Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

BSI-DSZ-CC-0943-2015

zu

Insurance Security Token Service (ISTS), Version 1.0

der

GDV Services 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-0943-2015

Netzwerk- und Kommunikationsprodukt

Insurance Security Token Service (ISTS)
Version 1.0

von	GDV Services GmbH
PP-Konformität	Keine
Funktionalität:	Produktspezifische Sicherheitsvorgaben Common Criteria Teil 2 erweitert
Vertrauenswürdigkeit:	Common Criteria Teil 3 konform EAL 2
Gültig bis:	8. März 2020

SOGIS
Recognition Agreement

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.

Common Criteria
Recognition
Arrangement

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, 9. März 2015

Bundesamt für Sicherheit in der Informationstechnik
Im Auftrag

Bernd Kowalski
Abteilungspräsident

L.S.

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

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-Zertifizierungs- und - Anerkennungsverordnung[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

---

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 von Sicherheitszertifikaten und Anerkennungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI-Zertifizierungs- und - Anerkennungsverordnung - BSIZertV) vom 17. Dezember 2014, Bundesgesetzblatt Jahrgang 2014 Teil I, Nr. 61, S. 2231

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

bis E3 (niedrig) ein. Der technische Bereich "smartcard and similar devices" wurde für 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.

Dieses Zertifikat wird für alle ausgewählten Komponenten unter SOGIS-MRA anerkannt.

2.2 Internationale Anerkennung von CC - Zertifikaten

Am 08. September 2014 wurde eine Vereinbarung über die gegenseitige Anerkennung von IT-Sicherheitszertifikaten und Schutzprofilen auf Basis der CC unterzeichnet (Common Criteria Recognition Arrangement, CCRA-2014).

Diese beinhaltet CC-Zertifikate aus Basis von cPPs (collaborative Protection Profiles, exact use), Zertifikate basierend auf Komponenten bis einschließlich der Vertrauenswürdigkeitsstufe EAL 2 oder/und der Vertrauenswürdigkeitsfamilie (ALC_FLR) sowie Zertifikate für Schutzproflie (Protection Profiles und collaborative Protection Profiles).

Die CCRA-2014 Vereinbarung ersetzt das alte CCRA, welches im Mai 2000 (CCRA-2000) unterzeichnet wurde. Zertifikate basierend auf CCRA-2000, die vor dem 08. September 2014 ausgestellt wurden unterliegen auch weiterhin der gegenseitigen Anerkennung entsprechend den CCRA-2000 Regularien. Für bereits vor dem 08. September 2014 beantragte Zertifizierungsverfahren und für die Aufrechterhaltung der Aussage zur Vertrauenswürdigkeit (d.h. Re-Zertifizierung oder Maintenance) zu Zertifikaten die den Regularien der CCRA-2000 (z.B. Komponenten bis einschließlich EAL 4 oder aus der Vertrauenswürdigkeitsfamilie (ALC_FLR)) unterliegen, gilt eine Übergangsfrist (transition period) bis zum 08. September 2017.

Der Vereinbarung sind zum September 2014 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.

Dieses Zertifikat wird für alle ausgewählten Komponenten unter CCRA anerkannt.

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 Insurance Security Token Service (ISTS), Version 1.0 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Produkts Insurance Security Token Service (ISTS), Version 1.0 wurde von TÜV Informationstechnik GmbH durchgeführt. Die Evaluierung wurde am 24. Februar 2015 beendet. Das Prüflabor TÜV Informationstechnik GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[6].

Der Sponsor und Antragsteller ist: GDV Services GmbH

Das Produkt wurde entwickelt von: GDV Services GmbH

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

4 Gültigkeit des Zertifikats

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

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

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

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

Das Zertifikat bestätigt die Vertrauenswürdigkeit des Produktes gemäß den Sicherheitsvorgaben zum Zeitpunkt der Ausstellung. Da sich Angriffsmethoden im Laufe der Zeit fortentwickeln, ist es erforderlich, die Widerstandsfähigkeit des Produktes regelmäßig überprüfen zu lassen. Aus diesem Grunde sollte der Hersteller das zertifizierte Produkt im Rahmen des Assurance Continuity-Programms des BSI überwachen lassen (z.B. durch eine Re-Zertifizierung). Insbesondere wenn Ergebnisse aus dem Zertifizierungsverfahren in einem nachfolgenden Evaluierungs- 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.

Da die Verwendung des Zertifikates jedoch auch und insbesondere in die Zukunft gerichtet ist, die mit dem Zertifikat verbundene Sicherheitsaussage angesichts des kontinuierlichen technischen Fortschritts aber nicht unbeschränkt Gültigkeit haben kann, ist es erforderlich, die im Zertifikat angegebene Höchstdauer der Geltung festzulegen.

