Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

# BSI-DSZ-CC-0930-2014

zu

# SegoAssurance Module, Version 1.2
# (als Teil des Produkts SegoSoft ab Version 7.0.7.0)

der

# Comcotec Messtechnik GmbH

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-0930-2014**

Gesundheitswesen: Software

**SegoAssurance Module**
Version 1.2

| | |
|---|---|
| von | Comcotec Messtechnik GmbH |
| PP-Konformität: | Keine |
| Funktionalität: | Produktspezifische Sicherheitsvorgaben<br>Common Criteria Teil 2 erweitert |
| Vertrauenswürdigkeit: | Common Criteria Teil 3 konform<br>EAL 1 |

Common Criteria
Recognition
Arrangement

Common Criteria

Das in diesem Zertifikat genannte IT-Produkt wurde von einer anerkannten Prüfstelle nach der Gemeinsamen Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 3.1 unter Nutzung der Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Version 3.1 (CC) 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, 19. August 2014

Bundesamt für Sicherheit in der Informationstechnik

Im Auftrag

Bernd Kowalski L.S.
Abteilungspräsident

SOGIS
IT SECURITY CERTIFIED
INFORMATION TECHNOLOGY SECURITY
MUTUAL RECOGNITION AGREEMENT

**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

## 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 (Common Criteria for Information Technology Security Evaluation/CC), Version 3.1[5] [1]
- Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Methodology for Information Technology Security Evaluation/CEM), Version 3.1 [2]
- BSI-Zertifizierung: Anwendungshinweise und Interpretationen zum Schema (AIS) [4]

## 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) Vertrauenswürdigkeitsstufen EAL1 bis EAL4 und ITSEC Vertrauenswürdigkeitsstufen E1 bis E3 (niedrig) ein. Der technische Bereich "smartcard and similar devices" wurde für

---

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 Informationstechnik (BSI-Kostenverordnung-BSI-KostV) vom 3. März 2005, Bundesgesetzblatt I S. 519

5 Bekanntmachung des Bundesministeriums des Innern vom 12. Februar 2007 im Bundesanzeiger, datiert 23. Februar 2007, S. 1941

höhere Anerkennungsstufen definiert. Er schließt Vertrauenswürdigkeitsstufen oberhalb von EAL4 bzw. E3 (niedrig) ein. Des Weiteren erfasst das Anerkennungsabkommen auch erteilte Zertifikate für Schutzprofile (Protection Profiles) basierend auf den Common Criteria.

Seit September 2011 wurde das Abkommen von den nationalen Stellen von Deutschland, Finnland, Frankreich, Großbritannien, Italien, Niederlande, Norwegen, Österreich, Schweden und Spanien unterzeichnet.

Weitere Informationen zum Abkommen und der Entwicklungsgeschichte des Abkommens finden Sie unter www.bsi.bund.de/zertifizierung.

Das SOGIS-MRA-Logo auf dem Zertifikat zeigt, dass das Zertifikat unter den Bedingungen des Abkommens von den oben genannten Nationen 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 September 2011 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 von den oben genannten Nationen anerkannt wird.

## 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 SegoAssurance Module, Version 1.2 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Produkts SegoAssurance Module, Version 1.2 wurde von secuvera GmbH durchgeführt. Die Evaluierung wurde am 16. Juli 2014 beendet. Das Prüflabor secuvera GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[6].

Der Sponsor und Antragsteller ist: Comcotec Messtechnik GmbH

Das Produkt wurde entwickelt von: Comcotec Messtechnik GmbH

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 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.

# 5 Veröffentlichung

Das Produkt SegoAssurance Module, Version 1.2 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] Comcotec Messtechnik GmbH
Gutenbergstraße 3
85716 Unterschleißheim

Dies ist eine eingefügte Leerseite.

# 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 „SegoAssurance Module Version 1.2“ (nachfolgend als SegoAssurance bezeichnet), bei der es sich um einen Teil der Software „SegoSoft-Prozessdokumentation“ handelt. Er umfasst die Erstellung einer signierten Freigabeentscheidung.

In der SegoSoft-Prozessdokumentation werden Prozessdaten von externen Geräten wie Sterilisatoren, Thermodesinfektoren, Inkubatoren und Siegelgeräte dargestellt. Der Benutzer bewertet anhand von physikalischen, chemischen und/oder biochemischen Indikatoren und/oder der Prozessdaten auf Grundlage seines Fachkönnens den Geräteprozess (z. B. die Sterilisation oder Desinfektion von Produkten). Anschließend gibt er den Geräteprozess sowie nach Sichtprüfung das durch den Geräteprozess aufbereitete Produkt frei.

