Zertifizierungsreport

MeSecure 1.03

MeTechnology Europe GmbH

debisZERT-DSZ-ITSEC-04003-1999

debis IT Security Services

Die Dienstleister der Moderne

Vorwort

Das Produkt MeSecure 1.03 der MeTechnology Europe GmbH 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:	Authentikation des Servers, Vertraulichkeit der Daten, Prüfen der Integrität der Daten, Einfügen und Prüfen von Paketnummern
Evaluationsstufe:	E3
Mechanismenstärke:	hoch

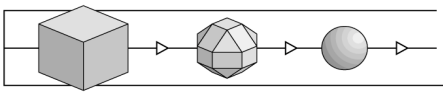
Für weitere Auskünfte und Kopien dieses Reports ist die Zertifizierungsstelle wie folgt erreichbar:

✉ 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 18.03.1999

Zertifizierer:	Leiter der Zertifizierungsstelle:
Dr. Hans-Reinhard Baader	Dr. Heinrich Kersten



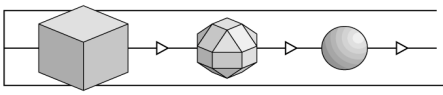
Revisionsliste

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	12.03.99	Vorversion (nach Musterreport 1.4)
1.0	16.03.99	Ersterstellung (nach Musterreport 1.4)

Inhalt



(Diese Seite ist beabsichtigterweise leer.)

1 Überblick

1.1 Evaluierung

1 Die Evaluierung wurde durch MeTechnology Europe GmbH, Ringstr.33, 04430 Dölzig / Leipzig beauftragt.

2 Die Evaluierung wurde durchgeführt von der Prüfstelle IT-Sicherheit der debis IT Security Services und am 12.03.1999 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 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 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

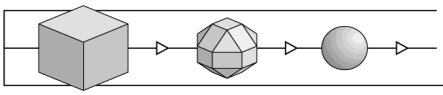
6 Dieser Zertifizierungsreport gibt die Ergebnisse der Evaluierung von MeSecure 1.03 wieder - im folgenden als EVG = Evaluationsgegenstand bezeichnet.

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 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 MeSecure 1.03.

10 Der Zertifizierungsreport enthält die Seiten 1 bis 46. 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-04003-1999.

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 Evaluations-

---

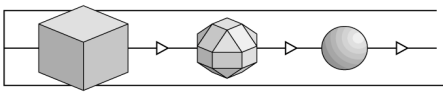
1 Aufgrund gesetzlicher Vorgaben /BSIG/ ist das BSI grundsätzlich gehalten, Bewertungen der genannten kryptographischen Algorithmen selbst nicht vorzunehmen und solche von anderen Zertifizierungsstellen nicht anzuerkennen.

stufe verringert sich allerdings die Wahrscheinlichkeit erheblich, daß ausnutzbare Schwachstellen unentdeckt bleiben.

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 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).

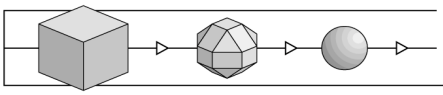
  ITSEC 3.12 bis 3.37 für die Wirksamkeit mit den Aspekten

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

- Die Mechanismen[2] M1 bis M8 des EVG sind kritische Mechanismen; sie sind vom Typ A. Sie haben eine Mindeststärke gemäß der Stufe hoch.

---

2 Vgl. Abschnitt 3.12.



2.3 Hinweise

22 Die Prüfstelle hat folgende Auflagen an den **Hersteller** auszusprechen: Das Evaluationsergebnis gilt nur unter Einhaltung der folgenden Auflagen, weiterzugeben an die Hersteller der Klient- und Server-Applikation bzw. den Server-Betreiber:

(1) Auflagen an die Klient-Applikation

Es bestehen folgende Auflagen an die Klient-Applikation:

(i) Initialisieren des Zufallszahlengenerators des EVG über den Konstruktor und Übergabe der Tastatureingaben und Mauseingaben mit der Zeit an den Zufallszahlengenerator,

(ii) Verwendung des MeSecure SSL-Klient-Stacks für alle übertragenen Daten nach Aufbau der gesicherten Verbindung mit dem Server,

(iii) Information des Klient-Anwenders über den erfolgreichen Aufbau des gesicherten Kanals mit dem EVG durch das Auslesen und Anzeigen des Prüfzertifikats und des durch den EVG positiv geprüften Server-Zertifikats,

(iv) Abbruch der Kommunikation mit dem Server und Information an den Klient-Benutzer nach Scheitern des Aufbaus des gesicherten Kanals mit dem Server oder nach Feststellung von Verletzungen der Datenintegrität der übertragenen Daten durch den EVG und

(v) die Klient-Applikation greift nur über die äußeren Schnittstellen auf den MeSecure SSL-Klient-Stack zu.

(2) Auflagen an die Server-Applikation

Es bestehen folgende Auflagen an die Server-Applikation:

(i) Verwendung des MeSecure SSL-Server-Stacks für alle übertragenen Nutzdaten nach Aufbau der gesicherten Verbindung mit dem Klienten,

(ii) Abruch der Kommunikation mit dem Klienten nach Scheitern des Aufbaus der gesicherten Verbindung oder nach Feststellung von Verletzungen der Datenintegrität der übertragenen Daten durch den EVG und

(iii) die Server-Applikation greift nur über die äußeren Schnittstellen auf den MeSecure SSL-Server-Stack zu.

(3) Auflagen zur Generierung des EVG

Das Schlüsselpaar des Servers ist durch den Dienstanbieter (Serverbetreiber) oder eine vertrauenswürdige Zertifizierungsstelle zu erzeugen; die Er-

zeugung ist durch ein Protokoll nachzuweisen. Die Generierung des EVG mit den anwenderspezifischen Komponenten Public-Key einer Zertifizierungsstelle (Nr. 2) und Namen des zugelassenen Servers (Nr. 3) im Prüfzertifikat Java-Klasse CA_ROOT.class, der Kodierung des Serverzertifikates (Nr. 5) durch den Hersteller des EVG oder den Dienstanbieter (Serverbetreiber) sowie des Private Keys durch den Dienstanbieter (Serverbetreiber) sind zu protokollieren. Durch das Protokoll muß es möglich sein, später exakt zu rekonstruieren, wie und wann der EVG generiert wurde.

