Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

# BSI-DSZ-CC-1265-2026

zu

# Insurance Security Token Server (ISTS), Version 2.1

der

# GDV Dienstleistungs-GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, 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

Bundesamt
für Sicherheit in der
Informationstechnik

# Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

**BSI-DSZ-CC-1265-2026** (*)

Serveranwendungen: Sonstige

**Insurance Security Token Server (ISTS)**
Version 2.1

| | |
|---|---|
| von | GDV Dienstleistungs-GmbH |
| PP-Konformität: | Keine |
| Funktionalität: | Produktspezifische Sicherheitsvorgaben<br>Common Criteria Teil 2 erweitert |
| Vertrauenswürdigkeit: | Common Criteria Teil 3 konform<br>EAL 2 |
| Gültig bis: | 09. Februar 2031 |

SOGIS
Recognition Agreement

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), CEM:2022 ergänzt um Interpretationen des Zertifizierungsschemas unter Nutzung der Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, CC:2022 (CC) evaluiert. CC und CEM sind ebenso als Norm ISO/IEC 15408 und ISO/IEC 18045 veröffentlicht.

(*) Dieses Zertifikat gilt nur für die angegebene Version des Produktes in der evaluierten Konfiguration und nur in Verbindung mit dem vollständigen Zertifizierungsreport und -bescheid. Details zur Gültigkeit sind dem Zertifizierungsreport Teil A, Kap. 5 zu entnehmen.

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, 10. Februar 2026

Bundesamt für Sicherheit in der Informationstechnik

Im Auftrag

Fabian Hodouschek
Leiter der Zertifizierungsstelle

L.S.

Sandro Amendola
Direktor Abteilung S

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

**Bundesamt für Sicherheit in der Informationstechnik**
Godesberger Allee 87 - 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.

# Gliederung

# A. Zertifizierung

## 1. 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.

## 2. Grundlagen des Zertifizierungsverfahrens

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

- BSI-Gesetz[1]
- BSI-Zertifizierungs- und - Anerkennungsverordnung[2]
- Besondere Gebührenverordnung BMI (BMIBGebV)[3]
- besondere Erlasse des Bundesministeriums des Innern
- die Norm DIN EN ISO/IEC 17065
- BSI-Zertifizierung: Verfahrensdokumentation zum Zertifizierungsprozess (CC-Produkte) [3]
- BSI Zertifizierung: Verfahrensdokumentation zu Anforderungen an Prüfstellen, deren Anerkennung und Lizenzierung (CC-Stellen) [3]
- Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria for Information Technology Security Evaluation/CC), CC:2022[4] [1], auch als Norm ISO/IEC 15408 veröffentlicht

1 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) vom 2 December 2025, BGBl. 2025 , Nr. 301, S. 2

2 Verordnung über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI-Zertifizierungs- und - Anerkennungsverordnung - BSIZertV) vom 02 Dezember 2025, Bundesgesetzblatt 2025, Nr. 301

3 Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen indessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) vom 2. September 2019, Bundesgesetzblatt I S. 1365

4 Bekanntmachung des Bundesamtes für Sicherheit in der Informationstechnik vom 14. April 2023 auf https://www.bsi.bund.de

- Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Methodology for Information Technology Security Evaluation/CEM), CEM:2022 [2] auch als Norm ISO/IEC 18045 veröffentlicht
- BSI-Zertifizierung: Anwendungshinweise und Interpretationen zum Schema (AIS) [4]

# 3. 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.

## 3.1. Europäische Anerkennung von 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 (SOGIS Technical Domain) auf höheren Anerkennungsstufen fest.

Die Basisanerkennungsstufe schließt die Common Criteria (CC) Vertrauenswürdigkeitsstufen EAL 1 bis EAL 4 ein. Für Produkte im technischen Bereich "smartcard and similar devices" ist eine SOGIS Technical Domain festgelegt. Für Produkte im technischen Bereich "HW Devices with Security Boxes" ist ebenfalls eine SOGIS Technical Domain festgelegt. Des Weiteren erfasst das Anerkennungsabkommen auch erteilte Zertifikate für Schutzprofile (Protection Profiles) basierend auf den Common Criteria.

Eine aktuelle Liste der Unterzeichnerstaaten bzw. der anerkannten Zertifizierungsstellen, Details zur Anerkennung sowie zur Historie des Abkommens können auf der Internetseite https://www.sogis.eu eingesehen werden.

Das SOGIS-MRA-Logo auf dem Zertifikat zeigt, dass das Zertifikat unter den Bedingungen des Abkommens von den jeweiligen Stellen der Unterzeichnerstaaten als gleichwertig anerkannt wird. Ein Hinweis unter dem Logo weist auf einen spezifischen Umfang der Anerkennung hin.

Dieses Zertifikat fällt mit allen ausgewählten Vertrauenswürdigkeitskomponenten unter die Anerkennung nach SOGIS-MRA.

## 3.2. Internationale Anerkennung von CC - Zertifikaten

Das internationale Abkommen zur gegenseitigen Anerkennung von Zertifikaten basierend auf CC (Common Criteria Recognition Arrangement, CCRA-2014) wurde am 8. September 2014 ratifiziert. Es deckt CC-Zertifikate ab, die auf sog. collaborative Protection Profiles (cPP) (exact use) basieren, CC-Zertifikate, die auf Vertrauenswürdigkeitsstufen bis einschließlich EAL 2 oder die Vertrauenswürdigkeitsfamilie Fehlerbehebung (Flaw Remediation, ALC_FLR) basieren und CC Zertifikate für Schutzprofile (Protection Profiles) und für collaborative Protection Profiles (cPP).

Eine aktuelle Liste der Unterzeichnerstaaten bzw. der anerkannten Zertifizierungsstellen kann auf der Internetseite https://www.commoncriteriaportal.org eingesehen werden.

Das CCRA-Logo auf dem Zertifikat zeigt, dass das Zertifikat unter den Bedingungen des Abkommens von den jeweiligen Stellen der Unterzeichnerstaaten als gleichwertig anerkannt wird. Ein Hinweis unter dem Logo weist auf einen spezifischen Umfang der Anerkennung hin.

Dieses Zertifikat fällt unter die Anerkennungsregeln des CCRA-2014 für alle ausgewählten Vertrauenswürdigkeitskomponenten.

# 4. 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 Server (ISTS), Version 2.1 hat das Zertifizierungsverfahren beim BSI durchlaufen. Es handelt sich um eine Rezertifizierung basierend auf BSI-DSZ-CC-1150-2021. Für diese Evaluierung wurden bestimmte Ergebnisse aus dem Evaluierungsprozess BSI-DSZ-CC-1150-2021 wiederverwendet.

Die Evaluation des Produkts Insurance Security Token Server (ISTS), Version 2.1 wurde von TÜV Informationstechnik GmbH durchgeführt. Die Evaluierung wurde am 27. Januar 2026 abgeschlossen. Das Prüflabor TÜV Informationstechnik GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[5].

Der Sponsor und Antragsteller ist: GDV Dienstleistungs-GmbH.

