Zertifizierungsreport

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0277-2004

zu

OPENLiMiT SignCubes 1.6, Version 1.6.0.5

der

OPENLiMiT Holding AG

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Telefon +49 228 9582-0, Infoline +49 228 9582-111, Telefax +49 228 9582-455

Deutsches
IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0277-2004

Signaturanwendungskomponente

OPENLiMiT SignCubes 1.6, Version 1.6.0.5

der

OPENLiMiT Holding AG

IT Security Certified

SOGIS-MRA

Das in diesem Zertifikat genannte IT-Produkt wurde von einer akkreditierten und lizenzierten Prüfstelle nach den *Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CC), Version 2.1 (ISO/IEC 15408:1999),* unter Nutzung der *Gemeinsamen Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Teil 1 Version 0.6, Teil 2 Version 1.0*, ergänzt um Final Interpretations in Übereinstimmung mit Common Criteria Version 2.2 und Common Methodology Part 2, Version 2.2 sowie Anweisungen der Zertifizierungsstelle für Komponenten oberhalb von EAL4 evaluiert.

Prüfergebnis:

Funktionalität:	**produktspezifische Sicherheitsvorgaben** **Common Criteria Teil 2 erweitert**
Vertrauenswürdigkeit:	**Common Criteria Teil 3 konform** **EAL3 / mit Zusatz von** **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)**

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.

Die auf der Rückseite aufgeführten Anmerkungen sind Bestandteil dieses Zertifikates.

Bonn, den 19.11.2004

Der Präsident des Bundesamtes für
Sicherheit in der Informationstechnik

Common Criteria

Dr. Helmbrecht L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Telefon (0228) 9582-0 - Telefax (0228) 9582-455 - Infoline (0228) 9582-111

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.

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)
- Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CC), Version 2.1[5]
- Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM)
  - Teil 1, Version 0.6
  - Teil 2, Version 1.0
- BSI-Zertifizierung: Anwendungshinweise und Interpretationen zum Schema (AIS)
- Informationen von der Zertifizierungsstelle zur Methodologie für Vertrauenswürdigkeitskomponenten oberhalb von EAL 4

Die Verwendung der CC Version 2.1, der CEM Teil 2 Version 1 und der Final Interpretations als Teil der AIS 32 ergibt eine Übereinstimmung des Zertifizierungsergebnisses mit CC Version 2.2 und CEM Version 2.2 wie durch die Gremien im CC Anerkennungsabkommen festgelegt.

---

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

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

[4] Kostenverordnung für Amtshandlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Kostenverordnung-BSI-KostV) vom 29. Oktober 1992, Bundesgesetzblatt I S. 1838

[5] Bekanntmachung des Bundesministeriums des Innern vom 22. September 2000 im Bundesanzeiger S. 19445

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. Zertifikate der Unterzeichnerstaaten werden damit in den jeweils anderen Unterzeichnerstaaten anerkannt.

2.1 ITSEC/CC - Zertifikate

Das SOGIS-Abkommen über die gegenseitige Anerkennung von IT-Sicherheitszertifikaten, auf Grundlage der ITSEC, ist am 03. März 1998 in Kraft getreten. Es wurde von den nationalen Stellen der folgenden Staaten unterzeichnet: Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Italien, Niederlande, Norwegen, Portugal, Schweden, Schweiz und Spanien. Das Abkommen wurde zur gegenseitigen Anerkennung von IT-Sicherheitszertifikaten auf Basis der CC bis einschließlich der Evaluationsstufe EAL7 erweitert.

2.2 CC - Zertifikate

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 zwischen den nationalen Stellen in Australien, Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Italien, Kanada, Neuseeland, Niederlande, Norwegen, Spanien und den USA unterzeichnet. Im November 2000 ist Israel der Vereinbarung beigetreten, Schweden im Februar 2002, Österreich im November 2002, Ungarn und Türkei im September 2003, Japan im November 2003.

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 OPENLiMiT SignCubes 1.6, Version 1.6.0.5 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Produkts OPENLiMiT SignCubes 1.6, Version 1.6.0.5 wurde von T-Systems GEI GmbH, Business Unit ITC-Security durchgeführt. Das Prüflabor T-Systems GEI GmbH, Business Unit ITC-Security ist eine vom BSI anerkannte Prüfstelle (ITSEF)[6].

Antragsteller und Vertreiber ist OPENLiMiT Holding AG.

Den Abschluß der Zertifizierung bilden

- die Vergleichbarkeitsprüfung und
- die Erstellung des vorliegenden Zertifizierungsreports.

Diese Arbeiten wurden am 19.11.2004 vom BSI abgeschlossen.

Das bestätigte Vertrauenswürdigkeitspaket gilt nur unter der Voraussetzung, dass

- alle Auflagen bzgl. Generierung, Konfiguration und Betrieb, soweit sie im nachfolgenden Bericht angegeben sind, beachtet werden,
- das Produkt in der beschriebenen Umgebung - sofern im nachfolgenden Bericht angegeben - betrieben wird.

Dieser Zertifizierungssreport gilt nur für die hier angegebene Version des Produktes. Die Gültigkeit kann auf neue Versionen und Releases des Produktes ausgedehnt werden, sofern der Antragsteller eine Re-Zertifizierung des geänderten Produktes entsprechend den Vorgaben beantragt und die Prüfung keine sicherheitstechnischen Mängel ergibt.

Hinsichtlich der Bedeutung der Vertrauenswürdigkeitsstufen und der bestätigten Stärke der Funktionen vgl. die Auszüge aus den technischen Regelwerken am Ende des Zertifizierungsreports.

[6] Information Technology Security Evaluation Facility

4 Veröffentlichung

Der nachfolgende Zertifizierungsbericht enthält die Seiten B-1 bis B-22.

Das Produkt OPENLiMiT SignCubes 1.6, Version 1.6.0.5 ist in die BSI-Liste der zertifizierten Produkte [5], die regelmäßig veröffentlicht wird, aufgenommen worden (siehe auch Internet: http://www.bsi.bund.de). Nähere Informationen sind über die BSI-Infoline 0228/9582-111 zu erhalten.

Weitere Exemplare des vorliegenden Zertifizierungsreports können beim Vertreiber[7] des Produktes angefordert werden. Unter der o. g. Internetadresse kann der Zertifizierungsreport auch in elektronischer Form abgerufen werden.

[7] OPENLiMiT Holding AG, Zuger Straße 76B, 6341 Baar, Schweiz

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.

Gliederung des Zertifizierungsberichtes

1 Zusammenfassung

Der Evaluationsgegenstand ist die Applikation (Signaturanwendungskomponente) OPENLiMiT SignCubes 1.6 , Version 1.6.0.5[8].

