

BSI-DSZ-CC-1150-2021

zu

**Insurance Security Token Server (ISTS),
Version 2.0.9**

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-1150-2021 (*)

Serveranwendungen: Sonstige

Insurance Security Token Server (ISTS), Version 2.0.9

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



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), Version 3.1 ergänzt um Interpretationen des Zertifizierungsschemas unter Nutzung der Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Version 3.1 (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.

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.

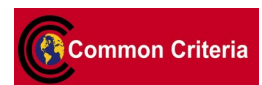
Bonn, 2. Februar 2021

Bundesamt für Sicherheit in der Informationstechnik

Im Auftrag

Sandro Amendola
Abteilungspräsident

L.S.



Common Criteria
Recognition Arrangement



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.

Gliederung

| | |
|---------------------------------------------------------|----|
| A. Zertifizierung..... | 7 |
| 1. Vorbemerkung..... | 7 |
| 2. Grundlagen des Zertifizierungsverfahrens..... | 7 |
| 3. Anerkennungsvereinbarungen..... | 8 |
| 4. Durchführung der Evaluierung und Zertifizierung..... | 9 |
| 5. Gültigkeit des Zertifizierungsergebnisses..... | 10 |
| 6. Veröffentlichung..... | 11 |
| B. Zertifizierungsbericht..... | 12 |
| 1. Zusammenfassung..... | 13 |
| 2. Identifikation des EVG..... | 14 |
| 3. Sicherheitspolitik..... | 14 |
| 4. Annahmen und Klärung des Einsatzbereiches..... | 14 |
| 5. Informationen zur Architektur..... | 14 |
| 6. Dokumentation..... | 15 |
| 7. Testverfahren..... | 15 |
| 8. Evaluierete Konfiguration..... | 15 |
| 9. Ergebnis der Evaluierung..... | 15 |
| 10. Auflagen und Hinweise zur Benutzung des EVG..... | 18 |
| 11. Sicherheitsvorgaben..... | 19 |
| 12. Definitionen..... | 20 |
| 13. Literaturangaben..... | 21 |
| C. Auszüge aus den Kriterien..... | 23 |
| D. Anhänge..... | 24 |

A. Zertifizierung

1. Vorbemerkung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat gemäß BSIG¹ 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-Gesetz¹
- BSI-Zertifizierungs- und -Anerkennungsverordnung²
- 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]

¹ Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) vom 14. August 2009, Bundesgesetzblatt I S. 2821

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 17. Dezember 2014, Bundesgesetzblatt Jahrgang 2014 Teil I, Nr. 61, S. 2231

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

- Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria for Information Technology Security Evaluation/CC), Version 3.1⁴ [1], auch als Norm ISO/IEC 15408 veröffentlicht.
- Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Methodology for Information Technology Security Evaluation/CEM), Version 3.1 [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).

⁴ Bekanntmachung des Bundesministeriums des Innern vom 12. Februar 2007 im Bundesanzeiger, datiert 23. Februar 2007, S. 1941

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 2.0.9 hat das Zertifizierungsverfahren beim BSI durchlaufen. Es handelt sich um eine Re-Zertifizierung basierend auf BSI-DSZ-CC-1038-2017. Für diese Evaluierung wurden bestimmte Ergebnisse aus dem Evaluierungsprozess BSI-DSZ-CC-1038-2017 wiederverwendet.

Die Evaluation des Produkts Insurance Security Token Server (ISTS), Version 2.0.9 wurde von TÜV Informationstechnik durchgeführt. Die Evaluierung wurde am 27. Januar 2021 abgeschlossen. Das Prüflabor TÜV Informationstechnik ist eine vom BSI anerkannte Prüfstelle (ITSEF)⁵.

Der 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 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 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 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 Neubewertung oder eine Re-Zertifizierung). Insbesondere wenn

⁵ Information Technology Security Evaluation Facility

Ergebnisse aus dem Zertifizierungsverfahren in einem nachfolgenden Evaluierungs- und Zertifizierungsverfahren oder in einer Systemintegration verwendet werden oder wenn das Risikomanagement eines Anwenders eine regelmäßige Aktualisierung verlangt, wird empfohlen, die Neubewertung der Widerstandsfähigkeit regelmäßig, z.B. jährlich vorzunehmen.

