Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

BSI-DSZ-CC-0564-2009

zu

Governikus – Teil der Virtuellen Poststelle des Bundes (Basis) Version 3.3.1.0

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-0564-2009

Signaturanwendungskomponente

Governikus – Teil der Virtuellen Poststelle des Bundes (Basis)
Version 3.3.1.0

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

Common Criteria Recognition Arrangement für Komponenten bis EAL4

Common Criteria

Das in diesem Zertifikat genannte IT-Produkt wurde von einer akkreditierten und lizenzierten 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, 20. März 2009
Bundesamt für Sicherheit in der Informationstechnik
Im Auftrag

IT Security Certified

SOGIS - MRA

Irmela Ruhrmann
Fachbereichsleiterin

L.S.

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

Gliederung

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

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 erstmalig in Kraft getreten (SOGIS-MRA).

Das Abkommen wurde zur gegenseitigen Anerkennung von IT-Sicherheitszertifikaten auf Basis der Common Criteria bis einschließlich der Evaluationsstufe EAL7 erweitert und von den nationalen Stellen der folgenden Staaten unterzeichnet: Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Italien, Niederlande, Norwegen, Schweden und Spanien. Das BSI erkennt die Zertifikate der nationalen Zertifizierungsstellen von

---

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 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

Frankreich und Großbritannien und seit Januar 2009 auch von den Niederlanden 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 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 (Basis),Version 3.3.1.0 Version 3.3.1.0 hat das Zertifizierungsverfahren beim BSI durchlaufen. Es handelt sich um eine Re-Zertifizierung basierend auf BSI-DSZ-CC-0331-2007.

Die Evaluation des Produkts Governikus – Teil der Virtuellen Poststelle des Bundes (Basis),Version 3.3.1.0 Version 3.3.1.0 wurde von T-Systems GEI GmbH durchgeführt. Die Evaluierung wurde am 17. Februar 2009 beendet. Das Prüflabor T-Systems GEI GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[6].

Der Antragsteller und Entwickler 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.

[6] Information Technology Security Evaluation Facility

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 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 Governikus – Teil der Virtuellen Poststelle des Bundes (Basis),Version 3.3.1.0 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 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
DEUTSCHLAND

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 Produkt Governikus – Teil der Virtuellen Poststelle des Bundes. Das Produkt ist eine Weiterentwicklung der Software, die für das Projekt BundOnline 2005 entstanden ist. Es stellt als zentrales Kommunikations-Gateway Sicherheitsdienste für die gesicherte Kommunikation zwischen Behörden und externen Kommunikationspartnern (Bürger, Wirtschaft und andere Behörden) bereit. Das Produkt Governikus wird dazu in drei Verfahren mit den Evaluationsgegenständen Basiskomponente (EVG 1, blau markiert in Abbildung 1 und Gegenstand dieses Zertifiakts), OSCI-Komponente (EVG 2, gelb markiert in Abbildung 1) und Verifikationsmodul (EVG 3, orange markiert in Abbildung 1) evaluiert und zertifiziert. Ausschließlich die in Abbildung 1 farblich gekennzeichneten Teile werden für die Erstellung der qualifizierten elektronischen Signatur benötigt und sind daher Bestandteil von Evaluierungs- und Bestätigungsverfahren. Alle weiteren Anteile, die in Abbildung 1 nicht farblich markiert sind, sind demzufolge nicht Gegenstand einer Evaluierung und Zertifizierung.

