Insurance Security Token Service (ISTS)

Common Criteria Evaluation
Security Target

Autor:	GDV Dienstleistungs-GmbH
	TÜV Informationstechnik GmbH
Kategorie:	CC Evaluation

Version:	1.4.0
Datum:	2020-07-27
Dateiname:	GDV_ST_1.4.0.docx

Zusammenfassung

Dieses Dokument ist das ST (Security Target) der ISTS Common Criteria Evaluierung.

Schlüsselwörter

CC, ST, Common Criteria, Security Target, ISTS

Erstellt für

GDV Dienstleistungs-GmbH

Glockengießerwall 1
20095 Hamburg, Germany
Tel.: +49 (40) 33449 - 0
http://gdv-dl.de

Erstellt von

TÜV Informationstechnik GmbH
Member of TÜV NORD Group
Langemarckstraße 20
45141 Essen, Germany
Tel: +49 (201) 8999 - 9
https://www.tuvit.de

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

1 ST Introduction (ST Einführung)

Dieses Kapitel enthält Informationen zur ST und TOE Identifikation. Es gibt eine Übersicht über den Evaluierungsgegenstand[1] und gibt einem potentiellen Anwender Informationen darüber, ob der Insurance Security Token Service (ISTS) für ihn von Interesse ist. Ein ST enthält die Sicherheitsvorgaben eines konkreten TOE und beschreibt die funktionalen Sicherheitsanforderungen und die Anforderungen an die Vertrauenswürdigkeit, die der TOE einhält. Ein ST definiert:

a) die TOE-Sicherheitsumgebung durch Annahmen an die operative Einsatzumgebung, Bedrohungen, denen der TOE entgegenwirken soll und weitere Regeln, die der TOE einzuhalten hat (Kapitel 3),

b) die TOE-Sicherheitsziele und TOE-Sicherheitsanforderungen, die die IT-Sicherheitsanforderungen beschreiben (Kapitel 4 und 6),

c) die Sicherheitsfunktionalität, die vom TOE bereitgestellt wird (Kapitel 7).

1.1 ST and TOE references (ST und TOE Referenzen)

Tabelle 1 – ST Identifikation

Titel:	Insurance Security Token Service (ISTS) Common Criteria Evaluation Security Target
Version:	1.4.0
Datum:	2020-07-27
Autor:	GDV Dienstleistungs-GmbH TÜV Informationstechnik GmbH
CertID:	BSI-DSC-CC-1150

Tabelle 2 – TOE Identifikation

TOE Identifikation:	Insurance Security Token Service (ISTS) und zugehörige Handbücher
TOE Version:	V2.0.9
TOE Entwickler:	GDV Dienstleistungs-GmbH
CC Identifikation:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017
Evaluation Assurance Level:	EAL2
PP Konformität:	Keine

[1] Im Folgenden wird als Kurzform die englische Bezeichnung TOE (Target of Evaluation) verwendet.

1.2 TOE overview (TOE Übersicht)

Kurzbeschreibung in Deutsch: / Short description in German:

Bei dem TOE handelt es sich vom Produkttyp um einen Security Token Service (STS). Dieser ist als reine Software-Applikation implementiert und wird aufgrund des Einsatzgebietes in der Versicherungsbranche im Folgenden als Insurance Security Token Service, oder kurz ISTS, bezeichnet.

Die Applikation stellt (Software-)Sicherheitstoken aus, die für Authentifizierungszwecke bei einem TGIC-Service verwendet werden. Zusätzlich verfügt der TOE über die Möglichkeit die ausgestellten Sicherheitstoken zu validieren und zu widerrufen. Weitere Funktionalitäten sind das Führen einer Logdatei, die Identifikation und Authentifizierung[2] von Nutzern und das Management von Sicherheitsfunktionalitäten. Detaillierte Informationen über die Sicherheitsfunktionen des TOE sind in Kapitel 1.3 und 7 dargelegt.

Kurzbeschreibung in Englisch: / Short description in English:

The TOE type is a Security Token Service (STS). It has been implemented as a pure software application and due to the field of operation in the class of insurance it is further referenced as Insurance Security Token Service, or short ISTS.

The software application provides (software based) security tokens used for authentication purposes of TGIC web services. In addition, the TOE provides the possibility to validate and to cancel the issued token. Further the TOE security features comprise the functionality Security Audit, Identification and Authentication[3] as well as Security Management. Detailed information about the security functionality of the TOE is given in chapter 1.3 and 7.

1.3 TOE description (TOE Beschreibung)

Bei dem TOE, dem Insurance Security Token Service (oder kurz ISTS), handelt es sich um die Hauptkomponente, eine Serveranwendung im Kontext des ITC Service Gateways. Neben dem ISTS umfasst das ITC Service Gateways noch die Firmware und Betriebssystem und die Hardware auf dem der ISTS läuft, wobei jene nicht Bestandteil der Zertifizierung sind.[4]

Die Hauptfunktionalitäten des ISTS umfassen das Ausstellen, Validieren und Zurückziehen von SAML Tokens bzw. Security Tokens[5].

In einem typischen Anwendungsszenario fordert ein Client (der User Agent) Zugriff auf eine sichere Webanwendung (einen Webservice der Trusted German Insurance Cloud: TGIC-Service) an. Andere Webanwendungen bzw. Webportale werden von dem in diesem Dokument

[2] Einige Authentisierungsmechanismen werden von der Umgebung bereitgestellt (vgl. Kapitel 6.1.2 und 7.2).

[3] Some authentication mechanisms are provided by the operational environment (see chapters 6.1.2 and 7.2).