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 2. Februar 2021, ist gültig bis 01. Februar 2026. 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 Weitergaberegulierung 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 2.0.9 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 werden⁶. Der Zertifizierungsreport kann ebenso in elektronischer Form von der oben angegebenen Internetadresse heruntergeladen werden.

⁶ GDV Dienstleistungs-GmbH
Glockengießerwall 1
20095 Hamburg

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 Authentifizierungsmechanismen von der Umgebung bereitgestellt werden, 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 | 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-Zertificate, eID, mTAN oder Time-based One-time Password Algorithmus (TOTP) realisiert. Dem entsprechend unterstützt der EVG vier Authentifizierungsmechanismen. |
| SF3 | SF3 – 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 | SF4 – Die Funktionalität Security Management wird dadurch realisiert, dass der EVG über die Möglichkeit verfügt, in Form einer XML-basierten Konfigurationsdatei die Gültigkeitsdauer <ul style="list-style-type: none"> • einer X.509-Session, • einer nPA-Session, • einer generierten mTAN, sowie |

| Sicherheitsfunktionalität des EVG | Thema |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <ul style="list-style-type: none"> einer TOTP Session einzustellen. <p>Diese Parameter werden durch den EVG bei jedem Aufruf eingelesen, sowie aufgrund des zugrunde liegenden XML Schemas für die Konfigurationsdatei syntaktisch geprüft.</p> |

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 Kapitel 3 dar.

Dieses Zertifikat umfasst die folgenden Konfigurationen des EVG: Der evaluierte EVG ist Insurance Security Token Service V2.0.9. Die zugrundeliegende Plattform des EVG ist IBM DataPower Gateway X2 (Type 8441, Model 53x) mit der Firmwareversion 2018.4.1.10. 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 kryptographischen 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 Server (ISTS), Version 2.0.9

Die folgende Tabelle beschreibt den Auslieferungsumfang:

| Nr | Typ | Identifizier | Version/ Datum | Auslieferungs- art |
|----|-----|---------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|------------------------|
| 1 | SW | TOE: idg-config-201120.ists-core-v2.zip (composed by constituents no. 1.1–1.52) | V2.0.9 5cb5547bce 4b7eb79eb7 96b37f40bfc 566b9522c6 3de25530e7 3112a0fad4b 19 | Download von GitLab |

| Nr | Typ | Identifizier | Version/ Datum | Auslieferungs- art |
|----|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|---------------------------------------------------------------------------------------------------------------------------|
| 2 | DATA | Hash values (SHA-256) for the TOE software parts (no. 1.1–1.52) idg-config-2011200.ists-core-v2.sha256 | -- | Download von GitLab Input for integrity check of compressed TOE software parts delivered via GitLab. |
| 3 | DOC | Insurance Security Token Service Operational User Guidance Common Criteria Evaluation AGD_OPE | 1.03 2020-05-12 | Download von GitLab |
| 4 | DOC | Insurance Security Token Service Preparative Procedures Common Criteria Evaluation AGD_PRE | 1.05 2020-11-26 | Download von GitLab |
| 5 | DOC | Insurance Security Token Service Anbindungsleitfaden für Service-Betreiber und Service- Nutzer in der TGIC | 2.1.1 2020-01-23 | Download von GitLab |
| 6 | DOC | Insurance Trust Center Anbindungsleitfaden für die ISTS-Web-Authentifikation | 1.6 2020-02-06 | Download von GitLab |
| 7 | DOC | Insurance Trust Center: Anbindungsleitfaden für die ITC-Smart-Authentifikation | 1.0 2020-06-30 | Download von GitLab |
| 8 | DOC | Insurance Trust Center: Service Gateways Fehlercodes | 1.9 2019-12-10 | Download von GitLab |
| 9 | zip | Insurance Trust Center Service Gateway / IDG X2 Deployment | 0.4 2019-10-10 | Download von GitLab |
| 10 | DOC | Insurance Trust Center: Service Gateway / IDG X2 –Installation & Konfiguration | 0.4 2019-10-24 | Download von GitLab |
| 11 | DOC | ZIP-Archiv mit der technischen Schnittstellenspezifikation des TOE (InsuranceSecurityTokenService-2.0.9.wsdl) | 2.0.9 2020-06-16 | Download von GitLab |
| 12 | DOC | Initializing the DP internal RAID HDD Volume Group | - 2013-10-17 | Download von GitLab |
| 13 | Web- Link | https://www.ibm.com/support/knowledgecenter/SS9H2Y_10.0/com.ibm.dp.doc/introduction.html | -- | Download von GitLab |
| 14 | DOC | Insurance Trust Center Betriebshandbuch | 0.16 2020-11-25 | Download von GitLab |
| 15 | DOC | Insurance Security Token Service: Database Server / DB2 – Deployment | 0.9 2020-09-15 | Download von GitLab |
| 16 | DOC | Insurance Security Token Service: Database Server / DB2 – Installation & Konfiguration | 1.04 2020-09-15 | Download von GitLab |
| 17 | DOC | Insurance Security Token Service: Kryptokonzept | 0.8 2020-07-10 | Download von GitLab |
| 18 | DOC | Insurance Security Token Service Directory Server / SDS Deployment (LDAP-Migration) | 0.5 2017-12-02 | Download von GitLab |