Das Produkt wurde entwickelt von: GDV Dienstleistungs-GmbH.

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

# 5. Gültigkeit des Zertifizierungsergebnisses

Dieser Zertifizierungsreport bezieht sich nur auf die angegebene Version des Produktes. Das Produkt ist unter den folgenden Bedingungen konform zu den bestätigten Vertrauenswürdigkeitskomponenten:

- alle Auflagen hinsichtlich der Generierung, der Konfiguration und dem Einsatz des EVG, die in der Guidance aufgeführt sind werden beachtet,
- das Produkt wird in der operativen Einsatzumgebung betrieben, die in den Sicherheitsvorgaben beschrieben ist.

Die Bedeutung der Vertrauenswürdigkeitskomponenten und -stufen kann direkt den CC entnommen werden. Detaillierte Referenzen sind in Teil C dieses Reportes aufgelistet.

Das Zertifikat bestätigt die Vertrauenswürdigkeit des Produktes gemäß den Sicherheitsvorgaben. 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 Neubewertung oder eine Re-Zertifizierung). Insbesondere wenn Ergebnisse aus dem Zertifizierungsverfahren in einem nachfolgenden Evaluierung- und Zertifizierungsverfahren oder in einer Systemintegration verwendet werden oder wenn das Risikomanagement

[5] Information Technology Security Evaluation Facility

eines Anwenders eine regelmäßige Aktualisierung verlangt, wird empfohlen, die Neubewertung der Widerstandsfähigkeit regelmäßig, z.B. jährlich vorzunehmen. Dabei behält sich das BSI das Recht vor das Zertifikat zurück zu ziehen, besonders wenn eine ausnutzbare Schwachstelle des zertifizierten Produktes bekannt wird.

Um in Anbetracht der sich weiter entwickelnden Angriffsmethoden eine unbefristete Anwendung des Zertifikates trotz der Erfordernis nach einer Neubewertung nach den Stand der Technik zu verhindern, wurde die maximale Gültigkeit des Zertifikates begrenzt. Dieses Zertifikat, erteilt am 10. Februar 2026, ist gültig bis 09. Februar 2031. Die Gültigkeit kann im Rahmen einer Re-Zertifizierung erneuert werden.

Der Inhaber des Zertifikates ist verpflichtet,

1. 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 zertifizierten Produktes zur Verfügung zu stellen,
2. die Zertifizierungsstelle des BSI unverzüglich über Schwachstellen des Produktes zu informieren, die nach dem Zeitpunkt der Zertifizierung durch Sie oder Dritte festgestellt wurden,
3. 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 Evaluierungsgegenstand oder aus dem Evaluierungs- und Zertifizierungsprozess, bei denen die Zertifizierung des Produktes aber von der Aufrechterhaltung der Vertraulichkeit für den Bestand des Zertifikates ausgegangen ist, nicht mehr gegeben ist. Insbesondere ist vor Herausgabe von vertraulichen Unterlagen oder Informationen zum Evaluierungsgegenstand oder aus dem Evaluierungs- und Zertifizierungsprozess, die nicht zum Lieferumfang gemäß Zertifizierungsreport Teil B gehören oder für die keine Weitergaberegelung vereinbart ist, an Dritte, die Zertifizierungsstelle des BSI zu informieren.

Bei Änderungen am Produkt kann die Gültigkeit des Zertifikats auf neue Versionen ausgedehnt werden. Voraussetzung dafür ist, dass der Antragsteller die Aufrechterhaltung der Vertrauenswürdigkeit (d.h. eine Re-Zertifizierung oder ein Maintenance Verfahren) in Übereinstimmung mit den entsprechenden Regeln beantragt und die Evaluierung keine Schwächen aufdeckt.

# 6. Veröffentlichung

Das Produkt Insurance Security Token Server (ISTS), Version 2.1 ist in die BSI-Liste der zertifizierten Produkte, die regelmäßig veröffentlicht wird, aufgenommen worden. Siehe auch auf der Website des BSI: https://www.bsi.bund.de/dok/Zertifizierung-Gesamtlisten. Nähere Informationen sind auch über die BSI-Infoline 0228/9582-111 zu erhalten.

Weitere Exemplare des vorliegenden Zertifizierungsreports können beim Hersteller des Produktes angefordert werden[6]. Der Zertifizierungsreport kann ebenso in elektronischer Form von der oben angegebenen Internetadresse heruntergeladen werden.

[6] GDV Dienstleistungs-GmbH
Frankenstraße 18
20097 Hamburg
Deutschland

# B. Zertifizierungsbericht

Der nachfolgende Bericht ist eine Zusammenfassung aus

- den Sicherheitsvorgaben des Antragstellers für den Evaluationsgegenstand,
- den entsprechenden Prüfergebnissen des Prüflabors und
- ergänzenden Hinweisen und Auflagen der Zertifizierungsstelle.

# 1. Zusammenfassung

Bei dem Evaluationsgegenstand (EVG) handelt es sich um den Produkttyp eines Security Token Services (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, und das Management von Sicherheitsfunktionalitäten.

Die Sicherheitsvorgaben [5] 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 [5] Kapitel 6.1 beschrieben. Sie wurden dem Teil 2 der Common Criteria entnommen und durch neu definierte funktionale Sicherheitsanforderungen ergänzt. Die im ST verwendeten SFRs sind daher erweitert zum Teil 2 der Common Criteria.

Die funktionalen Sicherheitsanforderungen werden durch die folgende Sicherheitsfunktionalität des EVG umgesetzt:

| **Sicherheitsfunktionalität des EVG** | **Thema** |
|---|---|
| SF1 | SF1 – 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 | SF2 – Die Funktionalität Identification & Authentication wird während der Authentifikation durch X.509-Zertifikate, mTAN, SSO token oder Time-based One-time Password Algorithmus (TOTP) realisiert. Dem entsprechend unterstützt der EVG vier Authentisierungsmechanismen. |
| SF3 | SF3 – Der Security Token Service wird vom TOE realisiert, da es nach erfolgreicher Authentifizierung im Falle eines Issue Bindings ein SAML- oder JWT-Token ausstellt. Das TOE unterstützt auch Anfragen für Cancel Binding (nur für SAML-Tokens) und Validation Binding. Der Dienstnutzer kann außerdem ein „SSO“ (Single Sign-On) Token über WS-Trust oder OAuth2 anfordern, welches verwendet werden kann, um weitere Authentifizierungstokens vom TOE anzufordern. Diese Tokens können für Authentifizierungszwecke der TGIC-Dienste genutzt werden, ohne dass eine neue Authentifizierung erforderlich ist.<br>Das Netzwerkprotokoll für die Kommunikation zwischen |

| Sicherheitsfunktionalität des EVG | Thema |
|---|---|
| | Benutzeragent und ISTS oder TGIC-Webdienst oder ISTS ist SOAP oder REST über HTTPS. Der vertrauenswürdige Kanal und die kryptografischen Operationen werden von der Betriebsumgebung bereitgestellt. |
| SF4 | SF4 – Die Funktionalität Security Management wird dadurch realisiert, dass der EVG über die Möglichkeit verfügt, in Form einer XML-basierten Konfigurationsdatei die Gültigkeitsdauer<br>• einer X.509-Session,<br>• einer generierten mTAN, sowie<br>• einer TOTP Session einzustellen.<br>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 [5] Kapitel 7 dargestellt.