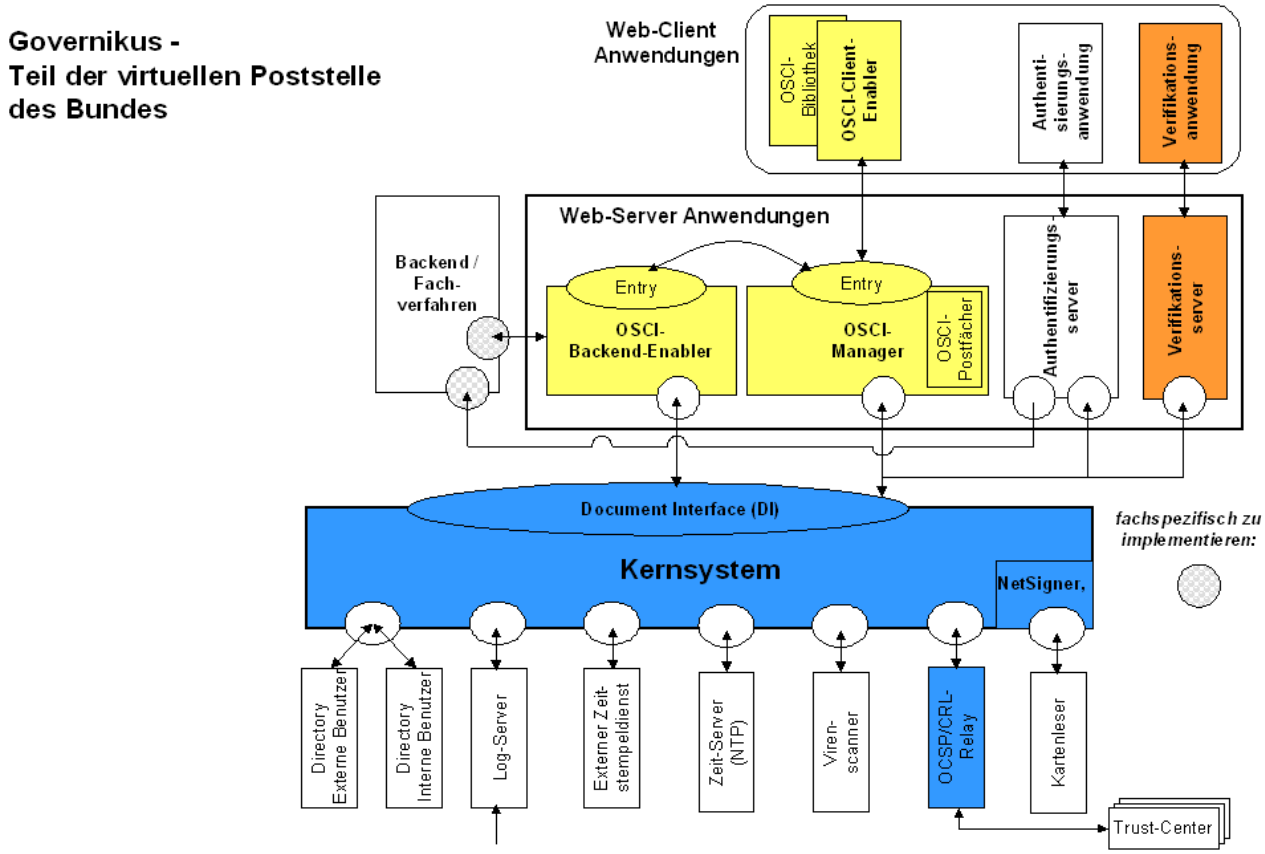

Abbildung 1: Aufbau von Governikus

Die Evaluierung der OSCI-Komponente (EVG 2) beinhaltet eine Funktionsbibliothek (OSCI-Bibliothek, 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) 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).

Bestandteil dieses Zertifikats ist ausschließlich die Basiskomponente (EVG 1), die in Abbildung 1 aus den Teilen Kernsystem mit NetSigner und OCSP/CRL-Relay besteht. Da sowohl die OSCI-Komponente als auch das Verifikationsmodul dem Endnutzer Möglichkeiten zum Zugriff auf Funktionalitäten der Basiskomponente bereitstellen, ist die Evaluierung und Zertifizierung der Basiskomponente Grundlage für eine Nutzung von Governikus im Rahmen der qualifizierten elektronischen Signatur. Die Basiskomponente stellt als zentrale Komponenten folgende Funktionalitäten zur Verfügung:

- Unterstützung bei der Erzeugung qualifizierter elektronischer Batchsignaturen,
- mathematische Prüfung qualifizierter elektronischer Signaturen (Verifikation),
- Statusprüfung qualifizierter Zertifikate (Validierung).

Die wesentlichen Aufgaben der oben genannten Teilsysteme sind:

- Das Kernsystem nimmt Anforderungen von außen über eine Schnittstelle (Document Interface, s. Abbildung 1) an und führt die Verifikation von elektronischen Signaturen durch.
- Der NetSigner ist dafür zuständig, zu signierende Daten der sicheren Signaturerstellungseinheit über einen angeschlossenen Kartenleser zuzuführen. Hierbei können mehrere Kartenleser angeschlossen werden, die Karten unterschiedlicher Signaturschlüssel-Inhaber enthalten können.
- Das OCSP/CRL-Relay stellt die Gültigkeit eines Zertifikats fest und nutzt dazu verschiedene Verzeichnisdienste. Auf ein OCSP/CRL-Relay können neben dem Kernsystem andere Systeme über eine zweite Schnittstelle, die ein anderes Protokoll unterstützt, zugreifen.