| Nr | Typ | Identifizier | Version/ Datum | Auslieferungs- art |
|----|-----|------------------------------------------------------------------------------|--------------------|------------------------|
| 19 | DOC | Insurance Trust Center Directory Server / SDS Installation & Konfiguration | 0.5 2017-10-29 | Download von GitLab |
| 20 | DOC | Insurance Trust Center: Application Server / WAS Deployment Nutzerverwaltung | 1.10 2020-02-22 | Download von GitLab |
| 21 | DOC | Insurance Trust Center Application Server / WAS Installation & Konfiguration | 1.9 2019-12-10 | Download von GitLab |
| 22 | DOC | Insurance Trust Center: Service Gateways / IDG – Fehlercodes | 0.25 2020-05-26 | Download von GitLab |

Tabelle 2: Auslieferungsumfang des EVG

Die Auslieferung des EVG sowie der Benutzerdokumentation und der Begleitdokumente zur Benutzerdokumentation erfolgt als Upload auf dem GitLab-System des Benutzers. Der Kommunikationskanal zu diesem Server wird über HTTPS gesichert. Des Weiteren wird gesondert noch eine Datei mit dem Hashwert des TOE Deployment Moduls 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.

Das Deploymentmodul des EVG besteht aus xsl-, xsd-, wsdl- and xml-Dateien und ist Teil eines gesamten Deploymentpakets idg-config-201120.ists-core-v2.zip für den ITC, welcher aus vier verschiedenen Modulen besteht.

Dabei ist die Bezeichnung des EVG-Moduls folgende: idg-config-201120.ists-core-v2.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 idg-config-201120.ists-core-v2.sha256 zur Verfügung gestellt.