---

[6] Information Technology Security Evaluation Facility

Der Zertifikatsinhaber ist verpflichtet

1. die in diesem Zertifizierungsverfahren evaluierten und für Tests verwendeten Bestandteile des Produktes (Evaluationsgegenstandes, EVG) und die im Evaluierungsbericht (ETR) bzw. in der Konfigurationsliste genannten Herstellernachweise für die Dauer der Gültigkeit des Zertifikates plus 3 Jahre dem BSI jederzeit auf Anfrage kostenlos zur Verfügung zu stellen, um die zu Grunde liegende Entscheidung und die technische Entscheidungsgrundlage weiterhin nachvollziehen und überprüfen zu können.
2. bei der Bewerbung des Zertifikates oder der Tatsache der Zertifizierung des Produktes auf den Zertifizierungsreport hinzuweisen sowie jedem Anwender des Produktes den Zertifizierungsreport und die darin referenzierten Sicherheitsvorgaben und Benutzerdokumentation für den Einsatz oder die Verwendung des zertifizieren Produktes zur Verfügung zu stellen,
3. die Zertifizierungsstelle des BSI unverzüglich über Schwachstellen des Produktes zu informieren, die nach dem Zeitpunkt der Zertifizierung durch Sie oder Dritte festgestellt wurden,
4. die Zertifizierungsstelle des BSI unverzüglich zu informieren, wenn sich sicherheitsrelevante Änderungen am geprüften Lebenszyklus, z. B. an Standorten oder Prozessen ergeben oder die Vertraulichkeit von Unterlagen und Informationen zum Produkt oder aus dem Evaluierungs- und Zertifizierungsprozess nicht mehr gegeben ist. Insbesondere ist vor Herausgabe von vertraulichen Unterlagen oder Informationen zum Produkt oder aus dem Evaluierungs- und Zertifizierungsprozess, die nicht zum Lieferumfang gemäß Zertifizierungsreport Teil B, Kap. 2 gehören, an Dritte, eine Genehmigung der Zertifizierungsstelle des BSI einzuholen.

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 Insurance Security Token Service (ISTS), Version 1.0 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] GDV Services GmbH
Wilhelmstraße 43 / 43 G
10117 Berlin

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 ein Security Token Service (STS). Dieser ist als reine Software-Applikation implementiert und wird aufgrund des Einsatzgebietes in der Versicherungsbranche als Insurance Security Token Service (ISTS) bezeichnet.

Die Applikation stellt (Software-)Sicherheitstoken aus, die für Authentifizierungszwecke bei einem Trusted German Insurance Cloud (TGIC) Webservice verwendet werden. Zusätzlich verfügt der EVG über die Möglichkeit die ausgestellten Sicherheitstoken zu validieren und zu widerrufen. Weitere Funktionalitäten sind das Führen einer Logdatei, die Identifikation und Authentifizierung von Nutzern, wobei einige Authentisierungsmechanismen von der Umgebung bereitgestellt werden (vgl. [6] Kapitel 6.1.2 und 7.2) , und das Management von Sicherheitsfunktionalitäten.

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 2.

Die funktionalen Sicherheitsanforderungen (Security Functional Requirements SFR) an den EVG werden in den Sicherheitsvorgaben [6] Kapitel 6.1 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
SF1 - Security Audit	Die Security Audit Funktionalität wird durch das Logging der ausgeführten Operationen von SF3 realisiert. Dadurch ermöglicht die Secure Audit Funktionalität dem EVG, sicherheitsrelevante Ereignisse zu protokollieren.
SF2 - Identification & Authentication	Der EVG unterstützt mehrere Authentisierungsmechanismen. Die Identifikation des Webservice-Nutzers wird grundsätzlich vom EVG durchgeführt. Die Authentifizierung erfolgt in einem zweiten Schritt und wird für die zertifikats- und eID-basierte Authentifizierung vollständig von der operativen Umgebung durchgeführt. Die mTAN-Authentifizierung per TAN führt der TOE teilweise selbst durch. Dabei werden lediglich die Bereitstellung der Zufallszahl, sowie die Überprüfung des Kennwortes von der Umgebung durchgeführt.
SF3 - Security Token Service	Die Funktionalität Security Token Service wird durch Ausgabe eines Security Tokens (Issuance Binding) nach erfolgreicher Authentifikation realisiert. Zusätzlich werden das Widerrufen eines Security Token (Cancel Binding) und das Validieren eines Security Token (Validate Binding) unterstützt.
SF4 - Security Management	Die Funktionalität Security Management wird dadurch realisiert, dass der EVG die über die Möglichkeit verfugt, in Form einer XML-basierten Konfigurationsdatei die Gültigkeitsdauer • einer X.509-Session, • einer nPA-Session sowie

Sicherheitsfunktionalität des EVG	Thema
	• einer generierten mTAN einzustellen. Diese Parameter werden durch den EVG bei jedem Aufruf eingelesen sowie aufgrund des zugrunde liegenden XMLSchemas für die Konfigurationsdatei syntaktisch geprüft.

Tabelle 1: Sicherheitsfunktionalität des EVG

Mehr Details sind in den Sicherheitsvorgaben [6], Kapitel 7 dargestellt.

Die Werte, die durch den EVG geschützt werden, sind in den Sicherheitsvorgaben [6], Kapitel 3.1, definiert. Basierend auf diesen Werten stellen die Sicherheitsvorgaben die Sicherheitsumgebung in Form von Annahmen, Bedrohungen und organisatorischen Sicherheitspolitiken in den Kapiteln 3.3, 3.4 und 3.5 dar.