Systeme, welche Funktionalitäten der Basiskomponente nutzen wollen und ihre Anfragen gemäß den Vorgaben des Document Interface mit Hilfe von elektronischen Signaturen absichern, werden als autorisiert anfordernde Systeme bezeichnet.

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 and AVA_VLA.4.

Die funktionalen Sicherheitsanforderungen (Security Functional Requirements SFR) an den EVG werden in den Sicherheitsvorgaben [6] Kapitel 5.1 beschrieben. Sie wurden komplett dem Teil der Common Criteria entnommen. Der EVG ist daher konform zum Teil 2 der Common Criteria.

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	Unterstützung bei der Erzeugung qualifizierter elektronischer (Batch-)Signaturen Darunter fällt insbesondere das Zuführen von Hashwerten zu einer sicheren Signaturerstellungseinheit, wobei die Signaturanforderung mit Hilfe von Signaturen auf Basis von Server-Zertifikaten abgesichert wird.
SF.2	Mathematische Prüfung qualifizierter Signaturen Dazu prüft das Kernsystem die mathematische Korrektheit der Signatur mittels zugehörigem Prüfschlüssel (öffentlichem Schlüssel aus qualifiziertem Zertifikat) und geeigneten kryptographischen Verfahren. Anschließend übermittelt der EVG einen entsprechenden Rückgabwert an den Aufrufer.
SF.3	Statusprüfung qualifizierter Zertifikate Mit dieser Sicherheitsfunktion wird gemäß SigG [12] die Prüfung durchgeführt, ob ein nachgeprüftes qualifiziertes Zertifikat im jeweiligen Zertifikatsverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt war.

Tabelle 1: Sicherheitsfunktionen des EVG

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

Die in den Sicherheitsvorgaben [6], Kapitel 8.4.2 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. §4 Abs. 3 Nr. 2 BSIG). Für Details siehe Kap. 9 dieses Berichtes.

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

Der EVG kann in mehreren 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 (Basis),Version 3.3.1.0

Die folgende Tabelle beschreibt den Auslieferungsumfang:

Nr.	Art	Teil	Version	Datum	Art der Auslieferung
1	Software	Governikus Basiskomponente	3.3.1.0	09.12.2008	auf CD-ROM oder als Download
2	Dokument	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
3	Dokument	Governikus - Teil der virtuellen Poststelle des Bundes, Release 3.3.1.0, Schnittstellenbeschreibung des Kernsystems	3.3.1.0_0	05.12.2008	pdf-Datei auf CD-ROM oder als Download

Tabelle 2: Auslieferungsumfang des EVG

Das Produkt wird auf CD-ROM oder online als Archiv an den Betreiber ausgeliefert. Separat von der Auslieferung veröffentlicht der Hersteller einen SHA-1 Wert über die ausgelieferte Software auf einer gesicherten Webseite. Dieser Hashwert ist auch im Anschluss an Tabelle 2 aufgeführt. Bei beiden Auslieferungswegen wird der Empfänger darauf hingewiesen, dass er mit einem geeigneten Werkzeug[8] den Hashwert über die erhaltene Software bilden und mit dem veröffentlichten Wert vergleichen muss.

Der SHA1-Hashwert des ausgelieferten zip-Archivs ist:

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

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 [10] und der –verordnung [11] zu erfüllen. Dabei handelt es sich hauptsächlich um die folgenden Sachverhalte:

- Der EVG zeigt dem Signaturschlüssel-Inhaber an, welches anfordernde System inklusive dessen Zweck (Fachaufgabe) nach Freischalten der Signaturkarte diese zur Erzeugung von Batchsignaturen innerhalb eines festen Zeitfensters oder für eine bestimmte Anzahl von Batchsignaturen nutzen kann.
- Der EVG setzt durch, dass Batchsignaturen nur für die bei der Freischaltung angezeigten anfordernden Systeme innerhalb des festgelegten Zeitfensters oder für eine bestimmte Anzahl erstellt werden.

[8] Der Hersteller nennt als Beispiel das Tool sha1sum, das unter der GPL im Sourcecode und als Binary für alle unterstützten Betriebssysteme erhältlich ist.