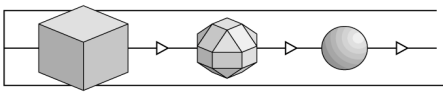
23 Die Prüfstelle hat folgende Auflagen an den **Anwender** (Betreiber des Servers) auszusprechen:
Für den sicheren Betrieb des EVG ist es notwendig, daß der Benutzer des Klienten vom Betreiber des Servers darüber informiert wird, folgendes zu beachten:

(1) Authentische Übertragung des Java-Applets über einen sicheren Kanal

Das Java-Applet, das die Klient-Applikation und die Klient-Komponente des EVG enthält, muß dem Benutzer des Klienten über einen sicheren Kanal zugänglich gemacht werden. Für eine Übertragung des Java-Applets an einen Browser, der Java ab Version 1.1 unterstützt (z. B. Microsoft Internet Explorer oder Netscape Navigator ab Version 4), muß das Java-Applet nach dem RSA-Verfahren mit mindestens einer Modullänge von 768 Bit signiert sein. Der Benutzer des Klienten muß sich beim Empfang von der Gültigkeit der Signatur überzeugen. Alternativ (z. B. für einen Browser, der nur Java der Version 1.02 unterstützt) kann das Java-Applet mittels HTTPS der Version 3.0 übertragen werden. In diesem Fall muß sich der Benutzer durch die Anzeige des Browsers über die Herstellung der gesicherten Verbindung und von der Gültigkeit der Signatur des Servers überzeugen. Der Benutzer des Klienten darf keine Zertifikate einer dem WWW-Browser unbekannten Zertifizierungsstelle akzeptieren.

(2) Prüfen des zugelassenen Servers

Das Java-Applet zeigt nach Herstellung der durch den EVG gesicherten Verbindung das geprüfte Zertifikat des Servers an. Der Benutzer des Klienten muß sich davon überzeugen, daß die Verbindung tatsächlich mit dem gewünschten Server hergestellt wurde. Der Gültigkeitszeitraum des Prüfzertifikates kann außerhalb des aktuellen Datums liegen. Das Nichtzustandekommen oder der Abbruch einer bestehenden Verbindung zum Anbieter kann entweder technische Ursachen (z.B. Timeout-Fehler durch eine Leitungsunterbrechung) haben oder auf einen unberechtigten Eingriff Dritter in die Verbindung zurückzuführen sein.



(Diese Seite ist beabsichtigterweise leer.)

3 Sicherheitsvorgaben

24 Die der Evaluierung zugrunde liegenden und im folgenden abgedruckten Sicherheitsvorgaben sind in deutscher Sprache bereitgestellt worden.

3.1 Produktbeschreibung

3.2 Einsatzzweck des EVG

MeSecure 1.03 ist ein Softwareprodukt der MeTechnology Europe GmbH, das für die sichere Kommunikation eines Klienten mit einem Server über einen öffentlichen Kommunikationskanal (z.B. das Internet) entwickelt wurde. MeSecure 1.03 sichert die Authentizität des durch den Klient kontaktierten Servers sowie die Vertraulichkeit und Integrität der übertragenen Daten. MeSecure 1.03 basiert auf dem Secure Socket Layer (SSL) Protokoll, Version 2.0.

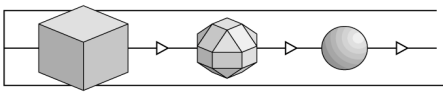
3.3 Bestandteile des EVG

Der EVG MeSecure 1.03 besteht aus:

Nr.	Typ	Bezeichnung	Übergabeform
1	SW	MeSecure SSL-Klient-Stack, ohne die Java-Klasse CA_ROOT.class	Java-Byte-Code
2	SW	MeSecure SSL-Klient-Stack, Public Key einer Zertifizierungsinstanz	Teil der Java-Klasse CA_ROOT.class
3	SW	MeSecure SSL-Klient-Stack, Name des zum Anwendungssystem gehörenden zugelassenen Servers	Teil der Java-Klasse CA_ROOT.class
4	SW	MeSecure SSL-Server-Stack, Dynamische Link-Bibliotheken	Dateien asn1w32.dll, crypw32.dll, ssl2w32.dll
5	SW	MeSecure SSL-Server-Stack, Zertifikat des Servers (X.509 Zertifikat)	Datei CTSERV.PEM
6	SW	MeSecure SSL-Server-Stack, Private Key des Servers	Datei keyserv.key
7	DK	Betriebsdokumentation „MeSecure 1.03, Anlauf und Betrieb“	Version 3.11

Tabelle 1: Bestandteile des EVG

Die EVG-Komponenten Nr. 1, 2 und 3 bilden die Klient-Komponente des EVG, den MeSecure SSL-Klient-Stack. Die EVG-Komponenten Nr. 4, 5 und 6 bilden die Server-Komponente des EVG, den MeSecure SSL-Server-Stack.



Die Klient-Komponente des EVG wird dem Anwender (Betreiber des Servers) in einem Java-Archiv MePrpApplet.jar und einer CAB-Datei MePrpApplet.cab ausgeliefert. Sie wird als Teil eines Java-Applets in einen handelsüblichen Web-Browser geladen und dort ausgeführt. Der MeSecure SSL-Klient-Stack besteht aus als Java-Byte-Code compilierte Klassen, die fest und anwenderunabhängig sind, und der Java-Klasse CA_ROOT.class, die die anwenderspezifischen Komponenten Nr. 2 und Nr. 3 enthält.

Die folgenden Class-Dateien sind Bestandteil der EVG-Komponente Nr.1.