Die Applikation OPENLiMiT SignCubes 1.6 ist eine modulare Client Applikation zur Erzeugung und Verifikation digitaler Signaturen auf Microsoft Windows Systemen ab Windows 98. In der Sicherheitsumgebung der Applikation werden eine Smartcard und ein Kartenleser mit sicherer Pin-Eingabe benötigt, um die kryptografischen Operationen zur Signaturerzeugung auf sichere Art und Weise durchzuführen. Die Applikation OPENLiMiT SignCubes 1.6 kann einfache, fortgeschrittene und qualifizierte digitale Signaturen erzeugen. Grundlage für die qualifizierte digitale Signatur sind das Signaturgesetz (SigG) [6] und die Signaturverordnung (SigV) [7].
Die Applikation selbst beschränkt sich auf die Erzeugung von kryptografischen Prüfsummen (Hashwerten) nach den Algorithmen SHA-1 und RIPEMD-160 und kann somit die Integrität und Vertrauenswürdigkeit signierter Daten gemeinsam mit den Komponenten für Sperrlistenprüfung, OCSP-Abfrage und gesicherter Anzeigeeinheit für TIFF- und Text- Dokumente sicherstellen.

Die Applikation OPENLiMiT SignCubes 1.6 besteht aus mehreren Komponenten, die in der folgenden Auflistung aufgeführt werden:

- SignCubes Basiskomponenten für die Erzeugung und Verifikation digitaler Signaturen (SignCubes Security Environment Manager (SSEM)). Der SignCubes Security Environment Manager bildet das Kernstück der Applikation OPENLiMiT SignCubes 1.6 und stellt eine sichere Umgebung für alle sicherheitsrelevanten Vorgänge im EVG zur Verfügung.
- SignCubes Viewer zur Visualisierung von zu signierenden Dokumenten und zur Anzeige signierter Dokumente auf Text und TIFF Basis.
- SignCubes Crypto-Service-Provider zum Einsatz mit Microsoft Outlook und Microsoft Outlook Express.
- SignCubes Shell Extension zur Erweiterung der Funktionen der Microsoft Explorer Kontextmenüs.
- SignCubes Integritätscheck zur Überprüfung der Integrität der installierten Software auf dem Rechner des Anwenders.

Das Produkt OPENLiMiT SignCubes 1.6 ist eine Anwendung, die zur Erzeugung und Verifikation digitaler Signaturen durch den Inhaber eines Signaturzertifikates bestimmt ist. Der Benutzer arbeitet mit verschiedenen grafischen Schnittstellen, die als Produktbestandteile dem Benutzer den Zugang zu den Sicherheitsfunktionen des Produktes erlauben. Als Anwendungsbereich ist

[8] Im Weiteren OPENLiMiT SignCubes 1.6

sowohl der Einsatz durch den Heimanwender als auch der Einsatz in größeren Infrastrukturen, z.B. im behördlichen Umfeld, anzusehen.

Durch die SignCubes Shell Extension wird die nahtlose Integration des Produktes in den Kontext des Microsoft Explorers vorgenommen, die sichere Anzeigeeinheit (SignCubes Viewer) stellt die Funktionen einer Betrachtung und Untersuchung der zu signierenden bzw. signierten TIFF- und Text- Dokumente zur Verfügung. Der SignCubes Crypto-Service-Provider erlaubt die Integration von Signaturmechanismen in die Umgebung eines E-Mail Clients und damit verbunden die Verwendung einer Smartcard für E-Mail Signaturen.

Die Evaluation des Produkts OPENLiMiT SignCubes 1.6 wurde von T-Systems GEI GmbH, Business Unit ITC-Security durchgeführt und am 13.10.2004 abgeschlossen. Das Prüflabor T-Systems GEI GmbH, Business Unit ITC-Security ist eine vom BSI anerkannte Prüfstelle (ITSEF)[9].

Antragsteller und Vertreiber ist die OPENLiMiT Holding AG.

1.1 Vertrauenswürdigkeitspaket

Das Produkt OPENLiMiT SignCubes 1.6 wurde erfolgreich nach den Common Criteria (CC) mit der Prüfstufe **EAL3+** (EAL3 mit Zusatz[10] AVA_VLA.4 (gegen ein hohes Angriffspotential), AVA_MSU.3 (eine vollständige Missbrauchsanalyse), ADV_IMP.1, ADV_LLD.1 und ALC_TAT.1) evaluiert.

1.2 Funktionalität

Kurzbeschreibung:

Das Produkt OPENLiMiT SignCubes 1.6 ist eine modulare[11] Client Applikation. Sie bietet folgende Sicherheitsfunktionalitäten:

- Hashwertberechnung und Anstoß der Erzeugung elektronischer Signaturen mit Zertifikaten unter Verwendung eines Kartenterminals und einer Smartcard.
- Prüfung von Hashwerten und Signaturen unter Verwendung von Sperrlisten und optionaler OCSP-Abfrage.
- Erkennung der Manipulation von Komponenten (Modulen) an der Applikation OPENLiMiT SignCubes 1.6.
- Sicherstellung der Unversehrtheit des OPENLiMiT SignCubes 1.6.
- Sichere Anzeige der zu signierenden und signierten Daten.
- Schutz vor Hashwertverfälschungen.

---

9 Information Technology Security Evaluation Facility

10 Gemäß § 11 Abs. 3 in Verbindung mit Anlage I Nr. 1 SigV.

11 Im Weiteren als Komponente bezeichnet.

Das Produkt OPENLiMiT SignCubes 1.6 läuft auf Basis von Microsoft Windows Systemen ab Windows 98. Mit der Sicherheitsumgebung der Applikation (Smartcard und ein Kartenleser mit sicherer Pin- Eingabe), werden die kryptografischen Operationen zur Signaturerzeugung auf sichere Art und Weise durchgeführt. Für die Erzeugung elektronischer Signaturen sind für die drei Fälle, wie oben bereits erwähnt, **immer** eine Smartcard und ein Kartenleser mit sicherer Pin- Eingabe erforderlich.

Das Produkt OPENLiMiT SignCubes 1.6 erfüllt die Anforderungen gemäß §17 Absatz 2 SigG und §15 Absatz 2 und Absatz 4 SigV.

1.3 Stärke der Funktionen

Die eingesetzten Sicherheitsfunktionen erreichen die Stärke **hoch** (SOF- hoch).

Es wurden vom Hersteller keine expliziten Sicherheitsfunktionen hinsichtlich der Stärke der Funktion bewertet.

