Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

BSI-DSZ-CC-0562-2011

zu

Governikus – Teil der Virtuellen Poststelle des Bundes (Verifikationsmodul) Version 3.3.1.3

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

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0562-2011

Signaturanwendungskomponente

Governikus – Teil der Virtuellen Poststelle des Bundes (Verifikationsmodul)
Version 3.3.1.3

von	bremen online services GmbH & Co. KG
PP-Konformität:	Keine
Funktionalität:	Produktspezifische Sicherheitsvorgaben; Common Criteria Teil 2 erweitert
Vertrauenswürdigkeit:	Common Criteria Teil 3 konform EAL3 mit Zusatz von ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.3, AVA_VLA.4

Common Criteria Recognition Arrangement für Komponenten bis EAL4

Common Criteria

Das in diesem Zertifikat genannte IT-Produkt wurde von einer anerkannten Prüfstelle nach der Gemeinsame 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, 15. April 2011

Bundesamt für Sicherheit in der Informationstechnik

Im Auftrag

Bernd Kowalski
Abteilungspräsident

L.S.

SOGIS IT SECURITY CERTIFIED – INFORMATION TECHNOLOGY SECURITY – MUTUAL RECOGNITION AGREEMENT

für Komponenten bis EAL4

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

Dies ist eine eingefügte Leerseite.

Vorbemerkung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat gemäß BSIG[1] 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 das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) vom 14. August 2009, Bundesgesetzblatt I S. 2821

Gliederung

A Zertifizierung....7
1 Grundlagen des Zertifizierungsverfahrens....7
2 Anerkennungsvereinbarungen....7
2.1 Europäische Anerkennung von ITSEC/CC – Zertifikaten (SOGIS-MRA)....7
2.2 Internationale Anerkennung von CC – Zertifikaten (CCRA)....8
3 Durchführung der Evaluierung und Zertifizierung....8
4 Gültigkeit des Zertifikats....9
5 Veröffentlichung....10
B Zertifizierungsbericht....11
1 Zusammenfassung....12
2 Identifikation des EVG....14
3 Sicherheitspolitik....16
4 Annahmen und Klärung des Einsatzbereiches....17
5 Informationen zur Architektur....17
6 Dokumentation....18
7 Testverfahren....19
7.1 Testverfahren des Herstellers....19
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....22
11 Sicherheitsvorgaben....23
12 Definitionen....23
12.1 Abkürzungen....23
12.2 Glossary....24
13 Literaturangaben....26
C Auszüge aus den Kriterien....29
D Anhänge....37

A Zertifizierung

1 Grundlagen des Zertifizierungsverfahrens

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

- BSIG[2]
- BSI-Zertifizierungsverordnung [3]
- BSI-Kostenverordnung [4]
- 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 2.3[5] [1]
- Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 2.3 [2]
- BSI-Zertifizierung: Anwendungshinweise und Interpretationen zum Schema (AIS) [4]
- 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 (SOGIS-MRA)

Das SOGIS-Anerkennungsabkommen (SOGIS-MRA) Version 3 ist im April 2010 in Kraft getreten. Es legt die Anerkennung von Zertifikaten für IT-Produkte auf einer Basisanerkennungsstufe und zusätzlich für IT-Produkte aus bestimmten Technischen Bereichen auf höheren Anerkennungsstufen fest.

Die Basisanerkennungsstufe schließt die Common Criteria (CC) Vertrauenwürdigkeitsstufen EAL1 bis EAL4 und ITSEC Vertrauenwürdigkeitsstufen E1 bis

---

2 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) vom 14. August 2009, Bundesgesetzblatt I S. 2821

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 Informati-onstechnik (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

E3 (niedrig) ein. Der technische Bereich "Smart card and similar Devices" wurde für höhere Anerkennungsstufen definiert. Er schließt Vertrauenswürdigkeitsstufen oberhalb von EAL4 bzw. E3 (niedrig) ein.

Das neue Abkommen wurde zu Beginn von den nationalen Stellen von Deutschland, Finnland, Frankreich, Großbritannien, Niederlande, Norwegen, Schweden und Spanien unterzeichnet.

Im Rahmen dieses Abkommens erkennt das Bundesamt für Sicherheit in der Informationstechnik (BSI) an:

- für die Basisanerkennungsstufe die Zertifikate von Großbritannien, Frankreich, Niederlande und Spanien, die ab April 2010 erteilt wurden.
- für höhere Anerkennungsstufen die Zertifikate für Produkte aus dem Bereich "Smart card and similar Devices" von Großbritannien, Frankreich und den Niederlanden, die ab April 2010 erteilt wurden.

Zusätzlich ist die Anerkennung von Zertifikaten, die für Common Criteria Schutzprofile erteilt werden, Bestandteil des Abkommens.

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

Das erste SOGIS-Anerkennungsabkommen Version 1 (nur ITSEC) trat im März 1998 in Kraft. Es wurde im Jahre 1999 auf Zertifikate nach Common Criteria erweitert (MRA Version 2). Zertifikate, die unter diesen älteren Versionen des Abkommen erteilt wurden, sind weiterhin anerkannt.