Dieses Zertifikat umfasst die folgenden Konfigurationen des EVG: Der evaluierte EVG ist Insurance Security Token Service V1.0. Die zugrundeliegende Plattform des EVG ist IBM WebSphere DataPower Service Gateway XG45 (Type 7198) mit der Firmwareversion 6.0. 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:

Insurance Security Token Service (ISTS)

Die folgende Tabelle beschreibt den Auslieferungsumfang:

Nr	Typ	Identifier	Version	Auslieferungs-methode
1	SW	Gesamtdeployment: ISTS-Release-v1.0-140731.zip *SHA256:* *8ba1433758899bd7187d6e558cfcff58052f3438b03dbd930d72d7e708f5651c*	Version 1.0	SharePoint download
2	SW	EVG: wdp-config-140731.ists-core.zip *SHA 256:* *628a362879f471a7f3e20a0ffe9f7ffc7c55bff7dc74699cb31223e3c05160d1*	Version 1.0.0.IBM.2014-07-31	SharePoint download

Nr	Typ	Identifier	Version	Auslieferungs-methode
3	DOC	Insurance Security Token Service Preparative Procedures Common Criteria Evaluation AGD_PRE	Version 0.8	SharePoint download
4	DOC	Insurance Security Token Service Operational User Guidance Common Criteria Evaluation AGD_OPE	Version 0.9	SharePoint download
5	DOC	Insurance Security Token Service Anbindungsleitfaden für Webservice-Betreiber und Webservice-Nutzer in der TGIC	Version 1.0.1	SharePoint download
6	DOC	ISTS-Fehlercodes-TOE.xls Beschreibung der Fehlercodes für die Module des TOE	Version 0.7	SharePoint download
7	DOC	Insurance Security Token Service Service Gateway / WDP Deployment	Version 0.9	SharePoint download
8	DOC	Insurance Security Token Service Application Server / WAS Installation & Konfiguration	Version 0.11	SharePoint download
9	DOC	ZIP-Archiv mit der technischen Schnittstellenspezifikation des TOE InsuranceSecurityTokenService.wsdl.zip	Version 1.0.1	SharePoint download
10	DOC	Insurance Security Token Service Database Server / DB2 Installation & Konfiguration	Version 0.14	SharePoint download
11	DOC	Insurance Security Token Service Database Server / DB2 Deployment	Version 0.8	SharePoint download
12	DOC	Insurance Security Token Service Directory Server / TDS Installation & Konfiguration	Version 0.12	SharePoint download
13	DOC	Insurance Security Token Service Directory Server / TDS Deployment	Version 0.6	SharePoint download
14	DOC	Insurance Security Token Service Betriebshandbuch	Version 0.9	SharePoint download
15	DOC	Insurance Security Token Service Kryptokonzept	Version 0.3	SharePoint download
16	DOC	WebSphere DataPower Type 7198 and 7199 Third Edition Installation and User's Guide	3rd edition	SharePoint download

Nr	Typ	Identifier	Version	Auslieferungs-methode
17	DOC	Insurance Security Token Service Application Server / WAS Deployment Nutzerverwaltung	Version 0.6	SharePoint download
18	DOC	Insurance Security Token Service Registry Server / WSRR Installation & Konfiguration	Version 0.11	SharePoint download
19	DOC	Insurance Security Token Service Registry Server / WSRR Deployment TGIC-Service-Register	Version 0.7	SharePoint download
20	DOC	ISTS-Fehlercodes-ServiceGateway.xls Insurance Security Token Server Service Gateways / WDP Fehlercodes	Version 0.9	SharePoint download
21	DOC	„Work Report: DataPower XG45 HSM Setup and Problem Analysis for GDV“ DP-XG45_Config-Work_2013-10-17.pdf	N/A	SharePoint download
22	DATEI	Hashwerte (SHA-256) für die EVG Softwareteile in wdp-config-140731.ists-core.zip (Nr. 2)	N/A	E-Mail (S/MIME-verschlüsselt und signiert)
23	DATEI	Hashwerte (SHA-256) für das Gesamtdeployment ISTS-Release-v1.0-140731.zip (Nr. 1)	N/A	E-Mail (S/MIME-verschlüsselt und signiert)

Tabelle 2: Auslieferungsumfang des EVG

Die Auslieferung des EVG sowie der Benutzerdokumentation und der Begleitdokumente zur Benutzerdokumentation werden auf dem SharePoint-Server des ITC-Betreibers zur Verfügung gestellt. Der Kommunikationskanal zu diesem Server wird über HTTPS gesichert und der Zugriff auf den SharePoint-Server wird durch den ITC-Betreiber durch entsprechende Nutzer-Accounts mit geeigneten Rechten eingeschränkt.

Das Deploymentmodul des EVG besteht aus xsl-, xsd-, wsdl- and xml-Dateien und ist Teil eines gesamten Deploymentpakets ISTS-Release-v1.0-140731.zip für den ITC, welcher aus fünf verschiedenen Modulen besteht.

Dabei ist die Bezeichnung des EVG-Moduls folgende: *wdp-config-140731.ists-core.zip*. Während der Erstellung des EVG-Moduls wird zusätzlich noch ein SHA256-Hashwert über das ZIP-Archiv berechnet und dem ITC-Betreiber als zweite Datei mit dem Namen wdp-config-140731.ists-core.sha256 zur Verfügung gestellt.

Die berechneten SHA256 Checksummen werden mit einer per S/MIME verschlüsselten und signierten E-Mail durch den Hersteller an den Benutzer übermittelt. Vor der Auslieferung muss ein Austausch der S/MIME-Zertifikate und der öffentlichen Schlüssel von Hersteller und Benutzer stattfinden.