1.4 Zusammenfassung der Bedrohungen und der organisatorischen Sicherheitspolitik, auf die das evaluierte Produkt ausgerichtet ist

Bedrohungen
Die Analyse der Bedrohungen gegen den EVG OPENLiMiT SignCubes 1.6 und die durch den EVG zu schützenden Objekte wurde unterstützt durch den Maßnahmenkatalog für technische Komponenten nach dem Signaturgesetz [8][12].

Alle Bedrohungen gehen von einem Angreifer mit einem hohen Angriffpotential aus.

Die zu schützenden Objekte sind: Eine Benutzerdatei, eine signierte Datei und der EVG mit seinen Daten. Bei der Benutzerdatei handelt es sich um jede Datei, die aus Sicht des Benutzers schützenswert ist. Bei der signierten Datei handelt es sich um jede Datei, die mit einer elektronischen Signatur zum Schutz vor z.B. Manipulationen versehen worden ist. Bei dem EVG handelt es sich um ein Softwareprodukt, das i.A. aus ausführbaren Dateien und aus Datendateien (z.B. Zertifikate) besteht.

T.DAT
Manipulation einer Benutzerdatei
Ein Angreifer manipuliert durch beliebige Mittel eine Benutzerdatei und die Manipulation bleibt unerkannt.

Die Bedrohung ist hier bewusst sehr allgemein gehalten worden, da sie sehr verschiedene Szenarien abdecken soll. Der Angreifer kann eine Datei mit Mitteln wie mit einem Editor oder mit einem Netzwerktool während der

12 Es ist anzumerken, dass dieser Maßnahmekatalog sich auf das „alte“ Signaturgesetz (vom 22.07.1997) bezieht. Die Referenzierung auf diesen Maßnahmenkatalog [8] ist dennoch zulässig, weil (nur gering eingeschränkt) die Maßnahmen auf das jetzt gültige Signaturgesetz übertragbar sind.

Datenübertragung usw. manipulieren. Eine Manipulation schließt gezielte und zufällige Veränderungen ein.

T.SIG_DAT

Manipulation einer signierten Datei

Ein Angreifer manipuliert durch beliebige Mittel eine signierte Datei und die Manipulation bleibt unerkannt.

Die Bedrohung ist hier bewusst sehr allgemein gehalten worden, da sie sehr verschiedene Szenarien abdecken soll. Bei der signierten Datei handelt es sich um jede Datei, die mit einer elektronischen Signatur versehen worden ist. Der Angreifer kann den Inhalt der Datei (also einschließlich der Daten der Signatur) mit Mitteln wie mit Editor oder mit einem Netzwerktool während der Datenübertragung usw. manipulieren. Eine Manipulation schließt gezielte und zufällige Veränderungen ein.

T. EVG

Manipulation des EVGs und seiner Daten

Ein Angreifer manipuliert oder tauscht Teile (Module) bzw. Daten des EVGs auf dem Rechner aus und die Manipulation bleibt unerkannt.

Die Manipulation der Teile des EVGs richtet sich direkt gegen die EVG-Software. Der Angreifer mit einem hohen Angriffspotential ändert/vertauscht bei dieser Bedrohung die Programmteile mit der Absicht die Sicherheitsfunktionalität des EVGs zu verändern und damit diese zu deaktivieren, zu umgehen usw.

T.VOR_SIG

Manipulation der Datei vor Entscheidung zu signieren

Ein Angreifer manipuliert durch beliebige Mittel den Inhalt einer Datei, bevor der Benutzer sich entscheidet einen Signaturvorgang einzuleiten und die Manipulation bleibt unerkannt.

Bei der Datei handelt es sich um eine Datei, für die der Benutzer eine Signatur erstellen will. Die Bedrohung geht von einem Angreifer mit einem hohen Angriffpotential aus, der in der Lage ist die Datei zu verändern in dem Zeitraum zwischen der Auswahl der Datei zur Unterschrift durch den Benutzer und der Mitteilung des Benutzers an den EVG, die Datei zu signieren.

T.NACH_SIG

Erzeugung einer gefälschten digitalen Signatur

Ein Angreifer manipuliert den Hashwert nach der Entscheidung des Benutzers, einen Signaturvorgang einzuleiten und die Manipulation bleibt unerkannt.

Die Bedrohung geht von einem Angreifer mit einem hohen Angriffpotential aus, der in der Lage ist, den einer zu signierenden Datei zugeordneten Hashwert zu verändern in dem Zeitraum zwischen der Mitteilung des Benutzers an den EVG, die Datei zu signieren und der Übergabe des Hashwertes an die Signaturkarte zur Erzeugung der elektronischen Signatur. Der Angreifer kann z.B. den Hashwert auf der Übertragungsleitung zu der Signaturkarte verändern.

Organisatorische Sicherheitspolitik

Für den EVG ist keine organisatorische Sicherheitspolitik definiert.

1.5 Spezielle Konfigurationsanforderungen

Der EVG OPENLiMiT SignCubes 1.6 ist eine Softwareapplikation und wird eindeutig durch eine Konfigurationsliste im Dokument [9] bestimmt.

Die Konfiguration des EVGs und die technische Einsatzumgebung können aus Kap. 1.6, 4.2 oder den Sicherheitsvorgaben [10] entnommen werden.

Bei der Installation des Produktes bestehen für den Benutzer aufgrund einer festen Konfiguration keine Einstellmöglichkeiten.

1.6 Annahmen über die Einsatzumgebung

Die Softwareapplikation OPENLiMiT SignCubes 1.6 läuft nur auf bestimmten Hardwareplattformen.

Des weiteren gelten bestimmte Anforderungen an das Personal, der Anbindung des EVGs an Netzwerke und für den physikalischen Zugriff.

Nähere Informationen, siehe Kapitel 4.2 und Kapitel 8.

1.7 Gewährleistungsausschluß

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 ausgelieferte EVG OPENLiMiT SignCubes 1.6 besteht aus den folgenden Teilen:

	Art	Teil	Version	Datum	Art der Auslieferung
1	Software	OPENLiMiT SignCubes 1.6	V1.6.0.5	29.07.2004	auf CD-ROM oder als Download

2	Dokumentation (deutsch und englisch)	Benutzerdokumentation, OPENLiMiT SignCubes 1.6, Version 1.6.0.5, OPENLiMiT SignCubes 1_6 Benutzerdokumentation.chm; OPENLiMiT SignCubes 1_6 User Documentation.chm	V1.6.0.5	01.10.2004 04.10.2004	Windowshilfe-Datei auf CD-ROM oder als Download

3 Sicherheitspolitik

Sicherheitsziele für den EVG

OT. DAT

Schutz einer Benutzerdatei

Der EVG muss einen Schutz gegen die Manipulation einer vom Benutzer definierten Datei durch die Errechnung eines Hashwertes über die Daten der Datei anbieten.

