debis

Services by DaimlerChrysler

Zertifizierungsreport

SafeGuard® Sign&Crypt, Version 2.0

Utimaco Safeware AG

debisZERT-DSZ-ITSEC-04007-1999

debis IT Security Services

Die Dienstleister der Moderne

Vorwort

Das Produkt SafeGuard® Sign&Crypt, Version 2.0 der Utimaco Safeware 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:	Beabsichtigte Erzeugung von Signaturen (einschl. sicherer Anzeigekomponente), beabsichtigte Signatur-Prüfung, symmetrische Datenverschlüsselung und –entschlüsselung
Evaluationsstufe:	E2
Mechanismenstärke:	alle Mechanismen zumindest: **mittel** Mechanismen für die Signatur-Funktionen (i.e. Hash-Funktionen SHA-1 und RIPEMD-160, asymmetrische Kryptographie): **hoch**

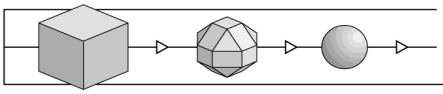
Für weitere Auskünfte und Kopien dieses Reports ist die Zertifizierungsstelle wie folgt erreichbar:

✉ 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 12.04.1999

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



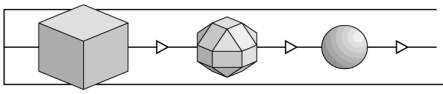
Revisionsliste

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	17.02.1999	Vorversion (nach Musterreport 1.4) in englischer Sprache
1.0	12.04.1999	Erstausgabe (nach Musterreport 1.4) in englischer Sprache
1.OD	25.05.1999	Übersetzung der englischen Originalfassung (Layout angepaßt an Musterreport 1.5) ins Deutsche

Inhalt



1 Überblick

1.1 Evaluierung

1 Die Evaluierung wurde durch Utimaco Safeware AG, Dornbachstr. 30, 61440 Oberursel beauftragt.

2 Die Evaluierung wurde durchgeführt von Prüflabor für IT-Sicherheit der Industrieanlagen-Betriebsgesellschaft mbH und am 15.03.1999 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 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

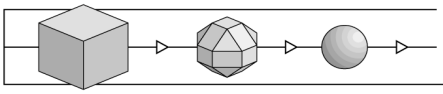
6 Dieser Zertifizierungsreport gibt die Ergebnisse der Evaluierung von SafeGuard® Sign&Crypt, Version 2.0 wieder - im folgenden als EVG = Evaluationsgegenstand bezeichnet.

7 Der Zertifizierungsreport gilt nur für die angegebene 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 SafeGuard® Sign&Crypt, Version 2.0.

10 Der Zertifizierungsreport enthält die Seiten 1 bis 47. 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-04007-1999.

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.

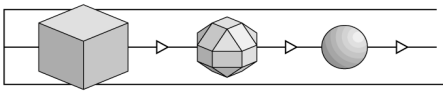
---

[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 E2 gemäß ITSEC, d.h. alle Anforderungen an die Korrektheit und Wirksamkeit gemäß dieser Stufe sind erfüllt. Dies sind:

  ITSEC E2.1 bis E2.37 für die Korrektheit mit den Phasen

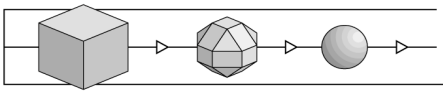
Konstruktion - Entwicklungsprozeß	(Anforderungen, Architekturentwurf, Feinentwurf, Implementierung),
Konstruktion - Entwicklungsumgebung	(Konfigurationskontrolle, Sicherheit beim Entwickler),
Betrieb - Betriebsdokumentation	(Benutzerdokumentation, Systemverwalter-Dokumentation)
Betrieb - Betriebsumgebung	(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 <SM1>, <SM2>, <SM3> und <SM4> des EVG sind kritische Mechanismen.

  – Die Mechanismen <SM1>, <SM2>, <SM3> (und <SM5>) sind vom Typ A; der Mechanismus <SM4> ist vom Typ B. Die Mechanismen des Typs A haben eine Mindeststärke gemäß der Stufe **mittel**. Die Mechanismen für die Signatur-Funk-



tionen (i.e. Hash-Funktionen SHA-1 und RIPEMD-160, asymmetrische Kryptographie) haben die Mechanismenstärke **hoch**.

2.3 Hinweise

22 Die Prüfstelle hat keine Auflagen an den Hersteller auszusprechen.

23 Die Prüfstelle hat folgende Auflagen an den Anwender auszusprechen: Das Ergebnis der Evaluation basiert auf der Annahme, daß der Anwender die Vorgaben in der Handbuchergänzung zu SafeGuard Sign&Crypt strikt befolgt und den Evaluationsgegenstand unter den Restriktionen der Sicherheitsvorgaben, Abschnitt 3.1.3 betreibt.

3 Sicherheitsvorgaben

24 Die der Evaluierung zugrunde liegenden Sicherheitsvorgaben, Version 2.2 vom 03.03.99, sind seitens des Auftraggebers in englischer Sprache bereitgestellt worden. Sie werden hier in deutscher Übersetzung wiedergegeben.

25 Soweit die Sicherheitsvorgaben auf das deutsche Signaturgesetz und / oder die Signaturverordnung Bezug nehmen und eine Einhaltung dieser Vorgaben erklären, weist die die Zertifizierungsstelle darauf hin, daß solche Konformitätserklärungen nicht Teil der Zertifizierung nach ITSEC / ITSEM sind.

26 Die Übereinstimmung mit dem deutschen Signaturgesetz und der Signaturverordnung wird separat im sogenannten „Bestätigungsverfahren“ behandelt (ausgeführt unter debisZERT DLB 2). Ergebnisse dieses Verfahrens sind den Bekanntmachungen der Regulierungsbehörde für Telekommunikation und Post unter www.regtp.de („Digitale Signaturen“) zu entnehmen.

3.1 Einsatzzweck des Produkts

3.1.1 Definition des Evaluationsgegenstandes

Der Evaluationsgegenstand (EVG) wird als folgendes Produkt definiert:

- SafeGuard Sign&Crypt, Version 2.0.

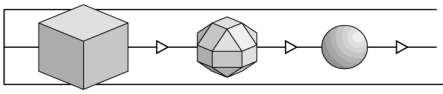
Es besteht aus den folgenden Produktelementen:

- SafeGuard Sign&Crypt Software,
- CardMan Chipkarten-Leser, bei dem es sich wahlweise handeln kann um
  - CardMan Chipkarten-Leser für den seriellen Port oder
  - CardMan Compact Chipkarten-Leser für den seriellen Port oder
  - CardMan Mobile PC-Card (PCMCIA) Chipkarten-Leser oder
  - CardMan Keyboard,
- SafeGuard Sign&Crypt Benutzerhandbuch (gedrucktes Dokument).

Der EVG unterstützt die folgenden Betriebssystem-Plattformen

- Microsoft Windows 95 und
- Microsoft Windows NT 4.0.

Die Unterstützung des Betriebssystems wird während der Installation des EVG reali-



siert, wobei für die verschiedenen Betriebssysteme unterschiedliche Komponenten des EVG installiert werden.

In dieser Definition des EVG sind die deutsche und die englische Sprachversion des EVG enthalten. Sie unterscheiden sich lediglich durch die unterschiedliche Sprache der Benutzeroberfläche und des Benutzerhandbuchs.

3.1.2 Beschreibung des Evaluationsgegenstandes und der beabsichtigten Art der Nutzung

3.1.2.1 Überblick

SafeGuard Sign&Crypt ist ein Produkt, das die Erstellung und Nachprüfung von digitalen Signaturen sowie die Erzeugung und Anzeige einer eindeutigen Dokumenten-Ansicht ermöglicht.[2] Diese Funktionen erfüllen das deutsche Signaturgesetz und die Signaturverordnung.

