debis

Services by DaimlerChrysler

Zertifizierungsreport

Siemens Sign@tor Version 1.0

Siemens AG Österreich

debisZERT-DSZ-ITSEC-04064-2001

debis IT Security Services

Die Dienstleister der Moderne

Vorwort

Das Produkt Siemens Sign@tor Version 1.0 der Siemens AG Österreich 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:	Produktspezifisch: sichere PIN-Eingabe, Vor- und Nachbereitung der digitalen Signatur, integerer Kanal zwischen den EVG-Teilen „Sign@tor PC“ und „Sign@tor Terminal“, (sicheres) Software Update.
Evaluationsstufe:	E2
Mechanismenstärke:	hoch

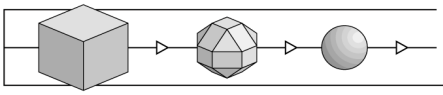
Die Ordnungsmäßigkeit der Evaluierung wird hiermit bestätigt.

Bonn, den 16.03.2001

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

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

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



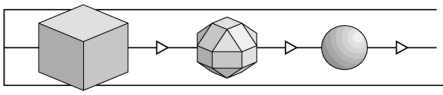
Revisionsliste

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

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

Revision	Datum	Vorgang
0.9	09.03.01	Vorversion (nach Musterreport 1.5)
1.0	13.03.01	Ersterstellung (nach Musterreport 1.5)
1.1	16.03.01	Aktualisierung: Abschluß der Evaluierung

Inhalt



(Diese Seite ist beabsichtigterweise leer.)

1 Überblick

1.1 Evaluierung

1 Die Evaluierung wurde durch die Siemens AG Österreich, Siemensstr. 82, A-1210 Wien beauftragt.

2 Die Evaluierung wurde durchgeführt von der Prüfstelle für IT-Sicherheit der debis IT Security Services und am 12.03.2001 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 DATech (Deutsche Akkreditierungsstelle Technik e.V.) 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

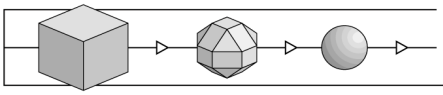
6 Dieser Zertifizierungsreport gibt die Ergebnisse der Evaluierung von Siemens Sign@tor Version 1.0 wieder - im folgenden als EVG = Evaluationsgegenstand bezeichnet.

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 Siemens Sign@tor Version 1.0.

10 Der Zertifizierungsreport enthält die Seiten 1 bis 44. 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 unter

- www.debiszert.de

angekündigt.

1.4 Zertifikat

12 Eine Kurzfassung der Ergebnisse enthält das Sicherheitszertifikat debisZERT-DSZ-ITSEC-04064-2001.

13 Die Inhalte des Zertifikats werden unter

- www.debiszert.de

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.

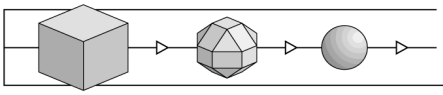
---

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

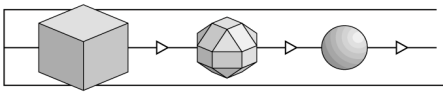
Konstruktion - Entwicklungsprozeß	(Anforderungen, Architekturentwurf, Feinentwurf, Implementierung),
Konstruktion - Entwicklungsumgebung	(Konfigurationskontrolle, Sicherheit beim Entwickler),
Betrieb - Betriebsdokumentation	(Benutzerdokumentation, Systemverwalter-Dokumentation)
Betrieb - Betriebsumgebung	(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 M1, M2, M3 und M5 für die Sicherheitsfunktionen SF1.1, SF1.2, SF2, SF3, SF4.1 und SF4.2 sind kritische Mechanismen; sie sind bis auf M1 und M2 (kryptographische Mechanismen) vom Typ B.

  Für Mechanismen des Typs B ist gemäß ITSEC und ITSEM keine Mechanismenstärke anzugeben. Im Rahmen der Schwachstellenanalyse konnte jedoch festgestellt werden, daß selbst unter Zugrundelegung eines Aufwands gemäß der



Stufe “hoch ” bei den angenommenen Einsatzbedingungen (s. Kapitel 3, Sicherheitsvorgaben) keine ausnutzbare Schwachstelle erkennbar ist.

2.3 Hinweise

22 Die Prüfstelle hat keine Auflagen an den Hersteller auszusprechen.

23 Die Prüfstelle hat folgende Hinweise für den Anwender ausgesprochen:

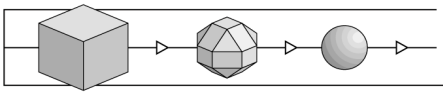
Hinweise zur sicheren Benutzung der Funktionalität „Datei signieren“:

