T · · Systems · · ·

Zertifizierungsreport

T-Systems-DSZ-ITSEC-04080-2002

Sign@tor Version 2.0

Siemens AG Österreich

T-Systems ISS GmbH

Vorwort

Das Produkt „Sign@tor Version 2.0“ (EVG) der Siemens AG Österreich wurde gegen die ITSEC evaluiert. Die Evaluierung wurde im Rahmen des Zertifizierungsschemas der T-Systems ISS GmbH durchgeführt. Die Zertifizierung erfolgte gemäß Verfahrenstyp 04: Deutsches IT-Sicherheitszertifikat.

Das Ergebnis lautet:

Sicherheitsfunktionen:	Sichere PIN-Eingabe, integerer Kanal zwischen dem Sign@tor PC und dem Sign@tor Terminal, Vor- und Nachbereitung der digitalen Signatur, sicheres Software Update
Vertrauenswürdigkeitsstufe:	**E2**
Mindeststärke der Sicherheitsmechanismen:	**hoch**

Hiermit wird bestätigt, daß die Evaluierung entsprechend dem Zertifizierungsschema der T-Systems ISS GmbH durchgeführt wurde.

Bonn, den 30.04.2002

Klaus-Werner Schröder

(Zertifizierer)

Dr. Heinrich Kersten

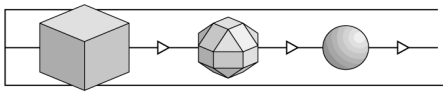
(Leiter der Zertifizierungsstelle)

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

✉ T-Systems ISS, - Zertifizierungsstelle -, Rabinstr.8, 53111 Bonn

☎ 0228/9841-0, Fax: 0228/9841-60

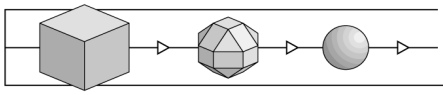
💻 www.t-systems-zert.com



Revisionsliste

Revision	Datum	Vorgang
1.0	30.04.2002	Erstellt nach Abschluß der Evaluierung; Musterreport: Version 3.2

Inhalt



(Diese Seite ist beabsichtigterweise leer.)

1 Zertifizierung

1.1 Allgemeines

1 Die Zertifizierung von Sign@tor Version 2.0 (EVG) wurde durch die Siemens AG Österreich bei der Zertifizierungsstelle der T-Systems ISS GmbH beauftragt.

2 Die Zertifizierungsstelle arbeitet im Einklang mit der DIN EN 45011 und ist im Hinblick auf diese Norm bei der DATech e.V. für Prüfungen nach den ITSEC und den Common Criteria akkreditiert (DAR-Registriernummer DIT-ZE-005/98).

3 Das Zertifizierungsschema ist auf den entsprechenden Web-Seiten der Zertifizierungsstelle veröffentlicht (www.t-systems-zert.com).

1.2 Zertifikat und Zertifizierungsreport

4 Eine Kurzfassung der Evaluierungsergebnisse zum EVG enthält das Sicherheitszertifikat T-Systems-DSZ-ITSEC-04080-2002 vom 30.04.2002.

Das Zertifikat trägt das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) genehmigte Logo [Deutsches IT-Sicherheitszertifikat] und wird vom BSI als gleichwertig zu seinen eigenen Zertifikaten anerkannt.

5 Das Zertifikat ist auf den Web-Seiten (www.t-systems-zert.com) der Zertifizierungsstelle veröffentlicht und wird in der Broschüre BSI 7148 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) referenziert.

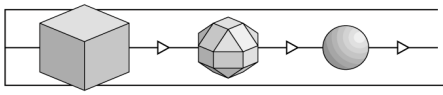
6 Der Zertifizierungsreport dient

- dem Auftraggeber als Nachweis der durchgeführten Evaluierung und
- dem Nutzer als Grundlage für den sicherheitsgerechten Einsatz des EVG.

7 Der Zertifizierungsreport enthält die Seiten 1 bis 42. Kopien des Zertifizierungsreports können beim Auftraggeber oder bei der Zertifizierungsstelle angefordert werden.

8 Die numerierten Paragraphen in diesem Zertifizierungsreport sind formelle Aussagen der Zertifizierungsstelle. Nicht numerierte Paragraphen enthalten Aussagen des Auftraggebers (Kapitel 3) oder informelles Material.

9 Der Zertifizierungsreport adressiert im Kapitel 3 die der Evaluierung zugrunde liegenden Sicherheitsvorgaben (Security Target), Version 2.2 vom 22.03.2002.



10 Die Sicherheitsvorgaben sind seitens des Auftraggebers in deutscher Sprache bereitgestellt worden.

11 Der Zertifizierungsreport gilt nur für die angegebene Fassung (Versionsnummer, Ausgabedatum, etc.) des EVG. Er kann jedoch auf neue bzw. andere Fassungen des EVG ausgedehnt werden, sobald eine erfolgreiche Re-Zertifizierung (s. Abschnitt 1.6) stattgefunden hat.

1.3 Anwendung der Ergebnisse

12 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.