2.2 Internationale Anerkennung von CC – Zertifikaten (CCRA)

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 Januar 2009 die nationalen Stellen folgender Nationen beigetreten: Australien, Dänemark, Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Indien, Israel, Italien, Japan, Kanada, Malaysia, Pakistan, 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 Governikus – Teil der Virtuellen Poststelle des Bundes (Verifikationsmodul), Version 3.3.1.3 hat das Zertifizierungsverfahren beim BSI durchlaufen. Es handelt sich um eine Re-Zertifizierung basierend auf BSI-DSZ-CC-504-2008. Für diese Evaluierung wurden bestimmte Ergebnisse aus dem Evaluierungsprozess BSI-DSZ-CC-504-2008 wiederverwendet.

Die Evaluation des Produkts Governikus – Teil der Virtuellen Poststelle des Bundes (Verifikationsmodul), Version 3.3.1.3 wurde von T-Systems GEI GmbH durchgeführt. Die Evaluierung wurde am 01. April 2011 beendet. Das Prüflabor T-Systems GEI GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[6].

Der Antragsteller und Hersteller 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.

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 sich Angriffsmethoden im Laufe der Zeit fortentwickeln, ist es erforderlich, die Widerstandsfähigkeit des Produktes regelmäßig überprüfen zu lassen. Aus diesem Grunde sollte der Hersteller das zertifizierte Produkt im Rahmen des Assurance Continuity-Programms des BSI überwachen lassen (z.B. durch eine Re-zertifizierung). Insbesondere wenn Ergebnisse aus dem Zertifizierungsverfahren in einem nachfolgenden Evaluierung- und Zertifizierungsverfahren oder in einer Systemintegration verwendet werden oder das Risikomanagement eines Anwenders eine regelmäßige Aktualisierung verlangt, wird empfohlen, die Neubewertung der Widerstandsfähigkeit regelmäßig, z.B. jährlich, vorzunehmen.

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.

[6] Information Technology Security Evaluation Facility

5 Veröffentlichung

Das Produkt Governikus – Teil der Virtuellen Poststelle des Bundes (Verifikationsmodul), Version 3.3.1.3 ist in die BSI-Liste der zertifizierten Produkte, die regelmäßig veröffentlicht wird, aufgenommen worden (siehe auch Internet: https://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 werden[7]. 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

Der Evaluierungsgegenstand (EVG) ist das Verifikationsmodul von Governikus. Governikus als Teil der virtuellen Poststelle des Bundes stellt als zentrales Kommunikations-Gateway Sicherheitsdienste für die gesicherte Kommunikation zwischen Behörden und externen Kommunikationspartnern (z. B. Bürger, Wirtschaft und andere Behörden) bereit. Dieses komplexe Produkt wird für die Version 3.3.1.3 in drei Verfahren mit den Evaluationsgegenständen Governikus (Basis) bzw. Basiskomponente (EVG 1, blau markiert in Abbildung 1, Zertifizierungs-ID BSI-DSZ-CC-0654), Governikus (OSCI) bzw. OSCI - Komponente (EVG 2, gelb markiert in Abbildung 1, Zertifizierungs-ID BSI-DSZ-CC-0563) und Governikus (Verifikationsmodul) bzw. Verifikationskomponente (EVG 3, orange markiert in Abbildung 1 und Gegenstand dieses Zertifikats) evaluiert und zertifiziert. Ausschließlich die in Abbildung 1 farblich gekennzeichneten Teile von Governikus sind Bestandteil von Zertifizierungsverfahren. Alle weiteren Anteile, die in Abbildung 1 nicht farblich markiert sind, sind demzufolge nicht Gegenstand einer Zertifizierung.