- Der EVG stellt fest, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikatverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.
- Der EVG prüft die Korrektheit einer Signatur zuverlässig und gibt das Ergebnis der Prüfung zutreffend zurück.

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 SigG-konformen Komponenten bereitstellen. Dazu gehören insbesondere sichere Signaturerstellungseinheiten mit qualifizierten Zertifikaten und unterstützte Chipkartenleser.
- Zum Betrieb von zentral betriebenen Serverkomponenten wird vertrauenswürdiges Personal eingesetzt, das die Auflagen der Bundesnetzagentur (siehe [13]) an einen „geschützten Einsatzbereich (Regelfall/Standardlösung)“ umsetzt.
- Ein SigG-konformer Verzeichnisdienst für Sperrlisten und Zertifikatsstatusabfragen zur Validierung von qualifizierten Zertifikaten ist vorhanden und es besteht eine Verbindung dorthin.

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

5 Informationen zur Architektur

Wie in Abbildung 2 dargestellt besteht die Basiskomponente aus den Teilsystemen

- Kernsystem mit NetSigner,
- OCSP/CRL-Relay und
- einer Administrationsanwendung als Graphical User Interface (GUI) zur Bedienung.

Auf ein OCSP/CRL-Relay können Systeme auch über eine zweite Schnittstelle, die ein anderes Protokoll unterstützt, zugreifen. Die wesentlichen Aufgaben der Teilsysteme sind:

- Das Kernsystem nimmt Anforderungen von außen über eine Schnittstelle an. Die Anforderungen sind:
  - Unterstützung bei der Erzeugung qualifizierter elektronischer (Batch-) Signaturen;
  - mathematische Prüfung qualifizierter elektronischer Signaturen (Verifikation);
  - Statusprüfung qualifizierter Zertifikate (Validierung).
- Der NetSigner ist dafür zuständig, zu signierende Daten der sicheren Signaturerstellungseinheit über einen angeschlossenen Kartenleser zuzuführen, wobei mehrere Kartenleser angeschlossen sein können, die Karten unterschiedlicher Signaturschlüssel-Inhaber enthalten können.
- Das OCSP/CRL-Relay stellt die Gültigkeit eines Zertifikats fest und nutzt dazu verschiedene Verzeichnisdienste.