- Der EVG verfügt über zwei Betriebsmodi. Die evaluierte Funktionalität ist nur im EVG Betriebsmodus vorhanden. Dieser ist an der Display-Anzeige des Sign@tor-Terminals mit „Betriebsbereit“ zu erkennen.
- Makros sollten vor Signierung entfernt werden.
- Dokumente, auf die mit Hyperlinks verwiesen wird, werden nicht signiert.
- Die angezeigten Hashwerte sind vom Benutzer zu vergleichen und nur bei Übereinstimmung ist der Signaturvorgang zu starten.
- Der auf dem Terminal angezeigte Dateiname, die Dateigrösse und das Erstellungsdatum sind nur zusätzliche Information (und nicht verlässlich).
- Die Beschreibung der Vorgehensweise, falls Hashwerte nicht identisch sind, ist zu befolgen (siehe Benutzerdokumentation – Sign@tor-Onlinehilfe).
- Es müssen alle vier Zeilen des Hashwertes auf dem Terminal durchgeblättert werden, bevor mit OK der Signiervorgang gestartet werden kann.
- Die Karten-PIN ist geheim zu halten.
- Nach dreimaliger Falscheingabe der PIN wird die Signatur-Karte gesperrt.
- Die PIN ist nur am Signator Terminal einzugeben.
- Der Signiervorgang kann mit der C-Taste am Terminal abgebrochen werden.
- Zur Sicherheit sollte die signierte Datei mittels „Signatur prüfen Offline“ überprüft werden.

Hinweise zur sicheren Benutzung der Funktionalität „Softwareupdate Sign@tor-PC und Terminal“:

- Die Original-CD muß sicher verwahrt werden.

- Das Software-Update soll nur mit Hilfe der Original-CD erfolgen.
- Die Hinweis auf mögliche Konsequenzen bei Update mit nicht zertifizierter Software sind zur Kenntnis zu nehmen.



(Diese Seite ist beabsichtigterweise leer.)

3 Sicherheitsvorgaben

24 Die der Evaluierung zugrunde liegenden Sicherheitsvorgaben, Version 1.7 vom 26.01.01, sind seitens des Auftraggebers in deutscher Sprache bereitgestellt worden.

3.1 Beschreibung des Evaluationsgegenstandes (EVG)

3.1.1 Definition und Art der Nutzung des EVG's

Der Evaluierungsgegenstand (EVG) ist das Produkt Sign@tor, Version 1.0. Er wird im folgenden kurz als Sign@tor bezeichnet.

Der Sign@tor dient zur Erzeugung von Signaturen des Benutzers sowie zum Prüfen anderer Signaturen.

Er besteht aus den folgenden 2 Komponenten:

1. dem Sign@tor PC und

2. dem Sign@tor Terminal.

Damit ergeben sich die folgenden komprimierten Angaben zum Produkt:

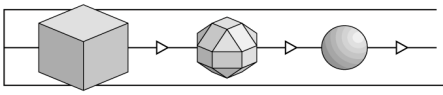
Art	Name	Versionsnummer	Lieferform
SW	SIGN@TOR PC (inkl. Installations- und Update-Programm)[2]	1.0	CD
HW und SW	SIGN@TOR Terminal	1.0	Gerät

Der Sign@tor vermittelt eine Benutzerschnittstelle zur Signaturkarte, die in das Terminal eingesteckt ist, aber nicht zum EVG, sondern seiner Einsatzumgebung gehört (s. Kapitel 2). Die Schnittstelle wird insbesondere benutzt, um Dateien, die zum Signieren bzw. zur Signaturprüfung verwendet werden sollen, auszuwählen. Der Sign@tor unterstützt die Auswahl und Anzeige der zu signierenden Datei sowie die Berechnung des HASH-Wertes, den er dann an die Signaturkarte schickt.

Die Signaturkarte gibt die in ihr erzeugte Signatur an den Sign@tor (genauer das Terminal) zurück. Der Sign@tor erstellt eine signierte Datei im Format PKCS#7, nachdem er die Signatur der Datei (die in der Signaturkarte gebildet wurde) und das Zertifikat der Signaturkarte übernommen hat.

---

2 Die CD enthält auch die Online Benutzerdokumentation; Anmerkung von debisZERT.



Im Rahmen dieser Nutzung dient das Terminal als Kartenleser für die Signaturkarte des Benutzers und als Eingabegerät für die PIN. Es stellt die Vertraulichkeit der PIN gegenüber dem (Sign@tor und restlichen) PC sicher. Weiterhin berechnet auch das Terminal den HASH-Wert und zeigt ihn an. Es ist für seine Sendung an die Karte zur Bildung der Signatur verantwortlich.

Der EVG gewährleistet sichere Software-Updates für den PC, indem er die Integrität der heruntergeladenen Software für ein Update auf dem Sign@tor PC anhand der Signatur überprüft.

Der EVG gewährleistet sichere Software-Updates für das Terminal, indem die Integrität der heruntergeladenen Software für ein Update auf dem Sign@tor Terminal anhand der Signatur überprüft wird.

Der Sign@tor unterstützt die Auswahl und Anzeige in einem Viewer von Dateien, deren Signatur zu prüfen ist.

Bei der Signaturprüfung wird überprüft, ob die Signatur mit einem Signaturschlüssel erzeugt wurde, der zum öffentlichen Schlüssel korrespondiert. Dieser öffentliche Schlüssel ist im Zertifikat der signierten Datei enthalten.

Die Signaturprüfung ist keine Sicherheitsfunktion und nicht Gegenstand der Evaluierung.

3.1.2 Aufgaben des EVG

Im folgenden werden die sicherheitsrelevanten Anteile der EVG-Funktionalität in Kurzfassung beschrieben.

Datei Signieren:

Das Sign@tor Terminal bildet gleichzeitig mit dem Sign@tor PC den HASH-Wert über die zu signierende Datei.