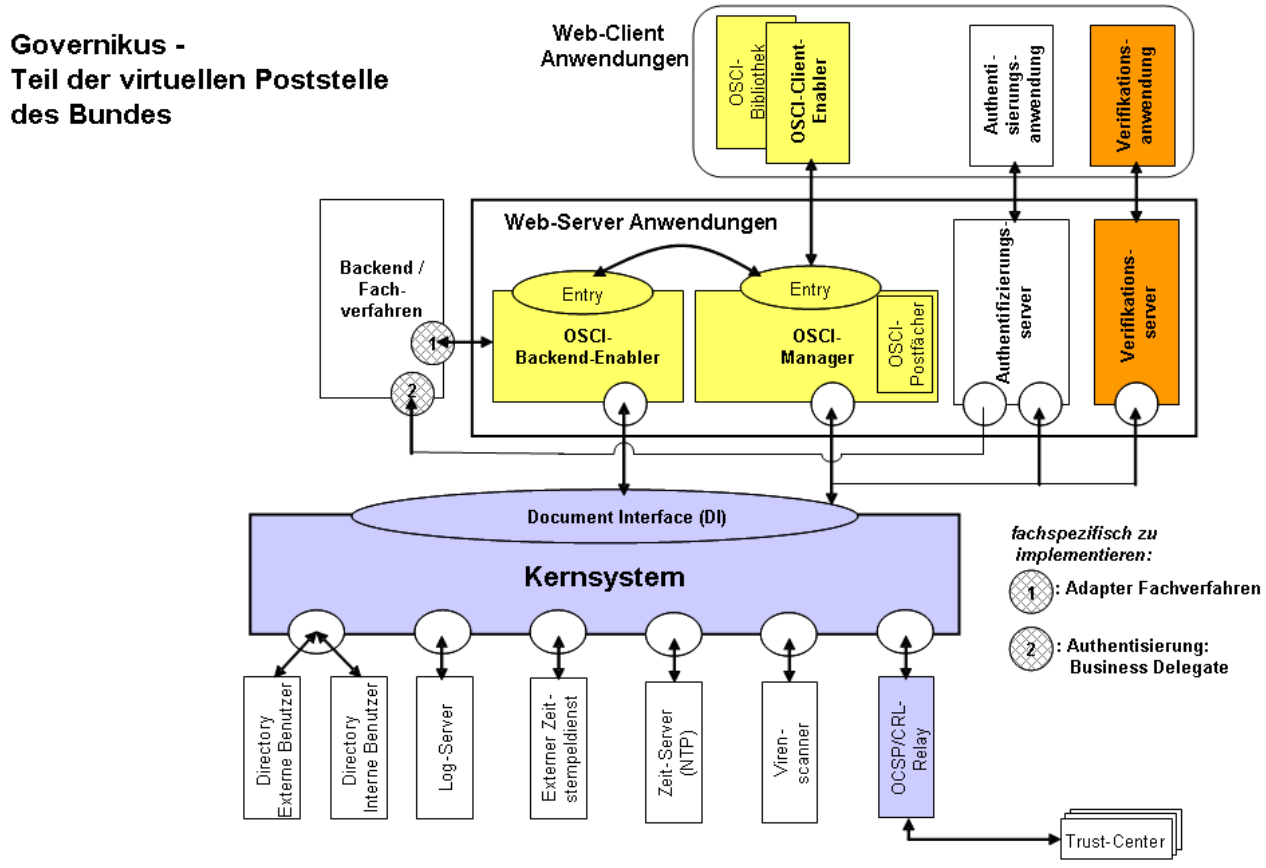

Abbildung 1: Aufbau von Governikus

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.

Die OSCI-Komponente (EVG 2) beinhaltet eine Funktionsbibliothek (OSCI-Client-Enabler) für die sichere Anzeige und das Signieren von Dokumenten am Arbeitsplatz sowie zur Kommunikation über das OSCI-Protokoll. Die weiteren Anteile der OSCI-Komponente bilden eine Funktionsbibliothek zur Integration in ein Fachverfahren (OSCI-Backend-Enabler), die eine Anbindung über das OSCI-Protokoll erlaubt sowie die zentrale Serverkomponente für den Betrieb einer OSCI-konformen IT-Infrastruktur (OSCI-Manager).

Das Verifikationsmodul (EVG 3) ist Gegenstand dieser Evaluierung und umfasst eine Signaturanwendungskomponente für das Verifizieren von Signaturen sowie von Zertifikaten am Arbeitsplatz des Endnutzers. Der EVG besteht aus einer Serverkomponente (Verifikationsserver), einem dazugehörigen Client (Verifikationsanwendung) und einem Tool zur Prüfung der Integrität der Verifikationsanwendung (Prüftool). Der Verifikationsserver wird zentral in einem gesicherten Bereich betrieben, während die Verifikationsanwendung für den Einsatz an Arbeitsplätzen im Home- oder Officebereich geeignet ist. Der Betrieb des EVG erfordert den Zugriff auf die Basiskomponente von Governikus mit Kernsystem und OCSP/CRL-Relay (s. Abbildung 1), wobei die Kommunikation zur Basiskomponente über den Verifikationsserver erfolgt.

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

Die Vertrauenswürdigkeitskomponenten (Security Assurance Requirements SAR) sind dem Teil 3 der Common Criteria entnommen (siehe Teil C oder [1], Teil 3). Der EVG erfüllt die Anforderungen der Vertrauenswürdigkeitsstufe EAL3 mit Zusatz von ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, 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 CC 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
SF.1	Verifikation einer elektronischen Signatur Der EVG prüft eine gegebene Signatur unter Nutzung des mitgelieferten Zertifikats mathematisch. Weiterhin erstellt der EVG eine Anfrage an die Basiskomponente zur Prüfung des Zertifikats. Mit Hilfe der Sicherheitsfunktion SF.2 wird das Ergebnis der Basiskomponente überprüft und mittels SF.3 dem Benutzer authentisch angezeigt.

Sicherheitsfunktion des EVG	Thema
SF.2	Verifikation einer OCSP/CRL-Relay-Antwort bei der Validierung eines Zertifikats Die Antwort des OCSP/CRL-Relays zur Überprüfung eines Zertifikats wird von diesem fortgeschritten elektronisch signiert. Der EVG prüft diese Signatur mit Hilfe hinterlegter Zertifikate nach und stellt somit sicher, dass die Daten von einem authentischen OCSP/CRL-Relay stammen.
SF.3	Sichere und zuverlässige Anzeige Das Verifikationsmodul bietet eine sichere Anzeige für TIFF- und Text-Dateien und stellt weitere Anzeigefunktionen gemäß Signaturgesetz §17, Abs. 2 (wie z.B. für Inhalte des zugehörigen Zertifikats) zur Verfügung.
SF.4	Prüftool Mit Hilfe des Prüftools stellt der EVG dem Benutzer die Möglichkeit zur Verfügung, die Integrität der installierten Komponenten vor Gebrauch zu prüfen.
SF.5	Schutz der Konfigurationsdaten Diese Sicherheitsfunktion zeigt an, wenn die für die Sicherheit der Kommunikation mit dem Verifikationsserver wichtigen Konfigurationsdaten Adresse des Verifikationsservers, Zertifikat des OCSP/CRL-Relays ohne Wissen des Benutzers verändert wurden.