Datum	Zeit	Größe	Name der Datei	Version
01.02.99	15:08	17.573	Bignum.class	1.1.3.3
01.02.99	15:08	4.824	Certificate.class	1.1.3.6
01.02.99	15:08	3.161	CertInfo.class	1.1.3.2
01.02.99	15:08	1.510	CipherList.class	1.1.3.2
19.02.99	17:38	1.836	CipherName.class	1.1.3.4
01.02.99	15:08	1.022	CipherType.class	1.1.3.3
19.02.99	17:38	392	Coder.class	1.1.3.3
01.02.99	15:08	298	Crypter.class	1.1.3.2
01.02.99	15:08	3.884	IDEA.class	1.1.3.3
19.02.99	17:38	1.500	IdeaCBCMD5.class	1.1.3.6
01.02.99	15:08	2.615	Include.class	1.1.3.6
01.02.99	15:08	535	KnownAlgorithm.class	1.1.3.2
01.02.99	15:08	5.464	MD5.class	1.1.3.2
01.02.99	15:08	372	MemCertificate.class	1.1.2.1
19.02.99	17:38	2.065	NullNullMD5.class	1.1.3.5
01.02.99	15:08	2.630	ObjectData.class	1.1.3.2
01.02.99	15:08	1.157	ObjectHeader.class	1.1.3.2
01.02.99	15:08	3.347	Randomizer.class	1.1.3.12
01.02.99	15:08	2.605	RSACrypt.class	1.1.3.3
01.02.99	15:08	10.745	SSL.class	1.1.3.13
01.02.99	15:08	1.518	SSLError.class	1.03
01.02.99	15:08	773	SSLException.class	1.1.3.3
01.02.99	15:08	818	XbitString.class	1.1.3.2
01.02.99	15:08	832	XInteger.class	1.1.3.2

Datum	Zeit	Größe	Name der Datei	Version
01.02.99	15:08	537	XobjectIdent.class	1.1.3.1
01.02.99	15:08	617	XprintableString.class	1.1.3.1
01.02.99	15:08	997	XpublicKey.class	1.1.3.2
01.02.99	15:08	504	Xsequence.class	1.1.3.1
01.02.99	15:08	428	XSet.class	1.1.3.1
01.02.99	15:08	949	Xsignature.class	1.1.3.2
01.02.99	15:08	859	XText.class	1.1.3.2
01.02.99	15:08	1.742	XValidity.class	1.1.3.3

Tabelle 2: Java-Klassen des EVG

Die Java-Klasse CA_ROOT.class hat die Form eines X.509-Zertifikates und wird als Prüfzertifikat bezeichnet (s. Beschreibung in Tabelle 5).

Ebenso Bestandteil des Java-Applets ist eine Klient-Applikation, die nicht Bestandteil der Evaluation ist, jedoch den EVG zur sicheren Kommunikation mit dem entfernten Server nutzt (siehe auch Anforderungen an die Einsatzumgebung).

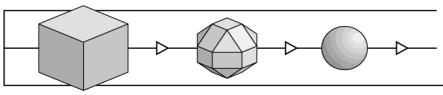
Die Server-Komponente des EVG, der MeSecure SSL-Server-Stack, befindet sich auf einem Server-Rechner und ist Teil des SSL-Routers der MeTechnology Europe GmbH. Die Dynamischen Link-Bibliotheken (DLLs) sind fest und anwenderunabhängig:

Typ	Name	Größe	Datum	Zeit	Version
SW	asn1w32.dll	241.161	19.02.99	15:23	1.7d
SW	crypw32.dll	356.476	01.12.98	15:02	1.4.1.1d
SW	ssl2w32.dll	313.087	19.02.99	15:24	1.8d

Tabelle 3: DLLs des EVG

Diese DLL-Dateien werden für die Erbringung des sicheren Kommunikationsdienstes von einer ausführbaren Datei sslroute.exe (SSL-Router) genutzt. Der SSL-Router wird von einer sich logisch darüber befindenden Server-Applikation eingesetzt, um einen sicheren Kommunikationskanal aufzubauen (Technisch gesehen ist die Server-Applikation ein Teil der sslroute.exe). Die Server-Komponente des EVG nutzt wiederum eine eigene Transportschicht (EsdTransportlayer), um Netzwerkpakete an die Transportschicht des Betriebssystems weitergeben zu können. Weder die verwendete Server-Applikation noch der spezifische EsdTransportlayer noch der ausführbare SSL-Router (sslroute.exe) sind Gegenstand der Evaluation.

Die Datei CTSERV.PEM (EVG-Komponente Nr. 5) ist das X509-Zertifikat des Servers (kurz Server-Zertifikat, zum Inhalt s. Tabelle 4), ausgestellt durch die Zertifizierungsinstanz. Die Datei keyserv.key (EVG-Komponente Nr. 6) enthält den zum Public Key im



Server-Zertifikat gehörenden Private Key des Servers. Beide Dateien sind anwenderspezifische Komponenten des EVG.

Die Betriebsdokumentation „MeSecure 1.03, Anlauf und Betrieb“ (EVG-Komponente Nr. 7) enthält eine Liste aller an den Anwender gelieferten EVG-Komponenten Nr. 1 bis Nr. 6. Sie unterliegt nur in den Angaben der EVG-Komponenten Nr. 2, 3, 5 und 6 anwenderspezifischen Veränderungen.

3.4 Art der Nutzung des EVG

Der EVG wird zur Sicherung der Kommunikation einer Anwendung zwischen einem Klienten und einem Server eingesetzt. Wenn der Klient die Anwendung durch Anwahl einer HTML-Seite des Server anfordert, wird

1. eine HTTPS-Verbindung zwischen Klient und Server aufgebaut,

2. ein Java-Applet mit dieser Anwendung und dem MeSecure SSL-Klient-Stack des EVG vom Server an den Klienten über die HTTPS-Verbindung übermittelt und in der Java Virtual Machine des Klienten gestartet,

3. auf dem Server wird ein eigener Prozeß (MeSecure SSL-Server-Stack des EVG) für den Klienten instantiiert.

Der MeSecure SSL-Klient-Stack stellt der ebenfalls im Applet enthaltenen Klient-Applikation eine weitere Netzwerkschicht zwischen der Transportschicht und der Applikationsschicht zur Verfügung, die eine durch den EVG gesicherte SSL-Verbindung ermöglicht. Der MeSecure SSL-Klient-Stack baut eine SSL-Verbindung zum MeSecure SSL-Server-Stack auf und prüft die Authentizität des Servers. Nach erfolgreichem Verbindungsaufbau überträgt und empfängt die Klient-Applikation die Nutzdaten über den MeSecure SSL-Klient-Stack, der die Vertraulichkeit und Integrität dieser Daten schützt.

Der MeSecure SSL-Server-Stack wird durch den SSL-Router zwischen einer Server-Applikation und einer Transportschicht eingebettet. Nach Eintreffen einer Verbindungsanfrage des MeSecure SSL-Klient-Stack baut der MeSecure SSL-Server-Stack in Zusammenarbeit mit dem MeSecure SSL-Klient-Stack des anfragenden Klienten eine SSL-Verbindung auf, in dessen Verlauf sich der Server beim Klienten authentisiert. Nach erfolgreichem Verbindungsaufbau erfolgt die Kommunikation zwischen der Klient- und Server-Applikation über den EVG verschlüsselt und integritätsgeschützt.