Zusätzlich zu den gesetzlichen Vorgaben können zu übertragene Daten vor dem Zugriff durch unbefugte Personen geschützt werden.

Auf diese Weise sichert der EVG die Authentizität, Integrität, Vertraulichkeit und Nichtabstreitbarkeit der Urheberschaft signierter Informationen, die von einem Urheber an einen Empfänger übertragen werden.

Der EVG realisiert dieses Ziel durch Erzeugung digitaler Signaturen für die Daten Informationen unter Verwendung eines asymmetrischen Schlüsselsystems und Verschlüsselung der Informationen unter Verwendung eines symmetrischen Verschlüsselungsalgorithmus.

3.1.2.2 Allgemeine Anforderungen an ein Signatur-System

Ein Signatur-System bewirkt die elektronische Signatur eines Dokuments.

Ein Signatur-System arbeitet hauptsächlich mit einer Hash-Funktion in Kombination mit einem asymmetrischen Verschlüsselungsalgorithmus. Für jedes Mitglied einer Signaturgruppe wird ein Schlüsselpaar erzeugt, das aus einem geheimen und einem öffentlichen Schlüssel besteht. Der Verschlüsselungsalgorithmus funktioniert so, daß nur die mit dem geheimen Schlüssel signierten Daten mit dem entsprechenden öffentlichen Schlüssel korrekt nachgeprüft werden können und Änderungen am Schlüssel oder an den Daten ein Mißlingen der Signatur-Nachprüfung zur Folge haben. Wichtig ist dabei die Tatsache, daß der geheime Schlüssel nicht aus der Kenntnis des öffentlichen Schlüssels abgeleitet werden kann.

Das Signatur-System verwendet den geheimen Schlüssel dazu, das Dokument mit einem signifikanten Hash-Wert zu signieren und diesen signierten Wert an das Dokument anzuhängen. Jeder Empfänger, der den öffentlichen Schlüssel des Dokumenten-Urhe-

---

2 Viewer-Komponente von SafeGuard Sign&Crypt: Internationales Patent angemeldet.

bers kennt, ist in der Lage, den Hash-Wert nachzuprüfen und ihn mit dem Inhalt des eingegangenen Dokuments zu vergleichen. So kann er die Integrität und Authentizität des Dokuments nachprüfen, und der Urheber kann nicht bestreiten, daß er das Dokument signiert hat (Nichtabstreitbarkeit der Urheberschaft).

3.1.2.3 Schlüssel-Management

Bei der Verwendung von SafeGuard Sign&Crypt wird davon ausgegangen, daß das Schlüssel-Management für die asymmetrische Verschlüsselung von einer Zertifizierungsstelle (ZS) durchgeführt wird, die auch als „Trust Center“ bezeichnet wird. Jedem Mitglied einer Signatur-Gruppe wird eine einzigartige Kennung zugeordnet. Die Zertifizierungsstelle teilt jedem Mitglied der Signatur-Gruppe einen persönlichen, geheimen Schlüssel zu. Um die Möglichkeiten eines Mißbrauchs auf ein Minimum zu reduzieren, wird der Schlüssel auf einer Chipkarte gespeichert. Der Inhaber der Chipkarte verwendet für seine Authentisierung gegenüber der Chipkarte eine PIN. Der geheime Schlüssel wird der Chipkarte von der Zertifizierungsstelle zugeordnet und darf diese Chipkarte niemals verlassen.

Die Chipkarte enthält ebenfalls Schlüssel der Zertifizierungsstelle selbst, die zur Erstellung von Zertifikaten verwendet werden, mit denen die Autorisierung des Urhebers einer Signatur durch diese spezielle Zertifizierungsstelle nachgewiesen wird. Ein solches Zertifikat wird an ein signiertes Dokument angehängt und kann auf der Empfängerseite mit den Schlüsseln der Zertifizierungsstelle nachgeprüft werden.

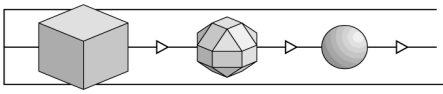
Die Mitglieder-Kennungen und ihre öffentlichen Schlüssel werden vom „Trust Center” mit Hilfe der Datenübertragung (durch Download, Disketten usw.) verteilt. Diese Schlüssel werden für die Verschlüsselung von Session Keys verwendet, wenn übertragene Dokumente zusätzlich verschlüsselt werden.

Mit Hilfe der Administrationskomponente von SafeGuard Sign&Crypt können diese Schlüssel und Kennungen in eine lokale Datenbank von SafeGuard Sign&Crypt importiert werden, wo sie während des Betriebs von SafeGuard Sign&Crypt nachgeschlagen werden können.

3.1.2.4 Nachrichten-Protokolle

Die von SafeGuard Sign&Crypt nach der Signierung von Informationen erzeugten Ausgabedaten haben das Format einer Nachricht, die von einem ausgewählten Kommunikationsprotokoll definiert wird. SafeGuard Sign&Crypt unterstützt derzeit die drei folgenden Protokolle:

- CMT, Version 1.4 (ein firmeneigenes Utimaco-Protokoll),
- S/MIME und
- MailTrusT (MTT), Version 1.0.



Diese Protokolle definieren alle eindeutig das Format der Ausgabe-Nachricht und unterstützen Nachrichtenfelder, in denen der digitale Signatur-Wert gespeichert werden kann.

3.1.2.5 Vom EVG unterstützte Datenformate

Der EVG bietet zwei Funktionsgruppen für das Dokumenten-Management. Einerseits wird ein Urheber mit den Funktionen zur Signierung und Verschlüsselung eines Dokuments unterstützt. Andererseits wird der Empfänger mit Funktionen zur Entschlüsselung und Nachprüfung eines eingegangenen Dokuments ausgestattet.

Der EVG akzeptiert die beiden folgenden Arten von Eingabedaten für digitale Signaturen:

<IN1> Datendatei
Die Dateneingabe kann aus jeder Datendatei bestehen, die durch ein vom EVG unterstütztes Anwendungsprogramm geöffnet und angezeigt werden kann.

<IN2> Geöffnetes Dokument
Der Inhalt eines konkreten Dokuments, das in einem der vom EVG unterstützten Anwendungsprogramme geöffnet ist.

Nach der Signatur eines Dokuments unterstützt der EVG die beiden folgenden Formate für Ausgabedaten:

<OUT1> Signierte Darstellung aus der Anzeigekomponente
Bei den Ausgabe-Daten handelt es sich um die Binärdaten der angezeigten Dokumenten-Darstellung, die von einer speziellen Anzeigekomponente erzeugt wurde. An die Ausgabe-Daten werden die digitale Signatur über die angezeigten Daten, ein Zertifikat des Urhebers und - entsprechend dem ausgewählten Protokoll - zusätzliche Informationen angehängt.

<OUT2> Signierte Original-Datei und Darstellung der Anzeigekomponente
Wenn es sich bei den Eingabe-Daten um eine Datei handelt (<IN1>), können die Ausgabe-Daten aus zwei Teilen bestehen. Dabei handelt es sich bei einem Teil um dieselbe Ausgabe, wie sie durch <OUT1> erzeugt wird, während der andere Teil aus dem Original-Dateiinhalt besteht, der um eine digitale Signatur sowie ein Zertifikat des Urhebers und - entsprechend dem ausgewählten Protokoll - zusätzliche Informationen ergänzt wird. Am Empfängerstandort können die zusätzlichen Informationen einschließlich der Signatur nach der Nachprüfung des Dokuments entfernt werden, so daß der Inhalt der Originaldatei wiederhergestellt werden kann.