Tabelle 1: Sicherheitsfunktionen des EVG

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

Die in den Sicherheitsvorgaben [6], Kapitel 8.3.4 für bestimmte Funktionen angegebene Stärke der Funktionen “hoch” wird bestätigt.

Die Bewertung der Stärke der Funktionen erfolgte ohne Einbeziehung der für die Ver- und Entschlüsselung eingesetzten Kryptoalgorithmen (vgl. §9 Abs. 4 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:

Governikus – Teil der Virtuellen Poststelle des Bundes (Verifikationsmodul), Version 3.3.1.3

Die folgende Tabelle beschreibt den Auslieferungsumfang, wobei der Wert "Alle" in der Spalte "System" bedeutet, dass der entsprechende Anteil von jedem System des EVG benötigt wird:

Nr	System	Typ	Identifier	Version	Datum	Auslieferungsart
1	Verifikationsanwendung	SW	Governikus Verifikationsmodul	3.3.1.0	5.12.2008	Auf CD-ROM oder als Download
2		SW	verificationclient.war	3.3.1.3	24.09.2009	Download
3		DOC	Governikus - Teil der Virtuellen Poststelle des Bundes – Benutzerhandbuch Verifier, Release 3.3.1.0	3.3.1.0_0	5.12.2008	PDF-Datei auf CD-ROM oder als Download
4		DOC	Plug-in SDK Funktions- und Schnittstellenbeschreibung Verifikationsmodul	3.3.1.0_0	5.12.2008	PDF-Datei auf CD-ROM oder als Download
5		DOC	Verifikationsmodul Funktions- und Schnittstellenbeschreibung	3.3.1.0_0	05.12.2008	PDF-Datei auf CD-ROM oder als Download
6	Verifikationsserver	SW	Governikus Verifikationsmodul	3.3.1.0	05.12.2008	auf CD-ROM oder als Download
7		DOC	Governikus - Teil der Virtuellen Poststelle des Bundes, Release 3.3.1.0, Betriebshandbuch	3.3.1.0_0	05.12.2008	PDF-Datei auf CD-ROM oder als Download
8		DOC	Verifikationsmodul Funktions- und Schnittstellenbeschreibung	3.3.1.0_0	05.12.2008	PDF-Datei auf CD-ROM oder als Download
9	Prüftool	SW	Governikus Verifikationsmodul	3.3.1.0	05.12.2008	auf CD-ROM oder als Download
10		DOC	Governikus - Teil der Virtuellen Poststelle des Bundes – Benutzer- und Betriebshandbuch Prüfwerkzeug, Release 3.3.1.0	3.3.1.0_0	05.12.2008	PDF-Datei auf CD-ROM oder als Download
11	Alle	SW	Kryptoprovider für Governikus bc.gov.server-jdk15-139-bos-0.2.jar		02.09.2009	Download

Tabelle 2: Auslieferungsumfang des EVG

Die grundlegende Version 3.3.1.0 des EVG (s. Tabelle 2, Punkt 1) wird an einen Betreiber von Governikus entweder online oder auf einem nicht wiederbeschreibbaren Medium als zip-Datei ausgeliefert. Um die zertifizierte Version 3.3.1.3 zu installieren, müssen bestimmte Anteile der Version 3.3.1.0 durch neuere Software-Komponenten ersetzt werden. Hierzu muss ein Betreiber die Software in Form eines zip-Paketes für das Release 3.3.1.3 und die Datei aus Punkt 11 in Tabelle 2 aus dem Download-Bereich des Herstellers herunterladen. Der Betreiber muss dann den Hashwert für das Release 3.3.1.3 überprüfen (s.u) und aus dem zip-Paket die Datei aus Punkt 2 in Tabelle 2 extrahieren. Gemäß den Release-Notes und der ReadMe-Datei, die jedem Release beiliegt, ist dann die entsprechende Software, die mit der Version 3.3.1.0 installiert wurde, durch die Software der Punkte 2 und 3 in Tabelle 2 zu ersetzen.

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

Im Falle einer Auslieferung der grundlegenden Version 3.3.1.0 des EVG auf einem nicht wiederbeschreibbaren Medium an einen Betreiber 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. Die beiden anderen Dateien (Punkte 2 und 3 in Tabelle 2) muss er über die Online-Auslieferung beziehen.