Die berechneten SHA256 Checksummen werden mit einer per S/MIME verschlüsselten und signierten Email 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 des SHA256-Hashwertes muss der Benutzer die Checksummen des EVG berechnen und mit den erhaltenen Daten vergleichen, indem er beispielsweise OpenSSL nutzt und folgenden Befehl in der Kommandozeile eingibt:

```
openssl dgst -sha256 idg-config-<datum>.ists-core-v2.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: 2.0.9-IBM-2020-11-20.

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:

- Security Audit,
- Identification and Authentication,
- Security Management, and
- 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.

| 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-256 erstellt wurden. |

Tabelle 3: Sicherheitsziele des TOE

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

5. Informationen zur Architektur

Der EVG besteht aus neun Subsystemen welche im Folgenden beschrieben sind:

ISTS_rule_IssueRST:

- Auslesen der Konfiguration aus der Operativen Umgebung des TOE.
- Anfrage zum Erstellen eines Tokens aufnehmen und gegen Spezifikation prüfen.
- Benutzerdaten abrufen und grobe Prüfung der Zulässigkeit der Anfrage durchführen.
- Solange im Request nicht vorgegeben, Art der unterstützbaren Authentifizierung feststellen (X.509, mTAN, TOTP oder nPA).
- Authentifizierungsrückfrage (Challenge Response) generieren.

ISTS_rule_IssueRSTR:

- Auslesen der Konfiguration aus der operativen Umgebung des TOE.
- Antwort auf die Authentifizierungsabfrage aufnehmen und gegen Spezifikation prüfen.
- Authentifizierung durchführen und durch das Erstellen des Tokens bestätigen.
- Erstellen des Tokens ins Protokoll revisionssicher schreiben.

ISTS_rule_IssueRST_TGT:

- Auslesen der Konfiguration aus der Operativen Umgebung des TOE.
- 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.

ISTS_rule_CancelRST:

- Auslesen der Konfiguration aus der operativen Umgebung des TOE.
- Anfrage zum Widerrufen eines Tokens aufnehmen und gegen Spezifikation prüfen.
- Benutzer- und Token-Daten abrufen und grobe Prüfung auf die Zulässigkeit der Anfrage durchführen.
- Solange im Request nicht vorgegeben, Art der unterstützbaren Authentifizierung feststellen (X.509, mTAN, TOTP oder nPA).
- Authentifizierungsrückfrage (Challenge Response) generieren.

ISTS_rule_CancelRSTR:

- Auslesen der Konfiguration aus der operativen Umgebung des TOE.
- Antwort auf die Authentifizierungsabfrage aufnehmen und gegen Spezifikation prüfen.
- Authentifizierung durchführen und durch das Widerrufen des Tokens bestätigen.
- Widerruf des Tokens ins Protokoll revisionssicher schreiben.

ISTS_rule_CancelRST_TGT:

- Auslesen der Konfiguration aus der operativen Umgebung des TOE.

- Anfrage zum Widerrufen eines Tokens sowie SSO-Token aufnehmen und gegen Spezifikation prüfen, validieren.
- Benutzer- und Token-Daten abrufen und grobe Prüfung auf die Zulässigkeit der Anfrage durchführen. Das Widerrufen des Tokens bestätigen.
- Widerruf des Tokens ins Protokoll revisionssicher schreiben.

ISTS_rule_Validate:

- Auslesen der Konfiguration aus der operativen Umgebung des TOE.
- Anfrage zur Überprüfung des Tokens aufnehmen und gegen 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 sieben Subsysteme realisieren die Funktionen der Sicherheitsfunktionalität SF3. Dadurch werden auch implizit die Funktionen der Sicherheitsfunktionalitäten SF1, SF2 und SF4 realisiert. Die letzten beiden Subsysteme implementieren explizit die Fehlerbehandlung des EVG. Alle Subsysteme wurden als SFR-enforcing (sicherheitsspezifisch) deklariert.

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 wurde in seiner operativen Einsatzumgebung getestet, wobei sowohl die für den Betrieb im Rahmen der CC-Zertifizierung verpflichtende, als auch die beiden Testkonfigurationen (siehe Abschnitt 3.1) für die Testfälle genutzt wurden.

Übereinstimmend mit der im ST spezifizierten und in Abschnitt 3.1 dargestellten operativen Einsatzumgebung des EVG, wurden sowohl die Hersteller- als auch die Prüfstellentests mit folgender Konfiguration durchgeführt:

Deployment-Einheit 1 (Service Gateway) jeweils zwei redundante Instanzen