13 Das Ergebnis der Evaluierung gilt nur unter der Voraussetzung, daß alle Angaben im Zertifizierungsreport beachtet werden. Hierzu zählen

- die genaue Produkt- und Versionsbezeichung (Abschnitt 1.1),
- die Sicherheitsvorgaben zum EVG - hier insbesondere die Informationen zur Art der Nutzung des zertifizierten Objektes, zu den Sicherheitszielen und den betrachteten Bedrohungen, zur Einsatzumgebung und zu den geprüften Konfigurationen (Kapitel 3),
- die Angaben zum Auslieferungsverfahren des EVG (Abschnitt 1.4),
- die Auflagen der Zertifizierungsstelle an den Auftraggeber (Abschnitt 1.5),
- die Hinweise und Auflagen der Zertifizierungsstelle an den Anwender (Abschnitt 1.5),
- die evaluierte Konfiguration (Abschnitt 2.2),
- die Auflagen der Prüfstelle an den Auftraggeber (Abschnitt 2.4),
- die Hinweise und Auflagen der Prüfstelle an den Anwender (Abschnitt 2.4),
- ggf. vorhandene technische Anhänge und Re-Zertifizierungen (s. Erläuterungen in Abschnitt 1.6).

14 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.

1.4 Auslieferungsverfahren

15 Die Auslieferung des EVG erfolgt nach folgendem Verfahren:

- Lieferung je nach Auftragsvolumina per Botendienst (kleinere Auftragsvolumina) oder über eine Siemens-eigene Logistikzentrale (größere Auftragsvolumina).
  Anmerkung: Der Anwender (Signaturschlüsselinhaber) erwirbt das Produkt vom Zertifizierungsdiensteanbieter oder im Handel in einer versiegelten Verpackung. Das Sign@tor Terminal ist zusätzlich durch inspizierbare Schweißpunkte gegen unbefugtes Öffnen gesichert.

1.5 Auflagen und Hinweise

16 Bei der Zertifizierung haben sich keine Auflagen und Hinweise an den Auftraggeber ergeben.

17 Bei der Zertifizierung haben sich folgende Auflagen und Hinweise für den sicherheitsgerechten Einsatz des EVG ergeben.

- Vor Installation und Inbetriebnahme soll der Anwender die versiegelte Verpackung des EVG und die Schweißpunkte des Sign@tor Terminals auf Unversehrtheit prüfen.

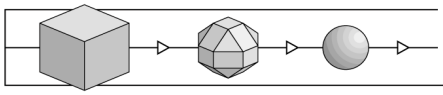
- Die Benutzung der Sicherheitsfunktion „sicheres Software Update“ gewährleistet, daß das heruntergeladene Update aus authentischer Quelle (hier: Siemens AG, Österreich) stammt. Sie impliziert jedoch keine Aussage über den Sicherheitswert des heruntergeladenen Updates. Der Anwender soll sich daher vor dem Herunterladen über die Sicherheitseigenschaften und eine etwa erfolgte Zertifizierung eines Updates auf den Webseiten des Herstellers oder der Zertifizierungsstelle informieren.

1.6 Technische Anhänge und Re-Zertifizierungen

18 Bei Änderungen an dem zertifizierten Objekt, seiner Einsatzumgebung oder seines Auslieferungsverfahrens muß nach Maßgabe der Verfahrensregeln der Zertifizierungsstelle eine Re-Zertifizierung erfolgen. Die Ergebnisse solcher Re-Zertifizierungen werden in entsprechenden technischen Anhängen zu diesem Zertifizierungsreport dokumentiert (Art der Änderungen, neue Produktversion).

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

20 Auf den Web-Seiten (www.t-systems-zert.com) der Zertifizierungsstelle werden Re-Zertifizierungen und technische Anhänge bekannt gegeben. Die Anhänge sind fortlaufend numeriert (DSZ-ITSEC-04080-2002***/1***, ...***/2***,...).



(Diese Seite ist beabsichtigterweise leer.)

2 Evaluierung

2.1 Allgemeines

21 Die Evaluierung von Sign@tor Version 2.0 (EVG) wurde durch Siemens AG Österreich bei der Prüfstelle für IT-Sicherheit der T-Systems ISS GmbH beauftragt.

22 Die Prüfstelle ist nach DIN EN 45001 bzw. ISO 17025 akkreditiert und besitzt eine gültige Lizenz der Zertifizierungsstelle für das hier vorliegende Prüfgebiet.

2.2 Evaluierung und Prüfbericht

23 Die Evaluierung wurde gegen die ITSEC /ITSEC/ unter Anwendung der Evaluationsmethodologie ITSEM /ITSEM/, der Joint Interpretation Library /JIL/ und der zum Zeitpunkt der Evaluierung gültigen nationalen Interpretationen (AIS) durchgeführt.

