) ausführen darf. Als sicherheitsspezifische Funktion wird die Rechteverwaltung eingesetzt.

3.2.5.7 Phase 7: Verbindungsabbau

Der Verbindungsabbau geschieht über Standardmechanismen der beteiligten Protokolle. Sicherheitsrelevante oder vertrauliche Informationen von Kunden können nach dem Verbindungsabbau nicht von Unbefugten unter Benutzung des EVG in Erfahrung gebracht werden, da die für die Zwischenspeicherung dieser Informationen benutzten Speicherbereiche vor der Beendigung des Hermes-Applets überschrieben werden.

3.3 Sicherheitseigenschaften

3.3.1 Subjekte / Objekte, Zugriffsarten

Für die Formulierung der Sicherheitseigenschaften des EVG werden folgende Objekte, Subjekte und Zugriffsarten beschrieben.

3.3.1.1 Objekte

Die vom EVG zu schützenden Objekte sind:

O1 Nutzdaten des Hermes-Kundensystems,

O2 kundenspezifische Kennungen und das

O3 Hermes-Applet.

3.3.1.2 Subjekte

Für die Formulierung der Sicherheitseigenschaften des EVG werden folgende Subjekte definiert:

S1 **Nutzer des Hermes Online Systems der Hermes Kreditversicherungs-AG**: alle Personen, die die Hermes-Kennung und eine kundenspezifische Kennung kennen

S2 **Nicht autorisierte Personen:** alle Personen, die keine kundenspezifische Kennung kennen

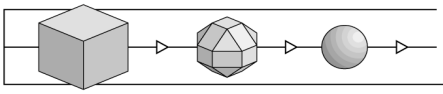
S3 **Webserver:** realisiert einen Teil des Internetzugang zum EVG. Der Webserver verschickt das signierte Hermes-Applet an den Kundenrechner.

S4 **Brokat-Server:** PC mit dem Betriebssystem Solaris, auf dem die Software X♦PRESSO Security Package 1.3 der Fa. Brokat installiert ist. Dieser Server dient als Proxy-Server und ver- und entschlüsselt Nutzdaten, die über die Internet-Verbindung mit dem Hermes-Applet auf dem Kundenrechner ausgetauscht werden.

3.3.1.3 Zugriffsarten

Andere Zugriffsarten als Lesen und Schreiben werden zur Formulierung der Bedrohungen nicht benötigt. Die folgende Darstellung dient daher eher der Information (vgl. die Phasen der Nutzung).

ZA 1 Nutzer des Hermes Online Systems der Hermes Kreditversicherungs-AG (S1) und nicht autorisierte Personen authentisieren sich gegenüber dem Domino-Webserver durch Angabe eines Benutzernamens und eines Paßwortes.



ZA 2 Der Webserver (S3) überträgt das signierte Hermes-Applet (O3) zum Kunden-PC. Das Hermes-Applet authentisiert sich gegenüber dem Kunden durch ein Zertifikat der Fa. TrustCenter GmbH, das vom Kunden geprüft werden muß.

ZA 3 Der Brokat-Server Server (S4) authentisiert sich gegenüber dem Kunden.

ZA 4 Nutzer des Hermes Online Systems der Hermes Kreditversicherungs-AG (S1) authentisieren sich gegenüber dem EVG durch Angabe ihrer kundenspezifischen Kennung.

ZA 5 Subjekte S1 übertragen Nutzdaten (O1) an den EVG oder rufen sie von diesem ab.

3.3.2 Sicherheitsziel und Bedrohungen

3.3.2.1 Sicherheitsziel

In Übereinstimmung mit der Firmen-Sicherheitspolitik und aus ihr abgeleitet, ergibt sich für den EVG ein Sicherheitsziel, das wie folgt formuliert wird:

> Das Hermes Online System der Hermes Kreditversicherungs-AG stellt nur **dem** Kundenkreis nur **die** Daten (Informationen) zur Verfügung, die auch auf konventionellem Wege (im persönlichen Gespräch oder schriftlich) von der Hermes Kreditversicherungs-AG dem entsprechenden Kundenkreis zur Verfügung gestellt würden.