OT.SIG_DAT

Schutz einer signierten Datei

Der EVG muss es dem Benutzer ermöglichen, eine Manipulation einer signierten Datei zu erkennen.

OT. EVG

Schutz des EVGs

Der EVG muss es dem Benutzer ermöglichen, Manipulationen seiner Komponenten bzw. seiner Daten zu erkennen.

OT.VOR_SIG

Schutz der Datei vor Entscheidung zu signieren

Der EVG soll eine Datei dem Benutzer derart darstellen, dass der Benutzer in der Lage ist, den Inhalt der Datei eindeutig zu erkennen.

OT.NACH_SIG

Schutz vor Fälschung der Signatur

Der EVG muss es dem Benutzer ermöglichen, eine Manipulation des Hashwertes einer zu unterschreibenden Datei nach Erzeugung der Signatur, zu erkennen.

Sicherheitsziele für die Umgebung des EVGs

Die Sicherheitsziele für die Umgebung des EVGs sind aus den Annahmen der EVG-Sicherheitsumgebung und aus der Bedrohung T.DAT abgeleitet.

OE.Plattform

Es muss durch geeignete organisatorische Maßnahmen sichergestellt werden, dass der Benutzer als Hardwareplattform einen Intel 586 kompatiblen Rechner,

der über mindestens 64 MB RAM und 60 MB freien Festplattenplatz verfügt, verwendet.

Es muss durch geeignete organisatorische Maßnahmen sichergestellt werden, dass der Benutzer auf dem Rechner eines der folgenden Betriebssysteme installiert: Microsoft Windows 98, Microsoft Windows 98 SE, Windows ME, Windows NT 4.0 mit Servicepack 6.0, Windows 2000 oder Windows XP. Des weiteren muss sichergestellt sein, dass der Internet Explorer ab Version 4.01 SP2 mit der Shell32.dll ab Version 4.0 und die Microsoft Smartcard Base Components ab Version 1.0 auf dem Rechner installiert sind.

Es muss durch geeignete organisatorische Maßnahmen sichergestellt werden, dass alle Komponenten des Betriebssystems und alle sonstig installierte Software korrekt und vertrauenswürdig sind.

Es muss durch geeignete organisatorische Maßnahmen sichergestellt werden, dass ein sicheres Signaturerzeugungssystem, welche aus Kartenleser mit sicherer Pin-Eingabe und Smartcard besteht, verwendet wird und dass eine der folgenden SigG [6] konformen Smartcards entsprechend den Vorgaben des Herstellers eingesetzt wird:

- TeleSec E4Netkey-Karte
- OPENLiMiT Karte als spezielle Konfiguration einer TeleSec E4NetKey-Karte
- TeleSec PKS Karte

Es muss durch geeignete organisatorische Maßnahmen sichergestellt werden, dass einer der folgenden Kartenleser mit sicherer Pin-Eingabe (Anmerkung: der EVG bietet keine Funktionalität zur Pin-Prüfung an) entsprechend den Vorgaben des Herstellers eingesetzt wird:

- Cherry SmartBoard G83-6700
- SCMMicrosystems SPx32/ChipDrive Pin-Pad
- Reiner SCT CyberJack e-com Version 2.0
- Reiner SCT CyberJack pinpad Version 2.0.

Bei den verwendeten peripheren Komponenten werden ausschliesslich im Sinne des SigG [6] bestätigte Komponenten verwendet, die zugehörigen Bestätigungen für diese Produkte können von den Seiten der RegTP bezogen werden (www.regtp.de).

OE.Personal

Es muss durch geeignete organisatorische Maßnahmen sichergestellt werden, dass der Benutzer, der Administrator und das Wartungspersonal vertrauenswürdig sind und die Anweisungen in der Benutzerdokumentation des EVGs befolgen. Insbesondere prüft der Benutzer die Integrität des EVGs entsprechend der Benutzerdokumentation [12].

OE.Netzwerk

Es muss durch geeignete organisatorische Maßnahmen sichergestellt werden in dem Fall, dass der Rechner an das Internet angeschlossen ist, z.B. durch die Verwendung einer Firewall, dass keine Systemdienste oder Systemkompo-

nenten durch Zugriffe aus dem Internet kompromitiert werden können. Weiterhin, dass ein Virenscanner, der in der Lage ist, sowohl klassische Virenprogramme wie Makroviren als auch Backdoor Programme zu erkennen und den Anwender im Falle eines Angriffs über diesen Zustand in Kenntnis zu setzen, eingesetzt wird.

Es muss durch geeignete organisatorische Maßnahmen sichergestellt werden in dem Fall, dass der Rechner über einen Intranetzugang verfügt, ein Virenscanner, welcher in der Lage ist, sowohl klassische Virenprogramme wie Makroviren als auch Backdoor Programme zu erkennen und den Anwender im Falle eines Angriffs über diesen Zustand in Kenntnis zu versetzen, eingesetzt wird.

OE.Zugriff
Es muss durch geeignete organisatorische Maßnahmen sichergestellt werden, dass der Rechner des Anwenders sich in einer Umgebung, in welcher der Anwender volle Kontrolle über eingelegte Datenträger und Netzwerkfreigaben hat, befindet. Weiterhin, dass der EVG so geschützt ist, dass er über eine Netzwerkfreigabe nicht erreichbar ist, und dass der Zugriff auf den EVG vom Rechner des Anwenders möglich ist.

OE.SIG_DAT
Schutz der Benutzerdateien
Es muss durch geeignete organisatorische Maßnahmen sichergestellt werden, dass die IT-Umgebung eine Funktionalität zur Errechnung einer digitalen Signatur aus einem Hashwert anbietet.

4 Annahmen und Klärung des Einsatzbereiches

4.1 Annahmen über den Einsatz

Die Softwareapplikation OPENLiMiT SignCubes 1.6 findet in den Bereichen Home-PC, öffentliche Verwaltung und Wirtschaftsunternehmen ihre Anwendung.

4.2 Angenommene Einsatzumgebung

A.Plattform
Der Benutzer verwendet als Hardwareplattform einen Intel 586 kompatiblen Rechner, der über mindestens 64 MB RAM und 60 MB freien Festplattenplatz verfügen.

Auf dem Rechner ist eines der folgenden Betriebssysteme Microsoft Windows 98, Microsoft Windows 98 SE, Windows ME, Windows NT 4.0 mit Servicepack 6.0, Windows 2000 oder Windows XP installiert. Es sind der Internet Explorer ab Version 4.01 SP2 mit der Shell32.dll ab Version 4.0 und die Microsoft Smartcard Base Components ab Version 1.0 auf dem Rechner installiert.