Die Werte, die durch den EVG geschützt werden, sind in den Sicherheitsvorgaben [5], Kapitel 3.1, definiert. Basierend auf diesen Werten stellen die Sicherheitsvorgaben die Sicherheitsumgebung in Form von Annahmen, Bedrohungen und organisatorischen Sicherheitspolitiken in Kapitel 3.5, 3.3 bzw. 3.4 dar.

Dieses Zertifikat umfasst die folgende Konfiguration des EVG: Der evaluierte EVG ist Insurance Security Token Service V2.1. Die zugrundeliegende Plattform des EVG ist IBM DataPower Gateway mit der Firmwareversion 10.6.0.7. Für mehr Details siehe Kapitel 8 dieses Berichtes.

Die Ergebnisse der Schwachstellenanalyse, wie in diesem Zertifikat bestätigt, erfolgte ohne Einbeziehung der für die Ver- und Entschlüsselung eingesetzten kryptographischen Algorithmen (vgl. §52 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 Server (ISTS), Version 2.1**

Die folgende Tabelle 2 beschreibt den Auslieferungsumfang. Bei den Hashwerten handelt es sich um SHA-512 Hashwerte.

| Nr | Typ | Identifier | Version | Auslieferungsart |
|---|---|---|---|---|
| 1 | SW<br>zip-Archiv | TOE:<br>idg-config-20251127.ists-core.zip<br>136ed8988898c19f65e698b52d1b268d6d1bde8798c372f3fc4d550415800892fe93e209b92949d1cc1219865af9ba9aea425b28a532bebc70f8c624bbd3ea58<br>und<br>idg-config-20251202.ists-oauth.zip<br>afb01d03c8962727f540ffdf3bd065d9957c93a41782bd8aaf13d70ea56252fe4481182f542e56a210de5cc086c185f052e95ff21bfb66ddf931cedc359ed567 | 2.1.0 | Auslieferung durch Upload auf GDV GitLab via VPN-Verbindung |
| 2 | DATA | Hash values (SHA-256) for the TOE software parts (no. 1.1–1.107)<br>idg-config-20251127.ists-core.sha512 and idg-config-20251202.ists-oauth.sha512 | - | S/MIME verschlüsselte und signierte E-Mail |
| 3 | DOC | Insurance Security Token Service<br>Operational User Guidance Common Criteria Evaluation AGD_OPE [8] | 1.05 | Auslieferung durch Upload auf GDV GitLab via VPN-Verbindung |
| 4 | DOC | Insurance Security Token Service<br>Preparative Procedures Common Criteria Evaluation AGD_PRE [9] | 1.10 | Auslieferung durch Upload auf GDV GitLab via VPN-Verbindung |
| 5 | DOC | Insurance Security Token Service<br>Anbindungsleitfaden für Service-Betreiber und Service-Nutzer in der TGIC [10] | 1.0 | Auslieferung durch Upload auf GDV GitLab via VPN-Verbindung |
| 6 | DOC | Insurance Trust Center Anbindungsleitfaden ISTS OAuth 2.0 für Service-Betreiber und Service-Nutzer in der TGIC [11] | 1.2 | Auslieferung durch Upload auf GDV GitLab via VPN-Verbindung |
| 7 | DOC | Insurance Trust Center Anbindungsleitfaden für die ISTS-Web-Authentifikation [12] | 2.0.1 | Auslieferung durch Upload auf GDV GitLab via VPN-Verbindung |
| 8 | DOC | Insurance Trust Center: Anbindungsleitfaden für die ITC-Smart-Authentifikation [13] | 1.3 | Auslieferung durch Upload auf GDV GitLab via VPN-Verbindung |
| 9 | zip-Archiv | Insurance Trust Center: Service Gateways Fehlercodes | 0.26 | Auslieferung durch Upload auf GDV GitLab via VPN-Verbindung |
| 10 | DOC | Insurance Trust Center Service Gateway / IDG X2 Deployment [14] | 1.0 | Auslieferung durch Upload auf GDV GitLab via VPN-Verbindung |
| 11 | DOC | Insurance Trust Center: Service Gateway / IDG X2 – Installation & Konfiguration [15] | 1.0.7 | Auslieferung durch Upload auf GDV GitLab via VPN-Verbindung |
| 12 | DOC | ZIP-Archiv mit der technischen Schnittstellenspezifikation des TOE InsuranceSecurityTokenService-2.1.0.wsdl | 2.1.0 | Auslieferung durch Upload auf GDV GitLab via VPN-Verbindung |

| Nr | Typ | Identifier | Version | Auslieferungsart |
|---|---|---|---|---|
| 13 | Web link | https://www.ibm.com/support/knowledgecenter/SS9H2Y_10.0/com.ibm.dp.doc/introduction.html | - | Auslieferung durch Upload auf GDV GitLab via VPN-Verbindung |
| 14 | DOC | Insurance Trust Center Betriebshandbuch [16] | 1.02 | Auslieferung durch Upload auf GDV GitLab via VPN-Verbindung |
| 15 | DOC | Insurance Security Token Service: Database Server / DB2 – Deployment [17] | 1.0 | Auslieferung durch Upload auf GDV GitLab via VPN-Verbindung |
| 16 | DOC | Insurance Security Token Service: Database Server / DB2 v12.1 – Installation & Konfiguration [18] | 0.3 | Auslieferung durch Upload auf GDV GitLab via VPN-Verbindung |
| 17 | DOC | Insurance Security Token Service: Kryptokonzept [19] | 2.0 | Auslieferung durch Upload auf GDV GitLab via VPN-Verbindung |
| 18 | DOC | ITC-Deploymentanleitung-VDS-Migration [20] | 1.0 | Auslieferung durch Upload auf GDV GitLab via VPN-Verbindung |
| 19 | DOC | Directory Server / VDS Installation & Konfiguration [21] | 1.0 | Auslieferung durch Upload auf GDV GitLab via VPN-Verbindung |
| 20 | DOC | Insurance Trust Center Application Server / WAS Deployment Nutzerverwaltung [22] | 2.0 | Auslieferung durch Upload auf GDV GitLab via VPN-Verbindung |
| 21 | DOC | Insurance Trust Center Application Server / WAS Installation & Konfiguration [23] | 1.0 | Auslieferung durch Upload auf GDV GitLab via VPN-Verbindung |
| 22 | DOC | Insurance Trust Center: Service Gateways / IDG – Fehlercodes [24] | 0.30 | Auslieferung durch Upload auf GDV GitLab via VPN-Verbindung |

Tabelle 2: Auslieferungsumfang des EVG

Die Auslieferung des EVG erfolgt in Form von zwei zip-Dateien. Der EVG sowie die Benutzerdokumentation und die Begleitdokumente zur Benutzerdokumentation, werden als Upload auf dem GitLab-System des Benutzers hinterlegt. Der Kommunikationskanal zu diesem Server wird über VPN gesichert. Des Weiteren werden gesondert noch zwei Dateien mit den Hashwerten der TOE Deployment-Module per E-Mail an den Benutzer versendet. Die Kommunikation zwischen Hersteller und Benutzer findet mittels verschlüsselter und signierter E-Mails statt. Dafür werden S/MIME Zertifikate verwendet und die zugehörigen Schlüssel werden regelmäßig ausgetauscht.