Der SHA-1-Hashwert der ausgelieferten zip-Datei für die Version 3.3.1.0 (Governikus_3_3_1_0.zip) lautet:

0E 3C B8 B5 93 47 4E BE 50 46 F7 9D 52 0D 88 31 F9 D8 E8 8C

Der SHA-1 Hashwert für die zip-Datei, die das Release 3.3.1.3 enthält und damit die Datei in Punkt 2 in Tabelle 2 beinhaltet (Governikus_3_3_1_3.zip) lautet:

A1 D1 78 EC 1D 6A 04 AD 4F E5 8B 66 35 CD 2A 38 5B 51 3B A8

Der SHA-1 Hashwert von Punkt 11 (Datei BC139_bos_2.zip) in Tabelle 2 lautet:

50 CB 1A 0B 51 2F 11 7F 5A 30 8F BA DD 2C 53 2C 5F 53 CA 76

Der Betreiber stellt die Verfikationsanwendung dem Endbenutzer zur Verfügung. Mit Hilfe des Prüftools, das der Betreiber dem Endbenutzer über eine gesicherte Webseite zur Verfügung stellen muss, kann der Endbenutzer sich von der Authentizität der installierten Verifikationsanwendung überzeugen.

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 [15] und der – verordnung [16] zu erfüllen. Dabei handelt es sich hauptsächlich um die folgenden Sachverhalte:

- Der EVG zeigt an, dass signierte Daten unverändert sind und welchem Signaturschlüssel-Inhaber die Signatur zugeordnet ist.
- Der EVG zeigt den Inhalt des Zertifikats, auf dem die Signatur beruht sowie die Prüfungsergebnisse des Zertifikats eindeutig an.
- Bei der Anzeige von Daten im 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 von Governikus ist der EVG in der Lage, die Gültigkeit einer elektronischen Signatur zur prüfen.
- Die Prüfung von Zertifikaten durch den EVG ergibt, ob nachgeprüfte Zertifikate im Verzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren. Weiterhin

prüft der EVG, ob zu einem gegebenen Zeitpunkt die im Rahmen der Signatur verwendeten Algorithmen zu den zugelassenen Algorithmen gem. dem Algorithmenkatalog der Bundesnetzagentur [14] gehören.

- 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 Server-Zertifikate mit geeigneten kryptographischen Verfahren zur Absicherung der Kommunikation zwischen den beteiligten Komponenten.

- Die Basiskomponente von Governikus muss entsprechend den Anweisungen in der Benutzerdokumentation installiert und einsatzbereit sein.
- Zum Betrieb von zentral betriebenen Serverkomponenten wird vertrauenswürdiges Personal eingesetzt, das den Verifikationsserver zusammen mit der Basiskomponente in einem vertrauenswürdigen Netz betreibt und sicherstellt, dass die Auflagen aus [17] an einen „geschützten Einsatzbereich (Regelfall/Standardlösung)“ umgesetzt werden.
- Der Endnutzer betreibt die Verifikationsanwendung in einer Umgebung, in der ein Zugriff Unbefugter ausgeschlossen ist oder zumindest mit hoher Sicherheit erkennbar wird und die Anforderungen an einen geschützten Einsatzbereicht gemäß [17] in einer Home- oder Officeumgebung umgesetzt werden.

Details finden sich in den Sicherheitsvorgaben [6], Kapitel 3.

5 Informationen zur Architektur

Die Governikus-Komponente (hier: der EVG) Governikus Verifikationsmodul besteht aus den Teilsystemen

- Verifikationsserver,
- Verifikationsanwendung und
- Prüfwerkzeug (auch Prüftool genannt).

Beim Verifikationsserver handelt es sich um eine Java-Anwendung, die auf einem Server in einem geschützten Bereich (z. B. einem Rechenzentrum) betrieben wird. Die Bedienung erfolgt durch Fachpersonal über Web-Oberflächen (GUIs). Im Regelfall arbeitet der Verifikationsserver im Produktivbetrieb automatisiert und ohne menschliche Aktivitäten.

Die Verifikationsanwendung ist eine Java Web Start-Anwendung, die über einen Link von einem Download-Server geladen und anschließend auf einem Rechner am Arbeitsplatz des Endnutzers betrieben wird. Abbildung 2 stellt das Governikus Verifikationsmodul schematisch ohne das separate Prüftool dar, Abbildung 3 zeigt die Teilsysteme und ihre Schnittstellen.

Der Betrieb des EVG erfordert den Zugriff auf die Basiskomponente von Governikus mit Kernsystem und OCSP/CRL-Relay. Die Kommunikation zur Basiskomponente erfolgt über den Verifikationsserver.

Der EVG wird durch folgende Teilsysteme realisiert, die in Abbildung 3 zusammen mit den externen und internen Schnittstellen illustriert sind:

- Sub_1: Verifikationsanwendung
- Sub_2: Verifikationsserver
- Sub_3: Prüftool
- Sub_4: Administrationsanwendung

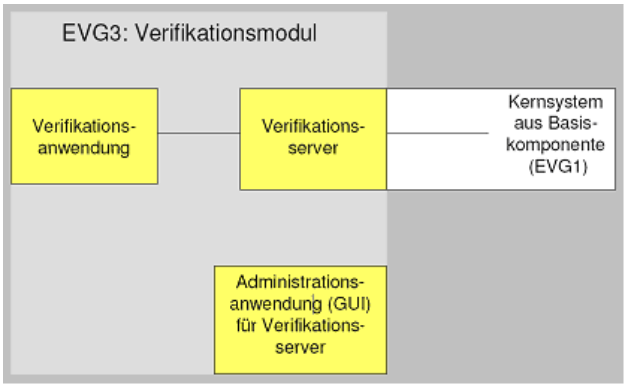

Abbildung 2: Schematischer Aufbau des Verifikationsmoduls (ohne Prüftool)

