

BSI-DSZ-CC-0505-2008

zu

Virtuelle Poststelle des Bundes, (OSCI)
Version 2.2.3.2

der

bremen online services GmbH & Co. KG

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Telefon +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Hotline +49 (0)228 99 9582-111



Deutsches IT-Sicherheitszertifikat

erteilt vom



Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0505-2008

Signaturanwendungskomponente

Virtuelle Poststelle des Bundes, (OSCI)

Version 2.2.3.2

von bremen online services GmbH & Co. KG

Funktionalität: Produktspezifische Sicherheitsvorgaben;
Common Criteria Teil 2 erweitert

Vertrauenswürdigkeit: Common Criteria Teil 3 konform
EAL3 mit Zusatz von
ADO_DEL.2 - Erkennung von Modifizierungen
ADV_IMP.1 - Teilmenge der Implementierung der TSF
ADV_LLD.1 - Beschreibender Entwurf auf niedriger
Ebene
ALC_TAT.1 - Klar festgelegte Entwicklungswerkzeuge
AVA_MSU.3 - Analysieren und Testen auf unsichere
Zustände
AVA_VLA.4 - Hohe Widerstandsfähigkeit



Common Criteria
Recognition
Arrangement
für Komponenten bis
EAL4



Das in diesem Zertifikat genannte IT-Produkt wurde von einer akkreditierten und lizenzierten Prüfstelle nach der Gemeinsamen Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 2.3 und Anweisungen der Zertifizierungsstelle für Komponenten oberhalb von EAL 4 unter Nutzung der Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Version 2.3 (CC) (ISO/IEC 15408:2005) evaluiert.

Dieses Zertifikat gilt nur für die angegebene Version des Produktes in der evaluierten Konfiguration und nur in Verbindung mit dem vollständigen Zertifizierungsreport.

Die Evaluation wurde in Übereinstimmung mit den Bestimmungen des Zertifizierungsschemas des Bundesamtes für Sicherheit in der Informationstechnik durchgeführt. Die im Evaluationsbericht enthaltenen Schlußfolgerungen der Prüfstelle sind in Einklang mit den erbrachten Nachweisen.

Dieses Zertifikat ist keine generelle Empfehlung des IT-Produktes durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte. Eine Gewährleistung für das IT-Produkt durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte, ist weder enthalten noch zum Ausdruck gebracht.

Bonn, 24. Oktober 2008

Bundesamt für Sicherheit in der Informationstechnik

Im Auftrag

Bernd Kowalski
Abteilungspräsident

L.S.



SOGIS - MRA

Dies ist eine eingefügte Leerseite.

Vorbemerkung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat gemäß BSIG¹ die Aufgabe, für Produkte (Systeme oder Komponenten) der Informationstechnik, Sicherheitszertifikate zu erteilen.

Die Zertifizierung eines Produktes wird auf Veranlassung des Herstellers oder eines Vertreibers - im folgenden Antragsteller genannt - durchgeführt.

Bestandteil des Verfahrens ist die technische Prüfung (Evaluierung) des Produktes gemäß den vom BSI öffentlich bekannt gemachten oder allgemein anerkannten Sicherheitskriterien.

Die Prüfung wird in der Regel von einer vom BSI anerkannten Prüfstelle oder vom BSI selbst durchgeführt.

Das Ergebnis des Zertifizierungsverfahrens ist der vorliegende Zertifizierungsreport. Hierin enthalten sind u. a. das Sicherheitszertifikat (zusammenfassende Bewertung) und der detaillierte Zertifizierungsbericht.

Der Zertifizierungsbericht enthält die sicherheitstechnische Beschreibung des zertifizierten Produktes, die Einzelheiten der Bewertung und Hinweise für den Anwender.

¹ Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz-BSIG) vom 17. Dezember 1990, Bundesgesetzblatt I S. 2834

Gliederung

A	Zertifizierung.....	7
1	Grundlagen des Zertifizierungsverfahrens.....	7
2	Anerkennungsvereinbarungen.....	7
2.1	Europäische Anerkennung von ITSEC/CC - Zertifikaten.....	7
2.2	Internationale Anerkennung von CC - Zertifikaten.....	8
3	Durchführung der Evaluierung und Zertifizierung.....	8
4	Gültigkeit des Zertifikats.....	8
5	Veröffentlichung.....	9
B	Zertifizierungsbericht.....	10
1	Zusammenfassung.....	11
2	Identifikation des EVG.....	14
3	Sicherheitspolitik.....	15
4	Annahmen und Klärung des Einsatzbereiches.....	15
5	Informationen zur Architektur.....	16
6	Dokumentation.....	18
7	Testverfahren.....	18
7.1	Testverfahren des Herstellers.....	18
7.2	Testverfahren der Prüfstelle.....	19
8	Evaluierte Konfiguration.....	20
9	Ergebnis der Evaluierung.....	20
9.1	CC spezifische Ergebnisse.....	20
9.2	Ergebnis der kryptographischen Bewertung.....	21
10	Auflagen und Hinweise zur Benutzung des EVG.....	21
10.1	Auflagen zur Benutzung des EVG.....	21
10.2	Empfehlungen und Hinweise an den Anwender.....	22
10.3	Unterstützung von Chipkartenlesern und sicheren Signaturerstellungseinheiten	22
11	Sicherheitsvorgaben.....	25
12	Definitionen.....	25
12.1	Abkürzungen.....	25
12.2	Glossary.....	25
13	Literaturangaben.....	27
C	Auszüge aus den Kriterien.....	30
D	Anhänge.....	38

A Zertifizierung

1 Grundlagen des Zertifizierungsverfahrens

Die Zertifizierungsstelle führt das Verfahren nach Maßgabe der folgenden Vorgaben durch:

- BSIG²
- BSI-Zertifizierungsverordnung³
- BSI-Kostenverordnung⁴
- besondere Erlasse des Bundesministeriums des Innern
- die Norm DIN EN 45011
- BSI-Zertifizierung: Verfahrensbeschreibung (BSI 7125) [3]
- Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CC), Version 2.3⁵
- Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 2.3
- BSI-Zertifizierung: Anwendungshinweise und Interpretationen zum Schema (AIS)
- Hinweise der Zertifizierungsstelle zur Methodologie für Vertrauenswürdigkeitskomponenten oberhalb von EAL 4 (AIS 34)

2 Anerkennungsvereinbarungen

Um die Mehrfach-Zertifizierung des gleichen Produktes in verschiedenen Staaten zu vermeiden, wurde eine gegenseitige Anerkennung von IT-Sicherheitszertifikaten - sofern sie auf ITSEC oder Common Criteria (CC) beruhen - unter gewissen Bedingungen vereinbart.

2.1 Europäische Anerkennung von ITSEC/CC - Zertifikaten

Ein Abkommen über die gegenseitige Anerkennung von IT-Sicherheitszertifikaten, auf deren Grundlage ITSEC-Zertifikate für IT-Produkte unter gewissen Bedingungen anerkannt werden, ist im März 1998 in Kraft getreten (SOGIS-MRA).

Es wurde von den nationalen Stellen der folgenden Staaten unterzeichnet: Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Italien, Niederlande, Norwegen, Portugal, Schweden, Schweiz und Spanien. Das Abkommen wurde zur gegenseitigen Anerkennung von IT-Sicherheitszertifikaten auf Basis der CC bis einschließlich der

² Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz-BSIG) vom 17. Dezember 1990, Bundesgesetzblatt I S. 2834

³ Verordnung über das Verfahren der Erteilung eines Sicherheitszertifikats durch das Bundesamt für Sicherheit in der Informationstechnik (BSI-Zertifizierungsverordnung-BSIZertV) vom 7. Juli 1992, Bundesgesetzblatt I S. 1230

⁴ Kostenverordnung für Amtshandlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Kostenverordnung-BSI-KostV) vom 3. März 2005, Bundesgesetzblatt I S. 519

⁵ Bekanntmachung des Bundesministeriums des Innern vom 10. Mai 2006 im Bundesanzeiger, datiert 19. Mai 2006, S. 19445

Evaluationsstufe EAL7 erweitert. Das BSI erkennt die Zertifikate der nationalen Zertifizierungsstellen von Frankreich und Großbritannien im Rahmen dieses Abkommens an.

Das SOGIS-MRA-Logo auf dem Zertifikat zeigt, dass das Zertifikat unter den Bedingungen des Abkommens anerkannt wird.