Der Benutzer stellt sicher, dass alle Komponenten des Betriebssystems und alle sonstig installierte Software korrekt und vertrauenswürdig sind.

Der Benutzer verwendet ein sicheres Signaturerzeugungssystem, welches aus Kartenleser mit sicherer Pin-Eingabe und Smartcard besteht. Der Benutzer setzt eine der folgenden SigG [6] konformen Smartcards entsprechend den Vorgaben des Herstellers ein:

- TeleSec E4Netkey-Karte
- OPENLiMiT Karte als spezielle Konfiguration der TeleSec E4NetKey-Karte
- TeleSec PKS Karte

Der Benutzer setzt einen der folgenden Kartenleser mit sicherer Pin-Eingabe entsprechend den Vorgaben des Herstellers ein:

- Cherry SmartBoard G83-6700
- SCMMicrosystems SPx32/ChipDrive Pin-Pad
- Reiner SCT CyberJack e-com Version 2.0
- Reiner SCT CyberJack pinpad Version 2.0.

Bei den verwendeten peripheren Komponenten werden ausschliesslich im Sinne des SigG [6] bestätigte Komponenten verwendet, die zugehörigen Bestätigungen für diese Produkte können von den Seiten der RegTP bezogen werden (www.regtp.de).

A.Personal
Der Benutzer, der Administrator und das Wartungspersonal sind vertrauenswürdig und befolgen die Anweisungen in der Benutzerdokumentation des EVGs. Insbesondere prüft der Benutzer die Integrität des EVGs entsprechend den Anweisungen im Benutzerhandbuch [12].

A.Netzwerk
Der Rechner, auf dem der EVG installiert ist, kann über einen **Internet**zugang verfügen. In diesem Falle wird eine Firewall verwendet, die sicherstellt, dass keine Systemdienste oder Systemkomponenten durch Zugriffe aus dem Internet kompromittiert werden können. Weiterhin setzt der Benutzer einen Virenscanner ein, der in der Lage ist, sowohl klassische Virenprogramme wie Makroviren als auch Backdoor Programme zu erkennen und den Anwender im Falle eines Angriffs über diesen Zustand in Kenntnis zu setzen.

Der Rechner, auf dem der EVG installiert ist, kann über einen **Intranet**zugang verfügen. In diesem Falle setzt der Anwender einen Virenscanner ein, welcher in der Lage ist, sowohl klassische Virenprogramme wie Makroviren als auch Backdoor Programme zu erkennen und den Anwender im Falle eines Angriffs über diesen Zustand in Kenntnis zu versetzen.

A.Zugriff
Der Rechner des Anwenders befindet sich in einer Umgebung, in welcher der Anwender volle Kontrolle über eingelegte Datenträger und Netzwerkfreigaben hat. Der EVG ist so geschützt, dass er über eine Netzwerkfreigabe nicht

erreichbar ist. Der Zugriff auf den EVG vom Rechner des Anwenders ist möglich.

4.3 Klärung des Einsatzbereiches

Mit Auslieferung des Produkts OPENLiMiT SignCubes 1.6 ist der Anwender auf die Einhaltung der oben genannten Einsatzbedingungen hinzuweisen.

Die folgenden Merkmale kann das Produkt OPENLiMiT SignCubes 1.6 **nicht leisten**:

- Sicherstellung des privaten Schlüsselmaterials. Die Sicherstellung der Unversehrtheit und der Geheimhaltung der privaten Schlüssel obliegt der Smartcard.
- Sicherstellung der korrekten Uhrzeit auf dem Rechner des Anwenders. Das Produkt OPENLiMiT SignCubes 1.6 enthält keine Mechanismen für die Verwendung von Zeitstempeln und kann auch keine Aussagen über die Plausibilität der eingestellten Uhrzeit treffen.
- Sicherstellung der Integrität des Betriebssystems OPENLiMiT SignCubes 1.6 enthält keine Mechanismen, um die Integrität seiner Umgebung zu überprüfen. Der Anwender muß sicherstellen, dass er geeignete Vorkehrungen trifft, um eine Kompromittierung seines Betriebssystems zu vermeiden.
- Sicherheit der kryptografischen Operationen. Das Produkt OPENLiMiT SignCubes 1.6 benutzt Bibliotheken zur Erzeugung elektronischer Signaturen über das RSA Public Key Verfahren. Er kann die Stärke der kryptografischen Mechanismen nicht garantieren und keine Aussagen über die Stärke der kryptografischen Funktionen postulieren.

Die Leistungsmerkmale des Produkts OPENLiMiT SignCubes 1.6 beschränken sich auf die Erzeugung kryptografischer Prüfsummen (Hashwerte) und die Verwendung einer sicheren Signaturerstellungseinheit (SSCD) für die Erzeugung elektronischer Signaturen sowie die Verwendung des RSA Algorithmus für die Verifikation elektronischer Signaturen. Für den Verifikationsprozess werden Sperrlisten verwendet, OCSP-Abfragen stehen als Mechanismus ebenfalls zur Verfügung. Das Produkt OPENLiMiT SignCubes 1.6 kann Manipulationen an Zertifikatsverzeichnissen ebenso wenig abwehren wie die Protokollierung elektronischer Signaturvorgänge auf dem Rechner des Anwenders.

Evaluiert wurde der SignCubes Security Environment Manager mit seinen beschriebenen Funktionen, die gesicherte Anzeigeeinheit (SignCubes Viewer) sowie als indirekte Zugänge zur Sicherheitsfunktionalität des SSEM die SignCubes Shell Extensions und der SignCubes CSP.

Anwendungen, die das Produkt OPENLiMiT SignCubes 1.6 nutzen, sind **nicht** Gegenstand dieser Zertifizierung.