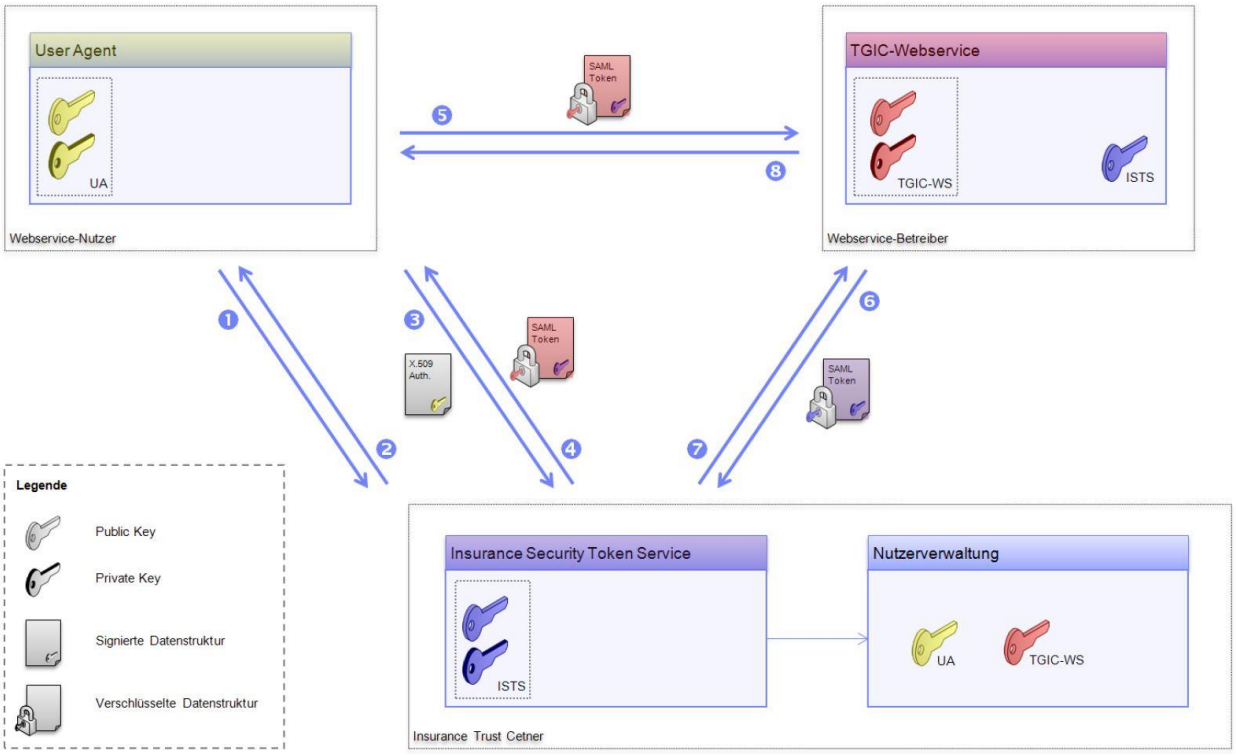
[4] Wird im Folgenden vom ISTS oder Insurance Security Token Service gesprochen, wird damit immer der TOE referenziert. Andere Komponenten werden mit einem entsprechenden Zusatz referenziert.

[5] In der TGIC wird zwischen folgenden zwei Security Token-Ausprägungen unterschieden: SSO-Token und Service Token. In diesem Dokument wird i.d.R. vom Security Token, SAML Token oder einfach Token gesprochen. Nur an Stellen, an denen eine Unterscheidung zwischen Service und SSO Token zur Verständlichkeit zwingend notwendig ist, wird die konkrete Ausprägung des Security Tokens genannt.

beschriebenen ISTS noch nicht unterstützt. Statt sich direkt bei dieser Anwendung (bzw. dem Dienstanbieter des TGIC-Services) zu authentifizieren, wendet sich der Client an den ISTS. Dieser authentifiziert diesen und stellt für weitere Zugriffe einen Sicherheitstoken aus. Mit diesem Token kann er sich anschließend bei der Webanwendung durch Vorlage des Tokens authentifizieren. Die Webanwendung kann die Korrektheit des Tokens dabei offline, also ohne Verbindung zum ISTS, oder online, durch direktes Nachfragen beim ISTS, prüfen und darauf basierend entscheiden, ob der Client auf die angeforderte Anwendung Zugriff erhält.

Im Folgenden wird der Standardablauf im Rahmen der ISTS-Kernfunktionalität (Ausstellen (Issuance) und Validieren (Validation) eines Security Token für den Aufruf eines TGIC-Services durch einen Webservice-Nutzer sowie das Widerrufen von Token (Cancel) in einzelnen Schritten kurz dargestellt.

Abbildung 1 – ISTS Standardablauf



1. Der Webservice-Nutzer fordert über seinen User Agent beim Insurance Security Token Service (ISTS) ein Security Token an (Issuance Binding) und übermittelt dafür im Request seine Partner-ID sowie die Service-ID des TGIC-Services (jeweils als eindeutige Identifikatoren). Zudem übermittelt er in diesem Request auch die von ihm gewünschte Gültigkeit für das auszustellende Security Token sowie die Claims, die vom ISTS zusätzlich in das Security Token eingebettet werden sollen.
2. Aufgrund der Service-ID ermittelt der ISTS über die lokale XML-Datenbank im Filesystem den TGIC-Service, inkl. der von diesem geforderten Authentifikationsmechanismen und Claims (insbesondere die geforderten Nutzergruppen), sowie auf Basis der Partner-ID

über die Nutzerverwaltung den Webservice-Nutzer mit den für ihn aktivierten Authentifikationsmechanismen und Zugehörigkeiten zu Nutzergruppen. Nach erfolgreichem Abgleich dieser Daten fordert der ISTS eine geeignete Authentifikation (in Form einer Challenge) durch den Webservice-Nutzer an.

3. Der Webservice-Nutzer weist gegenüber dem ISTS seine Identität nach.
4. Nach erfolgreicher Authentifikation erstellt der ISTS ein Security Token auf den Namen des Webservice-Nutzers und zur Verwendung mit dem vom Webservice-Nutzer identifizierten TGIC-Service. Das Security Token besitzt eine in der XML-Datenbank pro TGIC-Service jeweils einzeln konfigurierbare Gültigkeit und enthält zusätzlich ggf. vom Webservice-Nutzer angeforderte oder vom TGIC-Service vorausgesetzte Claims. Zudem ist das Security Token vom ISTS digital signiert und für den identifizierten TGIC-Service verschlüsselt worden.
5. Beim Aufruf des TGIC-Services übermittelt der User Agent des Webservice-Nutzers neben dem eigentlichen Request auch das vom ISTS erhaltene Security Token.
6. Der TGIC-Service entschlüsselt das erhaltene Token und kann lokal bereits die mathematische Gültigkeit der eingebetteten Signatur und mit dem Wissen über das Token-Zertifikat des ISTS auch die Vertrauenswürdigkeit des Tokens prüfen.
7. Zusätzlich bzw. alternativ sollte der TGIC-Service das Token auch vom ISTS prüfen lassen (Validation Binding), um auszuschließen, dass das Token widerrufen wurde. Hierzu muss das Token durch den TGIC-Service mit dem öffentlichen X.509-Zertifikat des ISTS aus dem Token erneut verschlüsselt werden.
8. Die Firmware des ITC Service Gateway prüft ebenfalls die mathematische Korrektheit des Tokens, die Vertrauenswürdigkeit der Signatur sowie dessen zeitliche Gültigkeit. Zudem prüft der ISTS, dass das Token nicht widerrufen wurde. Falls das Token erfolgreich validiert werden konnte, wird dies dem TGIC-Service abschließend mitgeteilt.