Das Sign@tor PC Programm zeigt den (von ihm berechneten) HASH-Wert der zu signierenden Datei an. Anschließend wird der (unabhängig gebildete) HASH-Wert auf dem Sign@tor-Terminal angezeigt.

Anmerkung: Der Benutzer muss beide HASH-Werte vergleichen und (bei Übereinstimmen) den Signierprozess (Senden des HASH-Wertes an die Signaturkarte) im Sign@tor Terminal starten.

In der Signaturkarte wird der HASH-Wert verschlüsselt und die Signatur wird gebildet.

Die zum Signieren ausgewählte Datei wird mit der digitalen Signatur versehen und in einem genormten Format (PKCS#7) abgespeichert.

Sicherung des Software Updates für PC:

Die Integrität der geladenen Software, die für ein Update auf dem Sign@tor-PC verwendet werden soll, wird geprüft.

Sicherung des Software Updates für Terminal:

Die Integrität der geladenen Software, die für ein Update auf dem Sign@tor-Terminal verwendet werden soll, wird geprüft.

PIN Eingabe:

Die Eingabe der PIN erfolgt am Sign@tor-Terminal. Die PIN wird anschließend ausschließlich an die Signaturkarte weitergegeben. Sie wird sofort nach der Übertragung an die Signaturkarte im Sign@tor-Terminal gelöscht und verlässt das Sign@tor-Terminal nicht in Richtung PC.

3.1.3 Angaben zum Produkt- bzw. Lieferumfang

In diesem Abschnitt werden insbesondere die Angaben zum Lieferumfang präzisiert. Dabei werden auch genauere Festlegungen getroffen, welche Produktteile der Evaluierung (ihrer Korrektheit und Wirksamkeit) unterliegen und damit Komponenten des EVG im eigentlichen Sinne sind.

Das Sign@tor Terminal (Hardware, vorinstallierte Software) wird als solches ausgeliefert und ist vollständig Teil des EVG. Die Software für das Sign@tor Terminal besteht aus den Komponenten:

- Signatur-API,
- Update Software Sign@tor Terminal

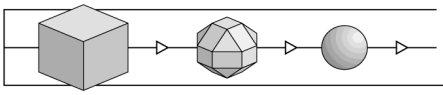
Die ausgelieferte CD (Produktteil) enthält im wesentlichen die

- Software für den Sign@tor PC
    - Signatur-API,
    - Benutzeroberfläche (High Level)
- und die Update Software Sign@tor PC.

Die (installierte) Software zur Benutzeroberfläche (High -Level) ist kein Teil des EVG.

Nach der Installation (der Software) des Sign@tor PC wird die folgende Funktionalität zur Verfügung gestellt, die zum EVG gehört (also nicht Bestandteil der technischen Einsatzumgebung ist; siehe Kapitel 2):

- Kommunikation mit dem Sign@tor Terminal über USB,
- Management der Masken,
- Abfrage der Buttons und Reaktion auf die Benutzereingaben,



- Aktivitäten im Zusammenhang mit dem Signiervorgang.

Die Software des Sign@tor Terminals gehört insgesamt zum EVG (und damit nicht zur technischen Einsatzumgebung; siehe Kapitel 2): sie stellt im wesentlichen die folgende Funktionalität zur Verfügung:

- Kommunikation mit dem Sign@tor PC über USB,
- Kommunikation mit der Chipkarte (T=1 Protokoll),
- Ansteuerung des Displays,
- Abfrage der Tastenfelder und Reaktion auf die Benutzereingaben,
- Aktivitäten im Zusammenhang mit dem Signiervorgang.

Genau genommen stellt die Terminal-Software zwei Betriebsmodi des Terminals her:

- den dargestellten “EVG-Modus”, der im Zusammenhang mit dem Signieren von Dateien relevant ist, und einen
- “Durchreichemodus”, bei dem Daten zwischen PC und Signaturkarte ohne Verarbeitung im Terminal nur ausgetauscht werden.

Ein Umschalten zwischen den beiden Modi setzt ein Reset des Terminals voraus. Der “Durchreichemodus” ist unter Sicherheitsgesichtspunkten ohne Bedeutung und wird im Weiteren nicht mehr behandelt.

3.2 Beschreibung der Einsatzumgebung

3.2.1 Technische Einsatzumgebung

Informationen zu den erforderlichen Eigenschaften in der technischen Einsatzumgebung lassen sich aus der folgenden Zusammenstellung entnehmen.

Die Software des Sign@tor PC benötigt die Unterstützung durch die Betriebssysteme

- Windows 98 SE,
- Windows ME,
- Windows 2000.

Anmerkung: der Sign@tor PC wird mit den aufgeführten drei Betriebssystemen Windows 98, ME und Windows 2000 getestet.

Die geforderte Hardware des PC umfasst folgende Bestandteile:

- CPU: ab Pentium I,

- USB-Schnittstelle,
- Internet Anschluss (optional),
- Festplatte: mindestens 10 MB,
- Hauptspeicher: 32 MB.

Weitere Anforderungen an die Hard- und Software des PC, auf dem der entsprechende EVG-Teil abläuft, bestehen nicht. An diesen PC wird das Sign@tor Terminal über ein USB-Kabel an den Sign@tor PC angeschlossen; aus diesem Grund werden nur PCs mit einer USB - Schnittstelle unterstützt.