Nach Erhalt des EVG und des SHA256-Hashwertes muss der Benutzer die Checksummen der Auslieferungspakete berechnen und mit den erhaltenen Daten vergleichen, indem er beispielsweise OpenSSL nutzt und folgenden Befehl in der Kommandozeile eingibt: *openssl dgst –sha256 wdp-config-140731.ists-core.zip*.

Auch kann er die Version des EVG verifizieren, indem er die Versionsdatei *local/config/ISTS_version.xml*, aufruft und die folgende Versionsnummer des EVG vorfindet: *1.0.0-IBM.2014-07-31*.

Der Integritätscheck nach Erhalt der Auslieferungsbestandteile und vor der Installation stellt sicher, dass der ITC-Betreiber die korrekte Version des EVG erhalten hat.

Nur nachdem der ITC-Betreiber den Inhalt des ZIP-Archivs erfolgreich geprüft hat und den SHA256-Hashwert verifizieren konnte, wird das ITC-Deploymentpaket an die jeweiligen ITC-Administration weitergeleitet.

3 Sicherheitspolitik

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

- Audit
- Identifikation und Authentifikation
- Security Management
- Security Token Service

4 Annahmen und Klärung des Einsatzbereiches

Die in den Sicherheitsvorgaben definierten Annahmen sowie Teile der Bedrohungen und organisatorischen Sicherheitspolitiken werden nicht durch den EVG selbst abgedeckt. Diese Aspekte führen zu Sicherheitszielen, die durch die EVG-Einsatzumgebung erfüllt werden müssen. Hierbei sind die folgenden Punkte relevant:

Ziele	Beschreibung
OE.ENVIRONMENT	Die operative Umgebung soll folgende Funktionalitäten zur Verfügung stellen: Zeitstempel, Dateisystem, kryptografische Funktionen und Datenbank. Weiterhin soll sichergestellt werden, dass nur autorisierte Personen Zugriff auf TSF Daten erhalten, die in der operativen Umgebung gespeichert werden.
OE.NOEVIL	TOE Administratoren, die in Berührung mit TSF Daten oder Funktionalität kommen, sollen nicht unachtsam, vorsätzlich fahrlässig oder feindlich eingestellt sein. Sie sollen der Anleitung, die dem TOE beiliegt, folgen. Sie sollen gut ausgebildet sein und die TOE Funktionalitäten sicher und verantwortungsvoll administrieren.
OE.PHYSEC	Der TOE soll gegen unautorisierten physikalischen Zugriff und Modifikation geschützt sein.
OE.PUBLIC	Die operative Umgebung in seiner Application Domain wird ausschließlich für den TOE verwendet. Andere Software, als die für den TOE und dessen Management notwendige und für die Wartung und Management der operativen Umgebung, ist in dieser Domäne nicht installiert.
OE.PKI	Die operative Umgebung soll mit der ITC PKI eine für den TOE vertrauenswürdige PKI-Struktur mit vertrauenswürdiger CA bereitstellen, die ausschließlich Zertifikate in den Umlauf bringt, die unter Verwendung von SHA-256 erstellt wurden.

Tabelle 3: Verbindliche Sicherheitsziele für die operative Umgebung

Details finden sich in den Sicherheitsvorgaben [6], Kapitel 4.2.

5 Informationen zur Architektur

Der EVG besteht aus sieben Subsystemen welche im Folgenden stichwortartig beschrieben sind:

- ISTS_rule_IssueRST: Auslesen der Konfiguration aus der operativen Umgebung des EVG. Anfrage zum Erstellen eines Tokens aufnehmen und gegen die Spezifikation prüfen. Benutzerdaten abrufen und grobe Prüfung der Zulässigkeit der Anfrage durchführen. Art der unterstützbare Authentifizierung feststellen (X.509, mTAN oder nPA). Authentifizierungsrückfrage (Challenge Response) generieren.
- ISTS_rule_IssueRSTR: Auslesen der Konfiguration aus der operativen Umgebung des EVG. Antwort auf die Authentifizierungsabfrage aufnehmen und gegen die Spezifikation prüfen. Authentifizierung durchführen und durch das Erstellen des Tokens bestätigen. Erstellen des Tokens ins Protokoll revisionssicher schreiben.
- ISTS_rule_CancelRST: Auslesen der Konfiguration aus der operativen Umgebung des EVG. Anfrage zum Widerrufen eines Tokens aufnehmen und gegen die Spezifikation prüfen. Benutzer- und Token-Daten abrufen und grobe Prüfung auf die Zulässigkeit der Anfrage durchführen. Art der unterstützbaren Authentifizierung feststellen (X.509, mTAN oder nPA). Authentifizierungsrückfrage (Challenge Response) generieren.
- ISTS_rule_CancelRSTR: Auslesen der Konfiguration aus der operativen Umgebung des EVG. Antwort auf die Authentifizierungsabfrage aufnehmen und gegen die Spezifikation prüfen. Authentifizierung durchführen und durch das Widerrufen des Tokens bestätigen. Widerruf des Tokens ins Protokoll revisionssicher schreiben.
- ISTS_rule_Validate: Auslesen der Konfiguration aus der operativen Umgebung des EVG. Anfrage zur Überprüfung des Tokens aufnehmen und gegen die Spezifikation prüfen. Token durch die Umgebung entschlüsseln und anschließend überprüfen. Den Vorgang der Prüfung ins Protokoll revisionssicher schreiben.
- ISTS_rule_Other: Abfangen und Behandlung von Fehlermeldungen welche nicht den Subsystemen ISTS_rule_IssueRST, ISTS_rule_IssueRSTR, ISTS_rule_CancelRST, ISTS_rule_CancelRSTR und ISTS_rule_Validate zugeordnet werden können.
- ISTS_rule_Error: Abfangen und Behandlung der Fehlermeldungen aus allen Subsystemen.