Mittels des SegoAssurance Moduls der SegoSoft-Prozessdokumentation wird die Freigabeentscheidung dieses Benutzers dokumentiert, indem über die Freigabe des Benutzers ein PDF/A-Dokument erzeugt und mit einer digitalen Signatur abgespeichert wird. Hierzu wird das dem Benutzer eindeutig zugeordnete Zertifikat verwendet. Die Freigabeentscheidung des Benutzers kann mittels AdobeReader überprüft werden, indem die Daten des Zertifikats mit den vom SegoAssurance erzeugten Zertifikatsdaten verglichen werden.

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 EAL 1.

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 werden durch die folgende Sicherheitsfunktionalität des EVG umgesetzt:

| Sicherheitsfunktionalität des EVG | Thema |
|---|---|
| Benutzerverwaltung | Benutzerverwaltung mit Erstellung eines eindeutigen Benutzerzertifikats auf Basis des ITU-T-Standards X.509 Version 3. Zur Erstellung des Benutzerzertifikats werden kryptographische Funktionen des Betriebssystems verwendet, die außerhalb des EVG liegen. |
| Dokumentation der Freigabeentscheidung | Dokumentation der Freigabeentscheidung mit einer digitalen Signatur. Die Erzeugung der Signatur findet in der Einsatzumgebung statt, die hierfür notwendigen kryptographischen Funktionen sind nicht Teil des EVG.<br><br>Eine Überprüfung der Signatur des Dokuments (und damit der Freigabeentscheidung) ist nach Import des Comcotec Messtechnik GmbH Wurzel-Zertifikats möglich. Das Wurzel-Zertifikat wird über die Webseite der Comcotec Messtechnik GmbH zum Download zur Verfügung gestellt oder mit der Software ausgeliefert und kann zur |

| Sicherheitsfunktionalität des EVG | Thema |
|---|---|
| | Überprüfung der Signatur des Dokuments über die Freigabeentscheidung verwendet werden. |

Tabelle 1: Sicherheitsfunktionalität des EVG

Mehr Details sind in den Sicherheitsvorgaben [6], Kapitel 6.1 dargestellt.

Dieses Zertifikat umfasst die folgenden Konfigurationen des EVG: SegoAssurance Module Version 1.2 als Teil der Software SegoSoft-Prozessdokumentation ab Version 7.0.7.0. Für mehr Details siehe Kapitel 8.

Die Ergebnisse der Schwachstellenanalyse, wie in diesem Zertifikat bestätigt, erfolgte ohne Einbeziehung der für die Ver- und Entschlüsselung eingesetzten krypthographischen Algorithmen (vgl. §9 Abs. 4 Nr. 2 BSIG). Für Details siehe Kap. 9 dieses Berichtes.

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:

**SegoAssurance Module, Version 1.2**

Die folgende Tabelle beschreibt den Auslieferungsumfang:

| Nr | Typ | Beschreibung | Version | Auslieferungsart |
|---|---|---|---|---|
| 1 | SW | SegoSoft | ab 7.0.7.0 | CD, Download, USB-Stick |
| 2 | SW | SegoAssurance Module | 1.2 | CD, Download, USB-Stick |
| 3 | DOC | SegoSoft Prozessdokumentation Installation und Administration [9] | Stand 13.06.2014 | CD, Download, USB-Stick |
| 4 | DOC | SegoSoft Prozessdokumentation Benutzerhandbuch [10] | Stand 17.06.2014 | CD, Download, USB-Stick |

Tabelle 2: Auslieferungsumfang des EVG

Die Auslieferung des EVG erfolgt per CD oder USB-Stick, sowie per Download.

Um sicherzustellen, dass es sich bei dem ausgelieferten EVG um die unverfälschte evaluierte Konfiguration handelt, beschreibt das Administratorhandbuch [9] im Kapitel "Sicherstellen der System-Integrität" die durchzuführende Prozedur zur Prüfung des EVG durch den Anwender:

- Auf der Webseite des Herstellers[8] erhält der Anwender nach der Übermittlung einer MD5-Prüfsumme als Identifikationsmerkmal seines EVG die SHA-256-Prüfsumme des EVG angezeigt. Diese Prüfsumme muss er mit seiner selbst ermittelten

[8] https://www.segosoft.info/index.php/support/zertifikate.html

SHA-256-Prüfsumme abgleichen. Das Handbuch fordert den Anwender auf, eine Installation nur durchzuführen, wenn beide Prüfsummen übereinstimmen.

- Auf der Webseite www.segosoft.info steht das Wurzel-Zertifikat zum Download bereit, welches für die Überprüfung der Signatur des Dokuments über die Freigabeentscheidung notwendig ist.