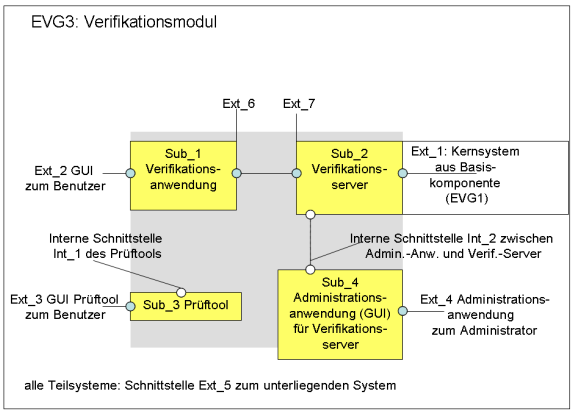

Abbildung 3: Schnittstellen des Verifikationsmoduls

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. Die Tests wurden während der Basisevaluierung vollständig und im Rahmen der aktuellen Re-Evaluierung für die Änderungen insbesondere der Sicherheitsfunktion SF5 "Schutz der Konfigurationsdaten" durchgeführt. Für die Tests wurden die folgenden Konfigurationen verwendet:

Hard- und Software für die Serverkomponenten:

Betriebssystem	**Hardware**	**Sonstiges**
Linux (SuSE Linux Enterprise Server 10)	i386-Architektur (Intel Xeon o.ä)	Java: 1.5.0_16 Application Server: JBoss 4.2.2 GA Datenbank: MySQL 5 Browser Administration: Internet Explorer 7
Windows 2003 Server	i386-Architektur (Intel Xeon o.ä)	Java: 1.5.0_16 Application Server: JBoss 4.2.2 Datenbank: Oracle 10.2.0.4 Browser Administration: Internet Explorer 7

Tabelle 3: Hard- und Software der Serverkomponenten

Hard- und Software der Clientkomponenten:

Betriebssystem	**Hardware**	**Sonstiges**
Linux (OpenSuSE Linux 10.3)	i386-Architektur (Intel Xeon o.ä)	Java: SUN 1.5.0_12
Windows XP	Chipkartenterminal: KOBIL Systems GmbH, KAAN Professional	

Tabelle 4: Hard- und Software der Clientkomponente

7.2 Testverfahren der Prüfstelle

Die Evaluatoren haben die nachfolgend aufgeführten Aktivitäten durchgeführt:

- 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.

Die Evaluatoren haben für alle potentiellen Schwachstellen, die von ihnen identifiziert wurden, Penetrationstests entworfen, um zu erkennen, ob diese potentiellen Schwachstellen in der beabsichtigten Einsatzumgebung des EVGs ausnutzbar sind. Weitere potentielle Schwachstellen wurden durch geeignete Tests des Herstellers abgedeckt. Aufgrund der Änderungen, die in dieser Re-Evaluierung betrachtet wurden, hat die Prüfstelle auf der folgenden Clientkomponente getestet:

Betriebssystem	Hardware	Sonstiges
Windows XP Professional, SP 2	i386 -Architektur, Intel Pentium 4 CPU, 1,8 GHz, 256 MB RAM, 40 GB HDD Chipkartenterminal: KOBIL Systems GmbH, KAAN Professional	Java: SUN 1.5.0_16

Tabelle 5: Hard- und Software der Clientkomponenten

8 Evaluierte Konfiguration

Zur Inbetriebnahme von Governikus sind 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 EAL 3 verwendet. Darüber hinaus wurde die in der AIS 34 [4] definierte Methodologie verwendet.

- Das Urteil PASS der Evaluierung wird für die folgenden Vertrauenswürdigkeits-komponenten bestätigt:
- Alle Komponenten der Klasse ASE
- Alle Komponenten der Vertrauenswürdigkeitsstufe EAL 3 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-504-2008 darstellt, konnten bestimmte Evaluierungsergebnisse wiederverwendet werden. Diese Re-Evaluierung konzentrierte sich insbesondere auf folgende Bereiche:

- Änderung der SF 5, Schutz der Konfiguration, aufgrund der Änderung der Java-Laufzeitumgebung.

Die Evaluierung hat gezeigt:

- PP Konformität: Keine
- Funktionalität: Produktspezifische Sicherheitsvorgaben
  Common Criteria Teil 2 erweitert
- Vertrauenswürdigkeit: Common Criteria Teil 3 konform
  EAL3 mit Zusatz von
  ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1,
  AVA_MSU.3, AVA_VLA.4
- Die folgenden Sicherheitsfunktionen erfüllen die behauptete Stärke der Funktionen: hoch:
  SF 5, Schutz der Konfiguration.