Die Deploymentmodule des EVG bestehen aus xsl-, xsd-, wsdl-, xml-, js- und json-Dateien und sind Teil der beiden Deploymentpakete idg-config-20251127.ists-core.zip und idg-config-20251202.ists-oauth.zip.

Während der Erstellung der EVG-Module werden zusätzlich noch jeweils SHA512-Hashwerte über die zip-Archive berechnet und dem ITC-Betreiber als weitere zwei Dateien mit den Namen idg-config-20251127.ists-core.sha512 und idg-config-20251202.ists-oauth.sha512 zur Verfügung gestellt. Die berechneten SHA512-Checksummen werden mit einer per S/MIME verschlüsselten und signierten E-Mail durch den Hersteller an den

Benutzer übermittelt. Wie oben erwähnt, muss vor der Auslieferung ein Austausch der S/MIME-Zertifikate und der öffentlichen Schlüssel von Hersteller und Benutzer stattfinden.

Nach Erhalt des EVG und der SHA512-Hashwerte muss der Benutzer die Checksummen des EVG berechnen und mit den erhaltenen Daten vergleichen, indem er beispielsweise OpenSSL nutzt und die folgenden Befehle in der Kommandozeile eingibt:

openssl dgst –sha512 idg-config-<datum>.ists-core.zip

und

openssl dgst –sha512 idg-config-<datum>. ists-oauth.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: 2.1.0.IBM.2025-11-27 für SAML und 1.2.3.IBM.2025-12-02 für oAuth.

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 die SHA512-Hashwerte verifizieren konnte, werden die ITC-Deploymentpakete an die jeweiligen ITC-Administration weitergeleitet.

Vor der Installation des EVG stellt der Integritätsprüfungsprozess, siehe [7] und [9], sicher, dass der Benutzer die korrekte Version des EVG erhalten hat. Im Detail wird die Integrität der Softwareteile des EVG, siehe Tabelle 2, anhand der SHA512-Hashwerte überprüft, die per E-Mail und als sha512-Dateien bereitgestellt werden. Der Benutzer muss die Hashwerte berechnen, beispielsweise durch die Verwendung von OpenSSL und Eingabe von folgenden Befehlen

openssl dgst –sha512 idg-config-<datum>.ists-core.zip

und

openssl dgst –sha512 idg-config-<datum>.ists-oauth.zip

in der Kommandozeile.

Nur wenn alle Vergleiche erfolgreich sind, wurde die bewertete Version des EVG bereitgestellt. Darüber hinaus kann die Integrität des EVG auch vom Kunden überprüft werden, indem die Versionsdatei local/config/ISTS_version.xml überprüft wird, in der die Anwendungsversion angegeben ist als 2.1.0.IBM.2025-11-27 für SAML und 1.2.3.IBM.2025-12-02 für oAuth.

# 3. Sicherheitspolitik

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

- Security Audit,
- Identification and Authentication,
- Security Token Service und
- Security Management.

Spezifische Einzelheiten zu den oben genannten Sicherheitsmaßnahmen sind in Kapitel 7 in [5] zu finden.

# 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 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-512 erstellt wurden. |

Tabelle 3: Sicherheitsziele für die operative Umgebung

Details finden sich in den Sicherheitsvorgaben [5], Kapitel 4.2. Der Administrator wird in [8] über die Maßnahmen informiert.

# 5. Informationen zur Architektur

Der EVG besteht aus den folgenden Subsystemen:

| Subsystem | Interface/ Domain | Beschreibung |
|---|---|---|
| InsuranceSecurityTokenService_rule_IssueRST_TGT | SAML / ISTS-CORE-Domain | Auslesen der Konfiguration aus der Operativen Umgebung des TOE.<br>Anfrage zum Erstellen eines Tokens aufnehmen und gegen Spezifikation prüfen. Mitgelieferten SSO-Token validieren und grobe Prüfung der Zulässigkeit der Anfrage durchführen. Korrektheit des SSO-Tokens durch das Erstellen des Tokens bestätigen. Das Erstellen des Tokens ins Protokoll revisionssicher schreiben. |
| InsuranceSecurityTokenService_rule_IssueRST | SAML / ISTS-CORE-Domain | Auslesen der Konfiguration aus der Operativen Umgebung des TOE.<br>Anfrage zum Erstellen eines Tokens aufnehmen und gegen Spezifikation prüfen. |

| | | |
|---|---|---|
| | | Benutzerdaten abrufen und grobe Prüfung der Zulässigkeit der Anfrage durchführen.<br>Solange im Request nicht vorgegeben, Art der unterstützbaren Authentifizierung feststellen (X.509, mTAN oder TOTP).<br>Authentifizierungsrückfrage (Challenge Response) generieren. |
| InsuranceSecurityTokenService_rule_IssueRSTR | SAML / ISTS-CORE-Domain | Auslesen der Konfiguration aus der operativen Umgebung des TOE.<br>Antwort auf die Authentifizierungsabfrage aufnehmen und gegen Spezifikation prüfen.<br>Authentifizierung durchführen und durch das Erstellen des Tokens bestätigen.<br>Erstellen des Tokens ins Protokoll revisionssicher schreiben. |
| InsuranceSecurityToken-Service_rule_CancelRST_TGT | SAML / ISTS-CORE-Domain | Auslesen der Konfiguration aus der operativen Umgebung des TOE.<br>Anfrage zum Widerrufen eines Tokens sowie SSO-Token aufnehmen und gegen Spezifikation prüfen, validieren.<br>Benutzer- und Token-Daten abrufen und grobe Prüfung auf die Zulässigkeit der Anfrage durchführen. Das Widerrufen des Tokens bestätigen.<br>Widerruf des Tokens ins Protokoll revisionssicher schreiben. |
| InsuranceSecurityToken-Service_rule_CancelRST | SAML / ISTS-CORE-Domain | Auslesen der Konfiguration aus der operativen Umgebung des TOE.<br>Anfrage zum Widerrufen eines Tokens aufnehmen und gegen Spezifikation prüfen.<br>Benutzer- und Token-Daten abrufen und grobe Prüfung auf die Zulässigkeit der Anfrage durchführen.<br>Solange im Request nicht vorgegeben, Art der unterstützbaren Authentifizierung feststellen (X.509, mTAN oder TOTP).<br>Authentifizierungsrückfrage (Challenge Response) generieren. |
| InsuranceSecurityToken-Service_rule_CancelRSTR | SAML / ISTS-CORE-Domain | Auslesen der Konfiguration aus der operativen Umgebung des TOE.<br>Antwort auf die Authentifizierungsabfrage aufnehmen und gegen Spezifikation prüfen.<br>Authentifizierung durchführen und durch das Widerrufen des Tokens bestätigen.<br>Widerruf des Tokens ins Protokoll revisionssicher schreiben. |
| InsuranceSecurityToken-Service_rule_Validate | SAML / ISTS-CORE-Domain | Auslesen der Konfiguration aus der operativen Umgebung des TOE. |