Für dieses Szenario wurde der WS Trust Standard [WS-Trust] definiert. Das Ziel dieses Standards ist es, innerhalb einer Domäne oder zwischen mehreren Domänen zugesicherte Eigenschaften durch den Einsatz von Sicherheitstoken zu vermitteln. Der Standard behandelt dabei die Herausgabe, das Erneuern und die Validierung von Sicherheitstoken mit Hilfe einer zentralen Authentifizierungsstelle[6]. WS Trust funktioniert ähnlich wie Kerberos, ist aber als offener Standard für den Einsatz mit Web Services konzipiert.

Sowohl der Webservice-Nutzer als auch der Webservice-Betreiber haben nach einer erfolgreichen Authentisierung die Möglichkeit ein zuvor für sie erstelltes Security-Token zu widerrufen. Dazu sendet der Webservice-Nutzer unter Verwendung des User Agents bzw. der Webservice-Betreiber via TGIC-Service eine Anfrage an den ISTS, die den zu widerrufenden Token enthält. Bevor das Token widerrufen werden kann, muss sich der Webservice-Nutzer bzw. der Webservice-Betreiber wie oben beschrieben authentifizieren. Die Authentifikation des Webservice-Betreibers kann dabei nur unter Verwendung der X.509-Zertifikate durchgeführt

[6] Dabei handelt es sich nicht um Single-Sign-On (Nutzung eines Security Token für verschiedene Anwendungen). Das Token wird jeweils für einen Webservice-Nutzer und für einen Webservice ausgestellt.

werden. War die Authentifizierung erfolgreich, so erhält der Webservice-Nutzer bzw. der Webservice-Betreiber eine Bestätigung, dass das entsprechende Token widerrufen wurde.

Der ISTS stellt mehrere Authentifizierungsarten bereit:

- X.509-Zertifikat,
- eID des neuen Personalausweises (nPA),
- mobile Transaktionsnummer (mTAN),
- TOTP (Time-based One-time Password).

Zur Durchführung dieser Authentifizierungen ist der ISTS auf weitere externe Komponenten angewiesen, die in Kapitel 1.3.1.2 behandelt werden. Nach erfolgter Authentifizierung stellt der TOE ein signiertes SAML Token aus, welches vom Client zur weiteren Authentifizierung verwendet werden kann.

Prinzipiell handelt es sich bei den vier Authentifizierungsverfahren um eine 2-Faktor-Authentifikation:

- X.509-Zertifikat: 2-Faktor-Authentifikation[7] („Besitz“ des Schlüsselspeichers mit X.509-Zertifikat und dazugehörigem privatem Schlüssel und „Wissen“ des Kennworts für den Zugriff zum Schlüsselspeichers),
- nPA: 2-Faktor-Authentifikation („Besitz“ des nPA und „Wissen“ der nPA-PIN)
- mTAN: 2-Faktor-Authentifikation („Besitz“ des Mobiltelefons mit der registrierten Telefonnummer zum Empfang der SMS mit der mTAN und „Wissen“ des Kennworts)
- TOTP[8]: 2-Faktor-Authentifikation („Besitz“ des TOTP-Secrets, „Wissen“ des Kennworts).

Webservices, welche die Authentifizierung an den ISTS auslagern, gehen mit dem ISTS ein Vertrauensverhältnis ein, d.h. wenn sie ein signiertes SAML Token erhalten, vertrauen sie darauf, dass alle im Token enthaltenen Informationen korrekt sind.

Der TOE setzt folgende Sicherheitsfunktionalitäten um:

- Secure Audit (die Erzeugung einer Logdatei),
- Identification & Authentication (die Identifizierung und Authentifizierung von Benutzern),
- Security Token Service (das Ausstellen, Widerrufen und Validieren von SAML Token),
- Secure Management (die Verwaltung einiger Sicherheitsfunktionalitäten),

Eine Zusammenfassung der TOE Sicherheitsfunktionalitäten ist in Kapitel 1.3.2 beschrieben, eine detaillierte Beschreibung dieser wird im Rahmen der TOE Übersichtsspezifikation in Kapitel 7 gegeben.

---

[7] Die X.509-Authentifikation stellt in der Regel keine echte 2-Faktor-Authentifikation dar, da das Kennwort nicht serverseitig geprüft wird, sondern nur clientseitig für den Zugriff auf den Schlüsselspeicher notwendig ist. Da die X.509-Authentifikation u.a. die Maschine-zu-Maschine-Kommunikation ermöglichen soll, ist davon auszugehen, dass das notwendige Kennwort einmal in der Client-Software konfiguriert wird und dann beim eigentlichen Authentifikationsvorgang nur noch der Besitz des Schlüsselspeichers relevant ist.

[8] TOTP (Time-based One-time Password) ist ein Verfahren zur Erzeugung von zeitlich limitierten Einmalkennwörtern basierend auf dem Keyed-Hash Message Authentication Code (HMAC). Entwickelt von der branchenübergreifenden Initiative For Open Authentication (OATH) und als RFC 6238 durch die Internet Engineering Task Force (IETF) im Juli 2011 veröffentlicht.

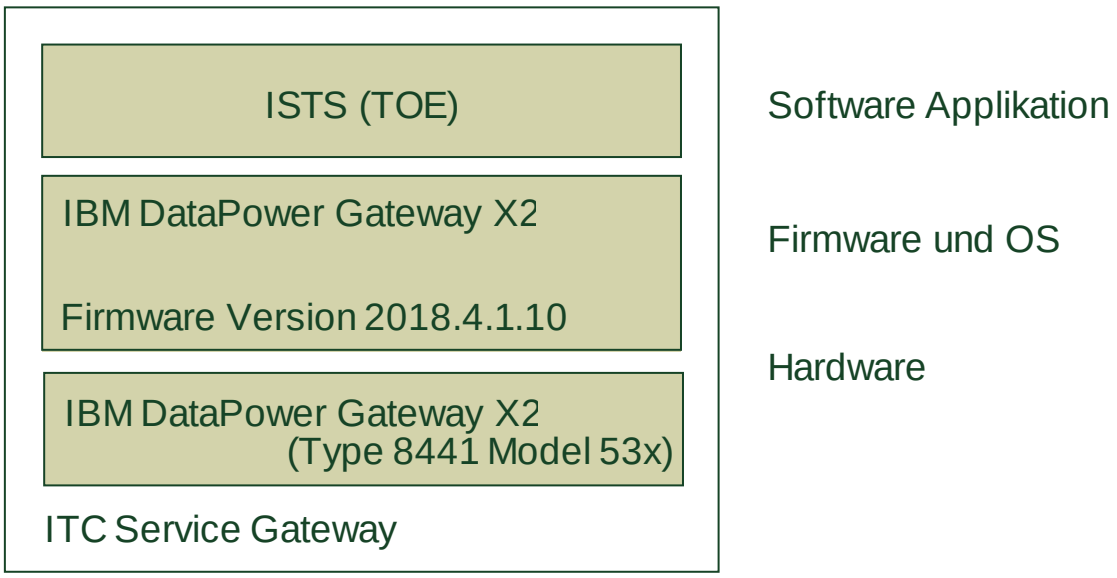
1.3.1 Physical scope (Physikalische Abgrenzung)

1.3.1.1 Description of the TOE components (Beschreibung der TOE Komponenten)

Der TOE ist eine Software-Applikation, die weitere Ressourcen des Betriebssystems verwendet und besteht aus verschiedenen Funktionskomponenten. Die Gesamtfunktionalität wird als ein Monolith (als eine Komponente) erstellt, der in einer logischen Applikations-Domäne in der operativen Einsatzumgebung installiert wird[9].