Dazu unterscheidet der EVG die einzelnen Kunden der Hermes Kreditversicherungs-AG untereinander und gegenüber allen anderen (potentiellen) Nutzern. Der EVG nimmt ferner die Zuordnung von Kunden der Hermes Kreditversicherungs-AG zu den Daten vor, die ihnen gemäß der technischen Sicherheitspolitik zur Verfügung gestellt werden dürfen.

3.3.2.2 Bedrohungen

Gegen den EVG richten sich Bedrohungen, die durch in Abschnitt 3.3.3 zu beschreibende Sicherheitsfunktionen abgewehrt werden. Da durch den EVG eine neue technische und für die Kunden der Hermes Kreditversicherungs-AG bequeme Möglichkeit geschaffen wurde, das Internet für die Abwicklung von Kundenkontakten zu nutzen, die bisher auf konventionellem Wege (im persönlichen Gespräch oder schriftlich) abgewickelt wurden, sind genau die Bedrohungen hier zu betrachten, die sich aus technischer Sicht durch die Bereitstellung des Internetzugangs für die Kunden der Hermes Kreditversicherungs-AG neu ergeben.

B1 Eine nicht autorisierte Person (S2) kann Verbindung zum Brokat-Server (S4) im Serverteil des EVG über das Internet aufnehmen mit der Absicht, Zugang zu Objekten O1 im Hermes-Kundensystem zu erlangen.

B2 Eine Person kann sich im Internet als Hermes Kreditversicherungs-AG (Brokat-Server (S4) im Serverteil des EVG) ausgeben mit der Absicht, Kenntnis von Objekten O2 zu erlangen.

B3 Eine Person S1 kann sich Zugriff auf Daten O1 im Hermes-Kundensystem verschaffen, die nicht ihr, sondern einem anderen Hermes-Kunden zugeordnet sind.

B4 Eine Person kann eine bestehende Verbindung (Phase 6) als Kunde übernehmen, um Kenntnis von Objekten O1 oder O2 zu erhalten.

B5 Eine Person kann eine bestehende Verbindung (Phase 6) als Brokat-Server übernehmen, um Kenntnis von Objekten O2 zu erhalten.

B6 Eine Person kann eine bestehende Verbindung (Phase 6) im Internet abhören und aufzeichnen, um Kenntnis von Objekten O1 oder O2 zu erhalten.

B7 Eine Person kann eine bestehende Verbindung (Phase 6) abhören und unbemerkt Manipulationen an über das Internet übertragenen Nutzdaten O1 und O2 vornehmen.

3.3.3 Sicherheitsfunktionen des EVG

Um das Sicherheitsziel zu erreichen und die dagegen gerichteten bekannten Bedrohungen abzuwehren, verfügt der EVG über Sicherheitsfunktionen, die nachfolgend unter Zuordnung des jeweiligen generischen Oberbegriffs aus [1] aufgeführt werden.

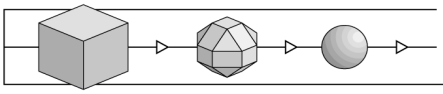
3.3.3.1 Identifizierung und Authentisierung

Von den genannten Subjekten besteht für alle Subjekte S1 und für S4 die Notwendigkeit der Identifizierung und Authentisierung. Bezüglich S4 wird auf das entsprechende Zertifikat und den zugehörigen Zertifizierungsreport verwiesen.