In beiden Fällen können die Ausgabe-Daten in einem zweiten Schritt komprimiert und / oder verschlüsselt werden. Nach diesem Verarbeitungsvorgang werden die Daten als eine oder zwei Dateien im Dateisystem gespeichert oder über ein Mail-System an den Empfänger weitergesendet. Für diese Kombination aus Signatur, optionaler Komprimierung und optionaler Verschlüsselung wird in diesem Dokument der Begriff „Versiegelung" benutzt (während der Begriff „Entsiegelung" für das umgekehrte Verfahren

verwendet wird).

Die Methode <OUT2> kann nur mit der Eingabe-Art <IN1> kombiniert werden, während die Methode <OUT1> im Zusammenhang mit <IN1> und <IN2> verwendet werden kann. Der Benutzer kann für jeden einzelnen Fall wählen, ob er die Methode <OUT1> oder (sofern anwendbar) <OUT2> einsetzen möchte.

Die Methode <OUT2> hat den Vorteil, daß die Daten von einem Empfänger elektronisch verarbeitet werden können; die Methode <OUT1> hat den Vorteil, daß das Anwendungsprogramm, mit dem das Dokument erzeugt wurde, nicht notwendigerweise am Standort des Empfängers installiert werden muß.

Alle Kombinationen sind jedoch in ihren sicherheitsspezifischen Funktionen identisch.

3.1.2.6 Allgemeine Beschreibung des Datenflusses

Die Verarbeitung eines Dokuments durch den EVG erfolgt über die folgenden Schritte:

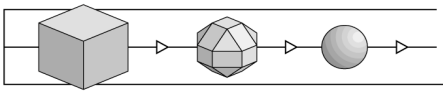
1. Das Dokument wird mit einem der von SafeGuard Sign&Crypt unterstützten Anwendungsprogramme erstellt. Dabei wird das Dokument entweder als eine Datei im Dateisystem gespeichert und SafeGuard Sign&Crypt wird mit Hilfe eines Datei-Managers (Explorer) aufgerufen oder SafeGuard Sign&Crypt wird direkt vom Anwendungsprogramm aus gestartet (nur für <OUT1>).

2. Das Dokument wird unter Verwendung der Anzeigekomponente angezeigt. Die Ausgabe der Anzeigekomponente ist vom bitmap Typ.

3. Die digitale Signatur wird erzeugt. Für diese Funktion muß die persönliche Chipkarte des Urhebers in den Chipkarten-Leser eingelegt werden, und der Benutzer muß seine Karten-PIN eingeben.
   Für die Methode <OUT1> wird eine Signatur über die Binärdaten der Anzeigekomponente erzeugt.
   Für die Methode <OUT2> wird zusätzlich eine Signatur über den binären Inhalt der Originaldatei erzeugt.
   An die Eingabe-Daten (die Datei bzw. Ausgabe der Anzeigekomponente) werden die Signatur, ein Zertifikat mit einer Kennung und dem öffentlichen Schlüssel des Urhebers und - entsprechend dem ausgewählten Protokoll - verschiedene weitere Informationen angehängt.
   Im folgenden wird der Begriff „Dokument" für die Original-Datei (für <IN1>) oder die von der Anzeigekomponente erzeugten und angezeigten binären Daten (für <IN2>) verwendet.

4. Die Dokument-Daten (ohne die Signatur und das Zertifikat) können komprimiert werden, wenn diese Funktion von dem ausgewählten Protokoll unterstützt und eine Komprimierung gewünscht wird.

5. Auf Wunsch kann das Dokument auch verschlüsselt werden. Für diese Funktion müssen dem SafeGuard Sign&Crypt-Programm jedoch die öffentlichen Schlüssel bekannt sein. Die Empfänger des Dokuments können vom Benutzer gewählt wer-



den. Das Dokument wird anschließend verschlüsselt und der Verschlüsselungscode an das Dokument angehängt und mit dem öffentlichen Schlüssel eines jeden Empfängers verschlüsselt.

6. Das Dokument wird über Datenaustausch (E-Mail, Datei-Upload, auf Datenträgern usw.) an den Empfänger bzw. die Empfänger übertragen.

7. Der Empfänger kann das Dokument entschlüsseln, dekomprimieren und verifizieren. Wenn das Dokument verschlüsselt worden ist und es sich beim Empfänger um einen der beabsichtigten Empfänger handelt, kann von diesem das Dokument unter Verwendung seines geheimen Schlüssels entschlüsselt werden. Für diese Funktion muß der Empfänger seine persönliche Chipkarte einsetzen und die PIN der Karte eingeben.

8. Das Dokument kann vom Empfänger verifiziert werden. Dazu gleicht der EVG auf der Empfänger-Seite das Zertifikat im Dokument mit einem auf der Chipkarte des Empfängers gespeicherten Schlüssel ab und erhält den öffentlichen Schlüssel des Urhebers. Mit der Kenntnis des öffentlichen Schlüssels kann der Empfänger die Signatur des Dokuments verifizieren.

   Bei der Methode <OUT1> können die bitmap Daten unter Verwendung der Anzeigekomponente von SafeGuard Sign&Crypt angezeigt werden; die Signatur über die bitmap Daten kann verifiziert werden.
   Bei der Methode <OUT2> können die bitmap Daten unter Verwendung der Anzeigekomponente von SafeGuard Sign&Crypt angezeigt werden. Zusätzlich kann die versiegelte Orginaldatei verifiziert und vom Empfänger extrahiert werden.

In den folgenden Absätzen werden die einzelnen Schritte dieses Verfahrens detailliert beschrieben, wobei zu jedem Schritt zusätzliche Informationen angegeben werden.

3.1.2.7 Dokumenten-Ansicht

In SafeGuard Sign&Crypt können alle Dateien eingegeben werden (im Format <IN1>), die durch ein unterstütztes Anwendungsprogramm erstellt wurden oder die das Format einer Datendatei dieser Anwendungsprogramme haben. Bei den unterstützten Anwendungsprogrammen handelt es sich um

- Microsoft Word 95 (= Word for Windows 7.0), Word 97,

- Microsoft Exchange und

- Microsoft Outlook.

Eine andere Form der Eingabe (im Format <IN2>) kann aus dem eigentlichen Inhalt eines Dokuments bestehen, das von einem der oben genannten Anwendungsprogramme aus geladen wird oder

- von einem anderen Anwendungsprogramm aus geladen wird, das die Standard-Druckschnittstelle von Windows unterstützt.

Solche Dateien oder die eigentlichen Daten-Inhalte werden in den folgenden Absätzen „Dokumente" genannt, wobei mit „Inhalt" immer der binäre Inhalt dieser Dateien oder Daten gemeint ist.

Die Anzeigekomponente von SafeGuard Sign&Crypt beinhaltet eine Methode, ein eindeutiges Bitmap-Bild für jedes Dokument zu erzeugen und anzuzeigen. Die Anzeigekomponente besteht aus zwei Unterkomponenten: einem Druckertreiber und einer Display-Komponente.

In einem ersten Schritt wird das Dokument in ein eindeutiges pixelorientiertes Bitmap-Bild konvertiert. Dies erfolgt über den speziellen Druckertreiber, der Teil der Anzeigekomponente ist.

Das von dem Druckertreiber erzeugte Bild hängt ab von

- dem Inhalt des Original-Dokuments (Text, Zahlen, Graphiken),
- den Anzeige-Optionen für das Original-Dokument (Schriftgröße, Farben) und
- den auf dem System installierten Schriftzeichensätzen (Schriftzeichenbilder).

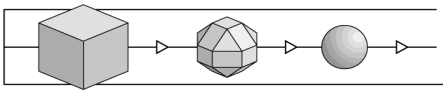
In einem zweiten Schritt wird das resultierende Bitmap-Bild über die Display-Komponente auf dem Benutzer-Bildschirm angezeigt. Mit der Display-Komponente kann das gesamte Dokument gezoomt und der Bildinhalt vertikal / horizontal bewegt werden. Der Bitmap-Bildinhalt läßt sich jedoch nicht verändern.