| | | |
|---|---|---|
| | | Anfrage zur Überprüfung des Tokens aufnehmen und gegen Spezifikation prüfen.<br>Token durch die Umgebung entschlüsseln und anschließend überprüfen.<br>Den Vorgang der Prüfung ins Protokoll revisionssicher schreiben. |
| InsuranceSecurityTokenService_rule_Other | SAML / ISTS-CORE-Domain | Abfangen sonstiger Anfragen. |
| InsuranceSecurityToken-Service_rule_Error | SAML / ISTS-CORE-Domain | Abfangen der Fehlermeldungen aus den Subsystemen oben. |
| InsuranceSecurityTokenService_rule_OAuthIssueRST_TGT | JWT / ISTS-O-AUTH-Domain | Auslesen der Konfiguration aus der Operativen Umgebung des TOE.<br>Anfrage zum Erstellen eines Tokens aufnehmen und gegen Spezifikation prüfen. Mitgelieferten SSO-Token validieren und grobe Prüfung der Zulässigkeit der Anfrage durchführen. Korrektheit des SSO-Tokens durch das Erstellen des Tokens bestätigen. Das Erstellen des Tokens ins Protokoll revisionssicher schreiben. |
| InsuranceSecurityTokenService_rule_OAuthIssueRSTR | JWT / ISTS-O-AUTH-Domain | Auslesen der Konfiguration aus der operativen Umgebung des TOE.<br>Antwort auf die Authentifizierungsabfrage aufnehmen und gegen Spezifikation prüfen.<br>Authentifizierung durchführen und durch das Erstellen des Tokens bestätigen.<br>Erstellen des Tokens ins Protokoll revisionssicher schreiben. |
| ISTS-OAuth_rule_oauth-challenge | JWT / ISTS-O-AUTH-Domain | Auslesen der Konfiguration aus der operativen Umgebung des TOE.<br>Validierung des Formats der oAuth-Anfrage.<br>Validierung der Authentifikationsinformationen aus dem oAuth-Request.<br>Erstellung einer Response-Nachricht.<br>Triggern der SAML-Schnittstelle für die Validierung der Anfrage.<br>Vorbereitung des Zertifikats.<br>Konvertieren des SAML in JWT.<br>Konvertieren eines JSONX in JSON-Format. |
| ISTS-OAuth_rule_oauth-token | JWT / ISTS-O-AUTH-Domain | Zuordnung von grant-type zu DataPower-Variablen.<br>Auslesen der Konfiguration aus der operativen Umgebung des TOE.<br>Validierung des Formats der oAuth-Anfrage.<br>Triggern der SAML-Schnittstelle für die Validierung der Anfrage. |

| | | |
|---|---|---|
| | | Erstellen finales JWT. |
| ISTS-OAuth_rule_oauth-introspection | JWT / ISTS-O-AUTH-Domain | Auslesen der Konfiguration aus der operativen Umgebung des TOE.<br>Validierung der Authentifikationsinformationen aus dem Request, Validierung der Tokengültigkeit |
| ISTS-OAuth_rule_deny | JWT / ISTS-O-AUTH-Domain | Blockieren sonstigen Anfragen. |
| ISTS-OAuth_rule_error | JWT / ISTS-O-AUTH-Domain | Fehlerbehandlung.<br>Konvertieren eines JSONX in JSON-Format. |
| ISTS-OAuth_rule_token-exchange | JWT / ISTS-O-AUTH-Domain | Vorbereitung zum Tockenbearbeitung.<br>Konvertieren aus dem JWT in SAML-Format.<br>Vorbereitung der SAML-Anfrage an ists-core.<br>Triggern des ists-core.<br>Vorbereitung des Zertifikats.<br>Konvertieren aus dem SAML-Format in JWT-Format.<br>Konvertieren eines JSONX in JSON-Format.<br>Setzen des ContentType. |

Tabelle 4: Subsysteme 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

Zusammenfassung der Testergebnisse und der Schwachstellenanalyse:

Der EVG hat die Prüfstellentests erfolgreich bestanden. 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.

## 7.1. Herstellertests

Testkonfiguration:

Der EVG ist ein Teil des gesamten Deploymentpakets Insurance Trust Center (ITC), welches aus vier verschiedenen Modulen besteht. Dabei wird der EVG-Teil durch idg-config-20251127.ists-core.zip und idg-config-20251202.ists-oauth.zip repräsentiert. Aus diesem Grunde werden alle vier Deploymenteinheiten des ITC für den Einsatz des EVG

und die Durchführung der Tests benötigt. Der Hersteller lieferte in [7] die komplette Installationsanleitung für jede der notwendigen Deploymenteinheiten.

Testmethode:

Der Hersteller hat folgende Werkzeuge zur Durchführung der Tests genutzt:

| Tools / Materialien | Zweck / Beschreibung |
|---|---|
| SoapUI, Version 5.9.1 | Testclient für den Zugriff auf den EVG, wobei das Verhalten von Web-Service-Benutzern und Web-Service-Betreibern im realen Betrieb simuliert wird. |
| Oracle Java Runtime Environment (JRE), Version 17.0.12 | Java-Laufzeitumgebung für die Durchführung der Testfälle. |
| Virtueller-PC | Intel(R) Xeon(R) Gold 6226R CPU @ 2.90GHz 2.89 GHz (2 Prozesso-ren), Windows 10 Enterprise, 21H2, 02.05.2022<br>Installation der Testwerkzeuge und Durchführung der Testfälle. |

Tabelle 5: Genutzte Testtools und Materialen

Sämtliche Testfälle wurden mit dem Virtuellen PC, welcher in Tabelle 5 aufgelistet ist, durchgeführt. Insgesamt hat der Hersteller systematisch alle TSF-Schnittstellen angegeben sind, getestet und diese mit den Testfällen abgedeckt.

Ergebnis:

Die vom Hersteller beschriebenen Tests decken alle in den Sicherheitsvorgaben [5] 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

EVG-Testkonfiguration:

Der Hersteller gibt in [8] an, dass für den Betrieb des EVG im Rahmen der CC-Zertifizierung keine unterschiedlichen Operationsmodi vorgesehen sind.

Der zugrundeliegende IBM DataPower Gateway Service besitzt aber den Parameter „BetriebsArt” welcher vier verschiedene Werte annehmen kann:

- Test – Rückgabe detaillierter Fehlermeldungen; Testkonfiguration für die mTAN-Authentifikation.
- TestMitMTAN – Rückgabe detaillierter Fehlermeldungen; mTAN-Authentifikation mit Versand realer SMS.
- TestMitTOTP – Rückgabe detaillierter Fehlermeldungen; TOTP-Authentifikation mit real berechnetem TOTP-Token.