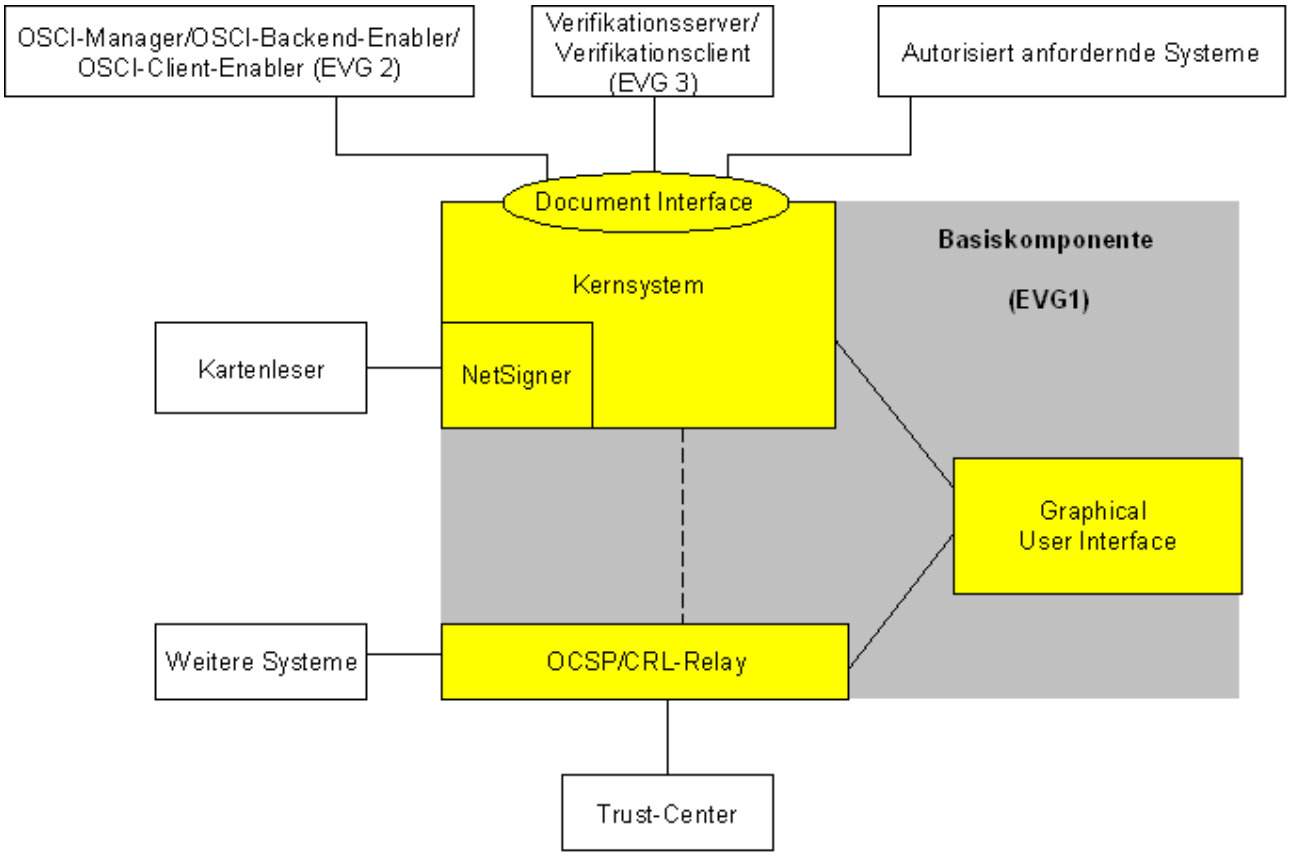

Abbildung 2: Teilsysteme von Governikus

6 Dokumentation

Die evaluierte Dokumentation, die in Tabelle 1 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 gemäß den Anforderungen der Common Criteria dokumentiert und mit den folgenden Hard- und Softwarekomponenten durchgeführt:

Betriebssystem	Hardware	Sonstiges
Windows® 2003 Server	PC mit i386-Architektur (Intel Xeon, Intel D)	Java: ● SUN 1.5.0_10 Application Server: ● JBoss 4.2.2 GA Datenbank: ● MySQL 5, ● Oracle DB 10.2.0.3.0 Chipkartenleser: ● KOBIL Systems GmbH, KAAN Professional ● Reiner SCT Kartengeräte GmbH & Co. KG, „cyberJack ecom“ bzw. „cyberJack pinpad“ Signaturkarte. ● D-TRUST Card_MS Version 1.0
Linux (SuSE Linux Enterprise Server 10)		
Solaris 10	SUN UltraSPARC-Architektur	

Tabelle 3: Hard- und Softwarekomponenten der Herstellertests

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

7.2 Testverfahren der Prüfstelle

Die Evaluatortests wurden auf folgendem System durchgeführt:

Betriebssystem	Hardware	Sonstiges
Windows® 2003 Server, Standard Edition, Service Pack 1	Intel® Pentium® 4 CPU, 3,4 GHz 1 GB RAM 80 GB HDD	Java: ● SUN 1.5.0_16 Application Server: ● JBoss 4.2.2 GA Datenbank: ● MySQL 5, Chipkartenleser: ● KOBIL Systems GmbH, KAAN Professional

Tabelle 4: Hard- und Softwarekomponenten der Prüfstellentests

Die Evaluatoren haben ihre Testaktivitäten folgendermaßen durchgeführt:

- Analyse der Testspezifikationen des Herstellers
- Wiederholung von Herstellertests und Vergleich mit den Testresultaten des Herstellers
- 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 potentielle 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.

Die Ergebnisse zeigen, dass es in den evaluierten Konfigurationen unter Beachtung der evaluierten Benutzerdokumention keine ausnutzbaren Schwachstellen gibt.

8 Evaluierte Konfiguration

Der EVG kann in zwei Konfigurationen betrieben werden, die im Rahmen der Evaluierung beachtet wurden:

- Das Kernsystem und das OCSP-Relay befinden sich in einem vertrauenswürdigen Netz.
- Kernsystem und OCSP-Relay sind über ein WAN miteinander verbunden. In diesem Fall sind insbesondere die Vorgaben aus der Benutzerdokumentation für den sicheren Betrieb dieser Konfiguration zu beachten.