Subjekte S1 werden in Phase 5 eindeutig identifiziert und authentisiert. Diese Funktionalität wird von TopSecret bereitgestellt. TopSecret ist ein Modul des Betriebs-sytems des IBM Großrechners, das eine Identifikation und Authorisierung von Benutzern des Betriebssystems sowie eine Zugriffskontrolle der Benutzer auf Ressourcen des Betriebssystems durchführt. Aktionen mit Bezug auf Objekte O1 finden erst nach erfolgreicher Identifizierung und Authentisierung sowie Zugriffskontrolle statt.

F1 Identifizierung und Authentisierung von Subjekten S1

F2 Identifizierung und Authentisierung von Subjekt S4



3.3.3.2 Zugriffskontrolle

Die Objekte O1 werden bezüglich der ihnen eindeutig zugeordneten Kunden unterschieden. Die Zugriffskontrolle wird durch das Betriebssystem des Webgate und durch TopSecret in Verbindung mit dem CGI-Skript sowie die Transaktionsprozesse durchgeführt. Das CGI-Skript wird vom Webserver aufgerufen und ruft seinerseits die Transaktionsprozesse auf. Die Aufrufe des Webservers und des CGI-Skripts unterliegen der Zugriffskontrolle des Betriebssystems des Webgate. Die Zugriffskontrolle durch TopSecret bewirkt, daß nur ein Nutzer S1 die Transaktionsprozesse ausführen darf. Die Transaktionsprozesse ihrerseits stellen sicher, daß ein Nutzer S1 nur auf die Objekte O1 zugreifen kann, die ihm durch das Hermes-Kundensystem zugeordnet sind.

F3 Zugriffskontrolle auf Objekte O1

Bemerkung: Während einer Verbindung des Browsers auf dem Kundenrechner zum Webserver im Serverteil des EVG werden keine Nutzdaten (O1) ausgetauscht. Während einer Verbindung des Hermes-Applets (Clientteil des EVG) mit dem Serverteil des EVG unterliegen alle Nutzdaten (O1) der Zugriffskontrolle.

3.3.3.3 Unverfälschtheit

Die Integrität und Authentizität des Hermes-Applets (O3), die in Phase 3 geprüft werden, werden durch eine digitale Signatur mit entsprechendem Signaturzertifikat nachgewiesen. Signatur und Signaturzertifikat werden vom Applet zur Verfügung gestellt und müssen vom Benutzer des EVG manuell überprüft werden (siehe Abschnitt 3.2.3.5).

Die zwischen Kundenrechner und EVG nach dem Herstellen einer gesicherten Verbindung ausgetauschten Daten werden gegen Verfälschung gesichert. Diese Funktionalität wird von S4 erbracht, auf das Zertifikat und den zugehörigen Zertifizierungsreport wird verwiesen.

F4 MAC-Sicherung der Nutzdaten (O1) einer gesicherten Verbindung

3.3.3.4 Übertragungssicherung

Alle nach Herstellung einer gesicherten Verbindung in Phase 4 übertragenen Daten, insbesondere die Objekte O1 und O2, sind während der Übertragung über das Internet gegen Ausforschen zu sichern. Diese Funktionalität wird von S4 erbracht, auf das Zertifikat und den zugehörigen Zertifizierungsreport wird verwiesen.

F5 Verschlüsselung der Nutzdaten (O1 und O2)

3.3.4 Bezug der sicherheitsspezifischen Funktionen zum Sicherheitsziel

Jede der genannten Sicherheitsfunktionen trägt auf ihre Weise zur Erreichung des in Abschnitt 3.3.2.1 genannten Sicherheitszieles bei. Wann jede einzelne Sicherheitsfunktion wirksam wird, geht aus Abschnitt 3.2.5, insbesondere aus den

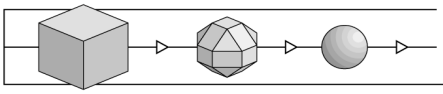
Unterabschnitten 3.2.5.3 bis 3.2.5.6 hervor. Zum Verständnis wird auch auf [5] hingewiesen.