24 Die Evaluierung erfolgte auf der Basis der Sicherheitsvorgaben, Version 2.2 vom 22.03.2002, (vgl. Kapitel 3).

25 Die Evaluierung wurde unter der Prüfbegleitung durch die Zertifizierungsstelle durchgeführt.

26 Das Ergebnis der Evaluierung ist im Evaluation Technical Report (ETR) der Prüfstelle dargestellt. Der ETR trägt die Versionsnummer 1.01 und das Datum 23.04.2002.

27 Die Evaluierung wurde am 24.04.2002 beendet.

28 Die evaluierte Konfiguration wird wie folgt beschrieben:

- Evaluiert wurde der EVG Sign@tor Version 2.0 mit den Bestandteilen Sign@tor PC und Sign@tor Terminal entsprechend dem Lieferumfang, wie er in den Sicherheitsvorgaben beschrieben ist (siehe Kapitel 3, Abschnitt 1.3). Die Tests wurden durchgeführt auf PCs (Industrie-Standard) mit den Betriebssystemen Windows® 2000, Windows® 98 SE und Windows® ME.

2.3 Ergebnis der Evaluierung

29 Die Prüfstelle kommt zu folgendem Ergebnis:

- Der EVG genügt den Anforderungen der Evaluationsstufe E2 der ITSEC, d.h. alle Anforderungen an die Korrektheit und Wirksamkeit in 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 des EVG für die Sicherheitsfunktion(en) sichere PIN-Eingabe, integerer Kanal zwischen dem Sign@tor PC und dem Sign@tor Terminal und sicheres Software Update sind kritische Mechanismen; sie sind von folgendem Typ: M1, M2 und M5: Typ A; M3: Typ B.

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

Für Mechanismen des Typs B ist gemäß ITSEC und ITSEM keine Mechanismenstärke anzugeben. Im Rahmen der Schwachstellenanalyse konnte jedoch festgestellt werden, daß selbst unter Zugrundelegung eines Aufwands gemäß der Stufe hoch bei den angenommenen Einsatzbedingungen (s. Kapitel 3) keine ausnutzbare Schwachstelle erkennbar ist.

2.4 Auflagen und Hinweise

30 Die Prüfstelle hat folgende Auflagen an den Auftraggeber ausgesprochen.

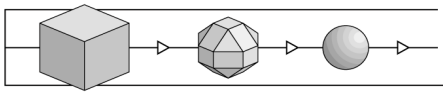
- Die Evaluierungsergebnisse gelten dann und nur dann, wenn die Veröffentlichung der Sourcen eines Musterprojektes TestApp.dsw im Internet spätestens am Tag der Erteilung des Zertifikates erfolgt.[1]

[1] Die Zertifizierungsstelle hat den Sachverhalt geprüft; die Auflage ist erfüllt.

31 Die Prüfstelle hat folgende Hinweise für den sicherheitsgerechten Einsatz des EVG 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, die durch Links eingezogen werden, werden nicht signiert.
  - Das Sign@tor-Terminal und der Sign@tor-PC bilden eine Einheit und müssen direkt vor dem Benutzer stehen, um mögliche Manipulationen zu verhindern.
  - Die Karten-PIN ist geheim zu halten.
  - Nach dreimaliger Falscheingabe der PIN wird die Signatur-Karte gesperrt.[2]
  - Die PIN ist nur am Sign@tor Terminal einzugeben.
  - Bei der Verwendung der Option 4.2 der offenen Schnittstellen, dürfen nur zugelassene Hash-Algorithmen (SHA-1 und RIPEMD-160) für die Erzeugung von SigG-konformen Signaturen benutzt werden.
  - Das Verhalten des EVG hängt von der Optionen der offenen Schnitt-stellen ab.
- Hinweise zur sicheren Benutzung der Funktionalität „Softwareupdate Signator-PC und Terminal“:
  - Die Original-CD muss sicher verwahrt werden.
  - Das Software-Update soll nur mit Hilfe der Original-CD erfolgen.
  - Die Hinweise auf mögliche Konsequenzen bei Update mit nicht zertifizierter Software sind zur Kenntnis zu nehmen.
  - Den Hinweisen zum Verhalten bei fehlerhafter Installation/Update ist Folge zu leisten (siehe Benutzerdokumentation – Sign@tor-Onlinehilfe).

[2] Anmerkung der Zertifizierungsstelle: Die Sperrung wird von der Signaturkarte selbst vorgenommen. Die Anzahl der Fehlversuche ist eine Eigenschaft der Signaturkarte, wobei drei ein gebräuchlicher Wert ist.



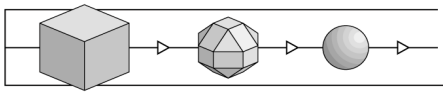
- Allgemeine Hinweise zur sicheren Benutzung:
  - Die Schweißnaht am Sign@tor Terminal ist auf Unversehrtheit zu prüfen.
  - Es ist stets ein aktueller Virenscanner zu benutzen.[3]
  - Es ist nur vertrauenswürdige Software einzusetzen.
  - Das Sign@tor Terminal und der Sign@tor PC müssen sich bei Benutzung in einem Raum befinden.