3.5 Einsatzumgebung

3.5.1 Einsatzumgebung des EVG - Klient

Im folgenden werden die Anforderungen an die Einsatzumgebung der Klient-Komponente des EVG zusammengefaßt:

UK1 Es muß ein Web-Browser installiert sein, der eine Java Virtual Machine enthält. Die Java Virtual Machine muß die Java Versionen 1.02 und 1.1 unterstützen.

UK2 Die Einsatzumgebung muß gewährleisten, daß die Klient-Komponente des EVG (Java-Bytecode, Public Key der Zertifizierungsinstanz und Namen des zugelassenen Servers) authentisch im Klient vorliegen.

UK3 Die authentische Übertragung des Java-Applets mit der Klient-Komponente des EVG wird durch eine externe Sicherheitsmaßnahme unterstützt.

UK4 Die Einsatzumgebung muß gewährleisten, daß Software Dritter die Integrität des EVG nicht stört und nicht auf sicherheitsrelevante Parameter des EVG (das Prüfzertifikat und die im EVG erzeugten symmetrischen Schlüssel) zugreifen kann.

UK5 Die Klient-Applikation muß den EVG ordnungsgemäß einsetzen, d.h.

- die Klient-Applikation muß alle zu sichernden Daten über den EVG als Nutzdaten (O1) austauschen,
- die Klient-Applikation darf ausschließlich über die externen Schnittstellen des EVG auf den EVG zugreifen,
- die Klient-Applikation muß den im EVG implementierten Zufallszahlengenerator (Randomizer) verwenden,
- die Klient-Applikation stellt sicher, daß der erfolgreiche Aufbau einer sicheren Verbindung und der Name des verbundenen Servers dem Benutzer der Klient-Komponente des EVG angezeigt wird. Sie nutzt dazu eine EVG-Funktion zur Ausgabe des Prüfzertifikats und des Server-Zertifikats.

UK6 Der Benutzer des Klienten wird durch den Betreiber des Servers über den ordnungsgemäßen Betrieb des EVG unterrichtet.

3.5.2 Einsatzumgebung des EVG - Serverrechner

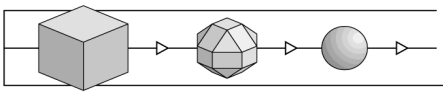
Im folgenden werden die Anforderungen an die Einsatzumgebung für die Server-Komponente des EVG zusammengefaßt:

US1 Die Server-Applikation und die Server-Komponente des EVG müssen auf einem Windows NT 4.0 System betrieben werden.

US2 Für jede sichere Verbindung zu einem Klient wird auf dem Server ein eigener Prozeß gestartet. Das Betriebssystem des Servers muß gewährleisten, daß diese Prozesse wirkungsvoll separiert werden.

US3 Die Server-Komponente des EVG (MeSecure SSL-Server-Stack) muß eingebettet zwischen der Server-Applikation und dem EsdTransport-Layer betrieben werden.

US4 Die Einsatzumgebung muß gewährleisten, daß der EVG und die darin enthaltenen Public Key und Private Key authentisch im Server vorhanden sind und die Vertraulichkeit des Private Key gewährleistet wird.



US5 Die Einsatzumgebung muß die Sicherheit des EVG einschließlich vorhandener sicherheitsrelevanter Parameter (Server-Zertifikat, Private Key des Servers, Session-Key der SSL-Verbindung) gewährleisten:

- Der Server-Rechner, der die Server-Applikation und die Server-Komponente des EVG betreibt, muß in einer räumlich gesicherten Umgebung betrieben werden.
- Zutritt zu den Räumlichkeiten haben nur berechtigte Personen.
- Ein Administrator führt alle systemadministrativen Aufgaben im laufenden Betrieb verantwortlich durch.

US6 Die Einsatzumgebung muß gewährleisten, daß Software Dritter die Integrität der EVG-Komponente nicht stört und nicht auf deren sicherheitsrelevante Parameter (z.B. vorhandene symmetrische Schlüssel) zugreifen kann.

3.5.3 Einsatzumgebung des EVG - weitere Voraussetzungen

Im folgenden werden die weiteren Anforderungen an die Einsatzumgebung des EVG zusammengefaßt:

UW1 Das Server-Zertifikat ist eindeutig diesem zugeordnet und wurde mit dem Private Key einer Zertifizierungsinstanz erstellt, dessen zugehöriger Public Key im MeSecure SSL-Klient-Stack authentisch vorhanden sein muß. Der Public Key des Zertifikatseigentümers (Subject) ist ein RSA-Schlüssel mit der Modullänge 1024 Bit. Die Signatur über der Zertifizierungsinstanz wird mit dem RSA-Algorithmus und einer Modullänge von 1024 Bit geleistet.

UW2 Das von der Zertifizierungsstelle ausgestellte Server-Zertifikat muß die folgenden Angaben beinhalten:

Feld	Inhalt
Version	Identifiziert die Version von X.509, die diesem Zertifikat zugrunde liegt
Serial Number	Von der Zertifizierungsstelle zugewiesene Nummer
Signature	Verweist auf den Algorithmus, der zum Unterschreiben verwendet wurde
Issuer	Identifiziert die Zertifizierungsinstanz
Validity	Beinhaltet die Gültigkeitsdauer

Feld	Inhalt
Subject	Name des zugelassenen Servers
PublicKey	Beinhaltet den Public Key des Betreibers des zugelassenen Servers, signiert mit dem Private Key der Zertifizierungsinstanz

Tabelle 4: Aufbau des Server-Zertifikates

UW3 Das Prüfzertifikat muß die Zertifizierungsinstanz, die das Server-Zertifikat ausgestellt hat, eindeutig identifizieren. Der Public Key des Zertifikatseigentümers (Subject) ist ein RSA-Schlüssel mit der Modullänge 1024 Bit. Die Signatur über der Zertifizierungsinstanz wird mit dem RSA-Algorithmus und einer Modullänge von 1024 Bit geleistet.