Weiterhin kann die Basiskomponente verschiedene Betriebszustände annehmen. 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 Vertrauenswürdigkeits-komponenten 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-0331-2007 darstellt, konnten bestimmte Evaluierungsergebnisse wiederverwendet werden. Diese Re-Evaluierung konzentrierte sich insbesondere auf die Hinzunahme zusätzlicher Algorithmen für die Signaturprüfung und -erstellung sowie Codeänderungen im Rahmen der Produktpflege.

Die Evaluierung hat gezeigt:

- PP Konformität: Keine
- Funktionalität: Produktspezifische Sicherheitsvorgaben; Common Criteria Teil 2 konform
- Vertrauenswürdigkeit: Common Criteria Teil 3 konform EAL 3 mit Zusatz von ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.3 and AVA_VLA.4

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:

  • RIPEMD-160, SHA-1, SHA-224, SHA-256, SHA-384 sowie SHA-512

– Algorithmen zur Signaturerstellung:

  • RSA mit einer Bitlänge von mindestens 1024 Bit

Dies gilt für die folgenden Sicherheitsfunktionen:

– SF1, Unterstützung bei der Erzeugung qualifizierter elektronischer (Batch-) Signaturen,

– SF2, Mathematische Prüfung qualifizierter Signaturen und

– SF3, Statusprüfung qualifizierter Zertifikate

Die Stärke der Kryptoalgorithmen wurde im Rahmen der Evaluierung nicht bewertet (vgl. §4 Abs. 3 Nr. 2 BSIG). Gemäß den Vorgaben der Bundesnetzagentur [12] sind die Kryptoalgorithmen abgesehen von den folgenden Einschränkungen geeignet für die Erstellung und Prüfung von qualifizierten elektronischen Signaturen:

- SHA-1
- RSA mit einer Schlüssellänge von weniger 1536 Bit

Der Zeitraum, für den diese Einschätzung gilt, ist im offiziellen Katalog [12] angegeben und im Kapitel 10 zusammengefasst.

10 Auflagen und Hinweise zur Benutzung des EVG

10.1 Hinweise für den Benutzer und Betreiber

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 folgen Hinweise zu beachten:

- Insbesondere, jedoch nicht ausschließlich, sollte der benutzte Application Server so konfiguriert werden, dass entfernte Zugriffe auf den Application Server ausgeschlossen sind. Alle Systeme, auf denen Komponenten des EVGs installiert sind, sollten für eine entfernte Administration gesperrt sein, so dass ihre Administration nur lokal durch autorisiertes Personal durchgeführt werden kann.
- Wenn einem Nutzer die Rolle "keyowner" zugewiesen wird, so darf ihm keine weitere Rolle zugewiesen werden. Diese Beschränkung wird durch die Installationsprozedur unterstützt. Diese Einschränkung unterstützt die Rollentrennung zwischen administrativen Nutzern des EVGs und Nutzern, die qualifizierte elektronische Signaturen erzeugen wollen.
- Die Webseite des Herstellers (http://www.bos-bremen.de/index.html) sollte regelmäßig angesehen und beachtet werden, da dort Hinweise des Herstellers für die Handhabung des EVGs bereitgestellt werden.
- Die mit dem EVG ausgelieferte Beispielkonfiguration sollte nur für Testzwecke verwendet werden. Alle Einstellungen der Beispielkonfiguration, die der Betreiber übernehmen möchte, sollten vorher explizit auf ihre Richtigkeit überprüft werden.

10.2 Gültigkeitszeitraum der verwendeten Algorithmen

Zur Erzeugung qualifizierter elektronischer Signaturen werden vom Produkt Governikus – Teil der virtuellen Poststelle des Bundes, Version 3.3.1.0, die Hashfunktionen SHA-224, SHA-256, SHA-384, SHA-512 und RIPEMD-160 bereitgestellt.

Zur Prüfung qualifizierter elektronischer Signaturen werden von der Basiskomponente die Hashfunktionen RIPEMD-160, SHA-224, SHA-256, SHA-384 und SHA-512 sowie der RSA-Algorithmus mit einer Schlüssellänge von mindestens 1536 Bit unterstützt.

Der verwendete Hashalgorithmus RIPEMD-160 wird als geeignet bis Ende 2010 und die verwendeten Hashalgorithmen SHA-224, SHA-256, SHA-384 und SHA-512 werden von der Bundesnetzagentur [12] als geeignet bis Ende 2015 eingestuft.