[3] Anmerkung der Zertifizierungsstelle: Die vom Anwender durchgeführte Prüfung sollte sich nicht nur auf Computerviren, sondern auch auf alle anderen Arten maliziöser Software erstrecken.

3 Sicherheitsvorgaben

32 Die Sicherheitsvorgaben, Version 2.2 vom 22.03.2002, zu „Sign@tor Version 2.0“ (EVG) werden im Folgenden vollständig wiedergegeben. Der Abdruck erfolgt mit freundlicher Genehmigung der Siemens AG Österreich.

33 Die Sicherheitsvorgaben haben ein separates Inhaltsverzeichnis und eigene Seitennummern, die in der Mitte der Fußzeile wiedergegeben sind.



(Diese Seite ist beabsichtigterweise leer.)

SIEMENS

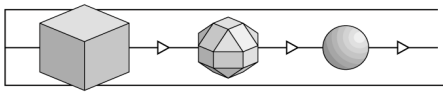
Sicherheitsvorgaben
Version 2.2
Sign@tor

Verteiler:

Name (alphab.)	Abteilung	Ort
Dr. Mahdjoobian	PSE PRO	MOOS
Fr. Oeckl	PSE PRO	MOOS
Hr. Sladek	PSE PRO	MOOS
Hr. Veit	EWW	SIE
Hr. Vucic	EWW	SIE

Ersteller:			**Prüfer:**	
Abt.:	PSE PRO SCS	Unterschrift:	Abt.: EWW TTI	Unterschrift:
Name:	Dr. Mahdjoobian		Name: Vucic	
Tel.:	+4351707/42977		Tel.:+4351707	

File:	Sicherheitsvorgaben Version V22.doc	Status:	Freigegeben
Datum:	22.03.2002		



Dokumentenverwaltung

Dokument-Historie

Version	Status	Datum	Verantwortlicher	Änderungsgrund
1.0	Entwurf	23.08.2000	Fr. Oeckl	Ersterstellung
1.1	Freigegeben	13.09.2000	Fr. Oeckl	Freigegeben
1.2	Entwurf	21.09.2000	Fr. Oeckl	Änderung nach Review
1.3	Freigegeben	19.10.2000	Fr. Oeckl	Änderung nach WS mit debis
1.4	Freigegeben	23.10.2000	Fr. Oeckl	Änderung nach Korrektur von debis
1.5	Freigegeben	28.11.2000	Fr. Oeckl	Änderung nach Korrektur von Versionsnummer und Dokumente
1.6	Freigegeben	20.12.00	Hr.Mahdjoobian	Einbringung A-Trust Karte Auswahl alle Dateien beim Signieren Erweiterung der administrativen Einsatzumgebung Plattform Windows ME
1.7	Freigegeben	24.01.2001	Hr.Mahdjoobian	Überarbeitung zur Behebung von Inkonsistenzen mit Architektur- und Feinentwurf und zur Erzielung eines veröffentlichungsreifen Textes
2	Freigegeben	20.12.2001	Hr.Mahdjoobian	Erweiterung der EVG (neue Signaturkarten und Verbesserungen)
2.1	Freigegeben	28.02.2002	Hr.Mahdjoobian	Änderung nach Review der Fa. Debis
2.2	Freigegeben	22.03.2002	Hr.Mahdioobian	Redaktionelle Überarbeitung

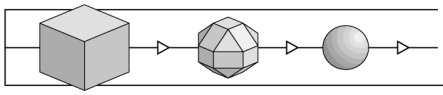
Änderungsberechtigte

Fr. Oeckl Silvia	PSE PRO SCS	MOOS
Hr. Dr. Mahdjoobian Kaveh	PSE PRO SCS	MOOS
Hr. Vucic Ivan	EWW TTI	SIE

Dokument wurde mit folgenden Tools erstellt:

MS Word 2000

Inhaltsverzeichnis



1 Beschreibung des Evaluationsgegenstandes (EVG)

1.1 Definition und Art der Nutzung des EVG‘s

Der Evaluierungsgegenstand (EVG) ist das Produkt Sign@tor, Version 2.0. Er wird im folgenden kurz als Sign@tor bezeichnet.

Der Sign@tor dient zur Erzeugung von Signaturen des Benutzers sowie zum Prüfen (Verifizierung) 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 Dokumentation	SIGN@TOR PC (inkl. Installations- und Update-Programm) sowie online Dokumentation für die Administration und Benutzerhandbuch	2.0	CD[4]
HW und SW	SIGN@TOR Terminal	2.0	Gerät

Der Sign@tor vermittelt eine Schnittstelle zur Signaturkarte, die in das Terminal eingesteckt ist, aber nicht zum EVG gehört, sondern zu seiner Einsatzumgebung (s. Kapitel 2).

Funktionen der Applikation des Sign@tor PCs:

Offene Schnittstelle für externe Applikationen:

Der Sign@tor vermittelt eine Applikationsschnittstelle zur Signaturkarte, die in das
Terminal eingesteckt ist (siehe oben). Die Schnittstelle wird insbesondere benutzt, um Daten, die signiert werden sollen, zu übergeben und die von der Signaturkarte erzeugte elektronische Signatur zu übernehmen.