Andere Interfaces zum PC sind nicht vorgesehen.

Das Sign@tor Terminal insgesamt ist kein Teil der technischen Einsatzumgebung (sondern des EVG). Trotzdem sind im folgenden die wichtigen technischen Merkmale seiner Hardware zusammengestellt.

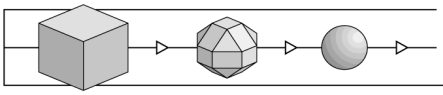
Die Hardware stellt folgende Komponenten, die nicht Bestandteil der technischen Einsatzumgebung sind, zur Verfügung:

- CPU: 8051-Familie,
- Programmspeicher: 64KB Flash-EPROM,
- Datenspeicher: mind. 1KByte statisches RAM,
- persistenter Datenspeicher: mind. 2KB EEPROM,
- Chipkarteninterface: ISO 7816 (T1- Protokoll),
- Tastatur: Matrix 3x4 ,
- Display: ohne Beleuchtung Größe: 16x1,
- USB: Übertragungsrate.

Bei einer Signierung wechselwirkt das Terminal mit einer (eingeschobenen) Signaturkarte, die Teil der technischen Einsatzumgebung ist. Sinnvoll möglich ist dies nur mit bestimmten Signaturkarten.

Eingesetzt werden können momentan die Smartcards

- der Firma „a-sign“
    - mit Prozessorchip Infineon
    - Chipkartenbetriebssystem: CardOS / M4.0 und
- der Firma „A-Trust“



- mit Prozessorchip Philipps

- Chipkartenbetriebssystem: Starcos SPK 2.2 + mod .

Anmerkung: Getestet wird mit den aufgeführten Signaturkarten der Firmen „a-sign (Datakom Austria)“ und „A-Trust“.

3.2.2 Annahmen zur administrativen Einsatzumgebung

Aus Sicherheitsgründen müssen die folgenden Annahmen beim EVG-Einsatz gültig sein. Diese setzen voraus, dass der Benutzer die entsprechenden (organisatorischen) Maßnahmen getroffen hat.

Annahmen allgemeiner Art:

Der Benutzer muss darauf achten, dass nur Dokumente ohne Makros signiert werden. Ggf. in Dokumenten enthaltene Makros, die sonst mitsigniert würden, müssen vor dem Signieren entfernt werden.

Der Benutzer muss seine PIN direkt am Sign@tor Terminal eingeben, bevor eine Signatur überhaupt gebildet werden kann.

Anmerkung: Mit der eingegebenen und an die Signaturkarte weitergeleiteten PIN identifiziert / authentisiert er sich gegenüber dieser. Die Sicherheitsmechanismen der Karte sorgen dabei für eine eindeutige Identifizierung. Der Benutzer muss die PIN vertraulich halten.

Annahmen im Zusammenhang mit der Hardware des Sign@tor Terminals:

Es wird durch geeignete materielle / physische Maßnahmen verhindert, dass unberechtigte Personen Manipulationen an der Hardware (EVG-Teil) vornehmen können.

Der Benutzer muss den Zustand des Sign@tor Terminals (anhand der Schweißpunkte) nach dem Kauf und vor der ersten Inbetriebnahme kontrollieren. Denn das Terminal muss verschweißt (geblieben) sein, um so eventuellen Angriffen auf das Sign@tor Terminal während der Lieferung zum Kunden vorzubeugen.

Annahmen im Zusammenhang mit der Software des Sign@tor Terminals:

Die Software des Sign@tor Terminals ist bei Erwerb des Gerätes bereits installiert.

Annahmen mit Bezug zur Software des Sign@tor PC:

Der Benutzer muss die Erstinstallation der Software mit der CD, die in der Verpackung des SIGN@TOR mitgeliefert wird, durchführen. Diese CD ist sicher aufzubewahren, da sie für ein Software-Update benötigt wird.

Anmerkung: Die Benutzerdokumentation wird als Online Dokumentation realisiert. Die Erstinstallation der Software wird mit einer CD und der Funktion Autorun (MS Windows) durchgeführt. Nach Installation der Software wird dem Benutzer eine umfangreiche

Hilfe angeboten. Die Benutzerdokumentation ist generell als Online-Dokumentation realisiert.

Der Benutzer muss bei einem Update der neuen Software für den Sign@tor PC die Signatur der neuen Software mit der Hilfe der Original-CD überprüfen.

Der Benutzer hat dafür zu sorgen, daß am Sign@tor PC mit der installierten Software immer ein aktueller Virenscanner installiert ist und dieser in regelmäßigen Abständen aktiviert wird.

Der Benutzer hat dafür zu sorgen, dass nur vertrauenswürdige Software eingesetzt wird.

Annahmen zur räumlichen Einsatzumgebung:

Das Sign@tor Terminal und der Sign@tor PC müssen sich aus den folgenden Gründen in einem Raum sowie bei der Nutzung direkt vor dem Benutzer befinden:

- die Validierung der Daten sowie des HASH-Wertes muss möglich sein,
- ein eventuelles Mithören oder Ändern des Dokumenteninhaltes während des Datentransfers zwischen dem Sign@tor –PC und dem Sign@tor-Terminal muss vermieden werden.