Besondere Beschränkungen und Ausnahmen

Der Kartenleser

- Reiner SCT CyberJack e-com Version 2.0 wird nicht von Windows 98

und

- Reiner SCT CyberJack pinpad Version 2.0 wird nicht von Windows NT 4.0 SP 6

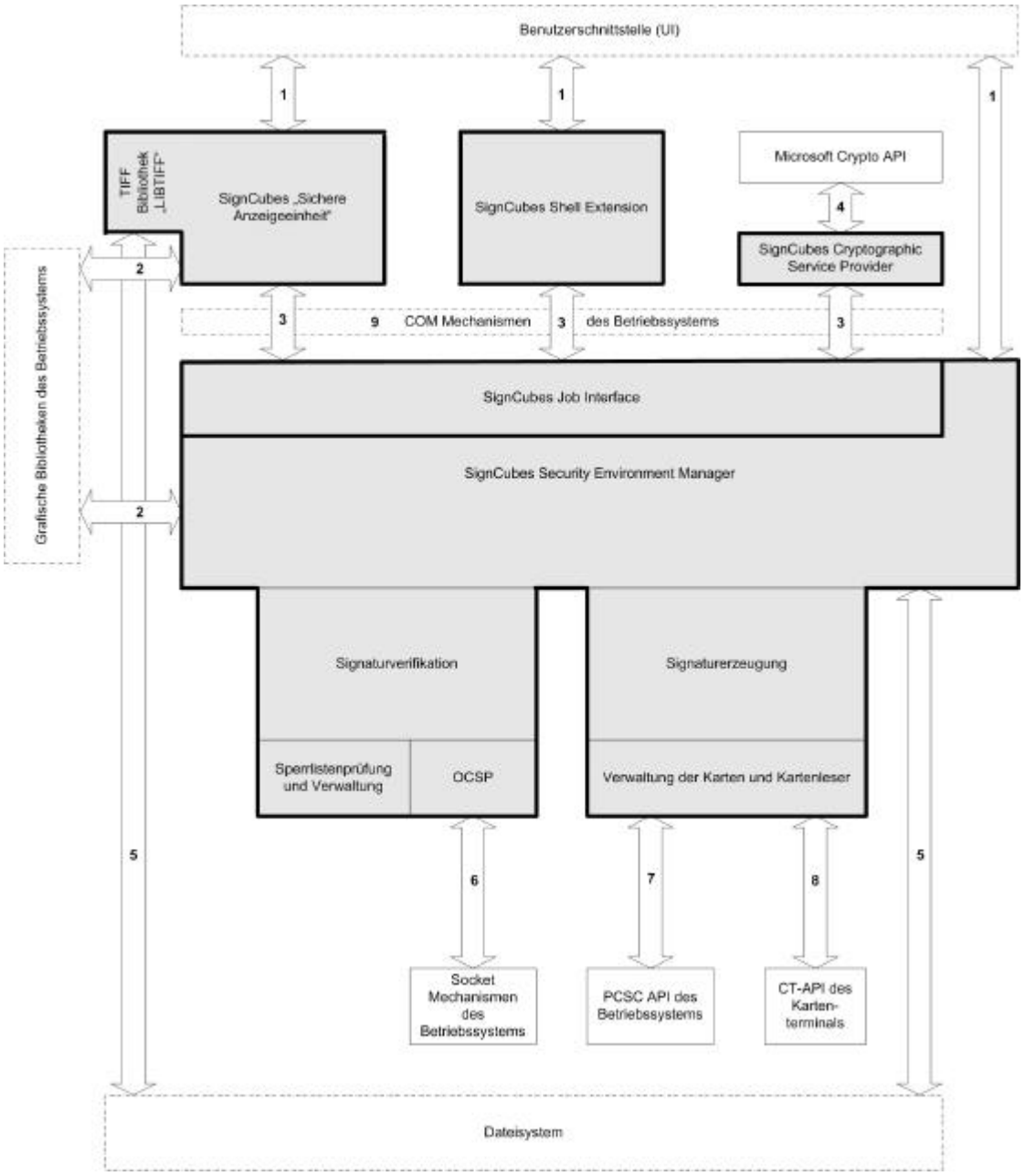
unterstützt.

Für diese Konfigurationen gilt diese Zertifizierung nicht.

5 Informationen zur Architektur

OPENLiMiT SignCubes 1.6 ist eine modulare Client Applikation zur Erzeugung und Verifikation digitaler Signaturen auf Microsoft Windows-Systemen.

Die folgende Grafik gibt eine Übersicht über den Entwurf auf hoher Ebene und die Schnittstellen des EVGs. Die Übersicht erfolgt auf Basis von identifizierten Subsystemen. Die logische Aufteilung in Subsysteme wie sie in der folgenden Grafik dargestellt ist, spiegelt sich nicht in jedem Falle in der realen physischen Abbildung auf ausführbare Dateien und Module wieder. Vielmehr wird eine logische Abgrenzung vorgenommen und die Abgrenzung in der Realisierung der einzelnen Module wird detailliert für die identifizierten Subsysteme beschrieben.



Abgrenzung des EVGs gegen seine Systemumwelt

Der EVG realisiert die folgenden Subsysteme:

- **SignCubes Viewer**
- **SignCubes Security Environment Manager** (Das SignCubes Job Interface ist Teil des SignCubes Security Environment Managers)
- **SignCubes Shell Extension**
- **SignCubes Security Environment Manager**

Das Subsystem **SignCubes Integritätscheck** wird in der einleitenden Grafik nicht dargestellt, sondern wird als entkoppeltes Subsystem beschrieben.
Eine Beschreibung der Subsysteme und ihrer Schnittstellen wird im High-Level Design gegeben.

6 Dokumentation

Die folgenden Dokumente geben dem Endanwender weitergehende Informationen über die Funktionsweise, Sicherheitseigenschaften und Installation der Softwareapplikation OPENLiMiT SignCubes 1.6.

Die Sicherheitsvorgaben [10] geben Auskunft über die Sicherheitseigenschaften des EVGs, d. h. Darlegung der Sicherheitsziele, Bedrohungen und Sicherheitsfunktionen, die die erkannten Bedrohungen abwehren.

Die Benutzerdokumentation [12] gibt wichtige Informationen über die Installation des EVGs auf den Arbeitsplatzrechner, den sicheren Gebrauch der Softwareapplikation und die Konfiguration.

7 Testverfahren

Der EVG OPENLiMiT SignCubes 1.6 wird eindeutig durch eine Konfigurationsliste im Dokument [9] bestimmt. Für alle Test wurde dieselbe Version des EVG verwendet.

Bei den Herstellertests wurden alle in [10] Kapitel 4.2 genannten Betriebssysteme, Smartcards und Kartenleser einbezogen. Durch die Evaluatoren wurden ein Teil der Herstellertests wiederholt und zusätzliche unabhängige Tests durchgeführt.

Die für die Tests verwendete Testkonfiguration ist im Evaluierungsbericht [11] beschrieben. Die Ergebnisse der von den Evaluatoren durchgeführten Tests finden sich ebenfalls in [11].