Die nachfolgende Abbildung 2 skizziert das ITC Service Gateway mit dem TOE (dem ISTS als Software Applikation), der Firmware, dem Betriebssystem und der eingesetzten Hardware.

Abbildung 2 – ITC Service Gateway



Der TOE mit seiner Sicherheitsfunktionalität wird als eine der Komponenten des Insurance Trust Centers (ITC) entwickelt. Entsprechend wird der TOE bzw. die Verwendung und der Betrieb des TOE als eine Komponente – neben anderen – in folgenden Dokumenten beschrieben:

- Anbindungsleitfaden für Service-Betreiber und Webservice-Nutzer in der TGIC,
- Systembeschreibung (Makrodesign und Mikrodesign),
- Betriebshandbuch,
- Benutzerhandbuch.

[9] Auf dem physikalischen Rechner wird der TOE (der ISTS) in einer eigenen Application Domain installiert, die durch die Firmware logisch von anderen Application Domains entkoppelt wird. Es ist vorgesehen, dass auf demselben System auch andere logische Domains aufgesetzt werden können z.B. als Proxy für die Nutzerverwaltung (also weitere Komponenten des ITC, die gemeinsam mit dem ISTS benötigt werden, um die Gesamtfunktionalität des ITC zu gewährleisten). ITC-fremde Komponenten werden weder auf dem physikalischen System noch auf anderen Systemen der erweiterten, operativen ITC-Umgebung laufen.

1.3.1.2 Description of the operational environment of the TOE (Beschreibung der TOE Einsatzumgebung)

Der TOE benötigt in seiner operativen Eisatzumgebung die folgenden Komponenten (vgl. Abbildung 3):

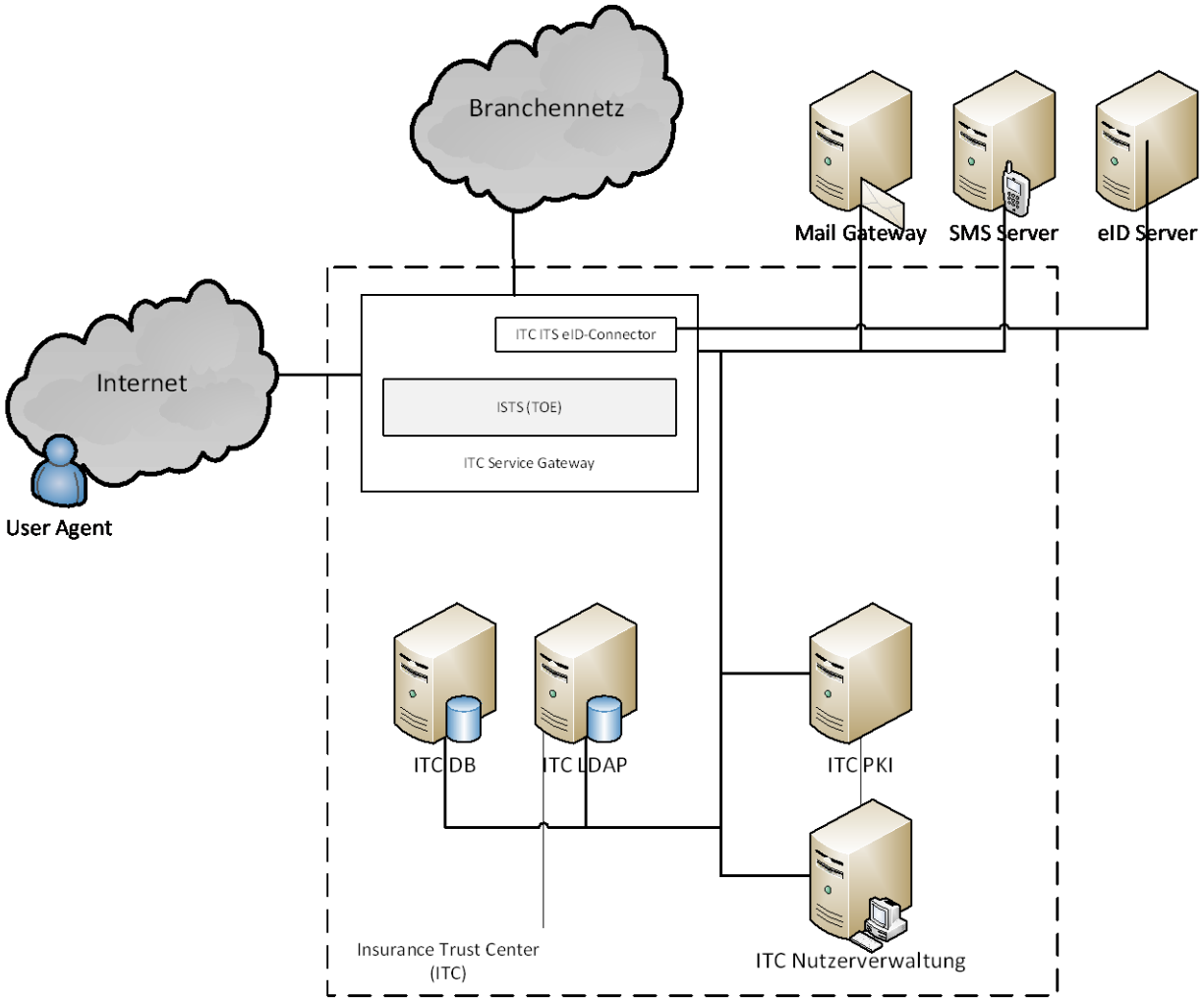
- SMS-Server
  Das SMS Gateway wird für den Versand von generierten mTANs an das Mobiltelefon eines Nutzers verwendet.
- ITC ISTS-eID-Connector
  Dient als Bindeglied zum eID-Server, der wiederum vollständig die Authentifizierung eines Benutzers durch die eID Funktion des neuen Personalausweises (nPA) übernimmt.
- ITC LDAP
  Datenbank im ITC, die alle Benutzerdaten vorhält.
- ITC DB
  Datenbank mit ISTS bezogenen Daten im ITC.