3.2.3 Definition der Objekte, Subjekte und Zugriffsarten

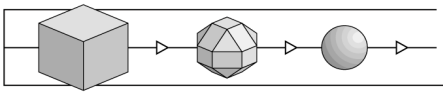
In diesem Kapitel werden alle zur Analyse der Sicherheitseigenschaften des EVG und in weiterer Folge zur Definition von Sicherheitszielen (Kapitel 3.3.1, Bedrohungen, Kapitel 3.3.2 und Sicherheitsfunktionen, Kapitel 3.4) notwendigen Subjekte, Objekte und Zugriffsarten definiert.

Subjekte

Subjekte sind Personen oder Prozesse, die Zugriffe auf Objekte, insbesondere Informationen ausüben können.

Subjekte sind im Zusammenhang mit dem Sign@tor:

- EVG-spezifische Prozesse, die auf dem PC und dem Terminal (speziell Signier-Prozeß) ablaufen.
- Prozesse bzw. Applikationen, die auf dem PC laufen und nicht Bestandteile des EVG sind.
- Prozesse, die in der Signaturkarte und damit in der EVG-Umgebung ablaufen.
- Personen, die Zugriff auf die Software des Sign@tor PC und/oder das Terminal haben (berechtigt oder unberechtigt).
- Dienstleistungsanbieter, der den Sign@tor (PC und Terminal), die dazugehörige Software sowie das Software Update zur Verfügung stellt.



Objekte

Mit Objekten sind in erster Linie passive, zu schützende Informationseinheiten gemeint.

Solche Objekte im Zusammenhang mit dem Sign@tor sind:

- zu signierende Dateien.
- die nicht ausgeführte (im internen Speicher liegende) Software des Sign@tor Terminals,
- die Software des Sign@tor PCs auf der CD oder der Festplatte des PC,
- die PIN des Benutzers.

Zugriffsarten

Datenobjekte können durch Subjekte (ggf. in bösartiger Absicht) gelesen, empfangen, geschrieben / geändert, gesendet und ausgeführt werden. Beim Sign@tor sind insbesondere manipulative (böswillig ändernde) oder ausspionierende (böswillig lesende) Zugriffe auf Daten vor, nach und während ihres Transfers von Bedeutung.

In der folgenden Auflistung sind die o.g. (klassischen) Zugriffsarten schon mit zusätzlichen Angaben (betreffende Objekte, Zeitpunkte) verknüpft:

- Laden einer falschen / manipulierten (Update-) Software in den Sign@tor PC bzw. das Sign@tor-Terminal,
- Manipulation der Daten (zu signierende Datei, Update-Software Terminal) während des Transfers vom Sign@tor PC zum Sign@tor Terminal,
- Ausspionieren der eingegebenen PIN (vor dem Transfer zur Signaturkarte)
- Änderung der Daten (Zertifikat der Signaturkarte, Signatur) während und nach dem Transfer vom Sign@tor Terminal zum Sign@tor PC,
- Änderung der Daten (fertig signierte Datei im PKCS#7-Format) vor, während und nach der Abspeicherung.

Anmerkung: Die beiden letzten Änderungen lassen sich durch den EVG selbst nicht verhindern. Sie sind jedoch bei einer Überprüfung der Datei-Signatur feststellbar. Konsequenterweise unterbleibt im folgenden Kapitel die entsprechende Bedrohungs- bzw. Sicherheitsziel-Definition.

3.3 Sicherheitsziele und die Bedrohungen

3.3.1 Sicherheitsziele

Das Ziel ist die Generierung der elektronischen Signatur mit größter möglicher Sicherheit für den Anwender. Im folgenden werden dazu die Teilziele definiert:

SZ1: Die Vertraulichkeit der PIN gegenüber den Prozessen auf dem PC soll gewährleistet werden.

SZ2: Die Integrität der vom Sign@tor PC an das Sign@tor Terminal gesendeten Datei soll vom Benutzer überprüfbar sein.

SZ3: Die Authentizität der Dateien, die für das Update des Sign@tor PCs bzw. des Sign@tor Terminals vorgesehen sind, soll überprüfbar sein.

3.3.2 Bedrohungen

Da der Sign@tor am freien Markt zu kaufen sein wird, hat ein potentieller Angreifer bei Erwerb die Möglichkeit, das komplette Terminal (Hardware, geladene Software) und die Inhalte der CD (des gekauften Produkts) zu manipulieren oder sich die Kenntnisse zu solcher Manipulation anzueignen. Die Hardware des Sign@tor Terminals besteht im übrigen selbst aus Standardbausteinen, die am Markt frei erhältlich sind.

In der vorgesehenen Einsatzumgebung werden für den EVG folgende Bedrohungen angenommen:

B1: Ausspionieren der PIN

Die für die Authentisierung des Benutzers mit der Signatur-Chipkarte vorgesehene PIN kann ausspioniert werden.

B2: Datei während Signatur fälschen

Die zu signierende Datei wird nach der Dateiauswahl auf dem Weg zwischen dem Sign@tor PC und dem Sign@tor Terminal verfälscht.

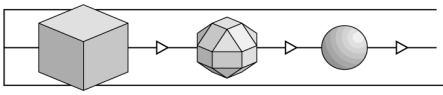
B3: Fälschen der SW bei Update

Die Software, die für das Update des EVG (PC- und Terminalteil) vorgesehen ist, wird auf dem Weg zwischen Hersteller und Benutzer unbemerkt verfälscht bzw. ausgetauscht.