Bei der Anzeige eines Dokuments zur Signierung auf der Seite des Urhebers und bei der Anzeige eines korrekt verifizierten Dokuments auf der Seite des Empfängers sind verschiedene Instanzen der Display-Komponente tätig.

3.1.2.8 Dokumenten-Signierung

Wenn der Urheber zur Signatur eines Dokuments bereit ist, öffnet er das Dokument mit der Anzeigekomponente. Dies kann durch explizite Öffnung der Anzeigekomponente oder - wenn ein unterstütztes Anwendungsprogramm verwendet wird - durch Betätigung einer speziellen Taste zur Aktivierung der Anzeigekomponente erfolgen. Diese Tasten werden während der Installation von SafeGuard Sign&Crypt zusätzlich in die Anwendungsprogramme aufgenommen. In der Anzeigekomponente kann der Benutzer dann bestimmen, ob er die Ausgabemethode <OUT1> oder (sofern anwendbar) <OUT2> anwenden möchte und ob das signierte Dokument gleichzeitig per E-Mail verschickt werden soll. Zum Starten des Signatur-Verfahrens muß eine spezielle Taste betätigt werden. Danach wird der Urheber aufgefordert, seine Chipkarte mit seinem geheimen Schlüssel in den Chipkarten-Leser einzulegen und seine Karten-PIN einzugeben. Die PIN wird auf der Chipkarte nachgeprüft.

Wenn die PIN korrekt ist, errechnet SafeGuard Sign&Crypt den Hash-Wert des binären Inhalts des Dokuments und der Ausgabe-Daten der Anzeigekomponente (Methode <OUT2>) oder nur der Ausgabe-Daten der Anzeigekomponente (Methode <OUT1>). Das Ergebnis bzw. die Ergebnisse der Hash-Funktion wird bzw. werden mit dem geheimen



Schlüssel des Urhebers verschlüsselt. Diese Verschlüsselung wird auf der Chipkarte durchgeführt.

Die verschlüsselten Hash-Werte werden als „Signaturen" bezeichnet. Für die Methode <OUT2> werden zwei Signaturen erzeugt; für die Methode <OUT1> wird hingegen nur eine Signatur erzeugt. An das Dokument wird außerdem ein Zertifikat - verschlüsselt mit einem Schlüssel der Zertifizierungsstelle - angehängt, durch das der Urheber identifiziert wird und das seinen öffentlichen Schlüssel enthält.

Danach zeigt SafeGuard Sign&Crypt dem Benutzer den korrekten Abschluß des Signatur-Verfahrens für das Dokument an.

Wenn das ausgewählte Protokoll Komprimierungsfunktionen unterstützt, kann der Benutzer das Dokument komprimieren, um die Übertragungskosten zu reduzieren. In einem solchen Fall wird die Komprimierung des Dokumenteninhalts nach der Signatur durchgeführt. Die Komprimierungsoption muß jedoch vor dem Beginn des Versiegelungsverfahrens gewählt werden (die Komprimierung wird nur unter dem Protokoll CMT, Version 1.4, unterstützt).

3.1.2.9 Dokumenten-Verschlüsselung

Wenn der Urheber das Dokument vertraulich behandeln möchte, kann er SafeGuard Sign&Crypt anweisen, das Dokument zu verschlüsseln. Diese Option muß jedoch vor Beginn des Versiegelungsverfahrens ausgewählt werden. Für die Verschlüsselungsfunktion müssen der Name des Empfängers bzw. die Namen der Empfänger ausgewählt werden. Der bzw. die öffentlichen Schlüssel müssen in einer lokalen Datenbank vorhanden sein.

Wenn die Verschlüsselung gewählt wird, wird das Dokument unter Verwendung eines symmetrischen Verschlüsselungsalgorithmus mit einem zufallsgenerierten Session Key verschlüsselt. Der Schlüssel selbst wird jedoch mit dem öffentlichen Schlüssel des Empfängers bzw. der Empfänger verschlüsselt. Gleichzeitig werden der Verschlüsselungscode bzw. die Verschlüsselungscodes zusammen mit den Kennungen des Empfängers bzw. der Empfänger an das verschlüsselte Dokument angehängt. Für diesen Schritt müssen in der Datenbank des Urheber-Systems Zertifikate der Empfänger vorhanden sein, aus denen die öffentlichen Schlüssel abgerufen werden können. Die Gültigkeit der Zertifikate wird anhand des Schlüssels der Zertifizierungsstelle auf der Chipkarte kontrolliert. Wenn eines der Zertifikate ungültig ist, wird die Verschlüsselung nicht durchgeführt.

Das Dokument kann jetzt an den Empfänger bzw. die Empfänger übertragen werden. Die Übertragung des Dokuments gehört nicht zum Leistungsumfang von SafeGuard Sign&Crypt.

3.1.2.10 Dokumenten-Entschlüsselung

Wenn das eingegangene Dokument verschlüsselt wurde, muß es zunächst entschlüsselt werden. Für diese Funktion muß der Empfänger (unter Einsatz desselben Verfahrens, wie es im Kapitel „Dokumenten-Signierung" beschrieben wird) seine Chipkarte mit dem

geheimen Schlüssel zur Verfügung stellen. Der verschlüsselte Session Key wird vom Dokument genommen und auf der Chipkarte entschlüsselt. Dieser Schlüssel wird dann zur Entschlüsselung des Datenteils des Dokuments (einschließlich der Signatur bzw. der Signaturen) verwendet.

Wenn das Dokument komprimiert wurde, muß es anschließend dekomprimiert werden.

Dies funktioniert für Ausgaben der Anzeigekomponente genauso wie für signierte Originaldateien.

3.1.2.11 Dokumenten-Nachprüfung

Nach der Entschlüsselung (sofern es sich um ein verschlüsseltes Dokument handelt) wird die Signatur verifiziert.

Zur Verifizierung eines eingegangenen Dokuments wird der Empfänger - bevor der Vorgang fortgesetzt wird - zunächst aufgefordert, seine Chipkarte in den Leser einzulegen und seine PIN für die Chipkarte einzugeben. Dies ist erforderlich, um das im Dokument enthaltene Zertifikat des Urhebers nachzuprüfen. Mit diesem Schritt wird der öffentliche Schlüssel des Urhebers aus dem Zertifikat abgerufen.

Wenn das Zertifikat bestätigt worden ist, wird der signierte Hash-Wert mit dem öffentlichen Schlüssel verifiziert. Andererseits wird unter Verwendung derselben Hash-Funktion ein Hash-Wert über den Binärinhalt des eingegangenen Dokuments errechnet. Der entschlüsselte eingegangene Hash-Wert und der vor Ort errechnete Hash-Wert werden miteinander verglichen.

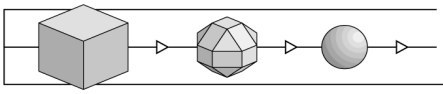
Wenn die Werte identisch sind, informiert SafeGuard Sign&Crypt den Benutzer mit einer Nachricht auf dem Bildschirm über den Urheber und die korrekte Signatur des Dokuments.

Diese Funktion ist für Ausgaben der Anzeigekomponente und signierte Originaldateien identisch.

Wenn es sich bei dem eingegangenen Dokument um Bitmap-Daten der Anzeigekomponente handelt, zeigt die Anzeigekomponente diese Daten auf dem Bildschirm an. Der Hinweis auf die korrekte Signatur erfolgt mit der Dokumentenanzeige im Hintergrund.