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

- ITC PKI (Public Key Infrastructure im Insurance Trust Center)
  Handhabt die gesamte Verwaltung, Signierung, Verifizierung von X.509 Zertifikaten.
- ITC Nutzerverwaltung
  Zuständig für die Nutzerverwaltung innerhalb des Insurance Trust Centers (ITC).
- eID-Server
  Übernimmt vollständig die Authentifikation eines Nutzers über die eID-Funktion des neuen Personalausweises (nPA) und stellt dem ITC ISTS-eID-Connector anschließend das entsprechende Ergebnis zur Verfügung.
- Mail-Gateway
  Mit dem Mail-Gateway werden 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 Nachrichten (Mitteilung über die erfolgreiche Nutzeranlage, Mitteilung über den Ablauf von X.509-Zertifikaten, erzeugte QR-Codes) zu senden.

Als Plattform des ISTS dient ein IBM DataPower Gateway X2 (Type 8441, Model 53x) mit Firmware Version 2018.4.1.10. Diese Firmware stellt auch weitere Funktionalitäten (z.B. Zeitstempel, Dateisystem, kryptografische Funktionen und Datenbank) für den TOE bereit.

Abbildung 3 – ISTS Abgrenzung



Eine direkte technische Schnittstelle zum/vom ISTS gibt es zu folgenden Komponenten:

- SMS-Server,
- ITC ISTS-eID-Connector,
- ITC DB,
- ITC LDAP.

Insbesondere das Mail-Gateway, die ITC PKI sowie die ITC Nutzerverwaltung werden nicht direkt angebunden. Hingegen nutzt die ITC Nutzerverwaltung das Mail-Gateway und die ITC PKI und legt für den ISTS relevante Daten in der ITC DB und dem ITC LDAP ab.

1.3.2 Logical scope (Logische Abgrenzung)

Die logische Abgrenzung des TOE wird in einzelne Sicherheitsfunktionalitäten aufgeteilt, die ausführlich in Kapitel 6 und 7 beschrieben werden. Die logische Abgrenzung liefert eine Beschreibung der Sicherheitsfunktionalitäten, wie sie vom TOE bereitgestellt werden.

Tabelle 3 – Logische TOE Abgrenzung

TOE Komponente	Beschreibung
Security Audit	Der TOE speichert die folgenden sicherheitsrelevanten Ereignisse in einer externen Datenbank: • Versuch ein Security Token auszustellen, • Versuch ein Security Token zu validieren, • Versuch ein Security Token zu widerrufen. Zusätzliche Informationen, wie Datum und Uhrzeit sowie Token ID und Partner ID, lassen Rückschlüsse auf den Zeitpunkt und den Verursacher des Ereignisses zu.
Identification & Authentication	Der TOE unterstützt mehrere Authentisierungsmechanismen. Die Identifikation des Webservice-Nutzers wird grundsätzlich vom TOE durchgeführt. Die Authentifizierung erfolgt in einem zweiten Schritt und wird für die zertifikats- und eID-basierte Authentifizierung vollständig von der operativen Umgebung durchgeführt. Die mTAN-Authentifizierung per TAN führt der TOE teilweise selbst durch. Dabei werden lediglich die Bereitstellung der Zufallszahl, sowie die Überprüfung des Kennwortes von der Umgebung durchgeführt. Bei TOTP wird das TOTP-Secret aus dem LDAP genommen.
Security Token Service	Die Hauptfunktionalität des TOE ist das Ausstellen, Verifizieren und Zurückziehen von SAML-Tokens, die für die Authentisierung gegenüber einem TGIC-Service verwendet werden können. Es können weitere Attribute[10] hinzugefügt werden.

[10] Zusätzliche Attribute, die für die Ausstellung der Sicherheitstoken verwendet werden, werden verschlüsselt abgelegt. Die Verschlüsselung erfolgt durch die operative Einsatzumgebung des TOE und ist nicht Bestandteil des TOEs.

TOE Komponente	Beschreibung
Security Management	Der TOE verfügt über die Möglichkeit über eine Konfigurationsdatei die folgenden Parameter einzustellen: • Gültigkeitsdauer einer mTAN Session, • Gültigkeitsdauer einer nPA Session, • Gültigkeitsdauer einer X.509 Session. • Gültigkeitsdauer einer TOTP Session. Hierüber kann definiert werden, wie lange die Sitzungsdaten im Cache gültig sind, also wie lange ein User Agent (inkl. Nutzerinteraktion) maximal Zeit hat, um beim jeweiligen Authentifikationsverfahren den Authentifikations-vorgang erfolgreich abzuschließen.

1.4 Conventions (Konventionen)

Die CC erlaubt folgende Operationen innerhalb funktionaler Anforderungen: Zuweisung (assignment), Verfeinerung (refinement), Auswahl (selection) und Aufzählung (iteration). Diese Operationen werden im Teil 2 der CC beschrieben und werden in diesem ST wie folgt dargestellt:

- Eine ausgeführte Zuweisung mit [*kursivem Text in Klammern*].
- Eine ausgeführte Auswahl mit [unterstrichenem Text in Klammern].
- Eine Verfeinerung durch **fetten Text**. Entfernter Text wird durchgestrichen (Beispiel: ~~TSF Data~~) und wird als Verfeinerung angesehen.
- Erweiterte funktionale Anforderungen und erweiterte Anforderungen an die Vertrauenswürdigkeit werden mit dem Präfix “EXT_” versehen.
- Eine Aufzählung wird durch ein der Komponentenbezeichnung nachgestelltes Suffix dargestellt. Als Beispiel wäre „FAU_GEN.1/XXX Audit Data Generation“ die erste Iteration und „FAU_GEN.1/YYY Audit Data Generation“ wäre die zweite Iteration.

2 Conformance Claims (Konformitätspostulate)

Dieser Abschnitt behandelt die relevanten Identifikationen für die CC, das Protection Profile (PP) und das verwendete EAL Paket. Für jede Erweiterung bzw. Augmentierung wird eine Erklärung gegeben. Dieser Abschnitt ist unterteilt in:

- CC conformance claims (CC Konformitätspostulat),
- PP claim (PP Postulat),
- Package claim (Paket Postulat),
- Conformance rationale (Konformitätserklärung).