Bemerkung: Die Bedrohung richtet sich gegen einen Bestandteil des EVG (Software zum Update). Dieser Bestandteil ist während der Übertragung über ein öffentliches Medium bedroht.

3.4 Sicherheitsfunktionen des EVG's

Die folgenden Sicherheitsfunktionen haben teilweise keine Bezüge zu den generischen Oberbegriffen der ITSEC. Ihre Definitionen sind ggf. um Anmerkungen zu den in ihrem Umfeld relevanten technisch-organisatorischen Maßnahmen ergänzt.



SF1 – Sichere PIN-Eingabe

SF1.1: Die Eingabe der PIN zur Benutzerauthentisierung mit der Signatur-Chipkarte erfolgt über die Tastatur des Sign@tor-Terminals. Das Sign@tor-Terminal gibt die eingegebene PIN ausschließlich an die Signatur-Chipkarte weiter.

SF1.2: Nachdem die PIN an die Signatur-Chipkarte gesendet wurde, wird sie gelöscht.

SF2 - Integerer Kanal zwischen dem Sign@tor PC und dem Sign@tor Terminal

Das Sign@tor Terminal und der Sign@tor PC zeigen beide einen selbstberechneten HASH-Wert der zu signierenden Datei an. Der Benutzer muss beide HASH-Werte vergleichen, bevor der eigentliche Signierprozess (Senden des HASH-Wertes an die Signatur-Chipkarte) gestartet werden kann.

SF3 - Vor- und Nachbereitung der digitalen Signatur

Das Sign@tor Terminal sendet den in SF2 beschriebenen HASH-Wert an die Signatur-Chipkarte und erhält von dieser die Signatur zurück.

Weitergehend kodiert der EVG das Ergebnis (Datei, Signatur und dazugehöriges Zertifikat) im PKCS#7-Format.

SF4 – Software Update

SF4.1: Die Integrität der für das Update des Sign@tor PCs bestimmten Software wird nach dem Herunterladen der Software vom Benutzer mit einem von der Original-CD zu startenden Programm überprüft (Bestandteil der CD ist der integere und authentische öffentliche Schlüssel zur Verifikation der Signatur). Die Software Komponenten für den Sign@tor PC, die für ein Update des Sign@tor PCs vorgesehen sind, wurden dazu von Siemens mit einer digitalen Signatur versehen.

SF4.2: Die für das Update des Sign@tor Terminals bestimmte Software wird vor der Installation im Sign@tor Terminal auf Integrität und Authentizität geprüft. Dazu verfügt die Update-Software über eine von Siemens geleistete digitale Signatur und das Sign@tor Terminal über einen korrespondierenden öffentlichen Schlüssel.

3.5 Zweckmäßigkeit der Sicherheitsfunktionen

Gegenüberstellung der Sicherheitsfunktionen mit: Art der Anwendung – Bedrohung – Sicherheitsziele.

1. Signaturkarte am Sign@tor Terminal / Ausspionieren der PIN.

   Die PIN könnte von einem Angreifer ausspioniert werden (B1). Um dem entgegen zu wirken, erfolgt die PIN-Eingabe am Terminal (SF1.1). Die PIN wird ausschließlich zur Karte weitergegeben und anschließend direkt gelöscht (SF1.2).

   Damit kann Bedrohung B1 abgewehrt werden.

2. Manipulation / Verfälschung der zur Signierung ausgewählten Datei

   Manipulationen können vom Benutzer erkannt werden, da sowohl der Sign@tor PC als auch das Sign@tor Terminal einen HASH-Wert der Datei errechnen und dem Benutzer anzeigen. Unterscheiden sich diese beiden Werte, hat eine Manipulation stattgefunden.

   Anschließend wird dann der Signaturprozess eingeleitet und das Ergebnis durch den EVG PKCS#7-kodiert gespeichert.

   Damit kann die Bedrohung B2 abgewehrt werden.

3. Verfälschen der Software für das Update (Sign@tor PC und Terminal) auf dem Weg zwischen Hersteller und Benutzer

   Die Update Software für den EVG wird mit einer digitalen Signatur versehen.

   Die digitale Signatur auf der PC-Software wird mit einer authentischen und integeren Software auf der Original-CD geprüft.

   Die digitale Signatur auf der Terminal Software wird im Sign@tor Terminal geprüft.

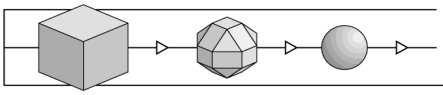
3.6 Evaluationsstufe und die Mindeststärke der Mechanismen

Die angestrebte Evaluationsstufe für den EVG ist E2, die angestrebte Mechanismenstärke ist hoch.

3.7 Begriffe

Die grundsätzlichen Verfahren und Begriffe der Bildung von elektronischen Unterschriften werden als bekannt vorausgesetzt. Ergänzend dazu werden folgende Begriffe hiermit definiert und in der Folge verwendet:

Applikation	Eigenständiger Programmteil, der in den Speicher des PC´s (mit dem Sign@tor-PC) oder des Terminals geladen werden kann, bestimmte, eigenständige Aufgaben durchführen kann und dabei auf Funktionen des Betriebssystems zugreift. Anmerkung: In dieser Allgemeinheit der Definition sind Sign@tor PC und Sign@tor Terminal selbst Applikationen. Speziell wird der Begriff im Zusammenhang mit externen Applikationen auf den PC, auf dem Sign@tor PC abläuft, verwendet.
Benutzer	Benutzer
Datei Information	Datei Information besteht aus: Dateiname, Dateilänge und Erstellungsdatum der Datei.
Dokument	Ein in Dateiform vorliegendes Dokument.