Die Authentizität der Handbücher und des Root-Zertifikats können anhand der Prüfsummen in der folgenden Tabelle 3 überprüft werden:

| Typ | Beschreibung | SHA-256-Prüfsumme |
|---|---|---|
| DOC | SegoSoft Handbuch Installation und Administration [9] | 9e0426ff60e29a5eb2ea0be08be94f40c1e35abe1b01d80f879d5dcf414620ad |
| DOC | SegoSoft Benutzerhandbuch [10] | 56e0329e4df471377521a8b248a6c78971daed8e84b301a342450347ef7f70ec |
| DOC | Sicherheitsvorgaben SegoAssurance Module 1.2 | 0c3e49bb9aa74032c9b2b16cbcda65ead7166d3954ac50d316fc9b3ab71ea7fb |
| SW | Comcotec Root-Zertifikat | 2741e18824de90ad035e02b07351c7eec544f50e31894b5c7eafa5e37a9b6758 |

Tabelle 3: SHA-256-Prüfsummen

# 3 Sicherheitspolitik

Die Sicherheitspolitik wird durch die funktionalen Sicherheitsanforderungen ausgedrückt und durch die Sicherheitsfunktionalität des EVG umgesetzt. Sie behandelt die folgenden Sachverhalte:

- Benutzerverwaltung mit Erstellung eines eindeutigen Benutzerzertifikats auf Basis des ITU-T-Standards X.509 Version 3.
- Dokumentation der Freigabeentscheidung durch Anhängen einer digitalen Signatur.

# 4 Annahmen und Klärung des Einsatzbereiches

Teile der Sicherheitsleistung werden nicht durch den EVG selbst abgedeckt. Diese Aspekte setzen voraus, dass bestimmte Sicherheitsziele durch die Einsatzumgebung des EVG erfüllt werden. Hierbei sind die folgenden Punkte relevant:

- Die Administratoren für den EVG und das Betriebssystem sind vertrauenswürdig. Sie sind für die Administration des EVG und des Betriebssystems geschult und halten die Vorgaben der Administrationshandbücher ein. Insbesondere vergeben Sie die Rechte zur Benutzerverwaltung nur an geschultes Personal und weisen die Benutzer in die Verwendung der elektronischen Signatur ein.
- Die Benutzer des EVG sind vertrauenswürdig. Sie sind für die Nutzung des EVG geschult und halten die Vorgaben der Benutzerdokumentation ein. Insbesondere wählen sie sichere Passwörter und halten diese geheim. Die Benutzer quittieren die für Sie erzeugten Zertifikate auf einem Einweisungsformular.
- Die Systeme mit dem EVG sind so untergebracht, dass nur autorisierte Personen hierzu Zugang haben.
- Der EVG benutzt zum Erzeugen von Zertifikaten mit Schlüsselpaaren sowie für die Erstellung digitaler Signaturen Funktionen des Betriebssystems. Die Funktionen des

Betriebssystems werden zur Generierung von kryptografisch sicheren RSA-Schlüsselpaaren, zur Erzeugung und Speicherung von X.509-Zertifikaten, zur Erzeugung von kryptografischen Hashwerten nach SHA-2 sowie zur Erzeugung von digitalen RSA-Signaturen auf Basis der X.509-Zertifikate zur Einbettung in PDF/A-Dokumente verwendet.

- Es wird eine Crypto-Library eingesetzt, die zur Zufallszahlenerzeugung für die Schlüsselerzeugung der Zertifikate geeignet ist.
- Die vom EVG genutzte Hardware stellt über das Betriebssystem eine zuverlässige Zeitangabe zur Verfügung.
- Das Betriebssystem ist vertrauenswürdig, es sind die aktuellen Sicherheitsupdates installiert.

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

# 5 Informationen zur Architektur

Der Evaluierungsgegenstand SegoAssurance ist Teil des Produkts SegoSoft. Zum EVG gehören die Komponenten Benutzerverwaltung und Dokumentation der Freigabeentscheidung in Form eines signierten Freigabedokuments. Alle anderen Komponenten sind nicht Bestandteil des EVG und gehören zu dessen Umgebung.

Die folgende Abbildung zeigt die Komponenten des Evaluierungsgegenstands in der Einsatzumgebung.