UW4 Das Prüfzertifikat muß folgenden Aufbau besitzen:

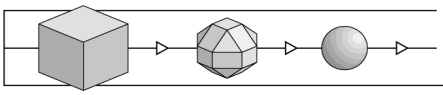
Feld	Inhalt
Version	Identifiziert die Version von X.509, die diesem Zertifikat zugrunde liegt
Serial Number	Von MeTechnology Europe GmbH zugewiesene Nummer
Signature	Verweist auf den verwendeten Algorithmus, der zum Unterschreiben verwendet wurde
Issuer	Name des zugelassenen Servers
Validity	Beinhaltet die Gültigkeitsdauer
Subject	Herausgeber des Server-Zertifikates
PublicKey	Beinhaltet den Public Key des Zertifizierungsstelle, die das Serverzertifikat erstellt hat

Tabelle 5: Aufbau Prüfzertifikat

Die durch den EVG erreichbare Sicherheit beruht auf der sicheren Erzeugung der beiden Schlüsselpaare (Server und Zertifizierungsinstanz), der Vertrauenswürdigkeit der Zertifizierungsinstanz und der Vertraulichkeit des Private Key der Zertifizierungsinstanz.

3.6 Objekte

Es werden die folgenden für den EVG relevanten Objekte definiert:



O1 **Nutzdaten**: Daten, die in Form aufeinanderfolgender Datenpakete zwischen der Klient-Applikation und der Server-Applikation über den EVG nach dem Aufbau des sicheren Kanals ausgetauscht werden und vom EVG für diesen Zweck zu Nachrichten (O3) aufbereitet wurden.

O2 **Authentisierungsdaten**: Daten, die beim Aufbau des sicheren Kanals (Initialisierung, Server-Authentisierung, Schlüsselaustausch) zwischen der EVG-Komponente des Klienten und der EVG-Komponente des Servers ausgetauscht werden.

O3 **Nachrichten**: Daten, die zwischen der EVG-Komponente des Klienten und der EVG-Komponente des Servers über das Netzwerk nach dem Aufbau des sicheren Kanals ausgetauscht werden und die Nutzdaten (O1) in gesicherter Form transportieren.

3.7 Subjekte

Es werden die folgenden für den EVG relevanten Subjekte definiert:

S1 **Angreifer**: Personen oder Prozesse, die weder über die sicherheitsrelevanten Daten und Parameter des Klienten noch des Servers verfügen, sondern allein Zugriff auf den Kanal (das öffentliche Netzwerk) und die darauf übertragenen Daten haben.

S2 **Klient-Applikation**: übergibt und empfängt Nutzdaten (O1) von der Klient-Komponente des EVG.

S3 **Server-Applikation**: übergibt und empfängt Nutzdaten (O1) von der Server-Komponente des EVG.

3.8 Zugriffsmodi

Es werden die folgenden für den EVG relevanten Zugriffsmodi definiert:

A1 Abhören von Nachrichten (O3) oder Authentisierungsdaten (O2) bei der Übertragung auf dem Kanal.

A2 Erzeugen von Nachrichten (O3) oder von Authentisierungsdaten (O2) und deren Einspielen in den Kanal.

A3 Einspielen von abgehörten (und aufgezeichneten) Nachrichten (O3) oder Authentisierungsdaten (O2) in den Kanal.

A4 Manipulation von Nachrichten (O3) oder Authentisierungsdaten (O2) bei der Übertragung auf dem Kanal.

A5 Entfernen von Teilen einer Nachricht (O3) bei der Übertragung auf dem Kanal.

3.9 Sicherheitsziele

Es werden für den EVG die folgenden Sicherheitsziele definiert:

Z1 Sicherung der Vertraulichkeit von Nutzdaten (O1)
Ein Angreifer (S1) soll nicht in der Lage sein, Kenntnis über Nutzdaten (O1) zu erhalten, während sie zwischen Klient-Applikation und Server-Applikation in der vom EVG dafür vorbereiteten Form über das öffentliche Netzwerk ausgetauscht werden.

Z2 Sicherung der Integrität von Nutzdaten (O1)
Ein Angreifer (S1) soll nicht in der Lage sein, erzeugte, abgehörte oder veränderte Nachrichten (O3) in den Kanal einzuspielen, wobei diese Manipulation nicht erkannt wird, wenn die Nachrichten vom Klienten oder Server über das öffentliche Netzwerk empfangen werden. Der vorgesehene Empfänger der Nutzdaten (O1) (die Klient-Applikation S2 bzw. die Server-Applikation S3) ist über eine festgestellte Verletzung der Integrität einer Nachricht (O3) zu informieren.

Z3 Server-Authentisierung
Die Klient-Applikation (S2) soll nur mit dem zum System gehörenden, zugelassenen Server Nutzdaten (O1) austauschen. Die Klient-Applikation (S2) stellt dazu sicher, daß sie erst dann Nutzdaten mit einem Server austauscht, wenn sie durch die Klient-Komponente des EVG davon informiert wurde, daß der Server tatsächlich der zum System gehörende, zugelassene Server ist.

3.10 Bedrohungen

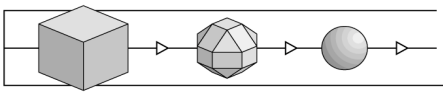
Den folgenden Bedrohungen soll der EVG entgegenwirken:

B1 **Verletzung der Vertraulichkeit von Nutzdaten**
Die Bedrohung besteht darin, daß ein Angreifer (S1) Kenntnis über Nutzdaten (O1) erhält, während sie zwischen Klienten und Server über das öffentliche Netzwerk ausgetauscht werden.

B2 **Verletzung der Integrität von Nachrichten durch Erzeugen und Einspielen**
Die Bedrohung besteht darin, daß ein Angreifer (S1) Nachrichten (O3) oder Teile davon erzeugt und in den Kanal einspielt, wobei diese Manipulation nicht erkannt wird, wenn die Nachrichten vom Klienten oder Server über das öffentliche Netzwerk empfangen werden.

B3 **Verletzung der Integrität von Nachrichten durch Aufzeichnen und Einspielen**
Die Bedrohung besteht darin, daß ein Angreifer (S1) Nachrichten (O3) abhört und Nachrichten (O3) oder Teile davon in den Kanal einspielt, wobei diese Manipulation nicht erkannt wird, wenn die Nachrichten vom Klienten oder Server über das öffentliche Netzwerk empfangen werden.