| | |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hardware | <ul style="list-style-type: none"> • IBM DataPower Gateway X2 <ul style="list-style-type: none"> ◦ Formfaktor: 2U high-density, rack-mount design ◦ Netzwerk: 2x 1GB Ports; 8x 10GB Ports |
| Firmware | <ul style="list-style-type: none"> • IBM DataPower Gateway X2, Firmware Version 2018.4.10 <ul style="list-style-type: none"> ◦ inkl. Data Integration Module (DIM) Option ◦ inkl. Hardware Security Module (HSM) |
| ITC Komponenten | <ul style="list-style-type: none"> • ITC Service Gateway <ul style="list-style-type: none"> ◦ TOE ◦ ITC BN-Adapter ◦ ITC ISTS-eID-Connector ◦ ITC Web und Webservice-Proxy ◦ ITC ISTS Web Authentifikation ◦ ITC VU-Authentifikation ◦ ITC Smart-Authentifikation |

Tabelle 4: Deployment-Einheit 1

| | |
|-----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Deployment-Einheit 2 (Application Server) jeweils zwei redundante Instanzen | |
| Hardware | <ul style="list-style-type: none"> • Intel Server: virtualisiert <ul style="list-style-type: none"> ◦ CPU: Intel Xeon E5-2643, 3.3 GHz, 1 Core ◦ Hauptspeicher: 8 GB ◦ Festplatte: mind. 64 GB ◦ Netzwerk: 1 Gbit port |
| OS | SuSE Linux Enterprise Server (SLES), Version 11 SP4 |
| Software | IBM WebSphere Application Server Fixpack Level 8.5.5.17 |
| ITC Komponenten | <ul style="list-style-type: none"> • ITC Nutzerverwaltung <ul style="list-style-type: none"> ◦ ITC PKI ◦ ITC Kennwortverwaltung ◦ ITC BatchControl |

Tabelle 5: Deployment-Einheit 2

| | |
|--------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| Deployment-Einheit 3 (Database Server) jeweils zwei redundante Instanzen | |
| Hardware | <ul style="list-style-type: none"> • Intel Server: virtualisiert |

| | |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <ul style="list-style-type: none"> ◦ CPU: Intel Xeon E5-2643, 3.3 GHz, 1 Core ◦ Hauptspeicher: 8 GB ◦ Festplatte: 500GB ◦ Netzwerk: 1Gbit Port • Shared File System <ul style="list-style-type: none"> ◦ SAN: 2 TB |
| OS | SuSE Linux Enterprise Server (SLES), Version 12 SP5, SuSE HAE Edition |
| Software | IBM DB2 Enterprise Server Edition Fixpack Level 11.5.4.0 |
| ITC Komponenten | ITC DB |

Tabelle 6: Deployment-Einheit 3

| Deployment-Einheit 4 (Directory Server) jeweils zwei redundante Instanzen | |
|---------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hardware | <ul style="list-style-type: none"> • Intel Server: virtualisiert <ul style="list-style-type: none"> ◦ CPU: Intel Xeon E5-2643, 3.3 GHz, 1 Core ◦ Hauptspeicher: 4 GB ◦ Festplatte: mind. 40 GB ◦ Netzwerk: 1 Gbit port |
| Software | IBM Security Directory Suite Enterprise Edition Fixpack Level 8.0.1.12 |
| ITC Komponenten | ITC LDAP |

Tabelle 7: Deployment-Einheit 4

Testmethode:

Der Hersteller hat folgende Werkzeuge zur Durchführung der Tests genutzt:

| Tool / Materials | Purpose / Field of application |
|-------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| SoapUI, Version 5.5.0 | Test client for the access to the TOE whereas the behaviour of web service user and web service operator in real operation is simulated. |
| Oracle Java Runtime Environment (JRE), Version 1.7.0 | Java runtime environment for the conduction of the test cases. |
| Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files, Version 7 | Necessary for the implementation of the required key lengths for the cryptographic algorithms (e.g. AES256). |
| Lenovo ThinkPad T460, Windows 10 | Installation of the test tools and conduction of the |

| | |
|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| (64bit, Build 2002) | test cases. |
| Test-nPA of the Bundesdruckerei, which is also activated for online identification. | This nPA has also a corresponding 6 digit PIN and the person which is identified by the nPA has to be registered as "natürliche Person" in the ITC-Nutzerverwaltung and the nPA-authentication has to be activated. |
| AusweisApp2 v1.20.2 | eID client for the authentication via nPA. |
| BSI certified Class-3 chip card reader ReinerSCT cyberJack RFID komfort | Card reader for the authentication via nPA. |