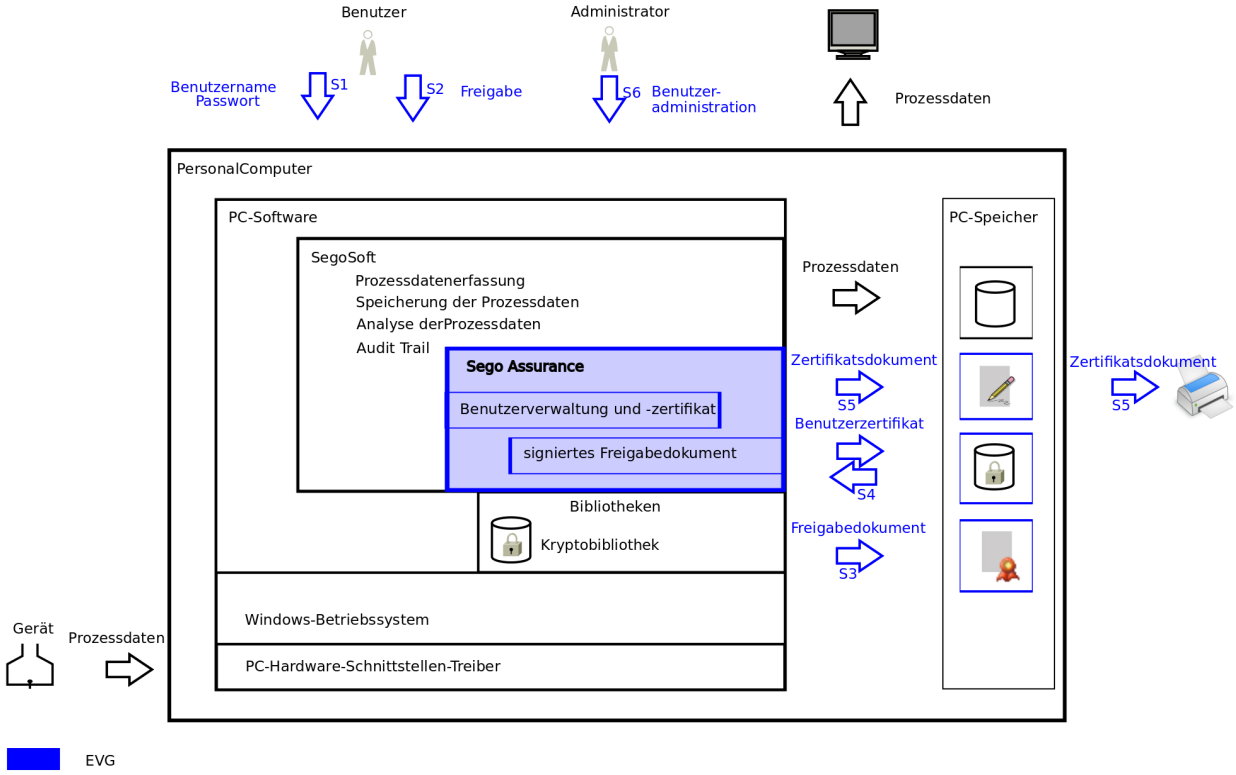


**Abbildung 1: EVG in der Einsatzumgebung**

Der EVG enthält folgende funktionale Komponenten:

- Benutzerverwaltung mit Erstellung eines eindeutigen Benutzerzertifikats auf Basis des ITU-T-Standards X.509 Version 3
- Dokumentation der Freigabeentscheidung mit einer digitalen Signatur

Die Prozessdokumentation SegoSoft enthält zusätzlich zu den Komponenten des EVG folgende funktionale Einheiten, die nicht Bestandteil des Evaluierungsgegenstandes sind:

- Prozessdatenerfassung und -parser
- Speicherung der Prozessdaten
- Analyse der Prozessdaten
- Audit-Trail

Der EVG stellt sechs Schnittstellen in die Umgebung bereit.

- Schnittstelle S1 Benutzername/Passwort: GUI-Schnittstelle zum Benutzer mit Eingabe des Benutzernamens und des Passworts
- Schnittstelle S2 Freigabeentscheidung: GUI-Schnittstelle zum Benutzer mit Eingabe der Freigabeentscheidung
- Schnittstelle S3 Freigabedokument: Schnittstelle zum Freigabedokument in PC-Speicher, Erzeugung eines Freigabe-Dokuments mit einer digitalen Signatur
- Schnittstelle S4 Zertifikatscontainer: Schnittstelle zum Zertifikatscontainer im PC-Speicher, das Benutzer-Zertifikat wird von der Benutzerverwaltung erzeugt, als pfx-Zertifikat im Zertifikatscontainer auf der PC-Hardware gespeichert.
- Schnittstelle S5 Zertifikats-Dokument: Schnittstelle zum Zertifikats-Dokument, nach dem Erzeugen des Benutzer-Zertifikats werden die Daten des Benutzerzertifikats als PDF/A-Dokument ausgegeben (Zertifikatsdokument) und ausgedruckt.
- Schnittstelle S6 Benutzeradministration: Schnittstelle für den Administrator zur Benutzerverwaltung sowie Schnittstelle für den Benutzer zur Änderung des eigenen Passworts.

# 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

Es wurde der EVG SegoAssurance Module in der Version 1.2 getestet. Der EVG ist Teil des größeren Produkts „SegoSoft“. SegoSoft wurde in der Version 7.0.7.0 getestet.

Die Tests wurden in 2 Phasen durchgeführt. Die erste Phase bestand aus den funktionalen Tests. In Phase 2 wurden potenzielle Schwachstellen getestet. Die Tests wurden in den Räumlichkeiten der Prüfstelle durchgeführt.