B4 **Verletzung der Integrität von Nachrichten durch Manipulation der Bits**
Die Bedrohung besteht darin, daß ein Angreifer (S1) Nutzdaten (O1) verändert, in-



dem er einzelne Datenbits in den Nachrichten (O3) manipuliert, während sie zwischen Klient und Server über das öffentliche Netzwerk ausgetauscht werden, wobei diese Manipulation nicht erkannt wird, wenn die Nachrichten vom Klienten oder Server über das öffentliche Netzwerk empfangen werden.

B5 **Verletzung der Integrität von Nachrichten durch Änderung der Paketreihenfolge**
Die Bedrohung besteht darin, daß ein Angreifer (S1) einzelne Pakete, aus denen die Nachrichten (O3) bestehen, in Ihrer Reihenfolge verändert, während sie zwischen Klienten und Server über das öffentliche Netzwerk ausgetauscht werden, wobei diese Manipulation durch den Empfänger nicht erkannt wird.

B6 **Verletzung der Integrität von Nachrichten durch Entfernen von Bits oder Paketen**
Die Bedrohung besteht darin, daß ein Angreifer (S1) die Integrität der Nutzdaten (O1) dadurch verletzt, in dem er einzelne Bits oder Pakete aus den Nachrichten (O3) entfernt, während sie zwischen Klient und Server über das öffentliche Netzwerk ausgetauscht werden, wobei diese Manipulation durch den Empfänger nicht erkannt wird.

B7 **Unautorisierter Aufbau einer Verbindung zum Klienten**
Die Bedrohung besteht darin, daß ein Angreifer (S1) durch Einspielen von Authentisierungsdaten (O2) gegenüber der Klient-Komponente des EVG einen Server simuliert, so daß die Klient-Applikation fälschlicherweise annimmt, mit dem zum Anwendungssystem gehörenden, zugelassenen Server zu kommunizieren und mit dem Austausch von Nutzdaten (O1) beginnt.

3.11 Sicherheitsspezifischen Funktionen des EVG

Der EVG realisiert die folgenden sicherheitsspezifischen Funktionen F1 bis F4, um den Bedrohungen B1-B7 entgegenzuwirken:

F1 **Authentisierung des Servers**
Mit der sicherheitsspezifischen Funktion Authentisierung des Servers wird sichergestellt, daß der Klient mit einem Server erst dann den Austausch von Nutzdaten beginnt, wenn er sich davon überzeugt hat, daß dieser der zum System gehörende, zugelassene Server ist. Die Authentisierung wird beim Verbindungsaufbau durchgeführt.
Bei einer erfolgreichen Authentisierung des Servers können der Klient und der Server nachfolgend Nutzdaten vertraulich und integritätsgeschützt austauschen. Bei nicht erfolgreicher Authentisierung des Servers werden keine Nutzdaten ausgetauscht, und es wird eine Fehlermeldung ausgegeben.

F2 **Vertraulichkeit der Daten**
Nach erfolgtem Aufbau des sicheren Kanals (siehe F1) verfügen beide Kommunikationspartner über gemeinsame geheime Schlüssel.
Durch Verschlüsselung der Nutzdaten (O1) der Applikation sichert die EVG-Komponente des Senders die Vertraulichkeit der Nutzdaten (O1), die er zur EVG-Kom-

ponente der Empfängerseite sendet. Die jeweilige EVG-Komponente des Empfängers entschlüsselt die Nachricht mit dem entsprechenden Schlüssel und übergibt die unverschlüsselten Nutzdaten (O1) an die Applikation.

F3 **Prüfen der Integrität der Daten**

Nach erfolgtem Aufbau des sicheren Kanals (siehe F1) verfügen beide Kommunikationspartner über gemeinsame geheime Schlüssel (Session-Keys).
Zur Überprüfung der Integrität der Nutzdaten (O1) wird über die Nutzdaten (O1), die Paketnummer und einen Session-Key ein Hashwert berechnet und in die Nachrichten (O3) eingefügt. Diese Nachricht (O3) wird mit Hilfe der sicherheitsspezifischen Funktion F2 verschlüsselt und übertragen. Durch Entschlüsselung der Nachricht (O3) und Vergleich des übertragenen Hashwertes mit einem selbst errechneten Hashwert kann der Empfänger feststellen, ob die Integrität der Nutzdaten (O1) gewahrt ist oder nicht.
Bei Verletzung der Integrität der übertragenen Nutzdaten wird die Applikation des Empfängers über die Integritätsverletzung informiert, und der sichere Kanal wird beendet.

F4 **Einfügen und Prüfen von Paketnummern**

Mit dieser sicherheitsspezifischen Funktion werden während einer Session ausgetauschte Datenpakete der Nachrichten (O3) mit Hilfe einer Paketnummer eindeutig identifiziert. Die Paketnummern werden durch interne Zähler in aufsteigender Reihenfolge erzeugt und gehen in die Bildung der Hashwerte mit ein (F3).
Im Zusammenhang mit der Funktion F3, die die Nutzdaten und die Paketnummer einbezieht, wird sichergestellt, daß das Vertauschen, Entfernen oder Wiedereinspielen von Paketen erkannt werden kann. Der Empfänger kann die Nachricht entschlüsseln, den mitgeschickten Hashwert mit einem auf seiner Seite aus den Nutzdaten, seiner Paketnummer und einem Session-Key berechneten Hashwert vergleichen. Laufen die Paketzähler auf Seiten des Empfängers und des Senders nicht synchron, wird der Fehler erkannt.
Bei Erkennen eines Fehlers wird die Applikation des Empfängers über die Integritätsverletzung informiert, und der sichere Kanal wird beendet.

3.12 Sicherheitsmechanismen des EVG

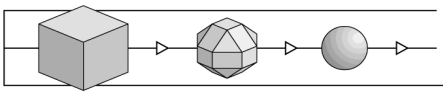
Der EVG definiert die folgenden Sicherheitsmechanismen zur Realisierung der oben definierten sicherheitsspezifischen Funktionen:

M1 **Erzeugung der Zufallszahl masterKey**

Der Mechanismus M1 erzeugt eine Zufallszahl masterKey der Länge 128 Bit. Zur Erzeugung der Zufallszahl wird ein nicht-deterministischer Startwert in die Berechnung einbezogen. Die Generierung des Startwertes erfolgt beim Mechanismus M1 durch Benutzerinteraktion (Tastatureingaben, Mausbewegungen), wobei sowohl deren Werte als auch deren zeitliche Abfolge einbezogen werden.