Die folgende Tabelle zeigt den Gültigkeitszeitraum für die unterschiedlichen Schlüssellängen beim RSA-Algorithmus:

Schlüssellänge	Gültig bis Ende
1536	2009
1728	2010
1976	2015

Tabelle 5: Gültigkeitszeitraum von Schlüssellängen für den RSA-Algorithmus

Für die Gewährleistung eines langfristigen Sicherheitsniveaus wird grundsätzlich die Verwendung von 2048 Bit empfohlen.

10.3 Unterstützte Kombinationen von Chipkartenlesern und Signaturkarten

Für den Betrieb der Basiskomponente können die folgenden SigG-konformen sicheren Signaturerstellungseinheiten und Chipkartenleser verwendet werden.

Signaturerstellungseinheiten:

- Signaturerstellungseinheit STARCOS 3.0
  (Nachträge zur Bestätigung TUVIT.93100.TE.09.2005 vom 08.08.2006, 20.10.2006 und 07.12.2006).
- Signaturerstellungseinheit „Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur “
  (Bestätigung T-Systems.02122.TE.05. 2005).

SigG-konformer Chipkartenleser:

- KOBIL Systems GmbH, KAAN Professional, nur RS232-Version
  (Bestätigungs-ID: TUVIT.09331.TE.03.2002)
- Reiner SCT Kartengeräte GmbH & Co. KG, cyberJack e-com, Version 2.0, nur USB und Windows
  (Bestätigungs-ID: TUVIT.09363.TE.06.2002)
- Reiner SCT Kartengeräte GmbH & Co. KG, cyberJack pinpad, Version 3, nur USB und Windows,
  (Bestätigungs-ID: TUVIT.93107.TU.11.2004)
- Cherry GmbH, Cherry SmartTerminal 2000 U
  (Bestätigungs-ID: BSI.02059.TE.02.2006)
- Omnikey GmbH, Omnikey CardMan 3821 und Omnikey CardMan 3621
  (Bestätigungs-ID: BSI.02057.TE.12.2005)

Die unterstützten Kartenlesegeräte sind nicht auf allen Betriebssystemen gleichermaßen einsetzbar. Es gelten die folgenden Einschränkungen:

- Die Kartenlesegeräte Omnikey CardMan 3821, Omnikey CardMan 3621, Cherry Smartterminal 2000 U werden auf dem Betriebssystem SUN Solaris nicht unterstützt.
- Die Kartenterminals CyberJack e-com und CyberJack pinpad V 3 werden auf den Betriebssystemen SUN Solaris und Suse Linux Enterprise Server nicht unterstützt
- Das Kartenlesegerät Kobil KAAN Prof. unterstützt die Signaturerstellungseinheiten STARCOS 3.0 nicht.

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-Errichtungsgesetz

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

OSCI Online Services Computer Interface

OCSP Online Certificate Status Protocol[9]

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.

[9] siehe auch www.osci.de

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 Sicherheits-spezifikationen, 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 - 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 [10].

[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-0564-2009, Version 1.13, 02.02.2009, Governikus – Teil der virtuellen Poststelle des Bundes, Version 3.3 (Basis), Sicherheitsvorgaben (ST), bremen online services GmbH & Co. KG

[7] Evaluierungsbericht, Version 1.1, 17.02.2009, Evaluierungsbericht Zertifizierungs-ID: BSI-DSZ-CC-0564-200x Signaturbestätigungs-ID: BSI.02013.TE.xx.200x, T-Systems GEI GmbH, (vertrauliches Dokument)

[8] Governikus - Teil der virtuellen Poststelle des Bundes, Version 3.3.1.0, Konfigurationsliste, Datei "configurationList_3310.txt", erhalten am 03.02.2009, bremen online services GmbH & Co. KG (vertrauliches Dokument)

[9] Governikus - Teil der virtuellen Poststelle des Bundes, Release 3.3.1.0, Schnittstellenbeschreibung des Kernsystems, Dokument-Version 3.3.1.0_0, 05.12.2008; Bremen online services GmbH & Co. KG

[10] Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 26. Februar 2007 (BGBl. I S. 179)

[11] Signaturverordnung vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch Artikel 9 Abs. 18 des Gesetzes vom 23. November 2007 (BGBl. I S. 2631)

[12] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 17. November 2008, Veröffentlicht am 27. Januar 2009 im Bundesanzeiger Nr. 13, Seite 346

[13] 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.

[10] Inbesondere:

- 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

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.

Dies ist eine eingefügte Leerseite.