Wenn es sich bei dem eingegangenen Dokument jedoch um eine signierte Originaldatei handelt, wird nur das Verifizierungsfenster angezeigt. Danach kann der Inhalt der Originaldatei aus den eingegangenen Daten entnommen und auf der Empfänger-Seite als Anwendungsdaten-Datei gespeichert werden.

Wenn das Zertifikat des Urhebers nicht nachgeprüft werden kann oder die Hash-Werte nicht identisch sind, wird der Benutzer über diese Tatsache informiert. In diesem Fall zeigt die Anzeigekomponente den Inhalt des Dokuments nicht an.



3.1.2.12 Produktinstallation und Benutzung

SafeGuard Sign&Crypt wird mit einem Installationsprogramm von Disketten installiert. Das Installationsprogramm fordert zur Eingabe verschiedener Optionen auf. So zum Beispiel

- Programmbinärpfad,
- Pfad der Schlüssel-Datenbank,
- gewähltes Kommunikationsprotokoll,
- Anwendungsprogramme, in die SafeGuard Sign&Crypt integriert werden soll, und
- Art des Chipkarten-Lesers.

Der Rest der Installation erfolgt dann vollautomatisch.

Die Benutzung von SafeGuard Sign&Crypt ist intuitiv. Die Versiegelung oder Entsiegelung der Dokumente kann über unterschiedliche Wege gestartet werden:

- Auswahl der zu signierenden oder zu verifizierenden Datei und Eröffnung mit dem Icon „Digitale Signatur" auf dem Desktop (z. B. durch Bewegen der Datei mittels Maussteuerung dorthin oder durch Versand der Datei dorthin unter Verwendung des Kontext-Menüs von „Explorer"). Dies jedoch funktioniert nur bei speziell unterstützten Anwendungsprogrammen.
- Aufruf von SafeGuard Sign&Crypt von einem der unterstützten Anwendungsprogramme (Word, Exchange, Outlook) aus und Signierung des tatsächlich geöffneten Dokuments oder Öffnung eines eingegangenen Dokuments. Dieser Start erfolgt über ein zusätzliches Menü-Element oder eine Taste, die während der Installation zusätzlich in das Anwendungsprogramm aufgenommen wurde.
- Start des SafeGuard Sign&Crypt Anwendungsprogramms vom Start-Menü des Betriebssystems aus. Das Anwendungsprogramm ermöglicht nach der einmal auf der Chipkarte erfolgten Authentisierung die Signierung mehrerer Dokumente.
- Aufruf von SafeGuard Sign&Crypt durch Drucken des Dokuments an den Druckertreiber „Digitale Signatur". Dies funktioniert bei allen Anwendungsprogrammen, die die Standard-Druckschnittstelle von Windows unterstützen.

Für die Signatur eines Dokuments können die Optionen zur Komprimierung und Verschlüsselung ausgewählt werden. Der Benutzer kann sich außerdem zwischen der Verwendung der Methode <OUT1> oder (sofern anwendbar) der Methode <OUT2> entscheiden und angeben, ob ein Dokument nur als Datei auf der Festplatte versiegelt oder gleichzeitig per E-Mail versandt werden soll.

Im EVG ist außerdem ein Tool enthalten, das jederzeit zur Überprüfung der Integrität der Binärdateien des installierten EVG eingesetzt werden kann.

3.1.2.13 Administrationsfunktionen

Die Verwaltung von SafeGuard Sign&Crypt enthält im wesentlichen die folgenden Funktionen:

- eine Funktion zur Änderung der Benutzer-PIN der Chipkarte und
- eine Funktion zur zusätzlichen Aufnahme oder Löschung von Kennungen und entsprechenden Zertifikaten (mit öffentlichen Schlüsseln) in der internen Datenbank des Systems.

Die Auswahl der Algorithmen und Protokolle kann durch Änderung einer Konfigurationsdatei für den EVG geändert werden. Dies darf jedoch nur durch ausgewählte Systemverwalter erfolgen.

3.1.3 Beabsichtigte Einsatzumgebung

3.1.3.1 Hardware-Voraussetzungen

Der EVG läuft auf Standard-Personal-Computern mit einem Intel Pentium (60 MHz) kompatiblen Mikroprozessor und darüber. Der Personal Computer benötigt einen freien seriellen Port für den Anschluß des CardMan / CardMan Compact Chipkarten-Lesers. Für die CardMan-Tastatur ist ebenfalls ein serieller Port für den Anschluß des Lesers erforderlich. Beim Einsatz von CardMan Mobile ist kein freier serieller Port notwendig; es sollte jedoch einer der vier zur Verfügung stehenden seriellen Port-Anschlüsse frei sein.

Für die restlichen Teile wie Festplatte und sonstige Ausrüstung sind (mit Ausnahme von ausreichend freiem Speicherplatz für die Installation und den Betrieb des EVG) keine speziellen Hardware-Voraussetzungen erforderlich.

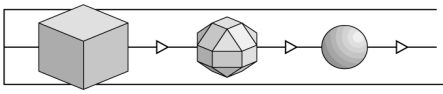
Für einen sicheren Betrieb des EVG ist eine der folgenden Chipkarten-Arten erforderlich:

- SLE CR80S mit T-COS Betriebssystem und 768-Bit RSA auf der Karte oder
- SLE 44CR80S mit CardOS Betriebssystem und 1024-Bit RSA auf der Karte.

(Der EVG unterstützt weitere Chipkarten; der zertifizierte Betrieb ist jedoch auf die genannten Chipkarten-Arten beschränkt.)

3.1.3.2 Software-Voraussetzungen

Die Funktionsfähigkeit des EVG wurde unter den folgenden Betriebssystemen nachgewiesen:



- Windows 95 und

- Windows NT 4.0 Workstation und Server.

Der EVG unterstützt Dokumente, die durch die folgenden Anwendungsprogramme erstellt wurden:

- Microsoft Word 95 (= Word for Windows, Version 7.0) und Microsoft Word 97,

- Microsoft Exchange, Version 4.0, for Windows 95 und Windows NT,

- Microsoft Outlook for Windows 95 und Windows NT sowie

- alle Anwendungsprogramme mit einer Standard-Windows-Druckschnittstelle.

3.1.3.3 Annahmen über die Einsatzumgebung

Der sichere Betrieb des EVG setzt die Sicherheit der Einsatzumgebung voraus, die für die Schlüsselerzeugung und -speicherung verantwortlich ist. Dazu gehören die folgenden Voraussetzungen:

- Die Zertifizierungsstelle garantiert die Vertraulichkeit der geheimen Schlüssel während der Erzeugung und Verteilung und ist für das entsprechende Verfahren zertifiziert.

- Die verwendete Chipkarte und ihr Betriebssystem sind für die Geheimhaltung der gespeicherten Schlüssel zertifiziert.

- Die geheimen Schlüssel dürfen in keiner Einsatzumgebung einer Offenlegung unterliegen.

- Das Betriebssystem der verwendeten Chipkarte ist für die Verarbeitung von asymmetrischen Verschlüsselungsalgorithmen (RSA) ordnungsgemäß zertifiziert.

- Die Länge der Chipkarten-PIN ist auf geeignete Weise definiert (6 Ziffern oder mehr).

- Die Chipkarte wird nach einer bestimmten Anzahl falscher PIN-Eingaben für den Benutzer gesperrt (empfohlen: 3 Versuche).

Die Erfüllung dieser Anforderungen liegt in der Verantwortung der Zertifizierungsstelle.

Bei der zertifizierten Verwendung des EVG darf sich der Benutzer nicht auf eine Zertifizierungsstelle verlassen, die die obigen Anforderungen nicht erfüllt.