3.3.5 Eignung zur Bedrohungsabwehr

Die genannten Sicherheitsfunktionen sind aufgrund ihrer Eigenschaften geeignet, die genannten Bedrohungen abzuwehren. Dabei ist es manchmal notwendig, daß zwei oder mehr Sicherheitsfunktionen zusammenwirken. Die Einzelheiten sind in nachfolgender Tabelle zusammengestellt.

Grundlage für die wirkungsvolle Abwehr der in Abschnitt 3.3.2.2 identifizierten Bedrohungen durch den EVG ist die Einhaltung der in Abschnitt 3.2.3.5 beschriebenen externen Sicherheitsmaßnahmen durch den Kunden. Der Kunde muß die Authentizität und Integrität des Hermes-Applets durch die Prüfung der Signatur des Applets bei jeder Nutzung des EVG manuell verifizieren. Dazu bedient er sich zum einen der Funktionalität des Browsers und zum anderen eines authentisch im Browser vorliegenden öffentlichen Schlüssels der CA TrustCenter GmbH. Erst dann erhält der Kunde die vom EVG bereitgestellte Sicherheitsfunktionalität F2 und darauf aufbauend F1 und F3 bis F5.

Bedrohung	Entgegenwirkende Sicherheits-funktion(en)	Begründung
B1	F1	Ohne Kenntnis einer kundenspezifischen Kennung kann niemand aus dem Internet Kenntnis von Objekten O1 erlangen, da F1 vor jeder weiteren Interaktion mit dem hierfür relevanten Teil des EVG ausgeführt wird.
B2	F2	Objekte O2 werden erst vom Hermes-Applet an den Serverteil des EVG über das Internet übertragen, nachdem die gesicherte Verbindung aufgebaut wurde. Dies geschieht erst in Phase 4 nach der Server-Authentisierung. Weitere Informationen dazu befinden sich in [5].
B3	F1, F3	Indem vor jeder Interaktion eine Identifizierung und Authentisierung der Kunden erfolgt, kann anschließend die Zugangskontrolle wirksam werden, wodurch einem Subjekt S1 nur solche Objekte O1 zugänglich werden, die ihm zugeordnet sind.



Bedrohung	Entgegenwirkende Sicherheits-funktion(en)	Begründung
B4	F1, F5	Daten O2 werden vom Serverteil des EVG nicht an den Clientteil übertragen, vgl. B1 und B2. Daten O1 werden erst in Phase 6 übertragen, wenn die gesicherte Verbindung zwischen Clientteil und Serverteil des EVG bereits besteht. Wird die bestehende Verbindung vor Erreichen der Phase 5 übernommen, so wirkt F1 gegen B4, und der Angreifer erlangt keine Kenntnis von Daten O1, wenn er nicht über die notwendige kundenspezifische Kennung verfügt. Wird die Verbindung nach Phase 4 übernommen, so wirkt F5 gegen die Bedrohung.
B5	F2, F5	Daten O2 werden vom Kunden erst in Phase 5 gesendet. Wird die bestehende Verbindung vor Erreichen der Phase 5 übernommen, so wirkt F2 gegen B5, und der Angreifer erlangt keine Kenntnis von Daten O2, wenn er sich nicht als EVG identifizieren und authentisieren kann. Wird die Verbindung nach Phase 4 übernommen, so wirkt F5 gegen die Bedrohung.
B6	F5	Daten O1 und O2 werden erst nach Erreichen der Phase 4 übertragen. Gegen das Ausforschen dieser Daten wirkt daher die Verschlüsselung, da mit Abschluß der Phase 4 eine gesicherte Verbindung zwischen den beiden Teilen des EVG besteht. Daß aus der Aufzeichnung der Verbindung vor Erreichen der Phase 5 keine Rückschlüsse auf den benutzten (ausgehandelten) Schlüssel gezogen werden können, geht aus dem Zertifikat für das X♦PRESSO Security Package 1.3 hervor, vgl. [5].