Besonders die ersten fünf Subsysteme realisieren die Funktionen der Sicherheitsfunktionalität SF3 (Security Token Service). Dadurch werden auch implizit die Funktionen der Sicherheitsfunktionalitäten SF1 (Security Audit), SF2 (Identification & Authentication) und SF4 (Security Management) realisiert. Die letzten beiden Subsysteme implementieren explizit die Fehlerbehandlung des EVG.

6 Dokumentation

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

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

7 Testverfahren

7.1 Herstellertests

Testkonfiguration

Der EVG ist ein Teil des gesamten Deploymentpakets ISTS-Release-v1.0-140731.zip welcher aus fünf verschiedenen Modulen besteht, wobei der EVG-Teil durch wdp-config-140731.ists-core.zip repräsentiert wird. Aus diesem Grund werden alle fünf Deployment-Einheiten (siehe nachfolgende Tabellen) des Insurance Trust Center (ITC) für den Einsatz des EVG und die Durchführung der Tests benötigt.

Übereinstimmend mit der im ST spezifizierten operativen Einsatzumgebung des EVG, wurden sowohl die Hersteller- als auch die Prüfstellentests mit folgender Konfiguration durchgeführt:

Service Gateway mit jeweils zwei redundanten Instanzen		**Operative Einsatzumgebung**
Hardware	IBM WebSphere DataPower Service Gateway XG 45 • Netzwerk: 4x 1 Gbit ports; 2x 10 Gbit ports	WebSphere DataPower XG45 6.0.1.3
Firmware	IBM WebSphere DataPower Service Gateway XG45, Firmware Version 6.0 • inkl. Data Integration Module (DIM) Option • inkl. Hardware Security Module (HSM)	WebSphere DataPower XG45 6.0.1.3
ITC Komponenten	ITC Service Gateway • TOE • ITC Branchennetz-Adapter • ITC ISTS-eID-Connector • ITC Web und Webservice-Proxy	ITC Service Gateway • TOE • ITC Branchennetz-Adapter • ITC ISTS-eID-Connector • ITC Web und Webservice-Proxy

Tabelle 4: Deployment - Einheit 1 (mit EVG)

Application Server mit jeweils zwei redundanten Instanzen		**Operative Einsatzumgebung**
Hardware	Intel Server: virtualised • CPU: Intel Xeon E5-2643, 3.3 GHz, 1 Core • RAM: 4 GB • Hard drive: min. 64 GB • Network: 1 Gbit port	Intel Server: virtualised • CPU: Intel Xeon E5-2643, 3.3 GHz, 1 Core • RAM: 4 GB • Hard drive: min. 64 GB • Network: 1 Gbit port
Betriebssystem	SuSE Linux Enterprise Server (SLES), Version 11	SuSE Linux Enterprise Server (SLES), Version 11
Software	IBM WebSphere Application Server ND	IBM WebSphere Application Server ND Version 8.5.5.1
ITC Komponenten	• ITC Nutzerverwaltung • ITC PKI	• ITC Nutzerverwaltung • ITC PKI

Tabelle 5: Deployment - Einheit 2

Registry Server mit jeweils zwei redundanten Instanzen		Operative Einsatzumgebung
Hardware	Intel Server: virtualised • CPU: Intel Xeon E5-2643, 3.3 GHz, 1 Core • RAM: 4 GB • Hard drive: min. 64 GB • Network: 1 Gbit port	Intel Server: virtualised • CPU: Intel Xeon E5-2643, 3.3 GHz, 1 Core • RAM: 4 GB • Hard drive: min. 64 GB • Network: 1 Gbit port
Betriebssystem	SuSE Linux Enterprise Server (SLES), Version 11	SuSE Linux Enterprise Server (SLES), Version 11
Software	IBM WebSphere Service Registry and Repository	IBM WebSphere Service Registry and Repository Version 8.0.0.3
ITC Komponenten	TC TGIC-Service-Register	TC TGIC-Service-Register

Tabelle 6: Deployment - Einheit 3

Database Server mit jeweils zwei redundanten Instanzen		Operative Einsatzumgebung
Hardware	Intel Server: virtualised • CPU: Intel Xeon E5-2643, 3.3 GHz, 1 Core • RAM: 2 GB • Hard drive: min. 64 GB • Network: 1 Gbit port	Intel Server: virtualised • CPU: Intel Xeon E5-2643, 3.3 GHz, 1 Core • RAM: 4 GB • Hard drive: min. 64 GB • Network: 1 Gbit port
Betriebssystem	SuSE Linux Enterprise Server (SLES), Version 11	SuSE Linux Enterprise Server (SLES), Version 11
Software	IBM DB2 Enterprise Server Edition	IBM DB2 Enterprise Server Edition Version 9.7.0.9
ITC Komponenten	ITC DB	ITC DB