3.1.3.4 Sondermaßnahmen

Die folgenden Sondermaßnahmen sind zur Sicherstellung der Sicherheitsfunktion des EVG erforderlich:

Sichere Einsatzumgebung

Die Workstation muß gegen den Zugriff unberechtigter Benutzer gesichert werden durch

- eine separate Unterbringung der Workstation in einem Raum, zu dem nur berechtigte Benutzer Zugang haben und / oder

- eine sichere Einsatzumgebung, in der zumindest die Sicherheitsfunktionen Identifikation und Authentisierung durch ein zertifiziertes Sicherheitssystem zur Verfügung stehen. (Beispiele für eine solche Einsatzumgebung sind Windows 95 zusammen mit SafeGuard Easy für Windows 95 bzw. Windows NT Workstation 4.0 zusammen mit SafeGuard Easy für Windows NT).
  In einer solchen Umgebung muß die Benutzung des EVG auf Benutzer begrenzt sein, die im Geltungsbereich des EVG als Urheber oder Empfänger von signierten Dokumenten bestimmt wurden.

Sicherer Betrieb

Das EVG muß so installiert und betrieben werden, daß die folgenden Optionen und Parameter gewählt werden:

- Hash-Generierung mit MD5, RIPEMD-160 oder SHA-1 (abhängig vom gewählten Protokoll),

  Hinweis: Nach den Vorschriften des deutschen Signaturgesetzes ist MD5 keine gültige Wahl.

- Verschlüsselung mit DES, Triple DES oder IDEA (abhängig vom gewählten Protokoll),

- CardMan Unterstützung,

- geheime Schlüssel nur auf Chipkarten,

- Dokumenten-Verschlüsselung gewählt für jedes Dokument.

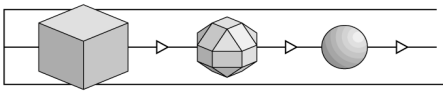
Benutzer-Hinweise

Wenn der EVG auf einer Workstation installiert ist, die mit einem externen Netzwerk (z. B. Internet) verbunden ist, müssen die Benutzer darauf hingewiesen werden, daß

- sie auf die Integrität des EVG und seiner Einsatzumgebung zu achten haben, und zwar insbesondere

  - keine Netzwerk-Anwendungen (Internet-Browser usw.) gleichzeitig mit dem EVG laufen lassen und

  - die Integrität des EVG (mit dem bereitgestellten Integritätskontroll-Tool) kontrollieren, wenn eine der Komponenten des EVG eingesetzt werden soll,



nachdem zwischen dem aktuellen Zeitpunkt und der letzten Integritätskontrolle eine Verbindung zu externen Netzwerken hergestellt worden ist.

Darüber hinaus müssen die Benutzer des EVG darauf hingewiesen werden, daß sie

- keine unzuverlässige Software auf die Workstation installieren dürfen, auf der der EVG installiert ist,
- ihre Chipkarten-PIN geheimhalten müssen,
- sich nicht auf ein Zertifikat verlassen dürfen, wenn es vom EVG unter Verwendung des öffentlichen Schlüssels der Zertifizierungsstelle auf der Chipkarte nicht verifiziert werden kann,
- die Konfiguration des EVG nicht verändern dürfen und,
- die Option „Verschlüsseln" während des Betriebs des EVG beibehalten sollten.

Organisatorische Maßnahmen

Die Personen, die zur Installation und Verwaltung von SafeGuard Sign&Crypt autorisiert werden, müssen sorgfältig ausgewählt werden und höchst vertrauenswürdig sein.

3.1.4 Subjekte, Objekte und Aktionen

3.1.4.1 Allgemeines

In den folgenden Definitionen bedeutet „Dokument" eine Reihe - normalerweise in einer Datei - miteinander verbundene Daten die von einem Urheber an einen oder mehrere Empfänger übertragen wird.

In diesem Zusammenhang werden hier zwei Formen des Dokuments - die ursprünglichen Daten und die von der Anzeigekomponente erzeugte Visualisierung - berücksichtigt.

Bei der Signatur handelt es sich um einen Satz von Daten, die der Urheber an das Dokument anhängt und der von jedem Empfänger verifiziert werden kann.

3.1.4.2 Subjekt

<S1> Urheber eines Dokuments.

<S2> Autorisierter Empfänger eines Dokuments (jemand, der vom Urheber als Empfänger beabsichtigt ist).

<S3> Unberechtigte Person (versucht entweder, den Inhalt eines Dokuments in Erfahrung zu bringen oder den Inhalt eines signierten Dokuments zu verändern).

<S4> Person, deren Identität vom tatsächlichen Urheber eines Dokuments (entweder absichtlich oder unabsichtlich) in Anspruch genommen wird.

3.1.4.3 Objekte

<O1> Visualisierung eines Dokuments. Bei dem Original-Dokument handelt es sich um eine Datendatei, die durch eines der unterstützten Anwendungsprogramme erzeugt wurde oder um ein Dokument, das in den Speicher eines der unterstützten Anwendungsprogramme geladen wurde. Die Visualisierung ist die von der Anzeigekomponente des EVG erzeugte binäre Abbildung dieses Dokuments.

3.1.4.4 Aktionen

<A1> Anzeigen und Signieren eines Dokuments.

<A2> Anzeigen eines Dokuments und Verifizierung der Signatur des Dokuments.

<A3> Änderung des Inhalts eines Dokuments.

<A4> Kenntnisnahme vom Inhalt eines Dokuments.

3.1.5 Sicherheitsziel und angenommene Bedrohungen

3.1.5.1 Sicherheitsziel

Der EVG wurde mit dem Ziel der Non-Repudiation (Nichtabstreitbarkeit der Urheberschaft) eines Dokuments entwickelt, das von seinem Urheber signiert wurde. Sowohl die Authentizität des Urhebers als auch die Integrität des Dokuments können durch Verwendung der Signatur-Funktionen des EVG nachgewiesen werden.

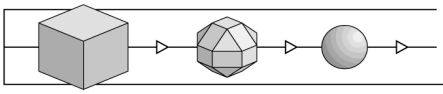
Dies wird unter der Voraussetzung behauptet, daß die Zertifizierungsstelle, die für die Bereitstellung der Benutzer-Zertifikate und der öffentlichen und geheimen Schlüssel verantwortlich ist, ihre Aufgaben auf eine sichere Weise erfüllt.

Wenn der EVG unter dieser Voraussetzung verwendet wird, kann der Urheber eines Dokuments sicher sein, daß nur er in der Lage ist, Dokumente mit seiner Signatur zu signieren. Zudem kann er sicher sein, daß nur die exakte Ansicht des von ihm signierten Dokuments auf der Seite des Empfänger als korrekt nachgeprüft wird.

Der Empfänger des Dokuments kann hingegen sicher sein, daß der angegebene Urheber genau die Ansicht des Dokuments signiert hat, die ihm mit dem Hinweis angezeigt wird, daß sie eine verifizierte Signatur des betreffenden Urhebers enthält.

Darüber hinaus stellt der EVG durch die Verwendung von Verschlüsselungsmechanismen die Vertraulichkeit des Dokuments zwischen der Signierung und der Verifizierung der Signatur sicher.

Unter den genannten Voraussetzungen ist der EVG in der Lage, die im folgenden aufgelisteten angenommenen Bedrohungen abzuwehren:



3.1.5.2 Angenommene Bedrohungen

<T1> Angriff auf die Daten-Integrität

Das Dokument <O1>, das vom Urheber <S1> angesehen und signiert wurde <A1>, ist von einer unberechtigten Person <S3> manipuliert worden <A3> und wird dem Empfänger <S2> trotzdem als korrekt nachgeprüft <A2> angezeigt.

<T2> Angriff auf die Urheber-Authentizität

Dem Empfänger <S2> wird ein Urheber <S4> angezeigt <A2>, der nicht der tatsächliche Urheber <S1> des Dokuments <O1> ist. Dies kann der Fall sein, wenn die Person <S1> ein Dokument ausgibt und (absichtlich oder unabsichtlich) den Anspruch erhebt, Person <S4> zu sein.