| Mobile Phones | Mobile Phones for the reception of text messages during the mTAN authentication of the registered test users. |

Tabelle 8: Testwerkzeuge und Materialien

Sämtliche Testfälle wurden mit dem Notebook welches in Table 13 aufgelistet ist durchgeführt. Zur Durchführung der Testfälle mit nPA Authentifikation wurde zusätzlich ein Kartenleser, das Werkzeug AusweisApp2 und Test-nPAs genutzt wohingegen zur Durchführung der Testfälle mit mTAN Authentifikation verschiedene Mobiltelefone (siehe Table 13) genutzt wurden.

Insgesamt hat der Hersteller systematisch alle TSF Schnittstellen welche in [ADV_FSP] angegeben sind, getestet und diese mit den Testfällen abgedeckt.

Ergebnis:

Die vom Hersteller beschriebenen Tests decken alle in den Sicherheitsvorgaben [ST] 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 Hersteller- und Prüfstellentests wurden mit der Hard- und Softwarekonfiguration durchgeführt, welche in der Testdokumentation angegeben ist.

Testabdeckung:

Alle EVG Sicherheitsfunktionalitäten wurden getestet:

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

Testurteil:

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

EVG Testkonfiguration

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 WebSphere DataPower Gateway X2 ist der Modus PRODUKTION verpflichtend. Dies führt zu der Tatsache, dass es nur eine evaluierte Konfigurationen 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.

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 |

| | |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | Ein Angreifer könnte operative Schwachstellen nutzen, welche direkt ausgenutzt werden oder auch andere Angriffswege öffnen können. Operationelle Robustheit umfasst den richtigen und sicheren Betrieb während der wechselnden Bedingungen von sich wiederholenden Cancel Binding Anfragen. |
| AS.2 | Nicht erlaubte Operationen Ein Angreifer kann Operationen des EVG verwenden, welche nicht für jeden zugänglich sein sollten. |
| AS.3 | Schwache Authentifikation 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 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 9: Angriffsszenarien des Penetration Testens

Urteil:

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

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.

8. Evaluierete Konfiguration

Dieses Zertifikat bezieht sich auf die folgenden Konfigurationen des EVG:

Der EVG ist Insurance Security Token Service V2.0.9. 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 X2 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 X2 (Type 8441, Model 53x) mit der Firmwareversion 2018.4.1.10. 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 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 Benachrichtigungen 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 (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)

Da die Evaluierung eine Re-Evaluierung zum Zertifikat BSI-DSZ-CC-1038-2017 darstellt, konnten bestimmte Evaluierungsergebnisse wiederverwendet werden. Diese Re-Evaluierung konzentrierte sich insbesondere auf folgende Bereiche

- Einführung TOTP als zusätzliche Authentifikationsmethode und
- Neue Versionen einiger TOE Komponenten.

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 Mechanismen nicht Gegenstand der Evaluierung.

10. Auflagen und Hinweise zur Benutzung des EVG

Die in Tabelle 2 genannte Betriebsdokumentation enthält die notwendigen Informationen zur Anwendung des EVG und alle darin enthaltenen Sicherheitshinweise sind zu beachten. Zusätzlich sind alle Aspekte der Annahmen, Bedrohungen und 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 [6] werden zur Veröffentlichung in einem separaten Dokument im Anhang A bereitgestellt.

12. Definitionen

12.1. Abkürzungen

| | |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AIS | Anwendungshinweise und Interpretationen zum Schema |
| API | Application Programming Interface |
| 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 |
| 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 |
| cPP | Collaborative Protection Profile |
| DB | Database / Datenbank |
| EAL | Evaluation Assurance Level - Vertrauenswürdigkeitsstufe |
| EVG | Evaluierungsgegenstand |
| ETR | Evaluation Technical Report |