Beschreibung der Schnittstelle:

Input: Daten zur Signierung (als Datei oder String) + Optionskennungen
Output: Datei (Format abhängig von den Optionskennungen) + Signatur + Zertifikat

Genauere Beschreibung der Schnittstelle siehe Kap. 1.2.

[4] Die CD kann optional eine Secure Viewer-Software eines Drittunternehmens enthalten, die jedoch nicht Bestandteil des EVGs ist.

Benutzerschnittstelle:

Der Sign@tor vermittelt auch eine Benutzerschnittstelle zur Signaturkarte. Die Schnittstelle wird insbesondere benutzt, um Dateien, die zum Signieren bzw. zur Signaturprüfung verwendet werden sollen, auszuwählen. Die Benutzerschnittstelle ruft die offene Schnittstelle (für Signieren) auf.

Der Sign@tor unterstützt zusätzlich 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 (Terminal) zurück. Der Sign@tor erstellt eine signierte Datei im Format PKCS#7 (optional), nachdem er die Signatur der Datei (die in der Signaturkarte gebildet wurde) und das Zertifikat der Signaturkarte übernommen hat.

Im Rahmen dieser Nutzung dient das Sign@tor -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.

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 Sign@tor 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.

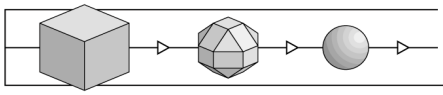
Die Signaturprüfung durch die Benutzeroberfläche (High-Level Komponente) ist keine Sicherheitsfunktion und nicht Gegenstand der Evaluierung.

1.2 Aufgaben des EVG

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

Daten Signieren:
Die offene Schnittstelle des Sign@tors bietet folgende Optionen:

Input:	Zu signierende Daten (File, String oder Hash-Wert), Option1, Option 2, Option 3, Option 4, Option 5
Output:	Datei PKCS # 7, Zertifikat, Signatur



Option 1

Option1.1

Das Sign@tor Terminal bildet gleichzeitig mit dem Sign@tor PC den Hash-Wert über die zu signierende Datei (Daten).

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 Übereinstimmung 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.

Option1.2

Wie Option 1.1, jedoch **kann** der Benutzer beide Hash-Werte vergleichen, bevor den Signierprozess (Senden des Hash-Wertes an die Signaturkarte) im Sign@tor Terminal gestartet wird.

Option1.3

wie Option 1.1, jedoch werden keine Hash-Werte (auf dem Sign@tor PC und dem Sign@tor Terminal) angezeigt. Der Benutzer gibt sofort seine PIN am Sign@tor Terminal ein.

Option1.4

Der Hash-Wert wird vom Sign@tor PC gebildet und an das Sign@tor Terminal übertragen. Das Sign@tor Terminal bildet keinen Hash-Wert. Der Hash-Wert des Sign@tor PCs wird an die Chipkarte gesendet. (Kein Hash-Wert angezeigt)

Option 2

Option2.1

Nur der Hash-Wert wird signiert.

Option2.2

Die SHA-ID-Kennung wird dem gebildeten Hash-Wert angehängt und dann durch die Karte signiert.

Option 3

Option3.1

Die zum Signieren ausgewählten Daten werden mit der digitalen Signatur versehen und in einem genormten Format (PKCS # 7) abgespeichert. Zusätzlich werden die Signatur und das Zertifikat an die aufrufende Applikation weitergereicht.

Option3.2

Es wird keine PKCS # 7 Datei gebildet.

Option 4

Option4.1

Der Hash-Wert wird von einer externen Applikation gebildet und angezeigt.

Option4.2
Der Hash-Wert wird von einer externen Applikation gebildet und zum Signieren übergeben.

Option 5

Option5.1
Mit Signatur-Prüfung nach Signiervorgang

Option5.2
Ohne Signatur-Prüfung nach Signiervorgang

Der Vergleich der beiden Keyed-Hashs für alle Optionen erfolgt über Software des Sign@tor Terminals.

Sicherung des Software Updates für den Sign@tor 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 das Sign@tor 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 bei allen Optionen 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.

1.3 Angaben zum Produkt- bzw. Lieferumfang

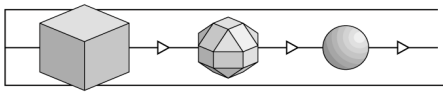
In diesem Abschnitt werden insbesondere die Angaben zum Lieferumfang präzisiert. Dabei werden auch genauere Festlegungen getroffen, welche Produktteile der Evaluierung (ihrer Korrektheit und Wirksamkeit) unterliegen und damit Komponenten des EVG im eigentlichen Sinne sind.

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

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

Die ausgelieferte CD (Produktteil) enthält im wesentlichen die

- Software für den Sign@tor PC
- Signatur-API
- Update Software Sign@tor PC
- Signatur Prüfen
- Benutzeroberfläche (High Level)
- Benutzerdokumentation und
- Optional: Externe Applikation (Secure Viewer-Software eines Drittunternehmens)



Die (installierte) Software zur Benutzeroberfläche (High -Level), das Signatur-Prüfen der signierten Dateien und Secure Viewer-Software sind nicht Bestandteile 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 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.