## 7.1 Test-Konfiguration

Der EVG wurde auf einem Standard-Client mit der folgenden Hardware- und Software-Ausstattung getestet:

- CPU: Intel Celeron 3.2 GHz
- RAM. 2 GB Arbeitsspeicher
- Grafik: Intel GMA 3000, 1280 x 1024 Pixel
- Festplatte: 465 GB (davon 439 GB frei)
- Schnittstellen: USB-Schnittstelle, Ethernet

Es wurde mit den folgenden Betriebssysteme getestet:

- Windows 7 Professional, Service Pack 1
- Windows 8.1 Pro

Des Weiteren war auf dem Test-Client die folgende Software installiert:

- Adobe Reader 11.0.06 (auf Windows 7 Professional)
- Adobe Reader 11.0.07 (auf Windows 8.1 Pro)

Der EVG wurde in Übereinstimmung mit dem SegoSoft Handbuch Installation und Administration [9] installiert. Die Konfiguration ist konsistent mit der im Security Target [6] spezifizierten EVG-Konfiguration.

## 7.2 Testabdeckung

In den funktionalen Tests und den Schwachstellentests werden alle Schnittstellen des EVG abgedeckt. Diese, in Abbildung 1 veranschaulichten Schnittstellen sind:

- S1: Schnittstelle zum Benutzer mit Eingabe des Benutzernamens und des Passworts
- S2 Schnittstelle zum Benutzer mit Eingabe der Freigabeentscheidung
- S3: Schnittstelle zum Freigabedokument in PC-Speicher
- S4: Schnittstelle zum Zertifikatscontainer in PC-Speicher
- S5: Schnittstelle zum Zertifikats-Dokument
- S6: Schnittstelle Benutzeradministration

Es wurde der Großteil der Sicherheitsfunktionen gemäß Sicherheitsvorgaben getestet. Dies betrifft insbesondere Funktionen der Erstellung eines eindeutigen Benutzerzertifikats und der Dokumentation der Freigabeentscheidung mit einer digitalen Signatur. Es erfolgte damit eine weitgehende Testabdeckung aller Funktionen des EVG. Insbesondere werden die besonders sicherheitskritischen Funktionen, wie Benutzerverwaltung, Freigabe und Zertifikatsdokument getestet.

## 7.3 Funktionale Tests

Die funktionalen Tests haben keine Auffälligkeiten ergeben. Die Sicherheitsfunktionen werden vom EVG wie dokumentiert erbracht.

### 7.4 Schwachstellentests

Zur Identifikation von Penetrationstests hat der Evaluator eine strukturierte Schwachstellenanalyse entsprechend AVA_VAN.1 durchgeführt. Zu den identifizierten Bedrohungen wurden Tests konzipiert und durchgeführt. Insbesondere wurde geprüft, ob die Benutzerverwaltung, ein Zertifikat, die Freigabeentscheidung und die externen Crypto-Bibliotheken manipuliert werden können.

Die Schwachstellenanalyse des Evaluators und die durchgeführten Tests haben gezeigt, dass es keine ausnutzbaren Schwachstellen in der angenommenen Einsatzumgebung bei einem Angriffspotenzial von "Basic" gibt.

## 8 Evaluierte Konfiguration

Dieses Zertifikat bezieht sich auf die folgenden Konfigurationen des EVG: Evaluiert wurde der EVG SegoAssurance Module in der Version 1.2. Der EVG ist Teil des größeren Produkts „SegoSoft“. SegoSoft wurde in der Version 7.0.7.0 evaluiert.

Der EVG ist auf Client-PCs mit den Betriebssystemen Windows 7 Professional und Windows 8.1 Pro lauffähig. Zusätzlich wird das Softwarepaket Adobe Acrobat Reader ab Version XI benötigt.

Anforderungen an die Hardware sind:

- CPU-Taktfrequenz mind. 1,6 GHz, empfohlen ab 2,0 GHz
- Hauptspeicher mind. 1 GB, empfohlen 4 GB
- Grafiksystem SVGA mit 1024 x 768 Bildpunkten, 17 Zoll Monitor oder besser
- Festplatte mit mind. 1 GB freiem Speicherplatz, empfohlen ab 10 GB
- CD-ROM-Laufwerk zur Installation
- USB-Schnittstelle zum Anschluss eines Konverterkabels von RS232 auf USB-Schnittstelle, alternativ serielle Schnittstelle nach RS232 (nur relevant bei Anbindung von seriellen Endgeräten)
- Ethernet (nur in Verbindung mit ethernetfähigen Geräten)

## 9 Ergebnis der Evaluierung

### 9.1 CC spezifische Ergebnisse

Der Evaluierungsbericht (Evaluation Technical Report, ETR), [7] wurde von der Prüfstelle gemäß den Gemeinsamen Kriterien [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 1 verwendet.