<T3> Angriff gegen die Daten-Vertraulichkeit

Der Dokumenten-Inhalt <O1> kann während der Übertragung der Daten zwischen <S1> und einem beliebigen <S2> von einem unberechtigten Benutzer <S3> gelesen werden <A4>.

3.1.5.3 Übereinstimmung mit dem deutschen Signaturgesetz

Die gemeinsame Abwehr von <T1> und <T2> deckt die Non-Repudiation (Nichtabstreitbarkeit der Urheberschaft) des Dokuments ab, d. h. der Urheber kann nicht bestreiten, daß er das Dokument in der angezeigten Version signiert hat.

Die oben aufgeführten Bedrohungen sind nicht mit den Bedrohungen identisch, die von einem Produkt abgewehrt werden sollten, das eine Übereinstimmung mit dem deutschen Signaturgesetz beansprucht.

Die Abwehrmaßnahmen gegen die oben genannten Angriffe wehren jedoch gemeinsam mit der korrekten Implementierung des Viewers und mit der benutzerfreundlichen Implementierung des EVG die vom deutschen Signaturgesetz berücksichtigten Bedrohungen ab.

Um den EVG in Übereinstimmung mit dem deutschen Signaturgesetz zu betreiben, sind die folgenden zusätzlichen Einschränkungen für den Einsatz des EVG und die folgenden zusätzlichen Voraussetzungen für die Einsatzumgebung zu erfüllen:

- Die Zertifizierungsstelle agiert auf eine Weise, die mit den Forderungen des deutschen Signaturgesetzes übereinstimmt und hat eine Betriebsgenehmigung von der Regulierungsbehörde für Telekommunikation und Post erhalten.

- Die verwendeten Chipkarten erfüllen die Vorgaben des deutschen Signaturgesetzes, und eine entsprechende Sicherheitsbestätigung wurde ausgestellt.

- Der EVG wird in einer nicht-öffentlichen Umgebung - z. B. in Privaträumen, bei einer Behörde oder in den Räumen eines Unternehmens - betrieben.

- Der EVG wird unter einer der folgenden Konfigurationen betrieben:

  - MailTrusT V. 1.0 Protokoll mit SHA-1 oder RIPEMD-160 zur Hashwert-Generierung oder

  - S/MIME Protokoll mit SHA-1 zur Hashwert-Generierung.

- Der EVG verwendet für die Signatur-Generierung das auf einer Chipkarte implementierte RSA-Verfahren mit mindestens 768 Bit Schlüssellänge.

- Der Benutzer wird angewiesen, beim Erzeugen einer digitale Signatur immer den Viewer zu benutzen.

3.2 Sicherheitsspezifische und sicherheitsrelevante Funktionen

3.2.1 <SF1> Beabsichtigte Signatur-Erzeugung

Die Signatur wird über den binären Inhalt eines Dokuments erzeugt.

Zwei grundsätzliche Methoden der Dokumenten-Übertragung implizieren eine Signatur-Generierung für unterschiedliche Daten:

- Methode <OUT1>
  Es wird eine Signatur nur für die Binärbild-Daten angelegt, die vom Viewer aus dem Dokumenteninhalt generiert werden.

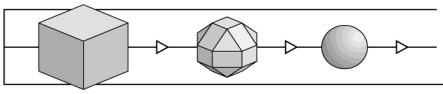
- Methode <OUT2>
  Es wird eine Signatur für den Binärinhalt des Dokuments und eine weitere Signatur für die Bitmap-Daten erzeugt, die vom Viewer aus dem Dokumenteninhalt generiert werden.

Signaturen werden immer durch Errechnung eines Hash-Wertes der entsprechenden Daten und Signierung des Hash-Wertes mit dem geheimen Schlüssel des Urhebers erzeugt, der unter Verwendung eines asymmetrischen Verschlüsselungsalgorithmus auf einer Chipkarte gespeichert wird.

Zusätzlich zur Dokumenten-Signatur wird zum Nachweis der Identität des Signatur-Urhebers ein Zertifikat der Zertifizierungsstelle an das Dokument angehängt. Dieses Zertifikat enthält außerdem den öffentlichen Schlüssel des Urhebers. Die Identität des Urhebers wird durch seine Autorisierung an der Chipkarte nachgewiesen.

Die Erzeugung der Signatur bzw. der Signaturen ist ein expliziter Willensakt: Der Benutzer muß die Erzeugung der Signatur bzw. der Signaturen explizit initiieren.

Der Benutzer wird über die korrekte Signatur der Daten informiert und muß diese Informationen zur Kenntnis nehmen.



3.2.2 <SF2> Beabsichtigte Signatur-Prüfung

Ein Dokument mit einer Signatur, die von <SF1> erzeugt wurde, wird durch Entschlüsselung des Hash-Wertes der eingegangenen Signatur mit dem öffentlichen Schlüssel des Urhebers und durch Berechnung eines neuen Hashwertes des eingegangenen Dokuments nachgeprüft. Der Vergleich der zueinander gehörenden Hash-Werte entscheidet darüber, ob das Dokument authentisch und unverändert ist (die Hash-Werte sind identisch).

Die Nachprüfung wird nur mit der expliziten Bestätigung des Benutzers durchgeführt.

Die korrekte Nachprüfung des eingegangenen Dokuments wird gleichzeitig mit der Anzeige des Inhalts des Dokuments durch den Viewer angezeigt.

Die Identität des Urhebers eines Dokuments und sein öffentlicher Schlüssel werden dem im Dokument enthaltenen Zertifikat entnommen.

3.2.3 <SF3> Symmetrische Daten-Verschlüsselung / -Entschlüsselung

Die Daten des Dokuments werden gemeinsam mit der Signatur nach der Signierung unter Verwendung eines symmetrischen Verschlüsselungsalgorithmus verschlüsselt.

Die Daten werden vor der Nachprüfung der Signatur durch den Empfänger entschlüsselt.

Der für die Verschlüsselung verwendete Schlüssel wird statistisch erzeugt („Session Key") und - verschlüsselt durch den öffentlichen Schlüssel des Empfängers - als Teil des Dokuments an den Empfänger versandt. Nur der Empfänger ist in der Lage, den Session Key mit seinem geheimen Schlüssel zu entschlüsseln und dann das Dokument und die Signatur zu entschlüsseln. Durch die Aufnahme zusätzliche Felder für verschlüsselte öffentliche Schlüssel in das Dokument sind mehrere Empfänger möglich.

3.2.4 Wirksamkeit der Sicherheitsfunktionen

Die folgende Tabelle gibt eine Übersicht darüber, welchen - unter „<Tx>" dargestellten - angenommenen Bedrohungen welche - unter „<SFx>" dargestellten – sicherheitsspezifische Funktionen entgegenwirken. Wenn mehr als eine Funktion für eine Bedrohung genannt wird, wehren alle Funktionen gemeinsam die Bedrohung ab.

	<T1>	<T2>	<T3>
<SF1>			
<SF2>			
<SF3>			

3.3 Mindeststärke der Mechanismen und Evaluationsstufe

Alle (in der deutschen und der englischen Version) aufgelisteten Produktanordnungen

des EVG sind in bezug auf ihre sicherheitsspezifischen und sicherheitsrelevanten Teile, Funktionen und Mechanismen identisch.

3.3.1 Mindeststärke der Mechanismen

Der Mechanismus der in 3.1.3 erwähnten Konfiguration des EVG soll die Mindeststärke **mittel** erreichen.

Die Hauptmechanismen <SM1> und <SM2> (siehe 3.4) sollen die Mindeststärke **hoch** erreichen. Dies ist zur Übereinstimmung mit dem deutschen Signaturgesetz erforderlich.