2.2 Internationale Anerkennung von CC - Zertifikaten

Im Mai 2000 wurde eine Vereinbarung (Common Criteria-Vereinbarung) über die gegenseitige Anerkennung von IT-Sicherheitszertifikaten und Schutzprofilen auf Basis der CC bis einschließlich der Vertrauenswürdigkeitsstufe EAL 4 verabschiedet (CC-MRA).

Der Vereinbarung sind bis Februar 2007 die nationalen Stellen folgender Nationen beigetreten: Australien, Dänemark, Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Indien, Israel, Italien, Japan, Kanada, Republik Korea, Neuseeland, Niederlande, Norwegen, Österreich, Schweden, Spanien, Republik Singapur, Tschechische Republik, Türkei, Ungarn, USA.

Eine aktuelle Liste der Unterzeichnerstaaten bzw. der anerkannten Zertifizierungsstellen kann auf der Internetseite <http://www.commoncriteriaportal.org> eingesehen werden.

Das Common Criteria-Logo auf dem Zertifikat zeigt, dass das Zertifikat unter den Bedingungen des Abkommens anerkannt wird.

Diese Evaluierung beinhaltet die Komponenten AVA_MSU.3 und AVA_VLA.4, die nicht unter der Common Criteria Vereinbarung über die gegenseitige Anerkennung von IT-Sicherheitszertifikaten anerkannt werden. Für die gegenseitige Anerkennung sind die EAL4-Komponenten dieser Vertrauenswürdigkeitsfamilien relevant.

3 Durchführung der Evaluierung und Zertifizierung

Die Zertifizierungsstelle führt für jede einzelne Evaluierung eine Prüfbegleitung durch, um einheitliches Vorgehen, einheitliche Interpretation der Kriterienwerke und einheitliche Bewertungen sicherzustellen.

Das Produkt Virtuelle Poststelle des Bundes, (OSCI) Version 2.2.3.2 hat das Zertifizierungsverfahren beim BSI durchlaufen. Es handelt sich um eine Re-Zertifizierung basierend auf BSI-DSZ-CC-0330-2007.

Die Evaluation des Produkts Virtuelle Poststelle des Bundes, (OSCI) Version 2.2.3.2 wurde von T-Systems GEI GmbH durchgeführt. Die Evaluierung wurde am 18. März 2008 beendet. Das Prüflabor T-Systems GEI GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)⁶.

Der Hersteller und Antragsteller ist: bremen online services GmbH & Co. KG

Die Zertifizierung wurde damit beendet, dass das BSI die Übereinstimmung mit den Kriterien überprüft und den vorliegenden Zertifizierungsreport erstellt hat.

4 Gültigkeit des Zertifikats

Dieser Zertifizierungsreport bezieht sich nur auf die angegebene Version des Produktes.

⁶ Information Technology Security Evaluation Facility

Das Produkt ist nur unter den folgenden Bedingungen konform zu den bestätigten Vertrauenswürdigkeitskomponenten:

- alle Auflagen hinsichtlich der Generierung, der Konfiguration und dem Einsatz des EVG, die in diesem Report gestellt werden, werden beachtet.
- das Produkt wird in der Umgebung betrieben, die in diesem Report und in den Sicherheitsvorgaben beschrieben ist.

Die Bedeutung der Vertrauenswürdigkeitsstufen und die Stärke der Funktionen werden in den Auszügen aus dem technischen Regelwerk am Ende des Zertifizierungsreports erläutert.

Das Zertifikat bestätigt die Vertrauenswürdigkeit des Produktes gemäß den Sicherheitsvorgaben zum Zeitpunkt der Ausstellung. Da Angriffe mit neuen oder weiterentwickelten Methoden in Zukunft möglich sind, besteht die Möglichkeit, die Widerstandsfähigkeit des Produktes im Rahmen des Assurance Continuity-Programms des BSI regelmäßig überprüfen zu lassen. Die Zertifizierungsstelle empfiehlt, regelmäßig eine Einschätzung der Widerstandsfähigkeit vornehmen zu lassen.

Bei Änderungen am Produkt kann die Gültigkeit des Zertifikats auf neue Versionen ausgedehnt werden. Voraussetzung dafür ist, dass der Antragsteller die Aufrechterhaltung der Vertrauenswürdigkeit (d.h. eine Re-Zertifizierung oder ein Maintenance Verfahren) in Übereinstimmung mit den entsprechenden Regeln beantragt und die Evaluierung keine Schwächen aufdeckt.

5 Veröffentlichung

Das Produkt Virtuelle Poststelle des Bundes, (OSCI) Version 2.2.3.2 ist in die BSI-Liste der zertifizierten Produkte, die regelmäßig veröffentlicht wird, aufgenommen worden (siehe auch Internet: <http://www.bsi.bund.de> und [5]). Nähere Informationen sind über die BSI-Infoline 0228/9582-111 zu erhalten.

Weitere Exemplare des vorliegenden Zertifizierungsreports können beim Hersteller des Produktes angefordert werden⁷. Der Zertifizierungsreport kann ebenso in elektronischer Form von der oben angegebenen Internetadresse heruntergeladen werden.

⁷ bremen online services GmbH & Co. KG
Am Fallturm 9
28359 Bremen

B Zertifizierungsbericht

Der nachfolgende Bericht ist eine Zusammenfassung aus

- den Sicherheitsvorgaben des Antragstellers für den Evaluationsgegenstand,
- den entsprechenden Prüfergebnissen des Prüflabors und
- ergänzenden Hinweisen und Auflagen der Zertifizierungsstelle.

1 Zusammenfassung

Im Rahmen des Projektes BundOnline 2005 wurde die Virtuelle Poststelle des Bundes entwickelt. Sie stellt als zentrales Kommunikations-Gateway Sicherheitsdienste für die gesicherte Kommunikation zwischen Behörden und externen Kommunikationspartnern (Bürger, Wirtschaft und andere Behörden) bereit. Dieses komplexe Produkt wird in drei Verfahren mit den Evaluationsgegenständen Virtuelle Poststelle des Bundes (Basis) bzw. Basiskomponente (EVG 1, blau markiert in Abbildung 1), Virtuelle Poststelle des Bundes (OSCI) bzw. OSCI -Komponente (EVG 2, gelb markiert in Abbildung 1 und Gegenstand dieses Zertifikats) und Virtuelle Poststelle des Bundes (Verifikationsmodul) bzw. Verifikationsmodul (EVG 3, orange markiert in Abbildung 1) evaluiert und zertifiziert. Ausschließlich die in Abbildung 1 farblich gekennzeichneten Teile der Virtuellen Poststelle des Bundes sind Bestandteil von Zertifizierungsverfahren. Alle weiteren Anteile, die in Abbildung 1 nicht farblich markiert sind, sind demzufolge nicht Gegenstand einer Zertifizierung.