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 folgenden Kryptoalgorithmen werden vom EVG verwendet, um seine Sicherheitspolitik umzusetzen:

- Hashfunktionen:
  - SHA-1, SHA-256, SHA-512 sowie RIPEMD-160
- Algorithmen zur Ver- und Entschlüsselung:
  - RSA mit einer Bitlänge von 1024 oder 2048 Bit

Dies gilt für die folgenden Sicherheitsfunktionen:

- SF1 Verifikation einer elektronischen Signatur
- SF2 Verifikation einer OCSP/CRL-Relay-Antwort bei der Validierung eines Zertifikats
- SF4 Prüftool

Die Stärke der Kryptoalgorithmen wurde im Rahmen der Evaluierung nicht bewertet (vgl. §9 Abs. 4 Nr. 2 BSIG).

Gemäß den Anforderungen der Bundesnetzagentur [14] sind die Kryptoalgorithmen, die in der Sicherheitsfunktionen SF1 zum Einsatz kommt, geeignet für die Prüfung von qualifizierten elektronischen Signaturen. Der Zeitraum, für den diese Einschätzung gilt, ist im offiziellen Katalog [14] angegeben und im Kapitel 10 zusammengefasst.

Die Kryptoalgorithmen, die in den Sicherheitsfunktionen SF2 und SF4 zum Einsatz kommen, beziehen sich lediglich auf elektronische Signaturen und unterliegen daher nicht den Regularien des offiziellen Katalogs [14].

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 alle Aspekte der Annahmen, Bedrohungen und Politiken wie in den Sicherheitsvorgaben dargelegt, die nicht durch den EVG selbst sondern durch die Einsatzumgebung erbracht werden müssen, zu berücksichtigen.

Der Anwender des Produktes muss die Ergebnisse dieser Zertifizierung in seinem Risikomanagmentprozess berücksichtigen. Um die Fortentwicklung der Angriffsmethoden und -techniken zu berücksichtigen, sollte er ein Zeitintervall definieren, in dem eine Neubewertung des EVG erforderlich ist und vom Inhaber dieses Zertifikates verlangt wird.

Zertifizierte Aktualisierungen des EVG, die die Vertrauenswürdigkeit betreffen, müssen verwendet werden sofern sie zur Verfügung stehen. Stehen nicht zertifizierte Aktualisierungen oder Patches zur Verfügung, sollte er den Inhaber dieses Zertifikates auffordern, für diese eine Re-Zertifizierung Zertifizierungen bereitzustellen. In der Zwischenzeit muss der Risikomanagementprozess für das IT-System in dem der EVG eingesetzt wird prüfen und entscheiden, ob noch nicht zertifizierte Aktualisierungen und Patches zu verwenden sind oder zusätzliche Maßnahmen getroffen werden müsse, um die Systemsicherheit Aufrecht zu erhalten.

Die Begrenzung der Gültigkeit der Verwendung der kryptographischen Algorithmen wie in Kapitel 9 dargelegt muss durch den Anwender und seinen Risikomanagementprozess für das IT-System berücksichtigt werden. Für die Hash- und Verschlüsselungsalgorithmen, die im Rahmen der qualifizierten elektronischen Signatur verwendet werden, gelten die folgenden Bedingungen:

Hashalgorithmen	Für die Anwendung bei qualifizierten elektronischen Signaturen erlaubt bis
SHA-224	Ende 2015
SHA-256	Ende 2017
SHA-512	Ende 2017

Tabelle 6: Laufzeit von Hashalgorithmen für qualifizierte elektronische Signaturen

Die Hashalgorithmen SHA-1 und RIPEMD-160 sind lediglich für die Prüfung von qualifizierten Zertifikaten erlaubt bis Ende 2015.

Bitlänge für RSA-Schlüssel	Für die Anwendung bei qualifizierten elektronischen Signaturen erlaubt bis
1976	Ende 2017
2048	Ende 2017

Tabelle 7: Erlaubte Bitlängen für qualifizierte elektronische Signaturen

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.

Die für die Verifikationsanwendung vorzunehmende Konfigurationseinstellung des Verifikationsservers sollte vor Inbetriebnahme explizit auf ihre Richtigkeit überprüft werden. Die für den Verifikationsserver vorzunehmende Konfigurationseinstellungen zur Verbindung mit dem Kernsystem und den anzubringenden Signaturen sollten vor Inbetriebnahme explizit auf ihre Richtigkeit überprüft werden.

Die Integrität der Verifikationsanwendung sollte vor Gebrauch mit dem Prüfwerkzeug geprüft werden. Wenn es dabei zu einem negativen Prüfergebnis kommt, sollte die Verifikationsanwendung nicht verwendet werden.

Zusätzlich sind die folgen Auflagen und Hinweise zu beachten:

- Auf die Einhaltung der Anforderungen entsprechend den Annahmen A.PKI, A.ServerBetrieb und A.ClientBetrieb aus den Sicherheitsvorgaben [6] sowie die besonderen Einsatzbedingungen [17] wird ausdrücklich hingewiesen.
- Die Gültigkeit der Evaluierungsergebnisse für die Verifikationsanwendung und das Prüftool ist gebunden an den Einsatz der unterstützenden Software "Java Development Kit: SUN 1.5.0" ab Version 1.5.0_10.