3.3.2 Evaluationsstufe

Die für den EVG angestrebte Evaluationsstufe ist **E2**.

3.4 Anhang: Sicherheitsmechanismen

Die folgenden Kapitel geben einen Überblick über die Sicherheitsmechanismen für SafeGuard Sign&Crypt. Eine detaillierte Beschreibung der Sicherheitsmechanismen wird im Dokument „Architekturentwurf und Feinentwurf" behandelt.

3.4.1 <SM1> Hash-Funktion

Zur Generierung eines Hashwertes über den Inhalt und / oder das binäre Bild eines Dokuments sind die folgenden Algorithmen implementiert worden:

- SHA-1,
- MD-5 (default für S / MIME und MailTrusT) und
- RIPEMD-160 (mit ISO 9796 Padding).

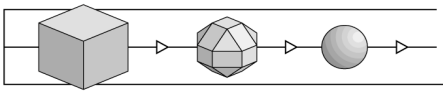
Nur zur Information: Die folgenden zusätzliche Algorithmen sind implementiert; doch ihre Verwendung liegt nicht innerhalb des Leistungsumfangs des zertifizierten Betriebs:

- DESMAC,
- NVB und
- MDC2.

3.4.2 <SM2> Asymmetrischer Verschlüsselungsalgorithmus

Für die asymmetrischen Verschlüsselungsfunktionen (Verschlüsselung mit geheimem Schlüssel, Entschlüsselung mit öffentlichem Schlüssel, Verschlüsselung mit öffentlichem Schlüssel, Entschlüsselung mit geheimem Schlüssel) wird der Standard-RSA-Algorithmus mit mindestens 768 Bit Schlüssellänge verwendet.

Der im EVG implementierte asymmetrische Verschlüsselungsalgorithmus wird nur an-



gewandt, wenn ein öffentlicher Schlüssel beteiligt ist. Wenn ein geheimer Schlüssel beteiligt ist, wird die Implementierung des asymmetrischen Verschlüsselungsalgorithmus auf der Chipkarte vom EVG verwendet.

3.4.3 <SM3> Symmetrischer Verschlüsselungsalgorithmus

Für die symmetrische Verschlüsselung / Entschlüsselung des Dokuments sind die folgenden Standard-Algorithmen im EVG implementiert worden:

- DES (CBC, 16 Runden, Schlüssellänge 56 Bits),
- TRIPLE DES (3x16 Runden CBC mit 2 verschiedenen Schlüsseln, wobei Schlüssel 1 = Schlüssel 3 ist) und
- IDEA (CBC, Schlüssellänge 128 Bits)

Nur zur Information: Es ist ein zusätzlicher Algorithmus implementiert worden; doch seine Verwendung liegt nicht innerhalb des Leistungsumfangs des zertifizierten Betriebs:

- SAFER.

3.4.4 <SM4> Dokument-Erzeugungsprotokoll

Das letztendlich übertragene und empfangene Dokument besteht aus den Ursprungsdaten und zusätzlichen Informationen.

Zu den zusätzlichen Informationen gehören

- ein Zertifikat des Urhebers,
- die Dokumenten-Signatur (verschlüsselter Hash-Wert),
- der Session Key für die Dokumenten-Verschlüsselung, für jeden Empfänger verschlüsselt und
- zusätzliche protokollspezifische Daten.

Zur Datenkomprimierung / Dekomprimierung (nur CMT 1.4 Protokoll) können die folgenden Algorithmen verwendet werden:

- LZSS und
- ZLIB.

3.4.5 <SM5> Kontrolle der Programmintegrität

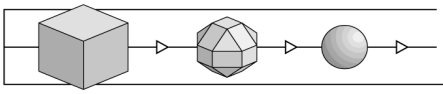
Die Integrität der Programmdateien kann jederzeit mit einem separaten Tool kontrolliert werden. Dieses Tool errechnet einen Hash-Wert der installierten Binär-Dateien des SafeGuard Sign&Crypt und vergleicht ihn mit einem Referenz-Hashwert, der nach der Installation von SafeGuard Sign&Crypt errechnet und in der Windows Registry gespeichert wird. Für die Errechnung des Hash-Wertes wird der SHA-1 Algorithmus verwendet.

3.4.6 Beziehung zwischen Sicherheitsfunktionen und Sicherheitsmechanismen

Die folgende Tabelle gibt einen Überblick darüber, welche Sicherheitsfunktionen „<SFx>“ durch welchen Sicherheitsmechanismus „<SMx>“ implementiert werden.

Wenn mehr als ein Mechanismus für eine Funktion aufgelistet wird, implementieren alle Mechanismen die Funktion gemeinsam.

	<SF1>	<SF2>	<SF3>
<SM1>			
<SM2>			
<SM3>			
<SM4>			
<SM5>	Nur für die Systemintegrität verwendet		

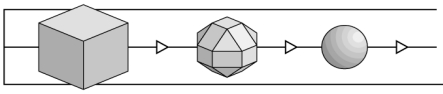


(Diese Seite ist beabsichtigterweise leer.)

4 Hinweise und Empfehlungen zum zertifizierten Objekt

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

28 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

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

5.1 Grundbegriffe

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

31 *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.

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

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

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

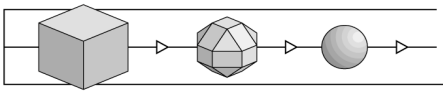
35 Es stellen sich dabei zwei Grundfragen:

- 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

36 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 unan-



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

37 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.

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

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

40 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."

41 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

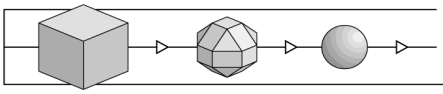
42 Typische Beispiele für Sicherheitsfunktionen sind die *Identifikation und Authentisierung* (von Subjekten), die *Zugriffskontrolle*, die *Beweissicherung* (Protokollierung), die *Protokollauswertung*, die *Übertragungssicherung*. Ein Produkt oder System kann solche Sicherheitsfunktionen beinhalten.

43 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.

44 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.



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

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

47 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."

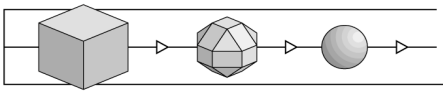
48 Wie wird nun bei Typ A Mechanismen die Stärke definiert?

"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."



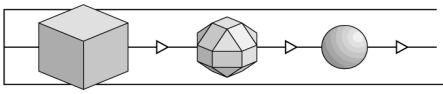
6 Anhänge

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.

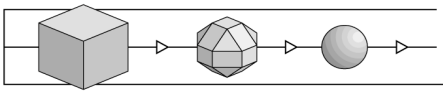
Akkreditierung	Verfahren zum Nachweis, daß eine Prüfstelle den Anforderungen der Norm DIN EN 45001 entspricht. Eine Akkreditierung wird durch eine *Akkreditierungsstelle* durchgeführt. Allgemein anerkannt sind Akkreditierungen von Akkreditierungsstellen, die im Deutschen Akkreditierungsrat (DAR) vertreten 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	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

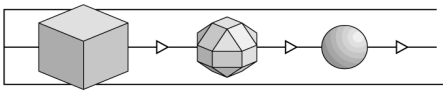
/V04/ Zertifikate mit Anerkennung durch das BSI, Dienstleistungsbereich 4, debisZERT, Version 1.4, 16.12.98

/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 (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

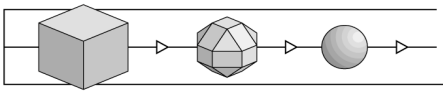
7 Re-Zertifizierungen

49 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.

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

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

52 Die nachfolgenden Anhänge sind fortlaufend numeriert.



Ende der Erstausgabe des Zertifizierungsreports.