| GDV | Gesamtverband der Deutschen Versicherungswirtschaft e.V. |
| IBM | International Business Machines (konkret: IBM Deutschland GmbH) |
| ISTS | Insurance Security Token Service |
| IT | Information Technology - Informationstechnologie |
| ITC | Insurance Trust Center (des GDV) |
| ITSEF | Information Technology Security Evaluation Facility - Prüfstelle für IT-Sicherheit |
| LDAP | Lightweight Directory Access Protocol |
| MTA | Mail Transfer Agent |
| mTAN | Mobile Transaktionsnummer |
| nPA | Neuer Personalausweis |
| NTP | Network Time Protocol |
| OASIS | Organization for the Advancement of Structured Information Standards |

| | |
|-------------------|------------------------------------------------------------------------|
| OS | Operating System |
| Partner ID | ID eines Nutzers oder einer Organisation |
| PKI | Public Key Infrastruktur |
| PP | Protection Profile – Schutzprofil |
| RFC | Request for Comments |
| SAML | Security Assertion Markup Language |
| 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 |
| SSL | Secure Socket Layer |
| SSO | Single Sign-On |
| ST | Security Target – Sicherheitsvorgaben |
| STS | Security Token Service |
| TGIC | Trusted German Insurance Cloud |
| TGIC-WS | TGIC-Service |
| TLS | Transport Layer Security |
| TOE | Target of Evaluation – Evaluierungsgegenstand |
| TOTP | Time-Based One-Time Password Algorithm |
| TSC | TSF Scope of Control - Anwendungsbereich der TSF-Kontrolle |
| TSF | TOE Security Functionality – EVG-Sicherheitsfunktionalität |
| TÜViT | TÜV Informationstechnik GmbH |
| UA | User Agent |
| VM | Virtuelle Maschine |
| 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
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
<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, Version 3.1, Rev. 5, April 2017, <https://www.commoncriteriaportal.org>
- [3] BSI-Zertifizierung: Verfaendokumentation zum Zertifizierungsprozess (CC-Produkte) und Verfaendokumentation 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 sind⁷ <https://www.bsi.bund.de/AIS>

⁷specifically

- 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.

- [5] Deutsche IT-Sicherheitszertifikate (BSI 7148), periodisch aktualisierte Liste, die auch auf der Internet-Seite des BSI veröffentlicht wird, <https://www.bsi.bund.de/zertifizierungsreporte>
- [6] Sicherheitsvorgaben BSI-DSZ-CCC-1150, Version 1.4.0 27.07.2020, Insurance Security Token Service (ISTS) Common Criteria Evaluation Security Target, GDV Dienstleistungs-GmbH
- [7] Evaluierungsbericht, Version 2, 18.01.2021, ETR Summary, TÜV Informationstechnik GmbH (vertrauliches Dokument)
- [8] Konfigurationsliste, Version 1.04, 24.11.2020, Insurance Security Token Service Life Cycle Support ALC, IBM Deutschland GmbH (vertrauliches Dokument)
- [9] Insurance Security Token Service, Operational User Guidance, Common Criteria Evaluation, V 1.03, 12.05.2020
- [10] Insurance Security Token Service, Preparative Procedures, Common Criteria Evaluation, V 1.05, 26.11.2020

- AIS 32, CC-Interpretationen im deutschen Zertifizierungsschema, Version 7, 2011-06-08, Bundesamt für Sicherheit in der Informationstechnik.
- AIS 41, Guidelines for PPs and STs, Version 2, 2011-01-31, Bundesamt für Sicherheit in der Informationstechnik.
- AIS 45, Erstellung und Pflege von Meilensteinplänen, Version 2, 2010-08-03, Bundesamt für Sicherheit in der Informationstechnik.

C. Auszüge aus den Kriterien

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

- Definition und Beschreibung zu Conformance Claims: CC Teil 1 Kapitel 10.5
- Zum Konzept der Vertrauenswürdigkeitsklassen, -familien und -komponenten: CC Teil 3 Kapitel 7.1
- Zum Konzept der vordefinierten Vertrauenswürdigkeitsstufen (evaluation assurance levels - EAL): CC Teil 3 Kapitel 7.2 und 8
- Definition und Beschreibung der Vertrauenswürdigkeitsklasse ASE für Sicherheitsvorgaben / Security Target Evaluierung: CC Teil 3 Kapitel 12
- Zu detaillierten Definitionen der Vertrauenswürdigkeitskomponenten für die Evaluierung eines Evaluierungsgegenstandes: CC Teil 3 Kapitel 13 bis 17
- Die Tabelle in CC Teil 3 Anhang E 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.