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

- Alle Komponenten der Vertrauenswürdigkeitsstufe EAL 1 der CC (siehe auch Teil C des Zertifizierungsreports)

Die Evaluierung hat gezeigt:

- PP Konformität: Keine
- Funktionalität: Produktspezifische Sicherheitsvorgaben
  Common Criteria Teil 2 erweitert
- Vertrauenswürdigkeit: Common Criteria Teil 3 konform
  EAL 1

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

Der EVG enthält keine kryptografischen Mechanismen. Folglich waren solche Mechanismen nicht Gegenstand der Evaluierung.

## 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 Sicherheitspolitiken 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 Risikomanagementprozess 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, sollten 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 bereitzustellen. In der Zwischenzeit sollte 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 müssen, um die Systemsicherheit aufrecht zu erhalten.

Zusätzlich sind die folgenden Auflagen und Hinweise zu beachten:

- Die Prüfung der elektronischen Unterschriften der Freigabedokumente darf nur mit dem Adobe Reader ab Version XI erfolgen. Mit älteren Versionen des Adobe Readers ist nicht sichergestellt, dass eine fehlerfreie Verifikation der unterzeichneten Freigabedokumente möglich ist.
- Zugang zum PC-Client dürfen nur vertrauenswürdige Personen besitzen. Daher sind auf dem PC-Client keine Freigaben für nicht vertrauenswürdige Personen anzulegen. Dies gilt insbesondere für Freigaben für „Alle“ und Freigaben, die keine Authentisierung erfordern. Weiterhin ist sicherzustellen, dass per Remote-Administration nur vertrauenswürdige Personen Zugriff haben und die Remote-Administration mit einem ausreichend starken Passwort und starker Verschlüsselung abgesichert ist.
- Zugang zum PC-Client dürfen nur vertrauenswürdige Personen besitzen. Insbesondere dürfen Personen, die nicht oder nicht mehr als vertrauenswürdig erachtet werden keinen lokalen Zugang oder Netzzugang zum PC-Client erhalten, auf dem der EVG läuft.

# 11 Sicherheitsvorgaben

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

# 12 Definitionen

## 12.1 Abkürzungen

**AIS** Anwendungshinweise und Interpretationen zum Schema

**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

**CEM** Common Methodology for IT Security Evaluation – Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik

**EAL** Evaluation Assurance Level - Vertrauenswürdigkeitsstufe

**ETR** Evaluation Technical Report

**EVG** Evaluierungsgegenstand (EVG)

**IT** Information technologie - Informationstechnologie

**ITSEF** Information Technology Security Evaluation Facility – Prüfstelle für IT-Sicherheit

**PDF, PDF/A** Portable Document Format

**PP** Protection Profile - Schutzprofil

**SAR** Security Assurance Requirement - Vertrauenswürdigkeitsanforderungen

**SF** Security Function - Sicherheitsfunktion

**SFP** Security Function Policy – Politik der Sicherheitsfunktion

**SFR** Security Functional Requirement – Funktionale Sicherheitsanforderungen

**SHA** Secure Hash Algorithm

**ST** Security Target – Sicherheitsvorgaben

**TOE** Target of Evaluation –Evaluierungsgegenstand

**TSC** TSF Scope of Control – Anwendungsbereich der TSF-Kontrolle

**TSF** TOE Security Functions - EVG-Sicherheitsfunktionalität

**TSFI** TSF Interface

## 12.2 Glossar

**Erweiterung** - Das Hinzufügen von funktionalen Anforderungen, die nicht in Teil 2 enthalten sind, und/oder von Vertrauenswürdigkeitsanforderungen, die nicht in Teil 3 enthalten sind.

**Evaluationsgegenstand –** Sofware, Firmware und / oder Hardware und zugehörige Handbücher.

**EVG-Sicherheitsfunktionalität** - Eine Menge, die die gesamte Hardware, Software, und Firmware des EVG umfasst, auf die Verlass sein muss, um die SFR durchzusetzen.

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

**Informell** - Ausgedrückt in natürlicher Sprache.

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

**Schutzprofil** - Eine implementierungsunabhängige Menge von Sicherheitsanforderungen für eine Kategorie von EVG.

**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 implementierungsabhängige Menge von Sicherheitsanforderungen für eine Kategorie von EVG.

**Subjekt** - Eine aktive Einheit innerhalb des EVG, die die Ausführung von Operationen auf Objekten bewirkt.

**Zusatz** - Das Hinzufügen einer oder mehrerer Anforderungen zu einem Paket.

# 13 Literaturangaben

[1] Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria for Information Technology Security Evaluation/CC), Version 3.1

[2] Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Methodology for Information Technology Security Evaluation/CEM), Version 3.1

[3] BSI-Zertifizierung: Verfahrensbeschreibung (BSI 7125)

[4] Anwendungshinweise und Interpretationen zum Schema (AIS), die für den EVG relevant sind [9].