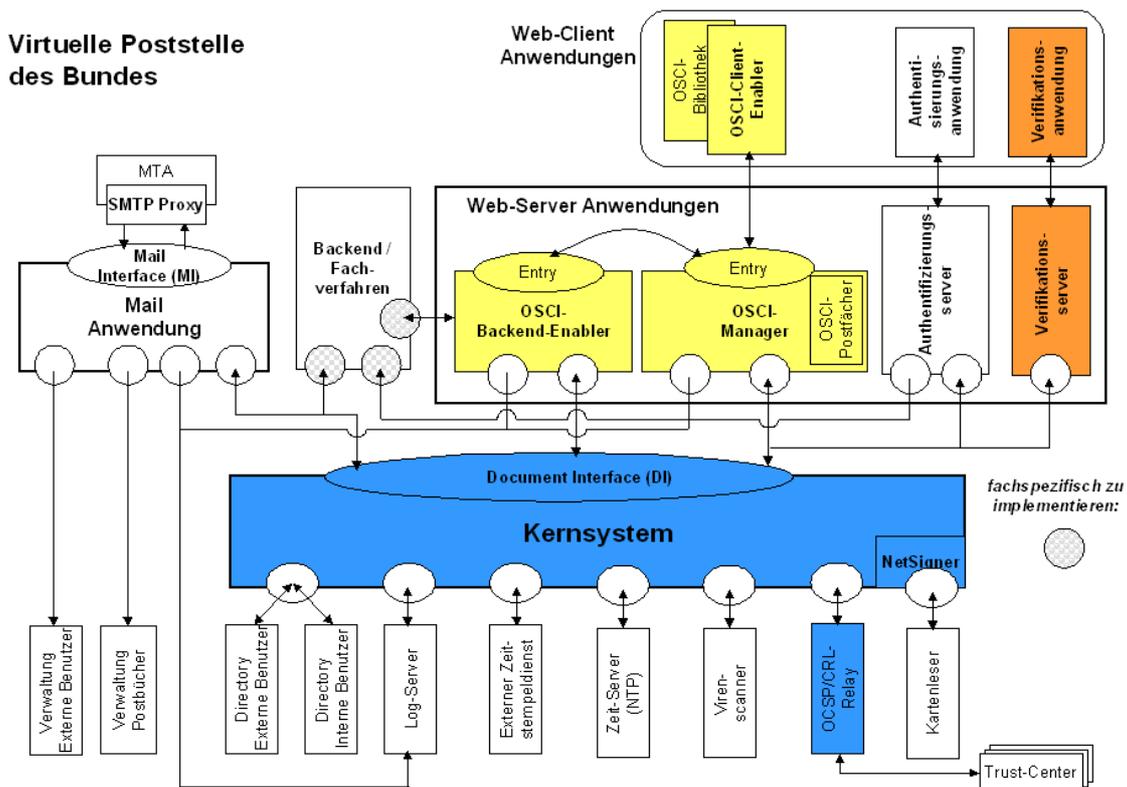


Abbildung 1: Aufbau der Virtuellen Poststelle des Bundes

Die Basiskomponente (EVG 1) wird zentral in einem gesicherten Bereich (z.B. in einem Rechenzentrum) betrieben und stellt folgende Funktionalitäten zentral zur Verfügung:

- Unterstützung bei der Erzeugung elektronischer Batchsignaturen,
- mathematische Prüfung elektronischer Signaturen (Verifikation) und
- Statusprüfung von Zertifikaten (Validierung).

Sowohl die OSCI-Komponente als auch das Verifikationsmodul greifen zur Bereitstellung ihrer eigenen Funktionalität auf die im Sinne eines Servers betriebene Basiskomponente

zurück, so dass die Zertifizierung der Basiskomponente eine Voraussetzung für den sicheren Einsatz von EVG 2 und EVG 3 darstellt.

Das Verifikationsmodul (EVG 3) umfasst eine Signaturanwendungskomponente für das Verifizieren von Signaturen und Zertifikaten am Arbeitsplatz des Endnutzers. Diese besteht aus einer Serverkomponente (Verifikationsserver) und einem dazugehörigen Client (Verifikationsanwendung).

Gegenstand dieses Zertifikats ist die OSCI-Komponente (EVG 2). Der EVG 2 beinhaltet die folgenden Anteile (siehe auch Kapitel 2 in diesem Report):

- Eine Funktionsbibliothek (OSCI-Client-Enabler) zur Integration in eine Client-Software, mit der die sichere Anzeige und das Signieren von Dokumenten am Arbeitsplatz sowie die Kommunikation über das OSCI-Protokoll zur Verfügung gestellt wird.
- Ein Prüftool, das über einen Browser vom Endbenutzer aufgerufen werden kann und die Integrität des OSCI-Client-Enablers überprüft.
- Eine Funktionsbibliothek (OSCI-Backend-Enabler) zur Integration in Fachverfahren, so dass diese Fachverfahren signaturgesetzkonform über das OSCI-Protokoll mit der Basiskomponente kommunizieren. Dabei werden die Fachverfahren in einer geschützten Einsatzumgebung betrieben.
- Die zentrale Serverkomponente für den Betrieb einer OSCI-konformen IT-Infrastruktur (OSCI-Manager), die zusammen mit der Basiskomponente in einem vertrauenswürdigen Netz eingesetzt wird.

Der OSCI-Client-Enabler und der –Backend-Enabler müssen entsprechend den Vorgaben der evaluierten Benutzerdokumentation in geeignete Programme eingebunden und zusammen mit geeigneter Hardware – insbesondere mit SigG-konformen Chipkartenlesern und sicheren Signaturerstellungseinheiten – entsprechend den Annahmen an die jeweilige Einsatzumgebung betrieben werden.

Die Sicherheitsvorgaben [6] stellen die Grundlage für die Zertifizierung dar. Sie verwenden kein zertifiziertes Protection Profile.

Die Vertrauenswürdigkeitskomponenten sind dem Teil 3 der Common Criteria entnommen (siehe Teil C oder [1], Teil 3). Der EVG erfüllt die Anforderungen der Vertrauenswürdigkeitsstufe EAL 3 mit Zusatz von ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, ADO_DEL.2, AVA_MSU.3, AVA_VLA.4.

Die funktionalen Sicherheitsanforderungen (Security Functional Requirements SFR) an den EVG werden in den Sicherheitsvorgaben [6], Kapitel 5.1 beschrieben. Sie wurden dem Teil 2 der Common Criteria entnommen und durch neu definierte funktionale Sicherheitsanforderungen ergänzt. Der EVG ist daher gekennzeichnet als Teil 2 erweitert.

Die funktionalen Sicherheitsanforderungen für die IT-Umgebung des EVG werden in den Sicherheitsvorgaben [6] im Kapitel 5.2 dargestellt.

Die funktionalen Sicherheitsanforderungen werden durch die folgenden Sicherheitsfunktionen des EVG umgesetzt:

Sicherheitsfunktion des EVG	Thema
SF1	Unterstützung bei der Erzeugung elektronischer Signaturen Hierunter fällt insbesondere das Bilden von Hashwerten zu Dokumenten und Zuführen der Hashwerte zu einer sicheren Signaturerstellungseinheit.
SF2	Schutz gegen Hashwertmanipulation Der OSCI-Client-Enabler prüft die von einer sicheren Signaturerstellungseinheit erzeugte Signatur mathematisch nach um sicherzustellen, dass der Hashwert nicht manipuliert worden ist.
SF3	Verifikation einer elektronischen Signatur Der OSCI-Client- und -Backend-Enabler prüfen elektronische Signaturen unter Zuhilfenahme des RSA-Algorithmus mit Bitlängen von 1024 und 2048 Bit sowie dem Hashalgorithmus SHA-1. Mit Hilfe der Sicherheitsfunktion SF 6 werden die zugehörigen qualifizierten Zertifikate validiert.
SF4	Verifikation eines OSCI-Laufzettels bei der Validierung eines Zertifikats Im Rahmen des OSCI-Protokolls fertigt der OSCI-Manger einen signierten OSCI-Laufzettel zur Dokumentation durchgeführter Prüfungen an (s. SF6). OSCI-Client und -Backend-Enabler prüfen die Signatur mathematisch anhand von hinterlegten Zertifikaten nach.
SF5	Sichere und zuverlässige Anzeige Der OSCI-Client-Enabler bietet eine sichere Anzeige für Tiff- und Text-Dateien und stellt weitere Anzeigefunktionen wie z.B. die Inhalte des zugehörigen Zertifikats zur Verfügung.
SF6	Unterstützung bei der Validierung qualifizierter Zertifikate Der OSCI-Manager übergibt zu validierende qualifizierte Zertifikate an die Basiskomponente der Virtuellen Poststelle (siehe Abbildung 1) und wertet das Ergebnis selber aus. Die Auswertung der Prüfung trägt der OSCI-Manager gemäß dem OSCI-Protokoll in den OSCI-Laufzettel ein und lässt ihn durch die Basiskomponente signieren. Der Laufzettel wird durch die dezentralen Komponenten OSCI-Client- bzw. -Backend-Enabler geprüft (s. SF4).
SF7	Identifikation und Authentisierung Der Zugriff auf die Administration des OSCI-Managers über eine Webschnittstelle ist nur nach erfolgreicher Identifikation und Authentisierung möglich.
SF8	Prüftool Mit Hilfe des Prüftools ist es möglich, die Integrität des dezentral auf Arbeitsplatzrechnern eingesetzten OSCI-Client-Enablers zu überprüfen.

Tabelle 1: Sicherheitsfunktionen des EVG

Mehr Details sind in den Sicherheitsvorgaben [6], Kapitel 6 dargestellt.

Die Stärke „hoch“ der Funktionen des EVG für bestimmte Funktionen, wie in den Sicherheitsvorgaben [6], Kapitel 8.3.4 angegeben, wird bestätigt.

Die Bewertung der Stärke der Funktionen erfolgte ohne Einbeziehung der für die Ver- und Entschlüsselung eingesetzten Kryptoalgorithmen (vgl. §4 Abs. 3 Nr. 2 BSIG). Für Details siehe Kap. 9 dieses Berichtes.