- PRODUKTION – Rückgabe von knappen Fehlermeldungen; mTAN-Authentifikation mit Versand realer SMS und real berechneten TOTP-Token

Für den Betrieb des EVG im Rahmen der CC-Zertifizierung ist allerdings 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 DataPower Gateway mit der Firmware Version 10.6.0.7. Die Firmware vergibt Zeitstempel, stellt für den EVG das Dateisystem, die kryptografischen Funktionen, sowie die Datenbank zur Verfügung.

Während der Prüfstellentests wurden alle Herstellertests wiederholt.

Ausgesuchte Untermenge:

Alle EVG Sicherheitsfunktionalitäten wurden getestet:

- SF1: Security Audit,
- SF2: Identification & Authentication,
- SF3: Security Token Service und
- SF4: Security Management.

Kriterien zur Wahl der Schnittstellenuntermenge: Der Evaluator hat beschlossen alle Herstellertests zu wiederholen. Diese Methode deckt alle Funktionalitäten des EVG ab, indem alle EVG Sicherheitsfunktionalitäten adressiert werden und bestätigt, dass der EVG wie spezifiziert agiert.

Getestete Schnittstellen: Der Evaluator hat alle in der funktionalen Spezifikation dokumentierten TSF-Schnittstellen getestet.

Ausgeführte Herstellertests: Der Evaluator hat alle Herstellertests wiederholt.

Urteil: 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

Überblick:

- 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 für die TÜViT Penetrationstests ergänzt.
- Im Kontext des CC-zertifizierten Betriebes der zugrundeliegenden IBM DataPower Gateway ist der Modus PRODUKTION verpflichtend. Dies führt zu der Tatsache, dass es nur eine evaluierte Konfiguration des EVG gibt und diese auch getestet wurde.
- Kein Angriffsszenario mit dem Angriffspotential Basic war erfolgreich.

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, wenn er der Meinung war, dass diese potentiellen Schwachstellen in der operativen Einsatzumgebung ausnutzbar sein könnten.

Dabei hat er auch die Aspekte der Sicherheitsarchitekturbeschreibung und alle anderen Inputs für Penetrationstests betrachtet. Insbesondere wurde die Testdokumentation des Herstellers genutzt, um herauszufinden, ob es bedenkliche Bereiche gibt, welche durch Prüfstellentests abgedeckt sein müssen.

EVG Testkonfiguration und Testaufbau:

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.

Fokus der Penetrationstests:

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 beide 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 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.

Getestete Angriffsszenarien:

| Angriffsszenario | Beschreibung |
|---|---|
| AS.1 | Operationelle Robustheit<br>Ein Angreifer könnte operative Schwachstellen nutzen, welche direkt ausgenutzt werden oder auch andere Angriffswege öffnen können.<br>Operationelle Robustheit umfasst den richtigen und sicheren Betrieb während der wechselnden Bedingungen von sich wiederholenden Cancel Binding Anfragen. |
| AS.2 | Nicht erlaubte Operationen<br>Ein Angreifer kann Operationen des EVG verwenden, welche nicht für jeden zugänglich sein sollten. |
| AS.3 | Schwache Authentifikation<br>Ein Angreifer könnte schwache Authentifikationsmechanismen nutzen, wenn diese zugänglich sind. |
| AS.4 | Zeitmanipulation |

| | |
|---|---|
| | Ein Angreifer könnte versuchen die Zeitquellen zu manipulieren, was die Nutzung der korrekten Zeit verhindern würde. |
| AS.5 | Ungültige Authentifikationsdaten<br>Ein Angreifer könnte versuchen ungültige Authentifikationsdaten an den EVG senden und dadurch Zugriff zum EVG erlangen was durch Fehler in der Implementierung zugelassen wird. |

Tabelle 6: Angriffsszenarien der Penetrationstests

Urteil: Kein Angriffsszenario mit dem Angriffspotential Basic war in der operativen Einsatzumgebung des EVG erfolgreich.

# 8. Evaluierte Konfiguration

Dieses Zertifikat bezieht sich auf die folgenden Konfigurationen des EVG: Der EVG ist Insurance Security Token Service V2.1. Der Hersteller gibt an, dass für den Betrieb des EVG im Rahmen der CC-Zertifizierung keine unterschiedlichen Operationsmodi vorgesehen sind.

Der zugrundeliegende IBM DataPower Gateway Service besitzt aber den Parameter „BetriebsArt" welcher vier verschiedene Werte annehmen kann:

- Test – Rückgabe detaillierter Fehlermeldungen; Testkonfiguration für die mTAN-Authentifikation.
- TestMitMTAN – Rückgabe detaillierter Fehlermeldungen; mTAN-Authentifikation mit Versand realer SMS.
- TestMitTOTP – Rückgabe detaillierter Fehlermeldungen; TOTP-Authentifikation mit real berechnetem TOTP-Token.
- PRODUKTION – Rückgabe von knappen Fehlermeldungen; mTAN-Authentifikation mit Versand realer SMS und real berechneten TOTP-Token.

Für den Betrieb des EVG im Rahmen der CC-Zertifizierung ist allerdings 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 DataPower Gateway mit Firmware Version 10.6.0.7. 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-Bridge: Die SMS Bridge kontrolliert und dokumentiert Versand von generierten mTANs an das SMS-Server und somit auf das Mobiltelefon eines Nutzers verwendet.
- ITC DB: Datenbank mit ISTS bezogenen Daten im ITC.
- ITC LDAP: Datenbank im ITC, die alle Benutzerdaten vorhält.

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).
- Mail-Gateway
- Mit dem Mail Gateway werden Nachrichten an den Nutzer versandt. Das Mail-Gateway ist für den ISTS (CC) nicht relevant. Es wird durch die gesonderte Komponente „ITC Nutzerverwaltung“ genutzt, um den Nutzer in verschiedenen Fällen die Mitteilungen (z.B. Mitteilung über die erfolgreiche Nutzeranlage, Mitteilung über den Ablauf von X.509Zertifikaten, erzeugte QR-Codes) zu senden.
- SMS Server: SMS-Server wird für die Übermittlung von durch ISTS generierte mTANs an Mobiltelefon eines Nutzers.