[5] Deutsche IT-Sicherheitszertifikate (BSI 7148), periodisch aktualisierte Liste, die auch auf der Internet-Seite des BSI veröffentlicht wird

[6] Sicherheitsvorgaben BSI-DSZ-0930-2014, Version 1.4, 11.07.2014, Sicherheitsvorgaben SegoAssurance Module Version 1.2, Comcotec Messtechnik GmbH

[7] Evaluierungsbericht, Version 3, 15.07.2014, Evaluation Technical Report BSI-DSZ-CC-930 for SegoAssurance Module Version 1.2, secuvera GmbH (vertrauliches Dokument)

[8] Konfigurationsliste für den EVG, Stand 11.07.2014, Konfigurationsliste (vertrauliches Dokument)

[9] Dokumentation für den EVG, 13.06.2014, SegoSoft Prozessdokumentation, Installation und Administration

[10] Dokumentation für den EVG, 17.06.2014, SegoSoft Prozessdokumentation, Benutzerhandbuch

[9] Inbesondere:

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

# C Auszüge aus den Kriterien

Anmerkung: Die folgenden Auszüge aus den technischen Regelwerken wurden aus der englischen Originalfassung der CC Version 3.1 entnommen, da eine vollständige aktuelle Übersetzung nicht vorliegt.

CC Part1:

**Conformance Claim** (chapter 10.4)

“The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - CC Part 3 extended - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in

which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

**Class APE: Protection Profile evaluation** (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

| Assurance Class | Assurance Components |
|---|---|
| Class APE: Protection Profile evaluation | APE_INT.1 PP introduction |
| | APE_CCL.1 Conformance claims |
| | APE_SPD.1 Security problem definition |
| | APE_OBJ.1 Security objectives for the operational environment<br>APE_OBJ.2 Security objectives |
| | APE_ECD.1 Extended components definition |
| | APE_REQ.1 Stated security requirements<br>APE_REQ.2 Derived security requirements |

APE: Protection Profile evaluation class decomposition”

**Class ASE: Security Target evaluation** (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

| Assurance Class | Assurance Components |
|---|---|
| Class ASE: Security Target evaluation | ASE_INT.1 ST introduction |
| | ASE_CCL.1 Conformance claims |
| | ASE_SPD.1 Security problem definition |
| | ASE_OBJ.1 Security objectives for the operational environment<br>ASE_OBJ.2 Security objectives |
| | ASE_ECD.1 Extended components definition |
| | ASE_REQ.1 Stated security requirements<br>ASE_REQ.2 Derived security requirements |
| | ASE_TSS.1 TOE summary specification<br>ASE_TSS.2 TOE summary specification with architectural design summary |

ASE: Security Target evaluation class decomposition

**Security assurance components** (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

| Assurance Class | Assurance Components |
|---|---|
| ADV: Development | ADV_ARC.1 Security architecture description |
| | ADV_FSP.1 Basic functional specification<br>ADV_FSP.2 Security-enforcing functional specification<br>ADV_FSP.3 Functional specification with complete summary<br>ADV_FSP.4 Complete functional specification<br>ADV_FSP.5 Complete semi-formal functional specification with additional error information<br>ADV_FSP.6 Complete semi-formal functional specification with additional formal specification |
| | ADV_IMP.1 Implementation representation of the TSF<br>ADV_IMP.2 Implementation of the TSF |
| | ADV_INT.1 Well-structured subset of TSF internals<br>ADV_INT.2 Well-structured internals<br>ADV_INT.3 Minimally complex internals |
| | ADV_SPM.1 Formal TOE security policy model |
| | ADV_TDS.1 Basic design<br>ADV_TDS.2 Architectural design<br>ADV_TDS.3 Basic modular design<br>ADV_TDS.4 Semiformal modular design<br>ADV_TDS.5 Complete semiformal modular design<br>ADV_TDS.6 Complete semiformal modular design with formal |