Die Sicherheitsvorgaben [6] stellen die Sicherheitsumgebung in Form von Annahmen, Bedrohungen und organisatorischen Sicherheitspolitiken in Kapitel 3 dar.

Der EVG kann nur in einer Konfiguration betrieben werden. Für mehr Details siehe Kapitel 8.

Dieses Zertifikat gilt nur für die angegebene Version des Produktes in der evaluierten Konfiguration und nur in Verbindung mit dem vollständigen Zertifizierungsreport. Dieses Zertifikat ist keine generelle Empfehlung des IT-Produktes durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte. Eine Gewährleistung für das IT-Produkt durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte, ist weder enthalten noch zum Ausdruck gebracht.

2 Identifikation des EVG

Der Evaluierungsgegenstand (EVG) heißt:

Virtuelle Poststelle des Bundes, (OSCI) Version 2.2.3.2

Die folgende Tabelle beschreibt den Auslieferungsumfang:

Nr	Typ	Identifizier	Version	Datum	Auslieferungsart
1	SW	OSCI-Manager	2.2.3.2	28.02.2008	auf CD-ROM oder als Download
2	DOKU	Virtuelle Poststelle des Bundes, Betriebshandbuch	2.2.7	25.02.2008	PDF-Dokument
3	SW	OSCI-Client-Enabler	2.2.3.2	28.02.2008	auf CD-ROM oder als Download
4	SW	OSCI-Backend-Enabler	2.2.3.2	28.02.2008	auf CD-ROM oder als Download
5	DOKU	Virtuelle Poststelle des Bundes, Release 2.2.3.2, Entwicklerhandbuch	2.3.4	25.02.2008	PDF-Dokument
6	SW	Prüftool	2.2.3.2	28.02.2008	auf CD-ROM oder als Download
7	DOKU	Virtuelle Poststelle des Bundes, Benutzer- und Betriebshandbuch Prüfwerkzeug	2.3.6	25.02.2008	PDF-Dokument

Tabelle 2: Auslieferungsumfang des EVG

Der EVG wird an einen Betreiber der Virtuellen Poststelle des Bundes entweder online oder auf einem nicht wiederbeschreibbaren Medium als zip-Archiv zusammen mit den übrigen Anteilen der VPS ausgeliefert.

Im Falle einer Online-Auslieferung wird der EVG in Form eines Archivs auf einem mit einem SSL-Zertifikat gesicherten Server bereitgestellt, auf dem auch der SHA-1-Wert des Archivs veröffentlicht wird. Auf einem zweiten Kommunikationsweg (E-Mail, Fax, o.ä.) wird dem Betreiber bzw. Anwendungsentwickler die URL zum Download des Archivs sowie dessen Hashwert mitgeteilt und auferlegt, den Hashwert vor der Installation des EVG gemäß den Sicherheitshinweisen zu prüfen.

Im Falle einer Auslieferung des EVG auf einem nicht wiederbeschreibbaren Medium an einen Betreiber bzw. Anwendungsentwickler wird dieser über den erfolgten Versand informiert. Außerdem wird dem Empfänger der Hashwert des auf dem Medium

enthaltenen Archivs mitgeteilt (z.B. per E-Mail oder Fax), den er dann gemäß den Sicherheitshinweisen prüfen muss.

Der SHA-1-Hashwert des ausgelieferten Archivs ist:

6b 73 0f 2b ec cd 9c 29 06 94 fd a0 92 a1 de ea 41 57 f0 54

Der Betreiber ist dafür verantwortlich, dem Endbenutzer das Prüftool sowie die Funktionsbibliotheken für den OSCI-Client bzw. -Backend-Enabler über eine mit SSL gesicherte Verbindung zur Verfügung zu stellen. Weiterhin stellt der Betreiber dem Endbenutzer die zur Konfiguration des OSCI-Client-Enabler benötigte Adresse des OSCI-Managers sowie dessen Zertifikat zur Verfügung. Die Authentizität des Prüftools wird weiterhin durch die Signatur des Applets mit Hilfe eines fortgeschrittenen Zertifikats sichergestellt, dessen zugehöriger geheimer Schlüssel ausschließlich beim Hersteller vertrauenswürdig verwahrt und angewendet wird. Der Endbenutzer kann mit Hilfe des Prüftools überprüfen, ob er den authentischen OSCI-Client-Enabler erhalten hat.

3 Sicherheitspolitik

Die Sicherheitspolitik wird durch die funktionalen Sicherheitsanforderungen ausgedrückt und durch die Sicherheitsfunktionen des EVG umgesetzt. Als Signaturanwendungskomponente hat der EVG dabei das Ziel, die relevanten Vorgaben aus dem Signaturgesetz [13] und der –verordnung [14] zu erfüllen. Dabei handelt es sich hauptsächlich um die folgenden Sachverhalte:

- Der EVG ermöglicht es, die Erzeugung einer elektronischen Signatur vorher eindeutig anzuzeigen und feststellen zu lassen, auf welche Daten sich die Signatur bezieht.
- Der EVG zeigt an, dass signierte Daten unverändert sind und welchem Signaturschlüssel-Inhaber die Signatur zugeordnet ist.
- Der EVG zeigt den Inhalt des qualifizierten Zertifikats, auf dem die Signatur beruht, sowie die Prüfungsergebnisse des Zertifikats eindeutig an.
- Bei der Anzeige von Daten in dem unterstützten Text-Format werden Regeln zur sicheren Behandlung von nicht-lesbaren Zeichen durchgesetzt. Bei der Anzeige von TIFF-Dateien ist es möglich, sich mit Hilfe verschiedener Optionen davon zu überzeugen, dass keine versteckten oder aktiven Inhalte in dem Dokument enthalten sind.
- Mit Unterstützung der Basiskomponente der Virtuellen Poststelle ist der EVG in der Lage, die Gültigkeit einer elektronischen Signatur zu prüfen und das Ergebnis der Prüfung anzuzeigen.
- Die Prüfung von qualifizierten Zertifikaten durch den EVG ergibt, ob nachgeprüfte qualifizierte Zertifikate im Verzeichnis der qualifizierten Zertifikate zum angegebenen Zeitpunkt vorhanden und ob sie nicht gesperrt waren.
- Der EVG gibt dem Endbenutzer auf dem Arbeitsplatz-PC die Möglichkeit, die Integrität der installierten Programmteile zu prüfen.

4 Annahmen und Klärung des Einsatzbereiches

Die Annahmen in den Sicherheitsvorgaben sowie Teile der Bedrohungen und organisatorischen Sicherheitspolitiken werden nicht durch den EVG selbst abgedeckt.

Diese Aspekte setzen voraus, dass bestimmte Sicherheitsziele durch die EVG-Einsatzumgebung erfüllt werden. Hierbei sind die folgenden Punkte relevant:

- Die IT-Umgebung muss die für den Betrieb benötigten Komponenten bereitstellen. Dazu gehören insbesondere sichere Signaturerstellungseinheiten mit Zertifikaten und unterstützte Chipkartenleser. Zur Absicherung der Kommunikation werden Server-Zertifikate mit geeigneten kryptographischen Verfahren bereitgestellt.
- Die Basiskomponente der Virtuellen Poststelle des Bundes muss entsprechend den Anweisungen in der Benutzerdokumentation installiert und einsatzbereit sein.
- Zum Betrieb von zentral betriebenen Serverkomponenten wird vertrauenswürdigen Personal eingesetzt, das den OSCI-Manager zusammen mit der Basiskomponente und entsprechenden Fachverfahren in einem vertrauenswürdigen Netz so betreibt und sicherstellt, dass die Auflagen aus [15] an einen „geschützten Einsatzbereich (Regelfall/Standardlösung)“ umgesetzt werden.
- Die IT-Umgebung muss einen OSCI-Client- oder -Backend-Enabler zur Verfügung stellen, welche die entsprechenden Funktionsbibliotheken des EVG gemäß der Benutzerdokumentation nutzen und die Anforderungen von Signaturgesetz und -verordnung an eine Signaturanwendungskomponente umsetzen. Insbesondere gewährleisten sie die Funktionalitäten hinsichtlich Identifikation und Authentisierung zum Management von Sicherheitsattributen, d. h. den kryptographischen Schlüsseln und den (System-) Zertifikaten.
- Der Endnutzer des OSCI-Clients gibt seine Identifikationsmerkmale nicht preis. Er betreibt den EVG in einer Umgebung, in der ein Zugriff Unbefugter ausgeschlossen ist oder zumindest mit hoher Sicherheit erkennbar wird und die Anforderungen an einen geschützten Einsatzbereich gemäß [15] in einer Home- oder Büroumgebung umgesetzt werden.
- Details finden sich in den Sicherheitsvorgaben [6], Kapitel 3.