Bedrohung	Entgegenwirkende Sicherheits-funktion(en)	Begründung
B7	F4, F5	Nutzdaten (O1) werden erst in Phase 6 vom EVG übertragen. Gegen die gezielte Manipulation dieser Daten werden die gesichert übertragenen Nutzdaten mit einem MAC-Wert versehen (F4), der eine Manipulation der Daten erkennbar macht.

3.4 Evaluationsstufe und Mechanismenstärke

Die Evaluierungsstufe ist **E1**.

Die angestrebte Mindeststärke der Mechanismen ist **hoch**.

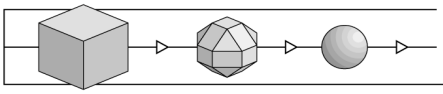
3.5 Glossar

Begriff	Bedeutung
Hermes-Kennung	von der Hermes Kreditversicherungs-AG vergebene Kombination von Identifikator (z. B. ”Hermes”) und Authentikator (z. B. ”Online”), deren Übermittlung an den Domino Webserver zum Herunterladen des Hermes-Applets berechtigt
Hermes-Applet	JAVA Applet der Hermes Kreditversicherungs-AG, das zum Aufbau einer gesicherten Verbindung zum EVG benötigt wird
Kundenspezifische Kennung	von der Hermes Kreditversicherungs-AG vergebene Kombination von Identifikator (z. B. ”KundeABC”) und Authentikator (z. B. ”CBA%ednuK”), deren Übermittlung an das TopSecret zum Ausführen von Operationen auf den dieser Kennung zugeordneten Daten der Hermes Kreditversicherungs-AG ermöglicht

3.6 Quellen

[1] Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC), Version 1.2, Juni 1991, Luxemburg: Amt für amtliche Veröffentlichungen der Europäischen Gemeinschaften, 1991, ISBN 92-826-3003-X

[2] Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEM), Version 1.0, September 1993, Luxemburg: Amt für amtliche Veröffentlichungen der Europäischen Gemeinschaften, 1994, ISBN 92-826-7078-2



[3] IT-Grundschutzhandbuch 1998. Maßnahmenempfehlungen für den mittleren Schutzbedarf, hrsg. vom BSI, Köln, Bundesanzeiger-Verlag 1998, ISBN 3-88784-853-5

[4] Schneier, Bruce: Applied Cryptography, Wiley and Son, 1996

[5] Zertifikat BSI-DSZ-ITSEC-0128-1998 vom 29.10.1998,
URL: http://www.bsi.de/aufgaben/ii/zert/index.htm

4 Hinweise und Empfehlungen zum zertifizierten Objekt

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

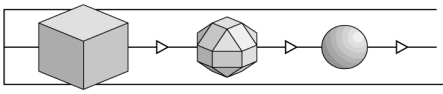
26 Bei der Zertifizierung haben sich folgende weitergehenden Hinweise oder Empfehlungen für den Anwender ergeben.

Abweichend von den Hinweisen für den Anwender aus dem Zertifizierungsbericht BSI-DSZ-ITSEC-0128-1998 zum X♦PRESSO Security Package 1.3 der BROKAT Infosystems AG wird das Hermes-Applet nicht unter Benutzung des SSL 3.0 in den Client-Rechner beim Benutzer geladen. Die Authentizität und die Integrität des Hermes-Applets werden vielmehr durch die Verwendung der digitalen Signatur mit entsprechendem Zertifikat überprüfbar sichergestellt. Das Verfahren der digitalen Signatur selbst wurde nicht geprüft. Die Prüfstelle hat jedoch festgestellt, daß für die Erzeugung und Prüfung der digitalen Signatur Algorithmen mit Schlüssellängen angewendet werden, die nach Feststellung der Regulierungsbehörde für Telekommunikation und Post (RegTP) für den Zeitraum der kommenden vier Jahre, d. h. bis zum Jahr 2003, als sicher gelten.