2.1 CC conformance claims (CC Konformitätspostulat)

Dieses Security Target ist konform zur Common Criteria 3.1:

- „Part 2 extended“ bezüglich [CC]:

  Um eine vollständige Beschreibung der funktionalen Anforderungen zu geben, wurden Komponenten aus Teil 2 des Common Criteria Rahmenwerks verwendet. Weiterhin wurden Erweiterungen zum Teil 2 definiert, um die Anforderungen an eine vollständige und konsistente TOE Beschreibung zu erfüllen.
- “Part 3 conformant” bezüglich [CC]:

  Für die Beschreibung der Anforderungen an die Vertrauenswürdigkeit des TOE, werden ausschließlich Vertrauenskomponenten aus dem Teil 3 des Common Criteria Rahmenwerks verwendet.

2.2 PP claim (PP Postulat)

Dieses ST postuliert keine Konformität zu einem bestehenden PP.

2.3 Package claim (Paket Postulat)

Dieses ST postuliert seine Konformität zu dem Security Assurance Requirements Paket EAL 2.

2.4 Conformance rationale (Konformitätserklärung)

Dieses ST postuliert keine Konformität zu einem bestehenden PP.

3 Security Problem Definition (Definition des Sicherheitsproblems)

3.1 Assets (Werte)

Tabelle 4 – Werte

Werte	Beschreibung
Benutzerdaten / Personenbezogene Daten	Daten, die vom und für den Benutzer erstellt werden und die den Betrieb der TSF nicht beeinflussen. Insbesondere umfasst dieser Wert die folgenden Daten: • Generierte Security Token mit den notwendigen Attributen o Token ID, o Ausstellungsdatum und -uhrzeit, o Partner ID, o Webservice ID, o XML-Signatur und Hash des Tokens, o X.509 Zertifikat und den optionalen Attributen o Vor- und Nachname, o E-Mail-Adresse, o Geschlecht, o Anschrift, o Geburtsdatum, o Organisation, o weitere freie Nutzergruppen, o Gültigkeitsdauer des Tokens. • Authentisierungsinformationen: o Partner-ID, o Service-ID des TGIC-Services, o X.509 Zertifikat, o mTAN-Mobilfunknummer, o TOTP-Secret, o Kennwort für mTAN- oder TOTP-Authentisierung, o nPA-Pseudonym.

Werte	Beschreibung
TSF Daten	Von und für den TOE erstellte Daten, die den Betrieb des TOE beeinflussen können. Insbesondere umfasst dieser Wert die folgenden Daten: • Gültigkeitsdauer einer mTAN Session, • Gültigkeitsdauer einer nPA Session, • Gültigkeitsdauer einer X.509 Session. • Gültigkeitsdauer einer TOTP Session.

3.2 Subjects (Subjekte)

Tabelle 5 – Subjekte

Subjekte	Beschreibung
Angreifer	Eine Person, die versucht das normale Verhalten des TOEs zu unterwandern und damit versucht unautorisierten Zugriff auf dessen geschützte Werte zu erhalten. Die Person hat Kenntnis von öffentlich verfügbaren Informationen über den TOE, verfügt aber über kein professionelles Fachwissen. Sie hat begrenzte Ressourcen zur Verfügung, um seine Parameter zu modifizieren, und hat auch keinen direkten physikalischen Zugriff auf den TOE.
User Agent	Um auf einen TGIC-Service zuzugreifen, benötigen Webservice-Nutzer zur Authentisierung gegenüber dem TGIC-Service einen Security Token des ISTS. Die Software, die ein Webservice-Nutzer verwendet, um sich gegenüber dem ISTS zu authentisieren und einen Security Token zu erhalten wird als User Agent bezeichnet.
TGIC-Service	Als TGIC-Service wird die Implementierung eines in der Trusted German Insurance Cloud (TGIC) registrierten Services bezeichnet. Dieser kommuniziert mit dem ISTS, um ein vom User Agent übermitteltes Security Token zu validieren und darauf basierend die Autorisation des Webservice-Nutzers zu prüfen.
Administrator	Der Administrator ist autorisiert den TOE zu verwalten. Er kann diesen sowohl physikalisch als auch remote administrieren und verfügt über das entsprechende Fachwissen.

3.3 Threats (Bedrohungen)

Tabelle 6 – Bedrohungen

Bedrohungen	Beschreibung
T.I&A	Angreifer können die Identität eines autorisierten TOE Benutzers vorgeben, um unbefugt ein Security Token zu erhalten.
T.UNDETECTED	Sicherheitsrelevante Aktionen von Benutzern könnten unerkannt durchgeführt werden. Dies könnte dazu führen, dass sicherheitsrelevante Ereignisse unerkannt bleiben und der Administrator nicht geeignet reagieren kann. Somit wäre die Sicherheit der TSF und Benutzer Daten gefährdet.

3.4 Organizational security policies (Organisatorische Sicherheits-politiken)

Tabelle 7 – Sicherheitspolitiken

Sicherheitspolitiken	Beschreibung
P.ACCOUNT	TOE Benutzer müssen für sicherheitsrelevante Aktionen, die sie mit dem TOE durchführen, verantwortlich gemacht werden können.

3.5 Assumptions (Annahmen)

Tabelle 8 – Annahmen

Annahmen	Beschreibung
A.ENVIRONMENT	Die operative Umgebung[11] stellt folgende Funktionalitäten zur Verfügung: Zeitstempel[12], Dateisystem, kryptografische Funktionen[13] und Datenbank[14]. Weiterhin wird sichergestellt, dass nur autorisierte Personen Zugriff auf TSF Daten erhalten, die in der operativen Umgebung gespeichert werden.
A.NOEVIL	Administratoren, die in Berührung mit TSF Daten oder Funktionalität kommen, sind nicht unachtsam, vorsätzlich fahrlässig oder feindlich eingestellt. Sie folgen der Anleitung, die dem TOE beiliegt. Sie sind gut ausgebildet die TOE Funktionalitäten sicher und verantwortungsvoll zu administrieren.
A.PHYSEC	Der TOE ist gegen unautorisierten physikalischen Zugriff und Modifikation geschützt.
A.PUBLIC	Die operative Umgebung[11] 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.
A.PKI	Die ITC PKI der operativen Umgebung bringt, als eine für den TOE vertrauenswürdige PKI-Struktur mit vertrauenswürdiger CA, ausschließlich Zertifikate in den Umlauf, die unter Verwendung von SHA-256 erstellt wurden.

[11] Auf dem physikalischen Rechner wird der TOE (die ISTS-Kernfunktionalität) in einer eigenen Application Domain installiert, die durch die Firmware logisch von anderen Application Domains entkoppelt wird. Es ist vorgesehen, dass auf dem selben System auch andere logische Domains aufgesetzt werden können z.B. als Proxy für die Nutzerverwaltung (also weitere Komponenten des ITC, die gemeinsam mit dem ISTS benötigt werden, um die Gesamtfunktionalität des ITC zu gewährleisten). ITC-fremde Komponenten werden weder auf dem physikalischen System noch auf anderen Systemen der erweiterten, operativen ITC-Umgebung laufen.