5 Informationen zur Architektur

Die OSCI-Komponente besteht aus den folgenden Teilsystemen:

- OSCI-Client-Enabler (Sub_1 in Abbildung 2)
- OSCI-Backend-Enabler (Sub_2 in Abbildung 2),
- OSCI-Manager (Sub_3 in Abbildung 2),
- Administrationsanwendung (Sub_4 in Abbildung 2) und
- Prüfwerkzeug (auch Prüftool genannt, Sub_5 in Abbildung 2).

Die Aufteilung in die obigen Teilsysteme ergibt sich aus der Architektur und der OSCI-Kommunikation, bei der ein OSCI-Client, ein -Intermediär und ein -Backend gefordert wird. Diese Rollen werden wie folgt durch die Teilsysteme belegt:

- OSCI-Client-Enabler für einen OSCI-Client,
- OSCI-Manager für den OSCI-Intermediär,
- OSCI-Backend-Enabler für ein OSCI-Backend.

Hierbei ist zur Realisierung des OSCI-Intermediärs neben dem OSCI-Manager zusätzlich eine SigG-konforme Basiskomponente der Virtuellen Poststelle des Bundes notwendig.

Die Administrationsanwendung ist für die Bedienung des OSCI-Managers zuständig. Das Prüftool wird zum Schutz vor unbefugter Veränderung des OSCI-Client-Enablers eingesetzt.

Der EVG stellt folgende Funktionen zur Verfügung:

- Der OSCI-Client-Enabler ist eine Funktionsbibliothek, die von einem OSCI-Client angesprochen wird und insbesondere folgende Dienste zur Verfügung stellt:
 - Unterstützung bei der Erzeugung elektronischer Signaturen;
 - mathematische Prüfung elektronischer Signaturen (Verifikation);
 - mathematische Prüfung elektronischer Signaturen des OSCI-Laufzettels (im Rahmen der Validierung);
 - sichere Anzeige von zu signierenden und signierten Daten sowie Verifikations- und Validierungsergebnissen.
- Der OSCI-Backend-Enabler ist eine Funktionsbibliothek, die von einem OSCI-Backend angesprochen wird und insbesondere folgende Dienste zur Verfügung stellt:
 - mathematische Prüfung elektronischer Signaturen (Verifikation);
 - mathematische Prüfung Signaturen des OSCI-Laufzettels (im Rahmen der Validierung).
- Der OSCI-Manager stellt folgende Funktionalitäten zur Verfügung:
 - Unterstützung bei der Validierung elektronischer Signaturen mit Hilfe der Basiskomponente;
 - Unterstützung bei der Erzeugung einer elektronischen Signatur für den OSCI-Laufzettel mit Hilfe der Basiskomponente.
- Die Administrationsanwendung dient zur Administration des OSCI-Managers. Sie erfolgt über dieselbe Browser-basierte Administrationsanwendung, die auch für die Administration und Bedienung der Basiskomponente genutzt wird.
- Der OSCI-Client-Enabler wird durch das Prüftool vor unbefugter Veränderung geschützt (Integritätsschutz). Dazu wird die Integrität der JAR-Files des OSCI-Client-Enablers geprüft.

Die Aufteilung des EVG in die entsprechenden Subsysteme zeigt auch die folgende Abbildung.

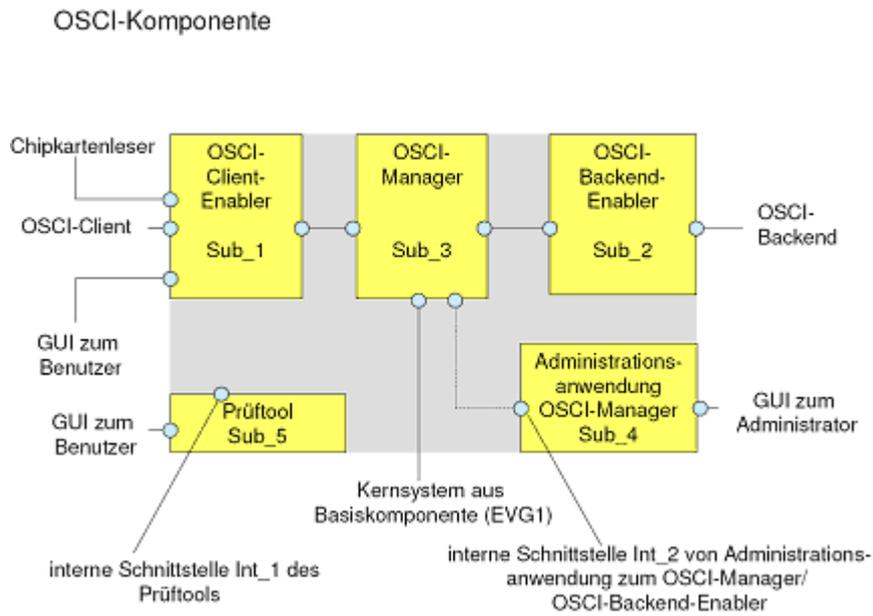


Abbildung 2: Aufteilung des EVG2 in Subsysteme

6 Dokumentation

Die evaluierte Dokumentation, die in Tabelle 2 aufgeführt ist, wird zusammen mit dem Produkt zur Verfügung gestellt. Hier sind die Informationen enthalten, die zum sicheren Umgang mit dem EVG in Übereinstimmung mit den Sicherheitsvorgaben benötigt werden.

Zusätzliche Hinweise und Auflagen zum sicheren Gebrauch des EVG, die im Kapitel 10 enthalten sind, müssen befolgt werden.

7 Testverfahren

7.1 Testverfahren des Herstellers

Der Hersteller hat das Verhalten jeder der in den Sicherheitsvorgaben (ST) [6] definierten Sicherheitsfunktionen getestet und dokumentiert. Die Tests wurden für folgende Systeme zuzüglich zum TOE durchgeführt:

Hard- und Software für die Serverkomponenten:

Betriebssystem	Hardware	Sonstiges
Linux (SuSE Linux Enterprise Server 9)	i386-Architektur (Intel Xeon o.ä)	Java: SUN 1.4.2_04
Windows 2003 Server		Application Server: JBoss 3.2.5 inkl. Tomcat 5.0.26
SUN Solaris 9	Sun UltraSparc-Architektur	Datenbank: MySQL 4.1 Browser zur Administration

Tabelle 3: Testkonfigurationen für OSCI-Manager und OSCI-Backend Enabler

Hard- und Software der Clientkomponenten:

Betriebssystem	Hardware	Sonstiges
Linux (SuSE Linux Professional 9.x)	i386-Architektur (Intel Xeon o.ä)	Java: SUN 1.4.2_04
Windows 2000		
Windows XP		

Tabelle 4: Testkonfigurationen von OSCI-Client-Enabler und Prüftool

Die Testdokumentation zeigt, dass die Tests sowohl auf der Ebene der Teilsysteme des EVGs als auch auf der Modulebene durchgeführt wurden. Die Tests haben gezeigt, dass die Sicherheitsfunktionen des EVGs so implementiert wurden, wie im ST angegeben.

7.2 Testverfahren der Prüfstelle

Die nächsten beiden Tabellen zeigen die Server- und Clientumgebungen zuzüglich zum TOE, die von der Prüfstelle in ihren Tests verwendet worden sind:

Betriebssystem	Hardware	Sonstiges
Windows Server 2003	i386-Architektur (Intel Xeon o.ä)	Java: SUN 1.4.2 JDK Application Server: JBoss 3.2.8 MySQL 4.1

Tabelle 5: Testkonfiguration der Prüfstelle für den Verifikationsserver

Betriebssystem	Hardware	Sonstiges
Windows XP Professional, SP 2	i386 -Architektur, verschiedene Chipkartenterminals und Signaturkarten, s. Kap. 10	Java: SUN 1.4.2_04

Tabelle 6: Testkonfiguration der Prüfstelle für Verifikationsanwendung und Prüftool

Die Evaluatoren haben die gemäß der gewählten Vertrauenswürdigkeitsstufe geforderten unabhängigen Tests anhand der folgenden Vorgehensweise ausgeführt:

- Analyse der Testspezifikationen des Herstellers
- Spezifikation eigener Tests der Evaluatoren
- Wiederholung von Herstellertests und Vergleich mit den Testresultaten des Herstellers
- Durchführung eigener Tests und Dokumentation der Testresultate

In Übereinstimmung mit den Anforderungen wurden die Tests (Herstellertests und Evaluatortests) auf der Ebene der Teilsysteme des EVGs durchgeführt.