| Assurance Class | Assurance Components |
|---|---|
| | high-level design presentation |
| AGD:<br>Guidance documents | AGD_OPE.1 Operational user guidance |
| | AGD_PRE.1 Preparative procedures |
| ALC: Life cycle support | ALC_CMC.1 Labelling of the TOE<br>ALC_CMC.2 Use of a CM system<br>ALC_CMC.3 Authorisation controls<br>ALC_CMC.4 Production support, acceptance procedures and automation<br>ALC_CMC.5 Advanced support |
| | ALC_CMS.1 TOE CM coverage<br>ALC_CMS.2 Parts of the TOE CM coverage<br>ALC_CMS.3 Implementation representation CM coverage<br>ALC_CMS.4 Problem tracking CM coverage<br>ALC_CMS.5 Development tools CM coverage |
| | ALC_DEL.1 Delivery procedures |
| | ALC_DVS.1 Identification of security measures<br>ALC_DVS.2 Sufficiency of security measures |
| | ALC_FLR.1 Basic flaw remediation<br>ALC_FLR.2 Flaw reporting procedures<br>ALC_FLR.3 Systematic flaw remediation |
| | ALC_LCD.1 Developer defined life-cycle model<br>ALC_LCD.2 Measurable life-cycle model |
| | ALC_TAT.1 Well-defined development tools<br>ALC_TAT.2 Compliance with implementation standards<br>ALC_TAT.3 Compliance with implementation standards - all parts |
| | ATE_COV.1 Evidence of coverage<br>ATE_COV.2 Analysis of coverage<br>ATE_COV.3 Rigorous analysis of coverage |
| ATE: Tests | ATE_DPT.1 Testing: basic design<br>ATE_DPT.2 Testing: security enforcing modules<br>ATE_DPT.3 Testing: modular design<br>ATE_DPT.4 Testing: implementation representation |
| | ATE_FUN.1 Functional testing<br>ATE_FUN.2 Ordered functional testing |
| | ATE_IND.1 Independent testing – conformance<br>ATE_IND.2 Independent testing – sample<br>ATE_IND.3 Independent testing – complete |
| AVA: Vulnerability assessment | AVA_VAN.1 Vulnerability survey<br>AVA_VAN.2 Vulnerability analysis<br>AVA_VAN.3 Focused vulnerability analysis<br>AVA_VAN.4 Methodical vulnerability analysis<br>AVA_VAN.5 Advanced methodical vulnerability analysis |

Assurance class decomposition

**Evaluation assurance levels** (chapter 8)

“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 8.1)

“Table 1 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 CC 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 augmented with extended assurance requirements.”

| Assurance Class | Assurance Family | Assurance Components by Evaluation Assurance Level | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | EAL1 | EAL2 | EAL3 | EAL4 | EAL5 | EAL6 | EAL7 |
| Development | ADV_ARC | | 1 | 1 | 1 | 1 | 1 | 1 |
| | ADV_FSP | 1 | 2 | 3 | 4 | 5 | 5 | 6 |
| | ADV_IMP | | | | 1 | 1 | 2 | 2 |
| | ADV_INT | | | | | 2 | 3 | 3 |
| | ADV_SPM | | | | | | 1 | 1 |
| | ADV_TDS | | 1 | 2 | 3 | 4 | 5 | 6 |
| Guidance Documents | AGD_OPE | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | AGD_PRE | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Life cycle Support | ALC_CMC | 1 | 2 | 3 | 4 | 4 | 5 | 5 |
| | ALC_CMS | 1 | 2 | 3 | 4 | 5 | 5 | 5 |
| | ALC_DEL | | 1 | 1 | 1 | 1 | 1 | 1 |
| | ALC_DVS | | | 1 | 1 | 1 | 2 | 2 |
| | ALC_FLR | | | | | | | |
| | ALC_LCD | | | 1 | 1 | 1 | 1 | 2 |
| | ALC_TAT | | | | 1 | 2 | 3 | 3 |
| Security Target Evaluation | ASE_CCL | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | ASE_ECD | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | ASE_INT | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | ASE_OBJ | 1 | 2 | 2 | 2 | 2 | 2 | 2 |
| | ASR_REQ | 1 | 2 | 2 | 2 | 2 | 2 | 2 |
| | ASE_SPD | | 1 | 1 | 1 | 1 | 1 | 1 |
| | ASE_TSS | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Tests | ATE_COV | | 1 | 2 | 2 | 2 | 3 | 3 |
| | ATE_DPT | | | 1 | 1 | 3 | 3 | 4 |
| | ATE_FUN | | 1 | 1 | 1 | 1 | 2 | 2 |
| | ATE_IND | 1 | 2 | 2 | 2 | 2 | 2 | 3 |
| Vulnerability assessment | AVA_VAN | 1 | 2 | 2 | 3 | 4 | 5 | 5 |

Table 1: Evaluation assurance level summary”

**Evaluation assurance level 1 (EAL1) - functionally tested** (chapter 8.3)

“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 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

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.”

**Evaluation assurance level 2 (EAL2) - structurally tested** (chapter 8.4)

“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 practise. 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 8.5)

“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 practises.

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 8.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises 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 8.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises 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 8.8)

“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 8.9)

“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.”

**Class AVA: Vulnerability assessment** (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

**Vulnerability analysis (AVA_VAN)** (chapter 16.1)

"Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

Dies ist eine eingefügte Leerseite.

# 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.