Tabelle 7: Deployment - Einheit 4

Directory Server mit jeweils zwei redundanten Instanzen		Operative Einsatzumgebung
Hardware	Intel Server: virtualised • CPU: Intel Xeon E5-2643, 3.3 GHz, 1 Core • RAM: 8 GB • Hard drive: min. 64 GB • Network: 1 Gbit port	Intel Server: virtualised • CPU: Intel Xeon E5-2643, 3.3 GHz, 1 Core • RAM: 4 GB • Hard drive: min. 64 GB • Network: 1 Gbit port
Betriebssystem	SuSE Linux Enterprise Server (SLES), Version 11	SuSE Linux Enterprise Server (SLES), Version 11
Software	IBM Tivoli Directory Server	IBM DB2 Enterprise Server Edition Version 6.3.0.24
ITC Komponenten	ITC LDAP	ITC LDAP

Tabelle 8: Deployment - Einheit 5

Testmethode

Der Hersteller hat folgende Werkzeuge zur Durchführung der Tests genutzt:

Werkzeug	Einsatzzweck
SoapUI, Version 5.0.0	OpenSource-Werkzeug welches als TestClient beim Zugriff auf den EVG das Verhalten von WS-Nutzer und WS-Betreiber auf Protokoll-Ebene simuliert.
Oracle Java Runtime Environment (JRE), Version 1.7.0	Java Laufzeitumgebung zur Durchführung der Testfälle.
Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files, Version 7	Notwendig zur Implementierung der benötigten Schlüssellängen für die kryptografischen Algorithmen (z.B. AES256).
• Lenovo ThinkPad T410 with RedHat Enterprise Linux (64bit, Version 6.5) • Lenovo ThinkPad T410 with Windows 7 (64bit and Service Pack 1) • Fujitsu Lifebook S752	Installation der Werkzeuge und Durchführung der Testfälle.
Für die Onlineidentifikation aktivierter Test-nPA der Bundesdruckerei	nPA mit entsprechender sechsstelliger PIN wobei die Person welche von der nPA identifiziert wird als “natürliche Person” in der ITC-Nutzerverwaltung registriert sein muss.
Open eCard App, Version 1.0.6	eID Client für die Authentifikation mit einem nPA.
BSI zertifizierter Class-3 Chipkartenleser ReinerSCT cyberJack RFID komfort (BSI-K-TR-0068-2011)	Kartenleser für die Authentifikation mit einem nPA.
Mobiltelefon	Mobiltelefon für den Erhalt von SMS während der mTAN Authentifikation.

Tabelle 9: Testwerkzeuge und Materialien

Sämtliche Testfälle wurden mit den Notebooks durchgeführt welche in Tabelle 9 aufgelistet sind. Zur Durchführung der Testfälle mit nPA Authentifikation wurde zusätzlich ein Kartenleser, das Werkzeug Open eCard App und eine Test-nPA genutzt wohingegen zur Durchführung der Testfälle mit mTAN Authentifikation ein Mobiltelefon genutzt wurde.

Insgesamt hat der Hersteller systematisch alle TSF Schnittstellen getestet und diese mit den Testfällen abgedeckt.

Ergebnis

Die vom Hersteller beschriebenen Tests decken alle in den Sicherheitsvorgaben [6] angegebenen Sicherheitsfunktionalitäten ab. Für jede prüfbare Aussage der sicherheitsspezifischen Funktionen wurde mindestens ein Testfall definiert und durchgeführt.

Die Testergebnisse demonstrieren, dass es keine Diskrepanzen zwischen dem EVG-Verhalten und der EVG-Spezifikation gibt.

7.2 Prüfstellentests

Testkonfiguration

Die Prüfstellentests wurden mit derselben Hard- und Softwarekonfiguration wie die Herstellertests durchgeführt.

Testabdeckung

Alle EVG Sicherheitsfunktionalitäten wurden getestet:

- SF1: Security Audit,
- SF2: Identification & Authentication,
- SF3: Security Token Service und

- SF4: Security Management.

Der Evaluator hat beschlossen alle Herstellertests zu wiederholen. Dieses Vorgehen deckt alle Funktionalitäten des EVG ab, indem alle EVG Sicherheitsfunktionalitäten adressiert werden und bestätigt, dass der EVG wie spezifiziert agiert. Der Evaluator hat alle in der funktionalen Spezifikation dokumentierten TSF-Schnittstellen getestet.

Testergebnis

Während der Prüfstellentests agierte der EVG wie spezifiziert. Der Evaluator konnte alle Ergebnisse der Herstellertests welche in der Testdokumentation angegeben sind verifizieren.

7.3 Penetrationstests der Prüfstelle

Testkonfiguration

Der EVG wurde in seiner finalen operativen Einsatzumgebung getestet wo es entsprechend seiner Benutzeranleitung installiert wurde. Die EVG-Parameter wurden während der Tests nur in den Bereichen gesetzt, welche in der Benutzeranleitung als erlaubt definiert sind. Jede zu Penetrationstestzwecken notwendige invasive Modifikation wurde nach den spezifischen Testfällen zurückgesetzt, um einen klar definierten Zustand für jedes Angriffsszenario zu haben.