2 Beschreibung der Einsatzumgebung

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 Microsoft Windows Betriebssysteme:

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

- **Anmerkung:** der Sign@tor PC wird mit den Betriebssystemen Windows 98 SE, 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,
- CD-Laufwerk.

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.

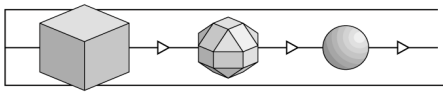
Andere Interfaces zum PC sind nicht vorgesehen.

- 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,
- zusätzlicher Speicherbaustein: 32KB RAM,
- persistenter Datenspeicher: mind. 2KB EEPROM,
- Chipkarteninterface: ISO 7816 (T1- Protokoll),
- Tastatur: Matrix 3x4 ,
- Display: ohne Beleuchtung Größe: 16x1,
- USB: Übertragungsmedium.

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



- mit Prozessorchip Infineon
  - Chipkartenbetriebssystem: CardOS/M4.0
  - Chipkartenbetriebssystem: TCOS
  - Chipkartenbetriebssystem: CardOS/M4.01 und

- mit Prozessorchip Philips
  - Chipkartenbetriebssystem: Starcos SPK 2.2 + mod
  - Chipkartenbetriebssystem: Starcos 2.3

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

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:

Jede externe Applikation, welche die in Kapitel 1.2 beschriebenen Voraussetzungen sowie die in diesem Kapitel definierten Anforderungen an die Einsatzumgebung erfüllt, kann die offene Schnittstelle des Sign@tors benützen.

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

Anmerkung: Die Benutzerdokumentation ist generell 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.

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 (je nach Optionsart),
- ein eventuelles Mithören oder Ändern des Dokumenteninhaltes während des Datentransfers zwischen dem Sign@tor –PC und dem Sign@tor Terminal muss vermieden werden.

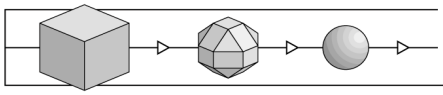
2.3 Definition der Objekte, Subjekte und Zugriffsarten

In diesem Kapitel werden alle zur Analyse der Sicherheitseigenschaften des EVG und in weiterer Folge zur Definition von Sicherheitszielen (Kapitel 3.1), Bedrohungen (Kapitel 3.2) und Sicherheitsfunktionen (Kapitel 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 Daten,
- 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 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 Sicherheitsziele und die Bedrohungen

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 Daten 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.

3.2 Bedrohungen

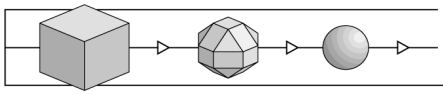
Da der Sign@tor am freien Markt zu kaufen sein wird, hat ein potentieller Angreifer bei Erwerb die Möglichkeit, das komplette Terminal (Hardware, geladene Software) und die Inhalte der CD (des gekauften Produkts) zu manipulieren oder sich die Kenntnisse zu solcher Manipulation anzueignen. Die Hardware 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: Daten während Signatur fälschen
Die zu signierende Datei wird 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.



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
Sign@tor PC bildet über den Hash-Wert einen Keyed-Hash und dieser wird vom Sign@tor Terminal überprüft.
Bemerkung:

- Bei den Optionen 1.1 und 1.2 zeigen beide (Sign@tor PC und Sign@tor Terminal) einen selbstberechneten Hash-Wert der zu signierenden Daten an. Der Benutzer muss/ kann beide Hash-Werte vergleichen, bevor der eigentliche Signierprozess (Senden des Hash-Wertes an die Signatur-Chipkarte) gestartet werden kann.
- Bei den Optionen 1.1, 1.2 und 1.3 wird der Hash-Wert im Sign@tor Terminal berechnet.

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.

SF4 – Sicheres Software Update

> **SF4.1:** Die Integrität der für das sichere Update des Sign@tor PCs bestimmten Software wird nach dem Herunterladen der Software vom Benutzer mit einem von der Original-CD zu startendem 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 sichere 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.

5 Zweckmäßigkeit der Sicherheitsfunktionen

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

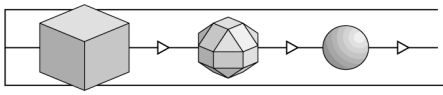
1. Signaturkarte am Sign@tor Terminal / Ausspionieren der PIN
   Die PIN könnte von einem Angreifer ausspioniert werden (B1). Um dem entgegen zu wirken, erfolgt die PIN-Eingabe am Terminal (SF1.1). Die PIN wird ausschließlich zur Karte weitergegeben und anschließend direkt gelöscht (SF1.2). Damit kann 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 sich in einem Raum befinden,
   - da über den Hash-Wert vom Sign@tor PC ein Keyed-Hash gebildet und dieser vom Sign@tor Terminal überprüft wird.