# 9. Ergebnis der Evaluierung

## 9.1. CC spezifische Ergebnisse

Der Evaluierungsbericht (Evaluation Technical Report, ETR) [6] 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 Vertrauenswürdigkeits-komponenten bestätigt: Alle Komponenten der Vertrauenswürdigkeitsstufe EAL 2 der CC (siehe auch Teil C des Zertifizierungsreports)

Da die Evaluierung eine Re-Evaluierung zum Zertifikat BSI-DSZ-CC-1150-2021 darstellt, konnten bestimmte Evaluierungsergebnisse wiederverwendet werden. Diese Re-Evaluierung konzentrierte sich insbesondere auf folgende Bereiche:

- Einführung einer neuen JSON-basierten Schnittstelle:
  - Token-Anforderung im JSON-Format (JSON Web Token/JSON Web Signature JWS),
  - Token-Antwort im JSON-Format (JWS und JSON Web Encryption – JWE),
  - Validierung des Tokens im JSON-Format (JWS/JWE).
- Erweiterung der SAML-Schnittstelle:
  - Einführung neuer Attribute im Sicherheitstoken,
  - Verwendung neuer Zertifikatlängen,
  - Einsatz besserer Hash-Algorithmen für Zertifikate,
  - Verwendung neuer Transportverschlüsselung (OAEP statt RSA 1.5) in Sicherheitstokens und Hash-Algorithmen.
- Neue Versionen und neue Komponenten:
  - TGIC-Benutzerverwaltung,
  - TGIC-Batch, ISTS-Core v2.1,

  - ITC-Web-Authentifizierung, ITC-SmathAuthentication (neu),
  - ITC-VUAuth-RedirectService (neu),
  - BN-Adapter (aufgrund des geänderten Token-Formats).
- Während der Evaluierung wurde die Funktion der Authentifikation mit eID aus dem Verfahren gestrichen und ist nicht Teil der Evaluierung.

Die Evaluierung hat gezeigt:

- PP Konformität: Keine
- 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.

Die Begrenzung der Gültigkeit der Verwendung der kryptographischen Algorithmen wie in Kapitel 9 dargelegt muss ebenso durch den Anwender und seinen Risikomanagementprozess für das IT-System berücksichtigt werden.

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 [5] werden zur Veröffentlichung in einem separaten Dokument im Anhang A bereitgestellt.

# 12. Spezifische regulatorische Aspekte (eIDAS, QES)

Keine

# 13. Definitionen

## 13.1. Abkürzungen

| | |
|---|---|
| **ADV** | Development |
| **AGD** | Guidance Documents |
| **AIS** | Anwendungshinweise und Interpretationen zum Schema |
| **ALC** | Life-Cycle Supporting |
| **ARC** | Security Architecture |
| **ASE** | Security Target Evaluations |
| **ATE** | Tests |
| **AVA** | Vulnerability Assessment |
| **BN** | Branchennetz (des GDV) |
| **BSI** | Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany |
| **BSIG** | BSI-Gesetz / Act on the Federal Office for Information Security |
| **CA** | Certificate Authority |
| **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 Information Technology Security Evaluation - Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik |
| **COV** | Coverage of Testing |
| **CPU** | Central Processing Unit |
| **DB** | Database / Datenbank |
| **DB2** | DB2 Datenbank (SW-Produkt der IBM) |
| **DEL** | Delivery |
| **DOC** | Documentation |
| **EAL** | Evaluation Assurance Level – Vertrauenswürdigkeitsstufe |
| **EBT** | Evaluation Body Testing |
| **ECT** | Extended Components Definition |
| **EVG** | Evaluierungsgegenstand |
| **ETR** | Evaluation Technical Report |
| **FSP** | Functional Specification |

| | |
|---|---|
| **FUN** | Functional Tests |
| **GDV** | Gesamtverband der Deutschen Versicherungswirtschaft e.V. |
| **IBM** | International Business Machines (konkret: IBM Deutschland GmbH) |
| **IDG** | IBM Datapower Gateway X2 (Nachfolgeprodukt von IBM WebSphere DataPower) |
| **ISTS** | Insurance Security Token Service (des GDV) |
| **IT** | Information Technology – Informationstechnologie |
| **ITC** | Insurance Trust Center (des GDV) |
| **ITSEF** | Information Technology Security Evaluation Facility - Prüfstelle für IT-Sicherheit |
| **ITU** | Integrationstestumgebung |
| **JSON** | JavaScript Object Notation |
| **JRE** | Java Runtime Environment |
| **JWE** | JSON Web Encryption |
| **JWT** | JSON Web Token |
| **JWS** | JSON Web Signature |
| **LDAP** | Lightweight Directory Access Protocol |
| **mTAN** | Mobile Transaktionsnummer |
| **NTP** | Network Time Protocol |
| **OASIS** | Organization for the Advancement of Structured Information Standards |
| **OAuth** | Open Authorization |
| **OBJ** | Security Objectives |
| **OS** | Operating System |
| **OSP** | Organisational Security Police |
| **Partner ID** | ID eines Nutzers oder einer Organisation |
| **PIN** | Persönliche Identifikationsnummer |
| **PKI** | Public Key Infrastructure |
| **PP** | Protection Profile – Schutzprofil |
| **REQ** | Security Requirements |
| **REST** | Representational State Transfer |
| **RSA** | Rivest, Shamir and Adleman (Kryptographie) |
| **RST** | Request Security Token (WS-Trust) |
| **RSTR** | Request Security Token Response (WS-Trust) |
| **SAML** | Security Assertion Markup Language |
| **SAR** | Security Assurance Requirement – Vertrauenswürdigkeitsanforderungen |
| **SF** | Security Function - Sicherheitsfunktion |

| | |
|---|---|
| **SFR** | Security Functional Requirement - Funktionale Sicherheitsanforderungen |
| **SHA** | Secure Hash Algorithm |
| **SMS** | Short Message Server |
| **SOAP** | Simple Object Access Protocol |
| **SSL** | Secure Socket Layer |
| **SSO** | Single Sign-On |
| **ST** | Security Target – Sicherheitsvorgaben |
| **STS** | Security Token Service |
| **TAN** | Transaction Number (deutsch: Transaktionsnummer) |
| **TGIC** | Trusted German Insurance Cloud |
| **TGIC-WS** | TGIC-Service |
| **TOE** | Target of Evaluation – Evaluierungsgegenstand |
| **TOTP** | Time-Based One-Time Password Algorithm |
| **TSF** | TOE Security Functionality – EVG-Sicherheitsfunktionalität |
| **VAN** | Vulnerability Analysis |
| **VDS** | IBM Verify Directory Server |
| **VPN** | Virtual Private Network |
| **VU** | Versicherungsunternehmen |
| **WAS** | WebSphere Application Server (SW-Produkt der IBM) |
| **WS** | Webservice |
| **X.509** | ITU-T-Standard für PKI-Zertifikate |
| **XML** | Extensible Markup Language |

## 13.2. 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.

**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.

# 14. Literaturangaben

[1] Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria for Information Technology Security Evaluation/CC),
ISO-Version:
ISO 15408:2022, Common Criteria for Information Technology Security Evaluation
- Part 1: Introduction and general model
- Part 2: Security functional components
- Part 3: Security assurance components
- Part 4: Framework for the specification of evaluation methods and activities
- Part 5: Pre-defined packages of security requirements
https://www.iso.org/standard/72891.html
https://www.iso.org/standard/72892.html
https://www.iso.org/standard/72906.html
https://www.iso.org/standard/72913.html
https://www.iso.org/standard/72917.html