Die Penetrationstests wurden durchgeführt, indem die Testumgebung des Herstellers genutzt wurde. Diese Testumgebung deckt die operative Einsatzumgebung sowie die vom Hersteller genannten Testwerkzeuge und Testkonfigurationen ab. Diese wurden durch Standardwerkzeuge der Prüfstelle für Penetrationstests ergänzt.

Im Kontext des CC-zertifizierten Betriebes ist für den zugrundeliegenden IBM WebSphere DataPower Service Gateway XG45 (BSI-DSZ-CC-0901) der Modus PRODUKTION verpflichtend (siehe Kapitel 8). Dies führt zu der Tatsache, dass es nur eine evaluierte Konfiguration des EVG gibt und diese auch getestet wurde.

Penetrationstestmethode

Der Evaluator entwickelte die Angriffsszenarios für die Penetrationstests auf Basis einer Liste von potentiellen Schwachstellen welche auf den EVG oder seine operative Einsatzumgebung zutreffen und in der operative Einsatzumgebung ausnutzbar sein könnten.

Dabei hat er auch die Aspekte der Sicherheitsarchitekturbeschreibung und alle anderen Inputs für Penetrationstests betrachtet.

Im Allgemeinen fokussierte sich der Evaluator auf die Abdeckung der TSF-Schnittstellen, Subsysteme und Funktionalitäten, ebenso wie auf die sichere Operation der zugrundeliegenden Komponenten.

Das Folgende wurde betrachtet:

- In Bezug auf die TSF-Schnittstellen wurde der Fokus der Penetrationstests auf alle TSF-Schnittstellen gesetzt, wobei die drei EVG-Funktionen Issuance-, Cancel- und Validation Binding sowie die Managementfunktionalität getestet wurden.
- In Bezug auf die getesteten Subsysteme und die EVG-Funktionalität stellte der Evaluator sicher, dass jedes Subsystem und seine bedrohten - im Rahmen der Schwachstellenuntersuchung betrachteten - Funktionalitäten getestet wurden.

- In Bezug auf sicherheitsrelevante Hardware und Software in der Umgebung, betrachtete der Evaluator Aspekte welche durch Missbrauch oder durch falsche Konfiguration der zugrundeliegenden Komponenten auftreten können.

Testergebnis

Der EVG hat die Prüfstellentests erfolgreich bestanden. Kein Angriffsszenario mit dem Angriffspotential Basic war in der operativen Einsatzumgebung des EVG erfolgreich. Insgesamt bestätigen die Tests die EVG-Funktionalitäten wie sie in den Herstellerdokumenten beschrieben sind. Mit der Durchführung der Schwachstellenanalyse hat die Prüfstelle festgestellt, dass der EVG frei von Schwachstellen ist, welche durch einen Angreifer mit dem Angriffspotential Basic ausnutzbar sind.

8 Evaluierte Konfiguration

Dieses Zertifikat bezieht sich auf die folgenden Konfigurationen des EVG: Der evaluierte EVG ist der Insurance Security Token Service V1.0. Der Hersteller gibt an, dass für den Betrieb des EVG im Rahmen der CC-Zertifizierung keine unterschiedlichen Operationsmodi vorgesehen sind. Der zugrundeliegende IBM WebSphere DataPower Service Gateway XG45 Service besitzt jedoch den Parameter „BetriebsArt" welcher drei verschiedene Werte annehmen kann:

- Test – Rückgabe detaillierter Fehlermeldungen; Testkonfiguration für die mTANAuthentifikation.
- TestMitMTAN – Rückgabe detaillierter Fehlermeldungen; mTAN-Authentifikation mit Versand realer SMS.
- PRODUKTION – Rückgabe von knappen Fehlermeldungen; mTAN-Authentifikation mit Versand realer SMS

Für den Betrieb des EVG im Rahmen der CC-Zertifizierung ist der Wert „PRODUKTION" verpflichtend. Falls keiner dieser drei Werte für die Betriebsart korrekt konfiguriert wurde, wird automatisch die Einstellung „PRODUKTION" verwendet, welches die sicherste Einstellung ist.

Die zugrundeliegende Plattform des EVG ist IBM WebSphere DataPower Service Gateway XG45 (Type 7198) mit der Firmwareversion 6.0. Die Firmware vergibt Zeitstempel, stellt für den EVG das Dateisystem, die kryptografischen Funktionen sowie die Datenbank zur Verfügung.

Die operative Einsatzumgebung des EVG kann wie folgend zusammengefasst werden:

- SMS-Server: Das SMS Gateway wird für den Versand von generierten mTANs an das Mobiltelefon eines Nutzers verwendet.
- ITC ISTS-eID-Connector: Dient als Bindeglied zum eID-Server, der wiederum vollständig die Authentifizierung eines Benutzers durch die eID Funktion des neuen Personalausweises (nPA) übernimmt.
- ITC TGIC-Service-Register (Trusted German Insurance Cloud Service Register im Insurance Trust Center): Beinhaltet Informationen über die bekannten Webservices.
- ITC LDAP: Datenbank im ITC, die alle Benutzerdaten vorhält.
- ITC DB: Datenbank mit ISTS bezogenen Daten im ITC.