   Bemerkung:
   - Bei den Optionen 1.1 und 1.2 zeigen beide (Sign@tor PC und Sign@tor Terminal) einen selbstberechneten Hash-Wert der zu signierenden Datei an. Der Benutzer muss / kann beide Hash-Werte vergleichen, bevor der eigentliche Signierprozess (Senden des Hash-Wertes an die Signatur-Chipkarte) gestartet werden kann.
   - Bei Option 3.1 wird zusätzlich 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.
   Damit kann die Bedrohung B3 abgewehrt werden.



6 Evaluationsstufe und die Mindeststärke der Mechanismen

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

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 den Sicherheitsvorgaben 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 dem PC, auf dem Sign@tor PC abläuft, verwendet.

Benutzer: Person, welche eine elektronische Unterschrift erstellen oder überprüfen will.

Dokument: Ein in Dateiform vorliegendes Dokument.

Signatur: Datei mit folgendem Inhalt: Daten zum Benutzer, Hash-Wert über das Dokument, Elektronische Unterschrift (aus dem Hash-Wert gebildet).

Hash-Wert: Über ein Dokument gerechnete Prüfsumme. Charakteristisch für ein Dokument, aber nicht unbedingt eindeutig.

Keyed Hash: Der Hash-Wert wird mit einem Geheim-Key erweitert und noch einmal gehasht.

Unterschrift: Signatur

Signaturkarte: Chipkarte, auf der die erforderlichen Schlüssel gespeichert sind. Die Berechnung der Unterschrift aus dem *Hash-Wert* erfolgt ebenfalls auf der Signaturkarte.

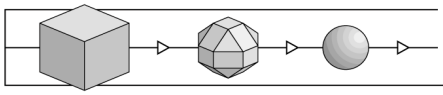
Zertifikat: Vom Trustcenter übermittelte Datei. Diese enthält Daten über einen Benutzer, sowie dessen Public-Key. Ein Zertifikat ist vom Trustcenter mit dessen Private-Key unterschrieben. Ist in diesem Dokument von einem Zertifikat die Rede, so ist, falls nicht anders angegeben, das Zertifikat eines Senders gemeint.

Datei Information: Datei Information besteht aus: Dateiname, Dateilänge und Erstellungsdatum der Datei

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



8 Abkürzungen

Abkürzung	Erklärung	
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	
SW	Software	
SFx	Sicherheitsfunktion	x= Laufende Nummer
SZx	Sicherheitsziele	x= Laufende Nummer
USB	Universal Serial Bus	

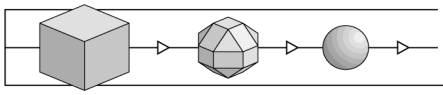
Ende der Sicherheitsvorgaben

4 Anhang

4.1 Glossar

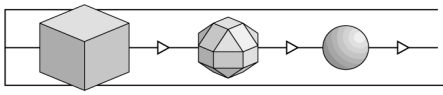
Das Glossar erläutert die in dieser Broschüre verwendeten Begriffe, erhebt allerdings keinerlei Anspruch auf Vollständigkeit oder Allgemeingültigkeit. Der Begriff *Sicherheit* meint hier stets Sicherheit im Kontext der Informationstechnik.

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.
Bestätigungsstelle	Stelle, die im Einklang mit SigG und SigV Sicherheitsbestätigungen für technische Komponenten und für die Umsetzung von Sicherheitskonzepten bei Trust Centern (Zertifizierungsdiensteanbietern 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 sind.
Dienstleistung	Hier: Eine durch ein Unternehmen angebotene, durch Geschäftsprozesse erbrachte und durch Nutzer in Anspruch nehmbare Leistung.
DIN EN 45000	Normen-Reihe, die einschlägige Standards insbesondere für Prüf- und Zertifizierungsstellen enthält.
Einzelprüfbericht	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.
Evaluation Technical Report	Schlußbericht einer Prüfstelle über den Ablauf und die Ergebnisse einer Evaluation (ITSEC: ETR).



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.
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 (Signaturerstellungseinheit, Signaturanwendungskomponente, etc.)
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 von IT-Produkten.
Prozeß (Unternehmens~)	Abfolge vernetzter Tätigkeiten (Prozeßelemente) in einer gegebenen Prozeßumgebung – mit dem Gesamtziel, eine bestimmte Dienstleistung zu erbringen.
Prüfbegleitung	Verfahren der Zertifizierungsstelle, um die Ordnungsmäßigkeit (Kriterienkonformität, einheitliche Vorgehensweise und Bewertungen, etc.) einer Evaluierung zu überprüfen.
Prüfbericht	Einzelprüfbericht oder Evaluation Technical Report
Prüfstelle	Stelle, die Evaluierungen durchführt.
Regulierungsbehörde	Die für den Bereich der elektronischen Signatur in Deutschland 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	SigG: 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.
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	Gesetz über die Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (in Deutschland)
Signaturverordnung - SigV	Amtliche Ausführungsbestimmungen zum Signaturgesetz (in Deutschland).
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 „Zertifizierungsdiensteanbieter“ bezeichnet.
Unternehmensprozeß	s. Prozeß
Verfahrenskennung	Code-Bezeichnung für ein Zertifizierungs- oder 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.
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.
Zertifizierungsdiensteanbieter	s. Trust Center
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.