Im Internet-Browser des Benutzers sind die Möglichkeiten zur Ausführung von JavaScript und ActiveX zu deaktivieren.

Die Firewalls und der Brokat-Server müssen so betrieben werden, daß Protokolldateien angelegt und automatisch geführt werden. Diese Protokolldateien müssen regelmäßig ausgewertet werden.

Die Prüfstelle hat festgestellt, daß das zertifizierte Produkt X♦PRESSO Security Package 1.3 der BROKAT Infosystems AG im Hermes Online System, Version 2.0 gemäß den Anforderungen des Zertifikates BSI-DSZ-ITSEC-0128-1998 zum Einsatz kommt, wobei die genannte Abweichung hinsichtlich der Art und Weise, in der die Authentizität und Integrität des Hermes-Applets sichergestellt wird, sich nicht nachteilig auf die Systemsicherheit auswirkt.



(Diese Seite ist beabsichtigterweise leer.)

5 Hinweise zu den Vorgaben und Kriterien

27 Dieses Kapitel soll einen Überblick über die Vorgaben und Kriterien geben, die bei der Evaluierung zugrunde lagen, und deren Bewertungsmaßstäbe erläutern.

5.1 Grundbegriffe

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

29 *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.

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

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

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

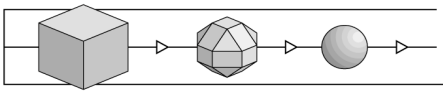
33 Es stellen sich dabei zwei Grundfragen:

- 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

34 Eine Evaluierung kann nur mit begrenztem Aufwand und in begrenzter Zeit durchgeführt werden. Die mögliche Tiefe einer Evaluierung ist also stets begrenzt. Das Angemessenheitsprinzip verbietet es andererseits, bei geringem Sicherheitsbedarf eine extrem aufwendige Prüfung durchzuführen; ebenso un-



angemessen wäre es, bei höchstem Sicherheitsbedarf nur “oberflächlich” zu prüfen.

35 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.

36 Die Vertrauenswürdigkeit eines Produktes oder Systems kann also in diesen Stufen “gemessen” werden.

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

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

39 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

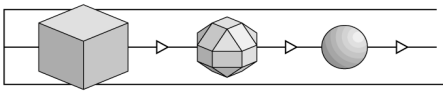
40 Typische Beispiele für Sicherheitsfunktionen sind die *Identifikation und Authentisierung* (von Subjekten), die *Zugriffskontrolle*, die *Beweissicherung* (Protokollierung), die *Protokollauswertung*, die *Übertragungssicherung*. Ein Produkt oder System kann solche Sicherheitsfunktionen beinhalten.

41 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.

42 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.



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

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

45 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."

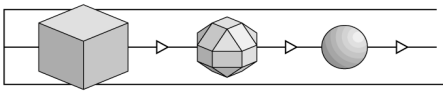
46 Wie wird nun bei Typ A Mechanismen die Stärke definiert?

"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."



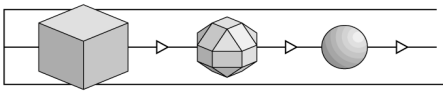
(Diese Seite ist beabsichtigterweise leer.)

6 Anhänge

6.1 Glossar

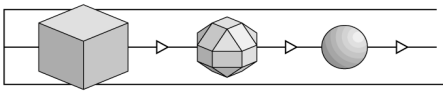
Das Glossar erläutert die in dieser Broschüre verwendeten Begriffe, erhebt allerdings keinerlei Anspruch auf Vollständigkeit oder Allgemeingültigkeit. Der Begriff *Sicherheit* meint hier stets Sicherheit im Kontext der Informationstechnik.

Akkreditierung	Verfahren zum Nachweis, 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.
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 bzw. zu evaluierende 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 IT-Produkts, IT-Systems oder einer IT-Dienstleistung.
Evaluationsstufen	s. Sicherheitsstufen.
Evaluator	Prüfer / in in einer Prüfstelle.