M2 **Schlüsselableitung**

Der Mechanismus M2 erzeugt mit Hilfe eines Hash-Verfahrens (M7-2) aus den



vier Parametern masterKey, keyArg, connId, challenge und einer Konstanten die Session-Keys wKey und rKey.

M3 **Asymmetrische Verschlüsselung / Entschlüsselung**
Der Mechanismus M3 sorgt für die vertrauliche Übertragung der mit Mechanismus (M1) erzeugten Zufallszahl masterKey vom Klienten an den Server. Dazu wird masterKey mit Hilfe des Public Key des Servers nach dem RSA-Verfahren verschlüsselt.

M4 **Zertifikatsprüfung**
Der Mechanismus M4 stellt sicher, daß der Klient den Public Key des Servers authentisch erhalten hat. Dazu überprüft der Mechanismus M4 das von einer Zertifizierungsinstanz signierte und vom Server übersandte Zertifikat mit Hilfe des authentisch beim Klient vorliegenden Public Key der Zertifizierungsinstanz.
Bei erfolgreicher Prüfung kann der vom Klienten erzeugte masterKey mit dem Public Key des Servers verschlüsselt übertragen werden. Bei nicht erfolgreicher Prüfung wird eine Fehlermeldung ausgegeben, und die Kommunikation zum Server wird beendet.

M5 **Prüfung zur Server-Authentisierung**
Der Mechanismus M5 dient der Prüfung der Identität des Servers mit dem durch M4 geprüften Server-Zertifikat. Der Server authentisiert sich durch den Besitz des zum Public Key im Zertifikat gehörenden Private Keys, mit dem er in der Lage ist, den vom Klient mit dem Public Key verschlüsselten masterKey zu entschlüsseln. Zum Nachweis der erfolgten Authentisierung des Servers leitet dieser die beiden Session-Keys (rKey, wKey) ab, und sendet eine vom Klienten erhaltene Zufallszahl challenge mit dem wKey verschlüsselt (M6) an den Klienten zurück. Dieser kann durch Entschlüsselung (M6) der empfangenen challenge und Vergleich mit der durch ihn erzeugten challenge die Authentisierung des Servers prüfen.
Bei erfolgreicher Prüfung wird der SSL-Verbindungsaufbau fortgesetzt. Bei nicht erfolgreicher Prüfung wird eine Fehlermeldung an die Klient-Applikation generiert und die Verbindung abgebrochen.

M6 **Symmetrische Verschlüsselung / Entschlüsselung**
Der Mechanismus M6 führt eine symmetrische Verschlüsselung unter Nutzung des IDEA Algorithmus mit den Session-Keys wKey und rKey durch.

M7 **Hash-Verfahren**
Das Hash-Verfahren wird in zwei Mechanismen realisiert.

M7-1 Der Mechanismus M7-1 dient der Sicherung der Integrität der Nutzdaten unter Nutzung des MD5 Algorithmus. Der Sender berechnet Hashwerte über die Nutzdaten, die Paketnummer seiner Zählung (M8), den Session-Key wKey und die Pad-Bytes und fügt sie den zu verschlüsselnden Daten hinzu. Der Empfänger berechnet Hashwerte über die empfangenen Nutzdaten, die Paketnummer seiner Zählung (M8), den Session-Key rKey und die Pad-Bytes und vergleicht den empfangenen und den berechneten Hashwert. Bei einer

Übereinstimmung werden die Nutzdaten zur Übergabe an die Applikation freigegeben, bei Abweichungen wird eine Fehlermeldung erzeugt und an die Applikation weitergereicht.

M7-2 Der Mechanismus M7-2 dient der Ableitung der symmetrischen Schlüssel (Session-Keys) Klient-wKey / Klient-rKey und Server-wKey / Server-rKey aus masterKey, challenge, connID und einem von der Übertragungsrichtung abhängigen Parameter unter Nutzung des MD5 Algorithmus.

M8 **Fortlaufende Paketnummern**

Der Mechanismus M8 liefert fortlaufend erzeugte Paketnummern von 0 bis 2^{32}-1 für deren Einbeziehung in die Berechnung des Hashwertes (M7-1). Erreicht einer der beiden, auf beiden Seiten implementierten Zähler während einer SSL-Verbindung 2^{32}-1, so bricht die entsprechende Seite die Kommunikation ab. Eine neue Session verwendet neue Session-Keys und beginnt die Zählung der Paketnummern mit 0.

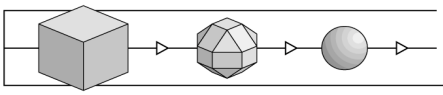
3.13 Zweckmäßigkeit der sicherheitsspezifischen Funktionen

Um die Zweckmäßigkeit der sicherheitsspezifischen Funktionen darzustellen, werden die angenommenen Bedrohungen B1-B4 den Funktionen F1-F4 gegenübergestellt (es bedeutet “P” primär und “S” sekundär):

	F1	F2	F3	F4
B1		P		
B2		S	P	
B3		S	S	P
B4		S	P	
B5		S	S	P
B6		S	P	P
B7	P			

Tabelle 6: Bedrohungen vs. Sicherheitsfunktionen

Wie oben beschrieben basieren die Sicherheitsfunktionen F2, F3 und F4 zusätzlich auf der Sicherheitsfunktion F1. Die Sicherheitsfunktion F1 dient zur Prüfung der Authentizität des Servers und wehrt damit die Bedrohung B7 ab. Zusätzlich enthält sie die Vereinbarung des geheimen Schlüssels für die Sicherheitsfunktion F2. Die Verschlüsselung F2 verhindert direkt die Bedrohung B1 durch die Verschlüsselung. Durch das Nachrechnen des Hashwertes in der Sicherheitsfunktion F3 werden im Zusammenhang mit der Verschlüsselung (Sicherheitsfunktion F2) die Bedrohungen B2, B4 und das Entfernen von Bits entsprechend B6 abgewehrt. Die Kontrolle der Paketnummer in der Sicherheitsfunktion F4 schützt im Zusammenhang mit der Verschlüsselung (Sicherheitsfunktion F2) gegen die Bedrohungen B3, B5 und die Entfernung von Paketen entsprechend B6.



Diese Analyse zeigt, daß jeder Bedrohung mindestens eine der Sicherheitsfunktionen entgegenwirkt.