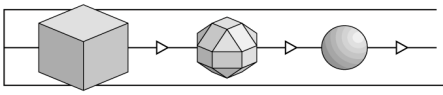


HASH-Wert	Über ein Dokument gerechnete Prüfsumme. Charakteristisch für ein Dokument, aber nicht unbedingt eindeutig.
PKCS#7	Generelle Syntax für die Verschlüsselung und Entschlüsselung der Daten
Private Key	Geheimer Teil eines RSA Schlüsselpärchens
Public Key	Öffentlicher Teil eines RSA Schlüsselpärchens
Signatur	Datei mit folgendem Inhalt: Daten zum Benutzer, HASH-Wert über das Dokument, Elektronische Unterschrift (aus dem HASH-Wert gebildet).
Signaturkarte	Chipkarte, auf der die erforderlichen Schlüssel gespeichert sind. Die Berechnung der Unterschrift aus dem HASH-Wert erfolgt ebenfalls auf der Signaturkarte.
Unterschrift	Signatur
Zertifikat	Vom Trustcenter übermittelte Datei. Diese enthält Daten über einen Benutzer, sowie dessen Public-Key. Ein Zertifikat ist vom Trustcenter mit dessen Private-Key unterschrieben. Ist in diesem Dokument von einem Zertifikat die Rede, so ist, falls nicht anders angegeben, das Zertifikat eines Senders gemeint.

3.8 Abkürzungen

Bx	Bedrohung, x= Laufende Nummer
CPU	Prozessor
EVG	Evaluierungsgegenstand
HW	Hardware
ISO	International Standardization Organization
OS	Betriebssystem
PC	Personal Computer
PIN	Persönliche Identifikationsnummer
RSA	Rivest Shamir Adleman
SFx	Sicherheitsfunktion, x= Laufende Nummer
SW	Software

SZx	Sicherheitsziele, x= Laufende Nummer
USB	Universal Serial Bus

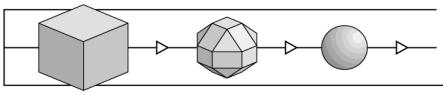


(Diese Seite ist beabsichtigterweise leer.)

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.

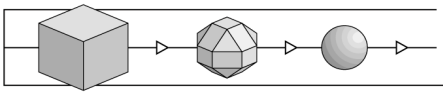
33 Es stellen sich dabei zwei Grundfragen:

- 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 unan-



gemessen 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 an 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

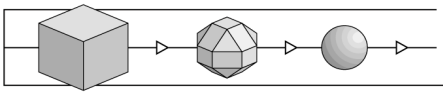
40 Typische Beispiele für Sicherheitsfunktionen sind die *Identifikation und Authentisierung* (von Subjekten), die *Zugriffskontrolle*, die *Beweissicherung* (Protokollierung), die *Protokollauswertung*, die *Übertragungssicherung*. Ein Produkt oder System kann solche Sicherheitsfunktionen beinhalten.

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 Widerstandskraft 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?

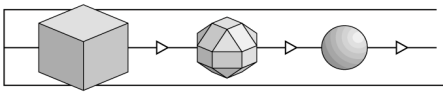
"Alle kritischen Sicherheitsmechanismen (d.h. diejenigen, deren Versagen eine Sicherheitslücke hervorrufen würde), werden hinsichtlich ihrer Fähigkeit bewer-

tet, 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."



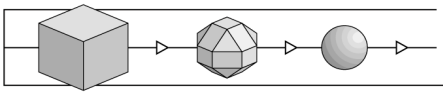
(Diese Seite ist beabsichtigterweise leer.)

6 Anhang

6.1 Glossar

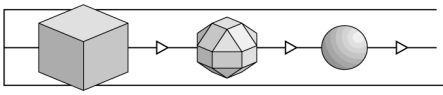
Das Glossar erläutert die in dieser Broschüre verwendeten Begriffe, erhebt allerdings keinerlei Anspruch auf Vollständigkeit oder Allgemeingültigkeit. Der Begriff *Sicherheit* meint hier stets Sicherheit im Kontext der Informationstechnik.

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).
Assoziiertes Labor	Ein per Vertrag mit debisZERT kooperierendes Entwicklungslabor, das optimierte Verfahren zur Vorbereitung von Evaluierungen einsetzt.
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.
Bestätigungsstelle	Stelle, die im Einklang mit SigG und SigV Sicherheitsbestätigungen für technische Komponenten und für die Umsetzung von Sicherheitskonzepten bei Trust Centern (Zertifizierungsstellen nach SigG) herausgibt.
Bestätigungsverfahren	Verfahren mit dem Ziel einer Sicherheitsbestätigung
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.
DebisZERT	Name des Zertifizierungsschemas von debis IT Security Services.
Dienstleistung	Hier: Eine durch ein Unternehmen angebotene, durch (Unternehmens-)Prozesse erbrachte und durch Nutzer in Anspruch nehmbare Leistung.
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	Sicherheitskriterien: funktional 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-) Sicherheits-management	Ein Unternehmensprozeß, dessen Ziel die Einrichtung und Aufrechterhaltung der (IT-)Sicherheit in einem Unternehmen ist.
IT-System	Eine in sich funktionsfähige Kombination von IT-Produkten. (ITSEC:) Eine reale Installation von IT-Produkten mit einer bekannten Einsatzumgebung.