Evaluierung	Prüfung eines IT-Produktes, IT-Systems oder einer IT-Dienstleistung auf der Basis von IT-Sicherheitskriterien oder einer IT-Sicherheitsnorm.
Evaluierungsbericht	Einzelbericht (s.d.) oder 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 / eines IT-Systems.
IT-Produkt	Software und / oder Hardware, die bei einem Anbieter (Hersteller, Vertreiber) erworben werden kann.
ITSEC	Information Technology Security Evaluation Criteria (ITSEC) [Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC)]: Europäischer de facto Standard für die Evaluierung von IT-Produkten und IT-Systemen.
ITSEM	Information Technology Security Evaluation Manual (ITSEM) [Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEM)]: Handbuch zu den ITSEC, das vor allem die Durchführung von Evaluierungen beschreibt.
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, z.B. die Interpretation der Sicherheitskriterien betreffend.
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	Funktion 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).



Signaturverordnung - SigV	Amtliche Ausführungsbestimmungen zum Signaturgesetz.
System-Akkreditierung	Freigabe eines IT-Systems 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 1.1, 16.12.98

/ 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 / Digitalsign / 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. 1997

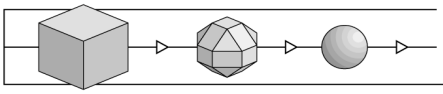
/ Mkat12 / Maßnahmenkatalog nach §12 Abs. 2, RegTP, http: / / www.RegTp.de / Fachinfo / DigitalSign / start.htm

/ 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 1.4, 16.12.98

/V02/ Bestätigungen für Produkte gemäß Signaturgesetz, Dienstleistungsbereich 2, debisZERT, Version 1.4, 16.12.98

/V04/ Zertifikate mit Anerkennung durch das BSI, Dienstleistungsbereich 4, debisZERT, Version 1.4, 16.12.98

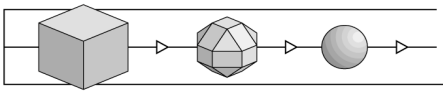
/Z01/ Zertifizierungsschema, debis IT Security Services, Version 1.4, 16.12.98

/Z02/ Zertifizierte IT-Produkte, IT- Systeme und IT-Dienstleistungen, debisZERT, Version 1.2 (fortlaufend numerierte Ausgaben)

6.3 Abkürzungen

AA	Arbeitsanweisungen
AIS	Anforderung einer Interpretation von Sicherheitskriterien
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI-Errichtungsgesetz
CC	Common Criteria for Information Technology Security Evaluation
CLEF	Lizenzierte Prüfstelle bei debisZERT (s. auch ITSEF)
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	Information Technology Security Evaluation Criteria (ITSEC)
ITSEF	IT Security Evaluation Facility (s. CLEF)
ITSEM	Information Technology Security Evaluation Manual (ITSEM)
IuKDG	Informations- und Kommunikationsdienstegesetz
LG	Lenkungsgremium
RegTP	Regulierungsbehörde für Telekommunikation und Post
SigG	Signaturgesetz

SigV	Signaturverordnung
TKG	Telekommunikationsgesetz
ZKA	Zentraler Kreditausschuß
ZL	Leiter der Zertifizierungsstelle
ZZ	(für ein Verfahren) zuständiger Zertifizierer



(Diese Seite ist beabsichtigterweise leer.)

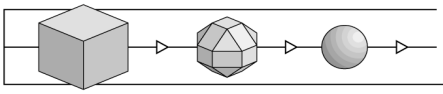
7 Re-Zertifizierungen

47 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.

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

49 Re-Zertifizierungen und neue technische Anhänge werden in der Druckschrift /Z02/ und über WWW angekündigt.

50 Die nachfolgenden Anhänge sind fortlaufend numeriert.



Ende der Erstausgabe des Zertifizierungsreports.