Die Testergebnisse zeigen, dass der EVG sich verhält, wie es erwartet wurde.

Basierend auf der Schwachstellenanalyse des Herstellers und ihrer eigenen unabhängigen Schwachstellenanalyse haben die Evaluatoren Penetrationstests

entworfen, um zu erkennen, ob die identifizierten potentiellen Schwachstellen in der beabsichtigten Einsatzumgebung des EVGs ausnutzbar sind. Weitere potentielle Schwachstellen wurden durch geeignete Tests des Herstellers abgedeckt.

Zusammenfassend kommen die Evaluatoren zu dem Ergebnis, dass beim vorliegenden EVG keine in der angenommenen Einsatzumgebung ausnutzbaren Schwachstellen gefunden wurden.

8 Evaluerte Konfiguration

Bei der Installation der Virtuellen Poststelle des Bundes sind bei der Installation alle Komponenten des EVG so zu installieren, wie es im Administrationshandbuch beschrieben ist. Weiterhin sind die Annahmen an die Einsatzumgebung sind zu beachten, wobei insbesondere eine funktionsfähige Basiskomponente zur Verfügung stehen muss. Der EVG wird nur in einer Konfiguration betrieben, bei der die serverseitigen Komponenten verschiedene Betriebszustände annehmen können. Die Evaluierung hat gezeigt, dass der EVG in allen Betriebszuständen die entsprechenden Sicherheitsleistungen zur Verfügung stellt.

9 Ergebnis der Evaluierung

9.1 CC spezifische Ergebnisse

Der Evaluierungsbericht (Evaluation Technical Report, ETR), [7] wurde von der Prüfstelle gemäß den Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Version 2.3 (CC) (ISO/IEC 15408:2005) [1], der Methodologie [2], den Anforderungen des Schemas [3] und allen Anwendungshinweisen und Interpretationen des Schemas (AIS) [4] erstellt, die für den EVG relevant sind. Die Evaluierungsmethodologie CEM [2] wurde für die Komponenten bis zur Vertrauenswürdigkeitsstufe EAL3 verwendet. Darüber hinaus wurde die in der AIS 34 [4] definierte Methodologie verwendet.

Das Urteil PASS der Evaluierung wird für die folgenden Vertrauenswürdigkeitskomponenten bestätigt:

- Alle Komponenten der Klasse ASE
- Alle Komponenten der Vertrauenswürdigkeitsstufe EAL3 der CC (siehe auch Teil C des Zertifizierungsreports)
- Die Komponenten
 - ADO_DEL.2 (Erkennung von Modifizierungen)
 - ADV_IMP.1 (Teilmenge der Implementierung der TSF)
 - ADV_LLD.1 (Beschreibender Entwurf auf niedriger Ebene)
 - ALC_TAT.1 (Klar festgelegte Entwicklungswerkzeuge)
 - AVA_MSU.3 (Analysieren und Testen auf unsichere Zustände)
 - AVA_VLA.4 (Hohe Widerstandsfähigkeit)

Da die Evaluierung eine Re-Evaluierung zum Zertifikat BSI-DSZ-CC-0330-2007 darstellt, konnten bestimmte Evaluierungsergebnisse wiederverwendet werden. Diese Re-Evaluierung konzentrierte sich insbesondere auf die sichere Anzeige von TIFF-Dokumenten.

Die Evaluierung hat gezeigt:

- Funktionalität: Produktspezifische Sicherheitsvorgaben; Common Criteria Teil 2 erweitert
- Vertrauenswürdigkeit:
 - Common Criteria Teil 3 konform
 - EAL3 mit Zusatz von
 - ADO_DEL.2 - Erkennung von Modifizierungen
 - ADV_IMP.1 - Teilmenge der Implementierung der TSF
 - ADV_LLD.1 - Beschreibender Entwurf auf niedriger Ebene
 - ALC_TAT.1 - Klar festgelegte Entwicklungswerkzeuge
 - AVA_MSU.3 - Analysieren und Testen auf unsichere Zustände
 - AVA_VLA.4 - Hohe Widerstandsfähigkeit
- Die folgenden Sicherheitsfunktionen erfüllen die behauptete Stärke der Funktionen:
hoch:
SF7 Identifikation und Authentisierung

Die Ergebnisse der Evaluierung gelten nur für den EVG gemäß Kapitel 2 und für die Konfigurationen, die in Kapitel 8 aufgeführt sind.

9.2 Ergebnis der kryptographischen Bewertung

Die Bewertung der Stärke der Funktionen erfolgte ohne Einbeziehung der eingesetzten Kryptoalgorithmen (vgl. §4 Abs. 3 Nr. 2 BSIG). Dies gilt für die folgenden Sicherheitsfunktionen:

- SF1 Unterstützung bei der Erzeugung elektronischer Signaturen
- SF2 Schutz gegen Hashwertmanipulation
- SF3 Verifikation einer elektronischen Signatur
- SF4 Verifikation eines OSCI-Laufzettels bei der Validierung eines Zertifikats
- SF6 Unterstützung bei der Validierung von Zertifikaten
- SF8 Prüftool

10 Auflagen und Hinweise zur Benutzung des EVG

Die in Tabelle 2 genannte Betriebsdokumentation enthält die notwendigen Informationen zur Anwendung des EVG und alle darin enthaltenen Sicherheitshinweise sind zu beachten. Zusätzlich sind die folgenden Auflagen und Hinweise zu beachten:

10.1 Auflagen zur Benutzung des EVG

Der EVG unterstützt nicht die Algorithmen, die zur Erstellung von qualifizierten elektronischen Signaturen gemäß dem Algorithmenkatalog [12] der Bundesnetzagentur zulässig sind. Der EVG darf somit nicht dazu verwendet werden, Dokumente mit der Hashfunktion SHA-1 zu hashen und den Hashwert einer sicheren Signaturerstellungseinheit zur Erzeugung einer qualifizierten elektronischen Signatur zuzuführen, da als Hashfunktion eine Funktion der SHA-2 Familie verwendet werden muss. Der EVG kann somit maximal zur Erzeugung von fortgeschrittenen Signaturen verwendet werden.

10.2 Empfehlungen und Hinweise an den Anwender

Der EVG unterstützt nicht die Algorithmen, die momentan für qualifizierte elektronische Signaturen vorgeschrieben sind. Daher kann der EVG nicht uneingeschränkt zur Prüfung qualifizierter elektronischer Signaturen eingesetzt werden, sondern lediglich solche qualifizierten elektronischen Signaturen prüfen, die in der Vergangenheit mit den von ihm unterstützten Algorithmen erstellt und bei denen die Daten nicht aufgrund von zu schwachen Algorithmen unbemerkt verändert wurden.

Die Webseite des Herstellers (<http://www.bos-bremen.de/index.html>) sollte regelmäßig angesehen werden, da dort Hinweise des Herstellers für die Handhabung des EVGs bereitgestellt werden.

Vor jeder Inbetriebnahme eines OSCI-Clients sollte die Integrität des OSCI-Client-Enablers und ggf. des OSCI-Clients mit dem Prüfwerkzeug geprüft werden. Bei negativen Prüfergebnissen darf die jeweilige Komponente nicht in Betrieb genommen werden.

Die für den OSCI-Manager vorzunehmenden Konfigurationseinstellungen zur Verbindung mit dem Kernsystem und den anzubringenden Signaturen sollten vor Inbetriebnahme explizit auf ihre Richtigkeit überprüft werden.

10.3 Unterstützung von Chipkartenlesern und sicheren Signaturerstellungseinheiten

Die folgenden Tabellen zeigen die Kombinationen aus Betriebssystemen, Chipkartenlesern und sicheren Signaturerstellungseinheiten, die erfolgreich getestet worden und daher Bestandteil dieses Zertifikats sind. Der Wert „OK“ in einer Spalte zeigt dabei, dass die entsprechende Kombination funktionsfähig ist. Der Wert „F“ zeigt, dass die Tests nicht erfolgreich ausgeführt werden konnten.