8 Evaluierte Konfiguration

Der EVG OPENLiMiT SignCubes 1.6 besteht aus einer festen und bei der Installation nicht einstellbaren Konfiguration. Die Installation der Softwareapplikation wird über das OPENLiMiT SignCubes Installationsprogramm vorgenommen. Es existiert keine Möglichkeit, das Produkt OPENLiMiT SignCubes 1.6 ohne Verwendung des Installationsprogramms auf dem Rechner des Anwenders zu installieren.
Die Annahmen aus den Sicherheitsanforderungen im Bezug auf Rechner, Arbeitsspeicher und Festplattenplatz müssen erfüllt sein. Die Tests wurden auf den folgenden Betriebsystemen durchgeführt:

- Windows 98

- Windows 98 SE
- Windows Millenium Edition
- Windows NT 4.0 SP 6
- Windows 2000
- Windows XP

Es muss der Internet Explorer ab Version 4.0.1 auf dem Rechner installiert sein. Die folgenden Smartcard Terminals wurden zu den Tests herangezogen:

- Cherry SmartBoard G83-6700
- SCMMicrosystems SPRx32/ChipDrive Pin-Pad
- Reiner SCT CyberJack e-com Version 2.0
- Reiner SCT CyberJack pinpad Version 2.0

Die folgenden Smartcards wurden zu den Tests verwendet:

- TeleSec E4Netkey-Karte
- OPENLiMiT Karte als spezielle Konfiguration der TeleSec E4NetKey-Karte
- TeleSec PKS Karte

Die Durchführung und die Ergebnisse der Testfälle wurde im Evaluationsbericht [11] festgehalten.

9 Ergebnisse der Evaluierung

Der Evaluierungsbericht [11] wurde nach den Erfordernissen der Common Criteria [1], den Common Evaluation Methodology [2], den Anforderungen des Zertifizierungs-Schemas [3] und den Anwendungshinweisen und Interpretationen (AIS) [4] von der Prüfstelle T-Systems GEI GmbH, Business Unit ITC-Security erstellt.

Der EVG OPENLiMiT SignCubes 1.6 erweitert die funktionalen Anforderungen der Common Criteria Teil 2, Version 2.1 und ist in seinen Anforderungen an die Vetrauenswürdigkeit konform zu Teil 3 der Common Criteria, Version 2.1.

Die Gesamtergebnisse gemäß der Common Criteria [1], Teil 3 Vertrauenswürdigkeitsklassen (entsprechend der EAL 3 mit Zusatz von **AVA_VLA.4, AVA_MSU.3, ADV_IMP.1, ADV_LLD.1 und ALC_TAT.1)** sind in der folgenden Tabelle zusammengefasst:

Vertrauenswürtigkeitsklassen und Komponenten:	Ergebnis
ASE, Prüfung und Bewertung der Sicherheitsvorgaben	**PASS**
ADV_FSP, Entwicklung_Funktionale Spezifikation	**PASS**
ADV_HLD, Entwicklung_Entwurf auf hoher Ebene	**PASS**
ADV_LLD, Entwicklung_Entwurf auf niedriger Ebene	**PASS**
ADV_IMP, Entwicklung_Darstellung der Implementierung	**PASS**

ADV_RCR, Entwicklung_Übereinstimmung der Darstellung	**PASS**
ACM_CAP, Konfigurationsmanagement_CM-Leistungsvermögen	**PASS**
ACM_SCP,Konfigurationsmanagement_CM-Anwendungsbereich	**PASS**
ADO_DEL, Auslieferung und Betrieb_Auslieferung	**PASS**
ADO_IGS, Auslieferung und Betrieb_Installation, Generierung und Anlauf	**PASS**
ALC_DVS, Lebenszyklus-Unterstützung_Sicherheit beim Entwickler	**PASS**
ALC_TAT, Lebenszyklus-Unterstützung_Werkzeuge und Techniken	**PASS**
AGD_ADM, Handbücher_Systemverwalterhandbuch	**PASS**
AGD_USR, Handbücher_Benutzerhandbuch	**PASS**
ATE_IND, Testen_Unabhängiges Testen	**PASS**
ATE_COV, Testen_Testabdeckung	**PASS**
ATE_DPT, Testen_Testtiefe	**PASS**
ATE_FUN, Testen_Funktionale Tests	**PASS**
AVA_MSU, Schwachstellenbewertung_Mißbrauch	**PASS**
AVA_SOF, Schwachstellenbewertung_Stärke der EVG-Sicherheitsfunktionen	**PASS**
AVA_VLA, Schwachstellenbewertung_Schwachstellenanalyse	**PASS**

Es wurde vom Hertsteller eine allgemeine Aussage zur Stärke der Funktionen von SOF-hoch gemacht, welche sich aber auf keine explizite Sicherheitsfunktion bezieht.

Erweiterung der Ergebnisse auf andere Konfigurationen

Die Ergebnisse der durchgeführten Evaluierung sind nur anwendbar auf OPENLiMiT SignCubes 1.6, Version 1.6.0.5. Die Ergebnisse der aktuellen Evaluierungen sind auf andere Konfigurationen ohne weitere Untersuchungen nicht erweiterbar.

10 Kommentare und Empfehlungen

Zur Erzeugung elektronischer Signaturen wird vom OPENLiMiT SignCubes 1.6 die Hashfunktionen SHA-1 bereitgestellt. Zur Prüfung elektronischer Signaturen werden vom Produkt OPENLiMiT SignCubes 1.6, die Hashfunktionen RIPEMD-160 sowie SHA-1 und der RSA-Algorithmus mit einer Schlüssellänge von 1024 Bit bereitgestellt.

Die verwendeten kryptografischen Algorithmen sind gemäß der Veröffentlichung im Bundesanzeiger Nr. 30 – S. 2537-2538 vom 13. Februar 2004 „Geeignete Algorithmen zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG vom 22. Mai 2001 in Verbindung mit Anlage 1 Abschnitt 1 Nr. 2 SigV vom 22. November 2001“ als geeignet eingestuft.

Die verwendeten Hashalgorithmen RIPEMD-160 und SHA-1 gelten bis **Ende 2009** als geeignet.

Der RSA-Algorithmus mit einer Schlüssellänge von 1024 Bit gilt bis **Ende 2007** als geeignet.

Bei der Nutzung des EVG sind die Annahmen an die Einsatzumgebung aus [10] Kapitel 3.1 beziehungsweise die daraus abgeleiteten Ziele für die Einsatzumgebung [10] Kapitel 4.2 sowie die Benutzungshinweise des Benutzerhandbuches [12] unbedingt zu berücksichtigen. Weitere Informationen dazu befinden sich auch in Kapitel 8 dieses Zertifizierungsreportes.

11 Anhänge

Keine

12 Sicherheitsvorgaben

Die Sicherheitsvorgaben [10] sind Bestandteil dieses Zertifizierungsreports.