Komponente nach SigG	Eine logische Funktionseinheit in IT-Systemen, die in SigG / SigV definierte Aufgaben erfüllt (Anzeigekomponente, Komponente zur Schlüsselerzeugung, etc.)
Lizenz (persönliche)	Bestätigung einer persönlichen Qualifikation (hier im Kontext von debisZERT, s. zertifizierter Ingenieur)
Lizenzierter Ingenieur	Eine Person, die im Zusammenhang mit Evaluierungen Qualifizierungsverfahren bei debisZERT durchlaufen hat (s. Lizenz).
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.
Produkt-Zertifizierung	Zertifizierung eines IT-Produktes.
Prozeß (Unternehmens~)	Abfolge vernetzter Tätigkeiten (Prozeßelemente) in einer gegebenen Prozeßumgebung – mit dem Gesamtziel, eine bestimmte Dienstleistung zu erbringen.
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.

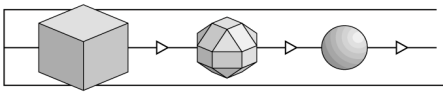


Sicherheitsfunktion	Funktionen eines IT-Produktes oder IT-Systems zur Abwehr bestimmter Bedrohungen.
Sicherheitskriterien	Dokument, das technische Anforderungen an Produkte, Systeme und / oder Dienstleistungen enthalten kann, zumindest aber die Evaluierung solcher Anforderungen beschreibt.
Sicherheitsnorm	Anforderungen an Produkte, Systeme oder Dienstleistungen die Sicherheit betreffend.
Sicherheitsstandard	Zusammenfassender Begriff für Sicherheitskriterien und Sicherheitsnormen.
Sicherheitsstufen	In Sicherheitskriterien 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).
System-Zertifizierung	Zertifizierung eines IT-Systems (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.
Unternehmensprozeß	s. Prozeß
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 1.6, 31.03.2000, http: / / www.debiszert.de /
/ ALG /	Geeignete Kryptoalgorithmen gemäß § 17 (2) SigV, veröffentlicht im Bundesanzeiger Nr. 230 – Seite 22.946 v. 07. Dezember 2000
/ 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, Version 2.1, Part 1 (Introduction and general model), Part 2 (Security functional requirements), Part 2 : Annexes, Part 3 (Security assurance requirements) , August 1999
/ CEM /	Common Methodology for Information Technology Security Evaluation, Part 1 (Introduction and general model), Version 0.6, January 1997, Part 2 (Evaluation Methodology), Version 1.0, August 1999
/ 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 2.0, Nov. 1998

/Mkat12/ Maßnahmenkatalog nach §12 Abs. 2, RegTP, www.RegTp.de

/Mkat16/ Maßnahmenkatalog nach §16 Abs. 6, RegTP, www.RegTp.de

/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 von debisZERT, Version 1.5, 30.06.1999, http://www.debiszert.de/

/V02/ Sicherheitsbestätigungen für Komponenten gemäß dem Signaturgesetz, Dienstleistungsbereich 2 von debisZERT, Version 1.5, 30.06.1999, http://www.debiszert.de/

/V03/ Sicherheitsbestätigungen für Zertifizierungsstellen gemäß dem Signaturgesetz, Dienstleistungsbereich 3 von debisZERT, Version 1.0, 29.10.1999, http://www.debiszert.de/

/V04/ Zertifikate mit Anerkennung durch das BSI, Dienstleistungsbereich 4 von debisZERT, Version 1.5, 30.06.1999, http://www.debiszert.de/

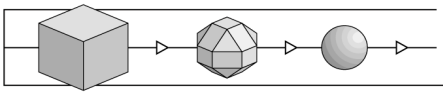
/Z01/ Zertifizierungsschema, debisZERT, Version 1.5, 30.06.1999, http://www.debiszert.de/

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
CEM	Common Methodology for Information Technology Security Evaluation
CTCPEC	Canadian Trusted Computer Products Evaluation Criteria
DAR	Deutscher Akkreditierungsrat
DBAG	Deutsche Bahn AG
debisZERT	Zertifizierungsschema der debis IT Security Services
DATech	Deutsche Akkreditierungsstelle Technik e.V.
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
RegTP	Regulierungsbehörde für Telekommunikation und Post
SigG	Signaturgesetz
SigV	Signaturverordnung
TKG	Telekommunikationsgesetz
ZKA	Zentraler Kreditausschuß



(Diese Seite ist beabsichtigterweise leer.)

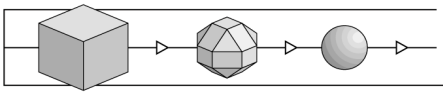
7 Re-Zertifizierungen

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 unter www.debiszert.de angekündigt.

50 Die nachfolgenden Anhänge sind fortlaufend numeriert.



Ende der Erstausgabe des Zertifizierungsreports.