Windows XP			
Kartenbezeichnung und Bestätigungsnummer	Kartenleser ReinerSCT e:com	Kartenleser ReinerSCT PinPad	Kartenleser Kobil KAAN Pro
Telesec Signaturkarte PKS-Card, Version 3.0 (TUVIT.09339.TE.12.2000)	OK	OK	OK
DATEV Signaturkarte e:secure-Card Version 1.20 (TUVIT.09341.TE.03.2001 (Nachtrag vom 05.03.2001))	OK	OK	OK
Signtrust Signaturkarte SEA-Card, Version 2.0 (TUVIT.09346.TU.03.2001)	OK	OK	OK
Signaturkarte D-TRUST Card Version 1.1, (TUVIT.09361.TE.10.2001 vom 23.10.2001(Nachtrag vom 24.03.2004))	OK	OK	OK
Signaturerstellungseinheit ZKA-Signaturkarte, Version 5.02 der Gemplus-mids GmbH (TUVIT.09385.TU.09.2004)	OK	OK	F
Signaturerstellungseinheit ZKA Banking Signature Card, Version 6.2b NP und 6.2f NP, Type 3 der Giesecke & Devrient GmbH (TUVIT.09395.TU.01.2005)	OK	OK	F

Tabelle 7: Unterstützung von Chipkartenlesern und sicheren Signaturerstellungseinheiten unter Windows XP Professional

Windows 2000			
Kartenbezeichnung und Bestätigungsnummer	Kartenleser ReinerSCT e:com	Kartenleser ReinerSCT PinPad	Kartenleser Kobil KAAN Pro
Telesec Signaturkarte PKS-Card, Version 3.0 (TUVIT.09339.TE.12.2000)	OK	OK	OK
DATEV Signaturkarte e:secure-Card Version 1.20 (TUVIT.09341.TE.03.2001 (Nachtrag vom 25.02.2004))	OK	OK	OK
Signtrust Signaturkarte SEA-Card, Version 2.0 (TUVIT.09346.TU.03.2001)	OK	OK	OK
Signaturkarte D-TRUST-CARD, Version 1.1 (TUVIT.09361.TE.10.2001 (Nachtrag vom 24.03.2004))	OK	OK	OK
Signaturerstellungseinheit ZKA-Signaturkarte, Version 5.02 der Gemplus-mids GmbH (TUVIT.09385.TU.09.2004)	OK	OK	F
Signaturerstellungseinheit ZKA Banking Signature Card, Version 6.2b NP und 6.2f NP, Type 3 der Giesecke & Devrient GmbH (TUVIT.09395.TU.01.2005)	OK	OK	F

Tabelle 8: Unterstützung von Chipkartenlesern und sicheren Signaturerstellungseinheiten unter Windows 2000

Suse Linux 9.3	
Kartenbezeichnung und Bestätigungsnummer	Kartenleser Kobil KAAN Pro
DATEV Signaturkarte e:secure-Card Version 1.20 (TUVIT.09341.TE.03.2001 (Nachtrag vom 25.02.2004))	OK
Signtrust Signaturkarte SEA-Card, Version 2.0 (TUVIT.09346.TU.03.2001)	OK
Signaturkarte D-TRUST-CARD, Version 1.1 (TUVIT.09361.TE.10.2001 (Nachtrag vom 24.03.2004))	OK

Tabelle 9: Unterstützte Chipkartenleser und sichere Signaturerstellungseinheiten unter Suse Linux 9.3

Die o.g. Chipkartenleser sind unter den folgenden IDs bestätigt worden:

- KOBIL KAAN Professional, nur RS232-Version, KOBIL Systems GmbH, (TUVIT.09331.TE.03.2002),
- cyberJack e-com, Version 2.0, nur USB und Windows, Reiner SCT Kartengeräte GmbH & Co. KG (TUVIT.09363.TE.06.2002);

- cyberJack pinpad, Version 2.0, nur USB und Windows, Reiner SCT Kartengeräte GmbH & Co. KG, (TÜVIT.09362.TE.05.2002).

11 Sicherheitsvorgaben

Die Sicherheitsvorgaben [6] werden zur Veröffentlichung in einem separaten Dokument im Anhang A bereitgestellt.

12 Definitionen

12.1 Abkürzungen

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation – Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik
EAL	Evaluation Assurance Level - Vertrauenswürdigkeitsstufe
EVG	Evaluierungsgegenstand (EVG)
IT	Information technologie - Informationstechnologie
ITSEF	Information Technology Security Evaluation Facility – Prüfstelle für IT-Sicherheit
OSCI	Online Services Computer Interface
PP	Protection Profile - Schutzprofil
SF	Security Function - Sicherheitsfunktion
SFP	Security Function Policy – Politik der Sicherheitsfunktion
SOF	Strength of Function – Stärke der Funktion
ST	Security Target – Sicherheitsvorgaben
TOE	Target of Evaluation –Evaluierungsgegenstand
TSC	TSF Scope of Control – Anwendungsbereich der TSF-Kontrolle
TSF	TOE Security Functions - EVG-Sicherheitsfunktionen
TSP	TOE Security Policy - EVG-Sicherheitspolitik

12.2 Glossary

Anwendungsbereich der TSF-Kontrolle - Die Menge der Interaktionen, die mit oder innerhalb eines EVG vorkommen können und den Regeln der TSP unterliegen.

Erweiterung - Das Hinzufügen von funktionalen Anforderungen, die nicht in Teil 2 enthalten sind, und/oder von Vertrauenswürdigkeitsanforderungen, die nicht in Teil 3 enthalten sind, zu den Sicherheitsvorgaben bzw. dem Schutzprofil.

Evaluationsgegenstand - Ein IT-Produkt oder -System - sowie die dazugehörigen Systemverwalter- und Benutzerhandbücher - das Gegenstand einer Prüfung und Bewertung ist.

EVG-Sicherheitsfunktionen - Eine Menge, die die gesamte Hardware, Software, und Firmware des EVG umfasst, auf die Verlass sein muss, um die TSP korrekt zu erfüllen.

EVG-Sicherheitspolitik - Eine Menge von Regeln, die angibt, wie innerhalb eines EVG Werte verwaltet, geschützt und verteilt werden.

Formal - Ausgedrückt in einer Sprache mit beschränkter Syntax und festgelegter Semantik, die auf bewährten mathematischen Konzepten basiert.

Informell - Ausgedrückt in natürlicher Sprache.

Objekt - Eine Einheit im TSC, die Informationen enthält oder empfängt und mit der Subjekte Operationen ausführen.

Schutzprofil - Eine implementierungsunabhängige Menge von Sicherheitsanforderungen für eine Kategorie von EVG, die besondere Anwenderbedürfnisse erfüllen.

Semiformal - Ausgedrückt in einer Sprache mit beschränkter Syntax und festgelegter Semantik.

Sicherheitsfunktion - Ein Teil oder Teile eines EVG, auf die zur Durchsetzung einer hierzu in enger Beziehung stehenden Teilmenge der Regeln der EVG-Sicherheitspolitik Verlass sein muss.

Sicherheitsvorgaben - Eine Menge von Sicherheitsanforderungen und Sicherheitspezifikationen, die als Grundlage für die Prüfung und Bewertung eines angegebenen EVG dienen.

SOF-Hoch - Eine Stufe der EVG-Stärke von Funktionen, bei der die Analyse zeigt, dass die Funktionen einen geeigneten Schutz gegen geplantes oder organisiertes Brechen der EVG-Sicherheit durch Angreifer bieten, die über ein hohes Angriffspotential verfügen.

SOF-Mittel - Eine Stufe der EVG-Stärke von Funktionen, bei der die Analyse zeigt, dass die Funktionen einen angemessenen Schutz gegen naheliegendes oder absichtliches Brechen der EVG-Sicherheit durch Angreifer bieten, die über ein mittleres Angriffspotential verfügen.

SOF-Niedrig - Eine Stufe der EVG-Stärke von Funktionen, bei der die Analyse zeigt, dass die Funktionen einen angemessenen Schutz gegen zufälliges Brechen der EVG-Sicherheit durch Angreifer bieten, die über ein geringes Angriffspotential verfügen.

Stärke der Funktionen - Eine Charakterisierung einer EVG-Sicherheitsfunktion, die den geringsten angenommenen Aufwand beschreibt, der notwendig ist, um deren erwartetes Sicherheitsverhalten durch einen direkten Angriff auf die zugrundeliegenden Sicherheitsmechanismen außer Kraft zu setzen.

Subjekt - Eine Einheit innerhalb des TSC, die die Ausführung von Operationen bewirkt.