3.14 Konfigurationen

3.14.1 Beschreibung der evaluierten Konfiguration

Die evaluierte Konfiguration des EVG besteht aus

(1) den im Abschnitt 3.3 beschriebenen EVG-Komponenten Nr. 1 MeSecure SSL-Klient-Stack, ohne die Java-Klasse CA_ROOT.class, und Nr. 4 Dynamische Link-Bibliotheken des MeSecure SSL-Server-Stacks,

(2) den in der Konfigurationsliste beschriebenen und für die Evaluationszwecke erzeugten EVG-Komponenten Nr. 2 Public Key einer Zertifizierungsinstanz, Nr. 3 Name des zum Anwendungssystem gehörenden zugelassenen Servers, Nr. 5 Server-Zertifikat und Nr. 6 Private Key des Servers sowie

(3) der Betriebsdokumentation „MeSecure 1.03, Anlauf und Betrieb“, allerdings mit den konkreten Angaben zu den variablen EVG-Bestandteilen Nr. 2, 3, 5 und 6 der Testkonfiguration.

Diese Konfiguration bildet eine für die Evaluation ausreichend praxisnahe EVG-Konfiguration nach.

Die Klient-Applikation wurde für die Evaluation durch ein Test-Applet nachgebildet. Für den Test stand ein WWW-Server und der SSL-Router des Servers zur Verfügung. Eine auf dem SSL-Router aufsetzende Applikation wurde durch ein Echo der durch die Klient-Applikation gesendeten Daten simuliert. Beide Applikationen und der SSL-Router sind in der Konfigurationsliste (EVG Fileliste, Version 3.12, 22.02.1999, MeTechnology Europe GmbH) beschrieben.

3.14.2 Übertragung der Ergebnisse auf andere Konfigurationen

Der vorliegende Evaluationsbericht gilt nur für EVG-Konfigurationen mit

(1) den im Abschnitt 3.3 und in der Konfigurationsliste beschriebenen unveränderlichen EVG-Komponenten, den MeSecure SSL-Klient-Stack (ohne die Java-Klasse CA_ROOT.class) (Nr. 1) und die Dynamische Link-Bibliotheken des MeSecure SSL-Server-Stacks (Nr. 4),

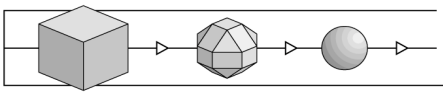
(2) den variablen EVG-Komponenten Public Key einer Zertifizierungsinstanz (Nr. 2), Name des zum Anwendungssystem gehörenden zugelassenen Servers (Nr. 3), Server-Zertifikat (Nr. 5) und Private Key des Servers (Nr. 6), die in Übereinstimmung mit den Beschreibungen in den Sicherheitsvorgaben erzeugt wurden,

(3) der Betriebsdokumentation „MeSecure 1.03, Anlauf und Betrieb“ (EVG-Komponente Nr. 7) mit den konkreten anwenderspezifischen Angaben in den variablen EVG-Bestandteilen Nr. 2, 3, 5 und 6.

3.15 Prüfvorgaben

Der EVG ist nach der Evaluierungsstufe E3 zu prüfen.

Die angestrebte Mindeststärke der Mechanismen ist ”hoch”.

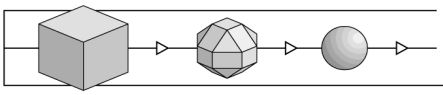


(Diese Seite ist beabsichtigterweise leer.)

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 keine weitergehenden Hinweise oder Empfehlungen für den Anwender ergeben.



(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.

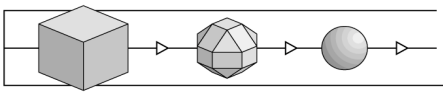
33 Es stellen sich dabei zwei Grundfragen:

- 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 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

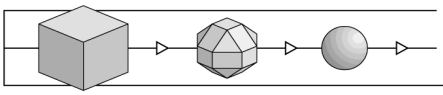
40 Typische Beispiele für Sicherheitsfunktionen sind die *Identifikation und Authentisierung* (von Subjekten), die *Zugriffskontrolle*, die *Beweissicherung* (Protokollierung), die *Protokollauswertung*, die *Übertragungssicherung*. Ein Produkt oder System kann solche Sicherheitsfunktionen beinhalten.

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?

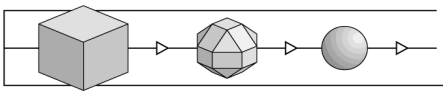
"Alle kritischen Sicherheitsmechanismen (d.h. diejenigen, deren Versagen eine Sicherheitslücke hervorrufen würde), werden hinsichtlich ihrer Fähigkeit be-

wertet, 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."



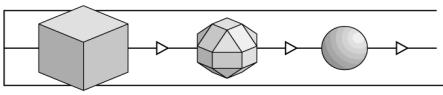
(Diese Seite ist beabsichtigterweise leer.)

6 Anhänge

6.1 Glossar

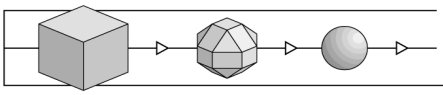
Das Glossar erläutert die in dieser Broschüre verwendeten Begriffe, erhebt allerdings keinerlei Anspruch auf Vollständigkeit oder Allgemeingültigkeit. Der Begriff *Sicherheit* meint hier stets Sicherheit im Kontext der Informationstechnik.

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 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 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 (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	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)
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 1.1, 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

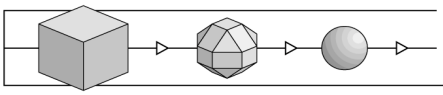
/ ITSEC / Information Technology Security Evaluation Criteria (ITSEC), Version 1.2 (1991), ISBN 92-826-3004-8

(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

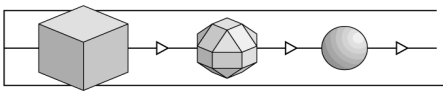
/ Z01 / Zertifizierungsschema, debis IT Security Services, Version 1.4, 16.12.98

/ Z02 / Zertifizierte IT-Produkte, IT- Systeme und IT-Dienstleistungen, debisZERT, Version 1.1 vom 16.12.98 (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.)

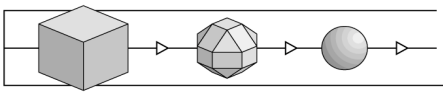
7 Re-Zertifizierungen

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.