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

BSIG BSI-Gesetz

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation – Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik

CRL Certificate Revocation List

EAL Evaluation Assurance Level - Vertrauenswürdigkeitsstufe

EVG Evaluierungsgegenstand (EVG)

IT	Information technologie - Informationstechnologie
ITSEF	Information Technology Security Evaluation Facility – Prüfstelle für IT-Sicherheit
OCSP	online certificate status protocol
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.

Online Services Computer Interface - Ein Branchenstandard der öffentlichen Verwaltung für die sichere Transaktion von Geschäftsprozessen über offene Netze, wie bspw. das Internet.

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 Sicherheitsspezifikationen, 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-0562-2011, Version 1.32, 25.09.2009, Governikus - Teil der Virtuellen Poststelle des Bundes, Version 3.3 (Verifikationsmodul), Sicherheitsvorgaben (ST), bremen online services GmbH & Co., KG; datenschutz nord GmbH

[7] Evaluierungsbericht, Version 1.2, 22.03.2011, Evaluation Technical Report Summary (Zusammenfassung), T-Systems GEI GmbH (vertrauliches Dokument)

[10] Konfigurationsliste für den EVG, 11.02.2010, „Governikus - Teil der Virtuellen Poststelle des Bundes, Version 3.3.1.3, Konfigurationsliste, Datei "configurationlist_3313.txt ", bremen online services GmbH & Co. KG (confidential document)

[11] Governikus - Teil der Virtuellen Poststelle des Bundes – Benutzerhandbuch Verifier, Release 3.3.1.0, Dokument-Version 3.3.1.0_0, 05.12.2008; Bremen online services GmbH & Co., KG

[12] Governikus - Teil der Virtuellen Poststelle des Bundes, Release 3.3.1.0, Betriebshandbuch, Dokument-Version 3.3.1.0_0, 05.12.2008; Bremen online services GmbH & Co. KG

[13] Governikus - Teil der Virtuellen Poststelle des Bundes – Benutzer- und Betriebshandbuch Prüfwerkzeug, Release 3.3.1.0, Dokument-Version 3.3.1.0_0, 05.12.2008; Bremen online services GmbH & Co., KG

[14] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), 22. Dezember 2010, veröffentlicht am 01. Februar 2011 im Bundesanzeiger Nr. 17, Seite 383

[15] Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091)

[8] Inbesondere:

- AIS 32, Version 6, 3 August 2010, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, 3. September 2009, Evaluation Methodology for CC Assurance Classes for EAL5+ (CCv2.3 & CCv3.1) and EAL6 (CCv3.1)
- AIS 38, Version 2.0, 28. September 2007, Reuse of evaluation results

[16] Signaturverordnung vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch die Verordnung vom 15. November 2010 (BGBl. I S. 1542)

[17] 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

[18] Verifikationsmodul Funktions- und Schnittstellenbeschreibung Governikus - Teil der virtuellen Poststelle des Bundes, Dokument-Version 3.3.1.0_0, 05.12.2008; Bremen online services GmbH & Co. KG

[19] Plug-in SDK Funktions- und Schnittstellenbeschreibung Governikus - Teil der virtuellen Poststelle des Bundes, Dokument-Version 3.3.1.0_0, 05.12.2008; Bremen online services GmbH & Co. KG

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 evaluatable 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 Components by Evaluation Assurance Level						
		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.

Anhang B: Evaluierungsergebnisse zur Entwicklungs- und Produktionsumgebung

Dies ist eine eingefügte Leerseite.

Anhang B zum Zertifizierungsreport BSI-DSZ-CC-0562-2011

Evaluierungsergebnisse zur Entwicklungs- und Produktionsumgebung

Das IT-Produkt Governikus – Teil der Virtuellen Poststelle des Bundes (Verifikationsmodul), Version 3.3.1.3 (Evaluierungsgegenstand – EVG) wurde von einer anerkannten Prüfstelle nach der Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 2.3 und Anweisungen der Zertifizierungsstelle für Komponenten oberhalb von EAL 4 in Übereinstimmung mit den Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Version 2.3 (CC) (ISO/IEC 15408:2005) evaluiert.

Die folgenden Ergebnisse der Zertifizierung vom 15. April 2011 in Hinsicht auf die Entwicklungs- und Produktionsumgebung wurden erzielt. Die Common Criteria Vertrauenswürdigkeitsanforderungen

- ACM – Konfigurationsmanagement (i.e. ACM_CAP.3, ACM_SCP.1),
- ADO – Auslieferung und Betrieb (i.e. ADO_DEL.2, ADO_IGS.1) und
- ALC – Lebenszyklus-Unterstützung (i.e. ALC_DVS.1, ALC_TAT.1),

sind für die folgenden Entwicklungs- und Produktionsstandorte des EVG erfüllt:

bremen online services GmbH & Co. KG

Am Fallturm 9

28359 Bremen

Für die oben genannten Standorte wurden die Anforderungen in Übereinstimmung mit den Sicherheitsvorgaben [6] erfüllt. Die Evaluatoren bestätigen, dass die Sicherheitsziele und Anforderungen an den EVG-Lebenszyklus bis hin zur Auslieferungen durch die Prozesse an diesen Standorten erfüllt werden (siehe auch das Sicherheitsvorgaben [6]).

Dies ist eine eingefügte Leerseite.