Zusatz - Das Hinzufügen einer oder mehrerer Vertrauenswürdigkeitskomponenten aus Teil 3 der CC zu einer EAL oder einem Vertrauenswürdigkeitspaket.

13 Literaturangaben

- [1] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005 - Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Version 2.3 (CC) (ISO/IEC 15408:2005)
- [2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2.3, August 2005 - Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 2.3
- [3] BSI-Zertifizierung: Verfahrensbeschreibung (BSI 7125)
- [4] Anwendungshinweise und Interpretationen zum Schema (AIS), die für den EVG relevant sind ⁸
- [5] Deutsche IT-Sicherheitszertifikate (BSI 7148, BSI 7149), periodisch aktualisierte Liste, die auch auf der Internet-Seite des BSI veröffentlicht wird
- [6] Sicherheitsvorgaben BSI-DSZ-0505-2008, Version 1.1, 11.03.2008, Virtuelle Poststelle des Bundes, Version 2.2.3.x (OSCI), Sicherheitsvorgaben (ST), bremen online services GmbH & Co. KG
- [7] Evaluierungsbericht, Version 1.0, 18.03.2008, Evaluierungsbericht Zertifizierungs-ID: BSI-DSZ-CC-0505-2008 Signaturbestätigungs-ID: BSI.02099.TE.xx.200x, T-Systems GEI GmbH (vertrauliches Dokument)
- [8] Konfigurationsliste, Datei "hashvalues_20080228.txt", 28.02.2008, bremen online services GmbH & Co. KG (vertrauliches Dokument)
- [9] Virtuelle Poststelle des Bundes, Benutzer- und Betriebshandbuch, Release 2.2.3.2, Prüfwerkzeug, Version 2.3.6, 25.02.2008; bremen online services GmbH & Co. KG
- [10] Virtuelle Poststelle des Bundes, Release 2.2.3.2, Betriebshandbuch, Version 2.2.7, 25.02.2008, bremen online services GmbH & Co. KG
- [11] Virtuelle Poststelle des Bundes, Release 2.2.3.2, Entwicklerhandbuch, Version 2.3.4, 25.02.2008, bremen online services GmbH & Co. KG
- [12] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 05.02.2008, Bundesanzeiger Nr. 19, S. 376
- [13] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) vom 16. Mai 2001 (BGBl. I S. 876) zuletzt geändert durch Art. 1 des Ersten Gesetzes zur Änderung des Signaturgesetzes (1. SigÄndG), 04.01.2005, BGBl. Teil I S. 2
- [14] Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) vom 16. November 2001 (BGBl. I S. 3074) zuletzt geändert durch Artikel 2 des 1. Gesetzes zur Änderung des Signaturgesetzes vom 04. Januar 2005 (BGBl. I S. 2)

⁸Inbesondere:

- AIS 34, Version 1.00, 1 Juni 2004, Evaluation Methodology for CC Assurance Classes for EAL5+
- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

- [15] Einheitliche Spezifizierung der Einsatzbedingungen für
Signaturanwendungskomponenten – Arbeitsgrundlage für Entwickler/Hersteller und
Prüf-/Bestätigungsstellen, Bundesnetzagentur für Elektrizität, Gas,
Telekommunikation, Post und Eisenbahnen (Bundesnetzagentur), Version 1.4,
19.07.2005

Dies ist eine eingefügte Leerseite.

C Auszüge aus den Kriterien

Anmerkung: Die folgenden Auszüge aus den technischen Regelwerken wurden aus der englischen Originalfassung der CC Version 2.3 entnommen, da eine vollständige aktuelle Übersetzung nicht vorliegt.

CC Part1:

Conformance results (chapter 7.4)

„The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to CC Part 2 (functional requirements), CC Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

- **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.
- **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

- **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.
- **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

- **Package name Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.
- **Package name Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

- **PP Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.“

CC Part 3:

Protection Profile criteria overview (chapter 8.2)

“The goal of a PP evaluation is to demonstrate that the PP is complete, consistent, technically sound, and hence suitable for use as a statement of requirements for one or more evaluable TOEs. Such a PP may be eligible for inclusion within a PP registry.”

“Assurance Class	Assurance Family
Class APE: Protection Profile evaluation	TOE description (APE_DES)
	Security environment (APE_ENV)
	PP introduction (APE_INT)
	Security objectives (APE_OBJ)
	IT security requirements (APE_REQ)
	Explicitly stated IT security requirements (APE_SRE)

Table 3 - Protection Profile families - CC extended requirements ”

Security Target criteria overview (Chapter 8.3)

“The goal of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.”

“Assurance Class	Assurance Family
Class ASE: Security Target evaluation	TOE description (ASE_DES)
	Security environment (ASE_ENV)
	ST introduction (ASE_INT)
	Security objectives (ASE_OBJ)
	PP claims (ASE_PPC)
	IT security requirements (ASE_REQ)
	Explicitly stated IT security requirements (ASE_SRE)
	TOE summary specification (ASE_TSS)

Table 5 - Security Target families - CC extended requirements ”

Assurance categorisation (chapter 7.5)

“The assurance classes, families, and the abbreviation for each family are shown in Table 1.

Assurance Class	Assurance Family
ACM: Configuration management	CM automation (ACM_AUT)
	CM capabilities (ACM_CAP)
	CM scope (ACM_SCP)
ADO: Delivery and operation	Delivery (ADO_DEL)
	Installation, generation and start-up (ADO_IGS)
ADV: Development	Functional specification (ADV_FSP)
	High-level design (ADV_HLD)
	Implementation representation (ADV_IMP)
	TSF internals (ADV_INT)
	Low-level design (ADV_LLD)
	Representation correspondence (ADV_RCR)
	Security policy modeling (ADV_SPM)
AGD: Guidance documents	Administrator guidance (AGD_ADM)
	User guidance (AGD_USR)
ALC: Life cycle support	Development security (ALC_DVS)
	Flaw remediation (ALC_FLR)
	Life cycle definition (ALC_LCD)
	Tools and techniques (ALC_TAT)
ATE: Tests	Coverage (ATE_COV)
	Depth (ATE_DPT)
	Functional tests (ATE_FUN)
	Independent testing (ATE_IND)
AVA: Vulnerability assessment	Covert channel analysis (AVA_CCA)
	Misuse (AVA_MSU)
	Strength of TOE security functions (AVA_SOF)
	Vulnerability analysis (AVA_VLA)

Table 1: Assurance family breakdown and mapping”

Evaluation assurance levels (chapter 11)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 11.1)

“Table 6 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 7 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Evaluation Assurance Level Components							by
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7	
Configuration management	ACM_AUT				1	1	2	2	
	ACM_CAP	1	2	3	4	4	5	5	
	ACM_SCP			1	2	3	3	3	
Delivery and operation	ADO_DEL		1	1	2	2	2	3	
	ADO_IGS	1	1	1	1	1	1	1	
Development	ADV_FSP	1	1	1	2	3	3	4	
	ADV_HLD		1	2	2	3	4	5	
	ADV_IMP				1	2	3	3	
	ADV_INT					1	2	3	
	ADV_LLD				1	1	2	2	
	ADV_RCR	1	1	1	1	2	2	3	
	ADV_SPM				1	3	3	3	
Guidance documents	AGD_ADM	1	1	1	1	1	1	1	
	AGD_USR	1	1	1	1	1	1	1	
Life cycle support	ALC_DVS			1	1	1	2	2	
	ALC_FLR								
	ALC_LCD				1	2	2	3	
	ALC_TAT				1	2	3	3	
Tests	ATE_COV		1	2	2	2	3	3	
	ATE_DPT			1	1	2	2	3	
	ATE_FUN		1	1	1	1	2	2	
	ATE_IND	1	2	2	2	2	2	3	
Vulnerability assessment	AVA_CCA					1	2	2	
	AVA_MSU			1	2	2	3	3	
	AVA_SOF		1	1	1	1	1	1	
	AVA_VLA		1	1	2	3	4	4	

Table 6: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 11.3)

“Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 11.4)

“Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 11.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed
(chapter 11.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL5) - semiformally designed and tested
(chapter 11.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested
(chapter 11.8)

“Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL7) - formally verified design and tested
(chapter 11.9)

“Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.“

Strength of TOE security functions (AVA_SOF) (chapter 19.3)

“Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.”

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

"Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.”

“Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential.”

D Anhänge

Liste der Anhänge zu diesem Zertifizierungsreport

Anhang A: Die Sicherheitsvorgaben werden in einem eigenen Dokument zur Verfügung gestellt.