Weitere Komponenten, die nicht direkt für die Funktion des EVG notwendig sind, aber zur unmittelbaren Umgebung des EVG gehören sind folgende:

- ITC PKI (Public Key Infrastructure im Insurance Trust Center): Handhabt die gesamte Verwaltung, Signierung, Verifizierung von X.509 Zertifikaten.
- ITC Nutzerverwaltung: Zuständig für die Nutzerverwaltung innerhalb des Insurance Trust Centers (ITC).
- EID-Server: Übernimmt vollständig die Authentifikation eines Nutzers über die eID-Funktion des neuen Personalausweises (nPA) und stellt dem ITC ISTS-eID-Connector anschließend das entsprechende Ergebnis zur Verfügung.
- Mail-Gateway: Mit dem Mail-Gateway werden Benachrichtigungen an den Nutzer versandt. Das Mail-Gateway ist für den ISTS (CC) nicht relevant. Es wird durch die gesonderte Komponente „ITC Nutzerverwaltung“ verwendet, um den Nutzer in verschiedenen Fällen (Mitteilung über die Erfolgreiche Nutzeranlage / Mitteilung über den Ablauf von X.509-Zertifikaten) zu benachrichtigen.

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 verwendet.

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

- Alle Komponenten der Vertrauenswürdigkeitsstufe EAL 2 der CC (siehe auch Teil C des Zertifizierungsreports)

Die Evaluierung hat gezeigt:

- PP Konformität: None
- Funktionalität: Produktspezifische Sicherheitsvorgaben
  Common Criteria Teil 2 erweitert
- Vertrauenswürdigkeit: Common Criteria Teil 3 konform
  EAL 2

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 kryptographischen Mechanismen. Folglich waren solche Mechnismen 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 Politiken wie in den Sicherheitsvorgaben dargelegt, die nicht durch den EVG selbst sondern durch die Einsatzumgebung erbracht werden müssen, zu berücksichtigen.

Der Anwender des Produktes muss die Ergebnisse dieser Zertifizierung in seinem 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.

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

AES Advanced Encryption Standard

BSI Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany

BSIG BSI-Gesetz

CA Certificate Authority

CBC Cipher Block Chaining

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

DB Database / Datenbank

EAL Evaluation Assurance Level - Vertrauenswürdigkeitsstufe

eID Elektronische Identifizierungsfunktion (des Personalausweises)

ETR Evaluation Technical Report

ISTS Insurance Security Token Services (GDV)

EVG Evaluierungsgegenstand (EVG)

GDV	Gesamtverband der Deutschen Versicherungswirtschaft e.V.
IBM	International Business Machines (konkret: IBM Deutschland GmbH)
IT	Information technologie - Informationstechnologie
ITC	Insurance Trust Center (des GDV)
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	Information Technology Security Evaluation Facility – Prüfstelle für IT-Sicherheit
LDAP	Lightweight Directory Access Protocol
mTAN	Mobile Transaktionsnummer
nPA	Neuer Personalausweis
PKI	Public Key Infrastructure
PP	Protection Profile - Schutzprofil
RST	Request Security Token (WS-Trust)
RSTR	Request Security Token Response (WS-Trust)
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
SMS	Short Message Service
ST	Security Target – Sicherheitsvorgaben
STS	Security Token Service
TGIC	Trusted German Insurance Cloud (GDV)
TOE	Target of Evaluation –Evaluierungsgegenstand
TSC	TSF Scope of Control – Anwendungsbereich der TSF-Kontrolle
TSF	TOE Security Functions - EVG-Sicherheitsfunktionalität
WS	Web Service
X.509	ITU-T-Standard für PKI-Zertifikate
XML	Extensible Markup Language

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 – Software, 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[8].

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

[6] Sicherheitsvorgaben BSI-DSZ-CC-0943-2015, Version 2.3, 27.01.2015, Insurance Security Token Service (ISTS), GDV Services GmbH

[7] Evaluierungsbericht, Version 5, 19.02.2015, ETR Summary, TÜV Informationstechnik GmbH (vertrauliches Dokument)

[8] Konfigurationsliste für den EVG, Version 0.9, 05.12.2014, Insurance Security Token Service, Life Cycle Support, Common Criteria Evaluation ALC (vertrauliches Dokument)

[9] Dokumentation für den EVG:
a) Insurance Security Token Service Betriebshandbuch,Version 0.9, 25.07.2014.
b) Insurance Security Token Service Preparative Procedures Common Criteria Evaluation AGD_PRE, Version 0.8, 2014-10-30.
c) Insurance Security Token Service Operational User Guidance Common Criteria Evaluation AGD_OPE, Version 0.9, 2014-10-29.
d) Insurance Security Token Service Anbindungsleitfaden für Webservice-Betreiber und Webservice-Nutzer in der TGIC, Version 1.0.1, 2014-05-23.

[10] XML Digital Signature Syntax and Processing, 2nd Edition, 10.06.2008, Eastlake et al.

[11] RFC6931: Additional XML Security Uniform Resource Identifiers (URIs). Internet Engineering Task Force (IETF), April 2013 (https://tools.ietf.org/rfc/rfc6931.txt).

[12] XML Encryption Syntax and Processing, Eastlake et al., 10.12.2002 (http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/)

[8] Insbesondere:

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

Dies ist eine eingefügte Leerseite.

C Auszüge aus den Kriterien

Anmerkung: Die folgenden Auszüge aus den technischen Regelwerken wurden aus der englischen Originalfassung der CC Version 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 APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements 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 ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification 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 ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation

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