13 Definitionen

13.1 Abkürzungen

BSI Bundesamt für Sicherheit in der Informationstechnik

CC Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik.

CRL Certificate Revocation List. Eine CRL ist eine Liste mit gesperrten Zertifikaten, die eine Negativprüfung von Zertifikaten ermöglicht.

CSP Cryptographic Service Provider. Microsoft stellt einen Mechanismus zur Realisierung einer eigenen Sicherheitsinfrastruktur auf Basis der CSPs zur Verfügung. Mit diesem Mechanismus ist es Applikationen sowohl möglich, CSPs, die vom Betriebssystem zur Verfügung gestellt werden, für kryptografische Operationen zu nutzen als auch die Realisierung eigener CSPs vorzunehmen und diese dem Betriebssystem zur Verfügung zu stellen. CSPs können verschiedene Aufgaben wahrnehmen, der SignCubes CSP wurde

	zur Erzeugung digitaler Signaturen im Kontext des Betriebssystems entwickelt.
CTL	Certifcate Trust List. Ist eine Zertifikatsvertrauensliste.
EAL	Evaluation Assurance Level – Vertrauenswürdigkeitsstufe
ETR	Evaluation Technical Report
EVG	Evaluationsgegenstand
IT	Informationstechnik
OCSP	Online Certificate Status Protocol. Dies ist ein Mechanismus der eine Positiv-Abfrage zu einem gegebenen Zertifikat ermöglicht.
PP	Protection Profile – Schutzprofil
RegTP	Regulierungsbehörde für Telekommunikation und Post
SF	Sicherheitsfunktion
SOF	Strength of Function - Stärke der Funktionen
SSCD	Secure Signature Creation Device. Unter einem SSCD wird ein Gerät verstanden, mit dem es möglich ist, auf sichere Art und Weise eine digitale Signatur zu erzeugen.
SSEM	SignCubes Security Environment Manager, Bestandteil des Produktes OPENLiMiT SignCubes 1.6
ST	Security Target - Sicherheitsvorgaben
TSC	TSF Scope of Control - Anwendungsbereich der TSF-Kontrolle
TSF	TOE Security Functions - EVG-Sicherheitsfunktionen
TSP	TOE security policy - EVG-Sicherheitspolitik

13.2 Glossar

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

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.

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 Konsumentenbedürfnisse erfüllen.

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

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

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

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.

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.

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-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.

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

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.

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

14 Literaturangaben

[1] Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CC), Version 2.1, August 1999

[2] Common Methodology for Information Technology Security Evaluation (CEM), Part 1, Version 0.6; Part 2: Evaluation Methodology, Version 1.0, August 1999

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

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

[5] Deutsche IT-Sicherheitszertifikate (BSI 7148, BSI 7149), periodisch aktualisierte Liste, die auch auf der Internet-Seite des BSI veröffentlicht wird.

[6] Gesetz über die Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) in der Fassung vom 16. Mai 2001 (BGBl. Jahrgang 2001 Teil I Nr. 22)

[7] Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) in der Fassung vom 16. November 2001 (BGBl. Jahrgang 2001 Teil I Nr. 59)

[8] Maßnahmenkatalog für technische Komponenten nach dem Signaturgesetz, Stand 15. Juli 1998, Hrsg. RegTP

[9] Konfigurationsmanagement, Version 0.1.3, 05. Oktober 2004, OPENLiMiT Holding AG

[10] Sicherheitsvorgaben BSI-DSZ-0277-2004, Version 1.0/20.07.2004, Titel: Sicherheitsvorgaben (ST), OPENLiMiT SignCubes 1.6, OPENLiMiT Holding AG

[11] Evaluierungsbericht, Version 1.0 vom 06.10.2004, T-Systems GEI GmbH, Business IT-Security, Prüfstelle IT-Sicherheit
(vertrauliches Dokument)

[12] Benutzerdokumentation, OPENLiMiT SignCubes 1.6, Version 1.6.0.5, OPENLiMiT Holding AG
(Windowshilfe-Dateien:
OPENLiMiT SignCubes 1_6 Benutzerdokumentation.chm, 01.10.2004
OPENLiMiT SignCubes 1_6 User Documentation.chm, 04.10.2004,
SignCubes GmbH)

Dies ist eine eingefügte Leerseite.

C Auszüge aus den technischen Regelwerken

CC Teil 1:

Kennzeichnung der Evaluationsergebnisse (Kapitel 5.4) / **Final Interpretation 008**

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 Part 2 (functional requirements), 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:

Part 2 conformant - A PP or TOE is Part 2 conformant if the functional requirements are based only upon functional components in Part 2

Part 2 extended - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2
plus one of the following:

Part 3 conformant - A PP or TOE is Part 3 conformant if the assurance requirements are based only upon assurance components in Part 3

Part 3 extended - A PP or TOE is Part 3 extended if the assurance requirements include assurance requirements not in 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 Teil 3

Assurance categorisation (chapter 2.5)

„The assurance classes, families, and the abbreviation for each family are shown in Table 2.1.

Assurance Class	Assurance Family	Abbreviated Name
Class ACM: Configuration management	CM automation	ACM_AUT
	CM capabilities	ACM_CAP
	CM scope	ACM_SCP
Class ADO: Delivery and operation	Delivery	ADO_DEL
	Installation, generation and start-up	ADO_IGS
Class 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
Class AGD: Guidance documents	Administrator guidance	AGD_ADM
	User guidance	AGD_USR
Class ALC: Life cycle support	Development security	ALC_DVS
	Flaw remediation	ALC_FLR
	Life cycle definition	ALC_LCD
	Tools and techniques	ALC_TAT
Class ATE: Tests	Coverage	ATE_COV
	Depth	ATE_DPT
	Functional tests	ATE_FUN
	Independent testing	ATE_IND
Class AVA: Vulnerability assessment	Covert channel analysis	AVA_CCA
	Misuse	AVA_MSU
	Strength of TOE security functions	AVA_SOF
	Vulnerability analysis	AVA_VLA

Table 2.1 -Assurance family breakdown and mapping“

Evaluation assurance levels (chapter 6)

„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 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 6.1)

Table 6.1 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 2 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 CC 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 6.1 - Evaluation assurance level summary“

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 6.2.1)

„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 6.2.2)

„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 6.2.3)

„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 6.2.4)

„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 6.2.5)

„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 6.2.6)

„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 6.2.7)

„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 14.3)

AVA_SOF Strength of TOE security functions

„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 14.4)

AVA_VLA Vulnerability analysis

„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), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential.“

Dies ist eine eingefügte Leerseite.