4.2 Referenzen

/ALG/ Geeignete Kryptoalgorithmen, veröffentlicht im Bundesanzeiger durch die Regulierungsbehörde für Telekommunikation und Post, gültige Fassung

/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: Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, August 1999
Teil 1: Einführung und allgemeines Modell,
Teil 2: Funktionale Sicherheitsanforderungen,
Teil 3: Anforderungen an die Vertrauenswürdigkeit

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

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

/JIL/ Joint Interpretation Library, Version 2.0, Nov. 1998

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

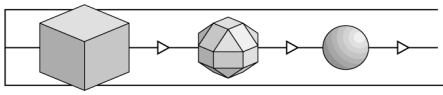
/Mkat16/ Maßnahmenkatalog nach §16 Abs. 6 (SigV), RegTP, www.RegTp.de

/SigG/ Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (Signaturgesetz – SigG) vom 16.05.2001 (BGBl. I, S. 876 ff.)

(ältere Fassung:)
Gesetz zur digitalen Signatur (Signaturgesetz – SigG) vom 22.07.1997 (BGBl. I., S. 1870, 1872)

/SigV/ Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 (BGBl. I., S. 3074 ff.)

(ältere Fassung:)
Verordnung zur digitalen Signatur (Signaturverordnung – SigV) vom 08.10.1997 (BGBl. I., S. 2498 ff.)



4.3 Abkürzungen

AIS	Anforderung einer Interpretation von Sicherheitskriterien (Verfahren des BSI)
BGBl	Bundesgesetzblatt
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
DATech	Deutsche Akkreditierungsstelle Technik e.V.
ETR	Evaluation Technical Report (Evaluierungsbericht)
EVG	Evaluationsgegenstand
IT	Informationstechnik
ITSEC	Information Technology Security Evaluation Criteria (ITSEC)
ITSEF	IT Security Evaluation Facility: Prüflabor
ITSEM	Information Technology Security Evaluation Manual (ITSEM)
RegTP	Regulierungsbehörde für Telekommunikation und Post
SigG	Signaturgesetz
SigV	Signaturverordnung

5 Erläuterungen zu den Sicherheitskriterien

Dieses Kapitel gibt einen Überblick über die angewendeten Sicherheitskriterien und deren Bewertungsmaßstäbe. Textpassagen innerhalb „...“ stellen Zitate aus den ITSEC bzw. den ITSEM dar.

5.1 Grundbegriffe

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

Sicherheitsziele setzen sich in der Regel aus Forderungen nach Vertraulichkeit, Verfügbarkeit und / oder Integrität von bestimmten Datenobjekten zusammen. Solche Sicherheitsziele werden durch den Auftraggeber der Evaluierung festgelegt. Normalerweise ist dies bei einem Produkt der Entwickler oder Vertreiber, bei einem System der Betreiber.

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

Aus solchen prinzipiellen Bedrohungen werden *Angriffe*, wenn Subjekte unerlaubt Datenobjekte mitlesen oder abhören, Dritten vorenthalten oder unbefugt ändern.

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

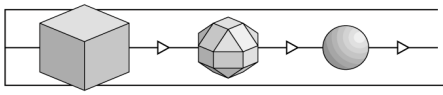
Es stellen sich dabei zwei Grundfragen: Funktionieren die Sicherheitsfunktionen korrekt? Sind die Sicherheitsfunktionen wirksam?

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

5.2 Evaluationsstufen

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 unangemessen wäre es, bei höchstem Sicherheitsbedarf nur „oberflächlich“ zu prüfen.

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



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

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

In allen E-Stufen müssen darüber hinaus Wirksamkeitsaspekte nach folgendem Schema untersucht werden:

"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 Sicherheitsfunktionen und Sicherheitsmechanismen

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.

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.

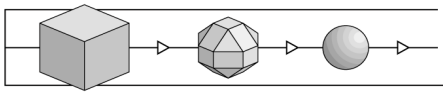
Jede Sicherheitsfunktion kann auf unterschiedlichste Weise realisiert werden. Beispiel: Die Funktion *Identifikation und Authentisierung* kann unter anderem durch ein Paßwort-Verfahren, durch Verwendung von Chipkarten mit Challenge-Response Verfahren oder durch biometrische Verfahren realisiert sein.

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

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

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 durch direkte Angriffe.

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.“

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."

Ende des Zertifizierungsreports zu T-Systems-DSZ-ITSEC-04080-2002.

T-Systems-DSZ-ITSEC-04080-2002
Zertifizierungsreport

Adresse: Rabinstr. 8, 53111 Bonn
Telefon: 0228/9841-0
Fax: 0228/9841-60
Web: www.t-systems-iss.com
www.t-systems-zert.com