CCRA-Version:
CC:2022 R1, Common Criteria for Information Technology Security Evaluation
- Part 1: Introduction and general model
- Part 2: Security functional components
- Part 3: Security assurance components
- Part 4: Framework for the specification of evaluation methods and activities
- Part 5: Pre-defined packages of security requirement
https://www.commoncriteriaportal.org

[2] Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology
ISO-Version:
ISO 18045:2022: Information technology Security techniques Methodology for IT security evaluation
https://www.iso.org/standard/72889.html
CCRA-Version:
CEM:2022 R1, Common Methodology for Information Technology Security Evaluation
https://www.commoncriteriaportal.org

[3] BSI-Zertifizierung: Verfahrensdokumentation zum Zertifizierungsprozess (CC-Produkte) und Verfahrensdokumentation zu Anforderungen an Prüfstellen, die Anerkennung und Lizenzierung (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Anwendungshinweise und Interpretationen zum Schema (AIS), die für den EVG relevant sind[7] https://www.bsi.bund.de/AIS

[5] Sicherheitsvorgaben, Insurance Security Token Service (ISTS) Common Criteria Evaluation Security Target, Version 1.5.12, 13. November 2025, GDV Dienstleistungs-GmbH

[6] Evaluierungsbericht, ETR Summary, Version 2, 26. Januar 2026, TÜV Informationstechnik GmbH (vertrauliches Dokument)

[7] Konfigurationsliste für den EVG, Life Cycle Support Common Criteria Evaluation ALC, Version 1.06, 22. November 2025, IBM Deutschland GmbH (vertrauliches Dokument)

[8] Insurance Security Token Service Operational User Guidance, Common Criteria Evaluation AGD_OPE, Version 1.05, 14. November 2025, IBM Deutschland GmbH (vertrauliches Dokument)

[9] Insurance Security Token Service Preparative Procedures, Common Criteria Evaluation AGD_PRE, Version 1.10, 22. November 2025, IBM Deutschland GmbH (vertrauliches Dokument)

[10] Insurance Security Token Service Anbindungsleitfaden für Service-Betreiber und Service-Nutzer an ISTS v2.1, Version 1.0, 31. Juli 2025, GDV Dienstleistungs-GmbH (vertrauliches Dokument)

[11] Insurance Trust Center Anbindungsleitfaden ISTS OAuth 2.0 für Service-Betreiber und Service-Nutzer in der TGIC, Version 1.2, 14. November 2025, GDV Dienstleistungs-GmbH (vertrauliches Dokument)

[12] Insurance Trust Center Anbindungsleitfaden für die ISTS-Web-Authentifikation, Version 2.0.1, 24. Februar 2025, GDV Dienstleistungs-GmbH (vertrauliches Dokument)

[13] Insurance Trust Center: Anbindungsleitfaden für die ITC-Smart-Authentifikation, Version 1.3, 24. Februar 2025, GDV Dienstleistungs-GmbH (vertrauliches Dokument)

[14] Insurance Trust Center Service Gateway / IDG X2 Deployment, Version 1.0, 12. September 2015, GDV Dienstleistungs-GmbH (vertrauliches Dokument)

[15] Insurance Trust Center: Service Gateway / IDG X2 – Installation & Konfiguration, Version 1.0.7, 11. September 2025, GDV Dienstleistungs-GmbH (vertrauliches Dokument)

[7] insbesondere

- AIS 14, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 7, 2010-08-03, Bundesamt für Sicherheit in der Informationstechnik.
- AIS 19, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 9, 2014-11-03, Bundesamt für Sicherheit in der Informationstechnik.
- AIS 32, CC-Interpretationen im deutschen Zertifizierungsschema, Version 7, 2011-06-08, Bundesamt für Sicherheit in der Informationstechnik.
- AIS 41, Application Notes and Interpretation of the Scheme (AIS) – AIS 41, Version 2, 2011-01-31, Guidelines for PPs and STs

[16] Insurance Trust Center Betriebshandbuch, Version 1.02, 18. November 2025, GDV Dienstleistungs-GmbH (vertrauliches Dokument)

[17] Insurance Security Token Service: Database Server / DB2 – Deployment, Version 1.0, 06. Februar 2025, GDV Dienstleistungs-GmbH (vertrauliches Dokument)

[18] Insurance Security Token Service: Database Server / DB2 v12.1 – Installation & Konfiguration, Version 0.3, 01. Oktober 2025, GDV Dienstleistungs-GmbH (vertrauliches Dokument)

[19] Insurance Security Token Service: Kryptokonzept, Version 2.0, 08. Juli 2025, GDV Dienstleistungs-GmbH (vertrauliches Dokument)

[20] ITC-Deploymentanleitung-VDS-Migration, Version 1.0, 06. November 2025, GDV Dienstleistungs-GmbH (vertrauliches Dokument)

[21] Directory Server / VDS Installation & Konfiguration, Version 1.0, 04. November 2025, GDV Dienstleistungs-GmbH (vertrauliches Dokument)

[22] Insurance Trust Center Application Server / WAS Deployment Nutzerverwaltung, Version 2.0, 01. April 2025, GDV Dienstleistungs-GmbH (vertrauliches Dokument)

[23] Insurance Trust Center Application Server / WAS Installation & Konfiguration, Version 1.0, 31. März 2025, GDV Dienstleistungs-GmbH (vertrauliches Dokument)

[24] Insurance Trust Center: Service Gateways / IDG – Fehlercodes, Version 0.3, 21. November 2025, GDV Dienstleistungs-GmbH (vertrauliches Dokument)

# C. Auszüge aus den Kriterien

Die Bedeutung der Vertrauenswürdigkeitskomponenten und -stufen kann direkt den Common Criteria entnommen werden. Folgende Referenzen zu den CC:2022 können dazu genutzt werden:

- Definition und Beschreibung zu Conformance Claims: CC:2022 Teil 1 Kapitel 10.5
- Zum Konzept der Vertrauenswürdigkeitsklassen, -familien und -kompomenten: CC:2022 Teil 3 Kapitel 6.1,
- Zum Konzept der vordefinierten Vertrauenswürdigkeitsstufen (evaluation assurance levels - EAL): CC Teil 5,
- Definition und Beschreibung der Vertrauenswürdigkeitsklasse ASE für Sicherheitsvorgaben / Security Target Evaluierung: CC:2022 Teil 3 Kapitel 9,
- Zu detaillierten Definitionen der Vertrauenswürdigkeitskomponenten für die Evaluierung eines Evaluierungsgegenstandes: CC:2022 Teil 3 Kapitel 7 bis 15,
- Die Tabelle 1 in CC:2022 Teil 5, Kapitel 4.2 fasst die Beziehung zwischen den Vertrauenswürdigkeitsstufen (EAL) und den Vertrauenswürdigkeitsklassen, -familien und -komponenten zusammen.

Die Common Criteria sind unter https://www.commoncriteriaportal.org/cc/ veröffentlicht.

# D. Anhänge

## Liste der Anhänge zu diesem Zertifizierungsreport

Anhang A: Die Sicherheitsvorgaben werden in einem eigenen Dokument zur Verfügung gestellt.