[12] auf Basis von NTP

[13] Die innerhalb der TOE Einsatzumgebung eingesetzten kryptografische Verfahren sind in Kapitel 8.1 aufgeführt.

[14] in Form eines (einfachen) Session-Caches

4 Security Objectives (Sicherheitsziele)

4.1 Security objectives for the TOE (Sicherheitsziele für den TOE)

Tabelle 9 – Sicherheitsziele für den TOE

Ziele	Beschreibung
O.ACCOUNT	TOE Benutzer sollen für sicherheitsrelevante Aktionen, die sie mit dem TOE durchführen, verantwortlich gemacht werden können.
O.AUDREC	Der TOE soll ein Logfile führen, in dem sicherheitsrelevante Ereignisse protokolliert werden.
O.I&A	Der TOE soll einen Benutzer identifizieren und authentisieren, bevor weitere Aktionen durchgeführt werden können.[15] Im Falle einer mTAN-Authentisierung soll der TOE den Benutzer selbst authentisieren (die Bereitstellung der Zufallszahl, sowie die Überprüfung des Kennwortes wird von der Umgebung durchgeführt), im Falle einer zertifikatsbasierten, eID- oder TOTP-Authentisierung soll die Authentisierung durch eine externe Entität erfolgen.
O.STS	Der TOE soll nach erfolgreicher Authentifikation WS-Trust-konforme SAML-Token ausstellen und ein für ihn generiertes Security Token widerrufen können. Des Weiteren soll der TOE Security Token validieren können.

4.2 Security objectives for the operational environment (Sicherheitsziele für die operative Umgebung)

Tabelle 10 – Sicherheitsziele für die operative Umgebung

Ziele	Beschreibung
OE.ENVIRONMENT	Die operative Umgebung soll folgende Funktionalitäten zur Verfügung stellen: Zeitstempel, Dateisystem, kryptografische Funktionen[16] 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.

[15] Die einzige Ausnahme bildet die Aktion Validierung eines Tokens. Diese Aktion kann ohne die Authentisierung des Benutzers erfolgen.

[16] Die innerhalb der TOE Einsatzumgebung eingesetzten kryptografische Verfahren sind in Kapitel 8.1 aufgeführt.

Ziele	Beschreibung
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.

4.3 Security objectives rationale (Erklärung der Sicherheitsziele)

Tabelle 11 – Erklärung der Sicherheitsziele

Threats and Assumptions vs. Security Objectives	O.ACCOUNT	O.AUDREC	O.I&A	O.STS	OE.ENVIRONMENT	OE.NOEVIL	OE.PHYSEC	OE.PUBLIC	OE.PKI
T.I&A			X	X					
T.UNDETECTED	X	X							
P.ACCOUNT	X	X	X						
A.ENVIRONMENT					X				
A.NOEVIL						X			
A.PHYSEC							X		
A.PUBLIC								X	
A.PKI									X

T.I&A wird begegnet durch

- **O.I&A**, indem Benutzer sich Identifizieren müssen, bevor weitere sicherheitsrelevante Aktionen möglich sind.
- **O.STS** dadurch, dass SAML-Token erst nach erfolgreicher Authentifizierung ausgestellt werden und vom entsprechenden Benutzer widerrufen werden können. Des Weiteren bietet der TOE die Möglichkeit Security Token zu validieren.

T.UNDETECTED wird begegnet durch

- **O.ACCOUNT**, indem Benutzer für sicherheitsrelevante Aktionen, die sie mit dem TOE durchführen, verantwortlich gemacht werden können.
- **O.AUDREC**, indem sicherheitsrelevante Ereignisse protokolliert werden.

P.ACCOUNT wird begegnet durch

- **O.ACCOUNT**, indem Benutzer für sicherheitsrelevante Aktionen, die sie mit dem TOE durchführen, verantwortlich gemacht werden können.
- **O.AUDREC** durch Führen einer Logdatei.
- **O.I&A**, indem Benutzer sich Identifizieren müssen, bevor weitere sicherheitsrelevante Aktionen möglich sind.

In der obigen Tabelle steht jede Bedrohung oder Sicherheitspolitik in Relation mit einer oder mehreren Sicherheitszielen. Diese Relationen zeigen, dass die definierten Sicherheitsziele alle Bedrohungen oder Sicherheitspolitiken vollständig abdecken.

A.ENVIRONMENT erfüllt

- OE.ENVIRONMENT, indem die operative Umgebung bestimmte Funktionalitäten verlässlich dem TOE zur Verfügung stellt.

A.NOEVIL erfüllt

- OE.NOEVIL, indem Administratoren, die in Berührung mit TSF Daten oder Funktionalität kommen, nicht unachtsam oder vorsätzlich fahrlässig mit diesen umgehen. Sie folgen der Anleitung, die dem TOE beiliegt und sind gut ausgebildet die TOE Funktionalitäten sicher und verantwortungsvoll zu administrieren.

A.PHYSEC erfüllt

- OE.PHYSEC, indem der TOE gegen unautorisierten physikalischen Zugriff und Modifikation geschützt ist.

A.PUBLIC erfüllt

- OE.PUBLIC, indem die operative Umgebung ausschließlich für den TOE verwendet wird.

A.PKI erfüllt

- OE.PKI, indem die operative Umgebung eine PKI mit den geforderten Eigenschaften bereitstellt.

Jede Annahme steht in Relation zu mindestens einem oder mehreren Sicherheitszielen für die Umgebung. Diese Relationen zeigen, dass die definierten Sicherheitsziele für die Umgebung alle Annahmen vollständig abdecken.

5 Extended Components Definition (Definition erweiterter Komponenten)

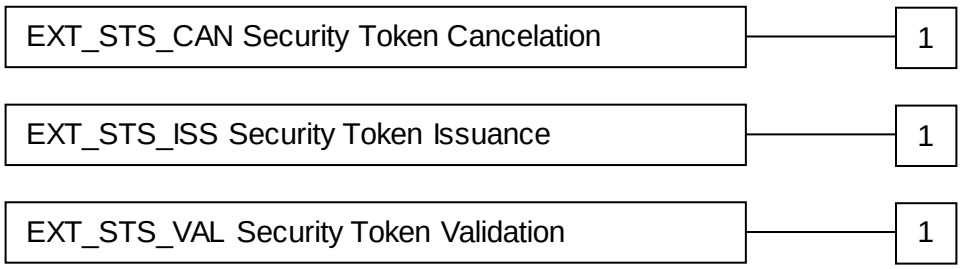
Dieses Kapitel definiert TOE Sicherheitsanforderungen, die nicht Bestandteil der CC 3.1 Teil 2 oder Teil 3 sind.

Um die beschriebenen Komponenten konsistent zu CC 3.1 Teil 2 zu beschrieben, erfolgt die Beschreibung nachfolgend ausschließlich in englischer Sprache.

5.1 Extended TOE Security Functional Components (Erweiterte funktionale Sicherheitsanforderungen für den TOE)

5.1.1 EXT_STS Security Token Service

The additional class EXT_STS Security Token Service defines the security functional requirements of the regarding the handling of security token. The handling includes issuance, validation and cancelation of security tokens. The Security Token Service class is structured as follows:

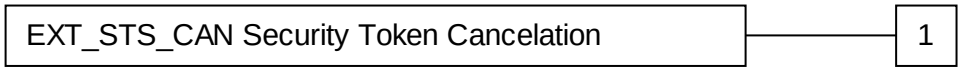


5.1.1.1 Security Token Cancelation (EXT_STS_CAN)

Family Behavior

This family defines the requirements of the TSF that describe how to cancel security tokens that were issued by the TSF. Especially this family defines the actions that shall be performed by the TSF to revoke an issued security token.

Component leveling



EXT_STS_CAN.1 Security Token Cancelation describes the actions that shall be performed by the TSF, if upon a user request a security token, which was issued by the TSF, shall be cancelled.

Management: EXT_STS_CAN.1

There are no management activities foreseen.

Audit: EXT_STS_CAN.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

- Cancelation of the security token.

At least the following information should be record:

- Date and time, when the cancelling was performed,
- Token ID of the cancelled token,
- Partner ID of that user who has initiated the cancelling.

EXT_STS_CAN.1 Security Token Cancelation

Hierarchical to: No other components

Dependencies: EXT_STS_ISS.1

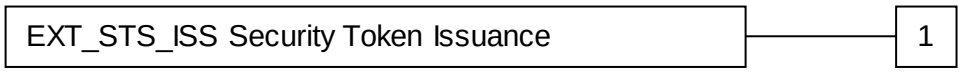
EXT_STS_CAN.1.1 The TSF shall be able to cancel an issued security token upon the request of [assignment: *list of authorized users or IT entities*].

5.1.1.2 Security Token Issuance (EXT_STS_ISS)

Family Behavior

This family defines the requirements on security token issuance by the TSF. This family includes requirements regarding the secure generation and delivery of a security token.

Component leveling



EXT_STS_ISS.1 Security Token Issuance describes the actions that shall be performed by the TSF to generate and deliver a security token.

Management: EXT_STS_ISS.1

For this component no management activities are foreseen.

Audit: EXT_STS_ISS.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

- Issuance of the security token,
- an unsuccessful issuance of the security token.

At least the following information should be record (in case of an unsuccessful issuance only as appropriate):

- Date and time of the event,
- Token ID,
- Partner ID.

EXT_STS_ISS.1 Security Token Issuance

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

EXT_STS_ISS.1.1	The TSF shall be able to generate a security token upon a request of an authenticated user.
EXT_STS_ISS.1.2	The TSF shall include at least the following information to the security token within the generation process: [assignment: *list of security attributes*].
EXT_STS_ISS.1.3	The TSF shall send the security token via [assignment: *list of transfer protocols*] only to the authenticated user, who causes the generation of the security token.

5.1.1.3 Security Token Validation (EXT_STS_VAL)

Family Behavior

This family defines the requirements on security token validation by the TSF. The requirements compose the actions that shall be performed by the TSF to verify the security token provided by a TOE user.

Component leveling

EXT_STS_VAL Security Token Validation	1

EXT_STS_VAL.1 Security Token Validation describes the actions that shall be performed by the TSF to verify a delivered security token.

Management: EXT_STS_VAL.1

For this component no management activities are foreseen.

Audit: EXT_STS_VAL.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

- Validation of the security token.

At least the following information should be record:

- Date and time of the event,
- Token ID,
- Partner ID.

EXT_STS_VAL.1 Security Token Validation

Hierarchical to: No other components

Dependencies: No dependencies

EXT_STS_VAL.1.1 The TSF shall perform the following actions to verify the validity of a security token [assignment: *actions that shall be performed by the TSF*].

5.2 Extended TOE Security Assurance Components (Erweiterte Anforderungen an die Vertrauenswürdigkeit des TOE)

There are no extended TOE Security Assurance Components.

6 Security Requirements (Sicherheitsanforderungen)

Dieses Kapitel definiert die TOE Sicherheitsanforderungen (SFR) und Anforderungen an die Vertrauenswürdigkeit (SAR) gemäß der CC 3.1 Teil 2 und Teil 3.

Um die beschriebenen Komponenten konsistent zu CC 3.1 zu beschrieben, erfolgt die Beschreibung nachfolgend ausschließlich in englischer Sprache.

6.1 Security functional requirements (Funktionale Sicherheits-anforderungen)

Die funktionalen Sicherheitsanforderungen sind konform zu Common Criteria v3.1 Teil 2.

Tabelle 12 – Funktionale Sicherheitsanforderungen

Name	Description
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User identity association
FIA_UAU.1	Timing of authentication
FIA_UAU.5	Multiple authentication mechanism
FIA_UID.1	Timing of identification
FMT_SMF.1	Specification of management functions
EXT_STS_CAN.1/SRV	Security Token Cancelation
EXT_STS_CAN.1/SSO	Security Token Cancelation
EXT_STS_ISS.1/SRV	Security Token Issuance
EXT_STS_ISS.1/SSO	Security Token Issuance
EXT_STS_VAL.1/SRV	Security Token Validation
EXT_STS_VAL.1/SSO	Security Token Validation

6.1.1 Class FAU – Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions[17];

b) All auditable events, for the [not specified] level of audit; and

c) [*all events that are listed in Tabelle 13].*

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the ST, [*additional information as listed in Tabelle 13.*]

Tabelle 13 – Auditable Events

Security Functional Requirement	Auditable Event(s)	Additional recorded information
FAU_GEN.1	None	None
FAU_GEN.2	None	None
FIA_UAU.1	None[18]	None
FIA_UAU.5	None[18]	None
FIA_UID.1	None[18]	None
FMT_SMF.1	None[19]	None
EXT_STS_CAN.1/SRV	Each attempt to cancel a security token	Token ID, Partner ID

[17] Diese Anforderung wird implizit erfüllt, da diese Ereignisse während des Betriebs des TOE nicht eintreten können. Die sicherheitsrelevanten Ereignisse werden vom TOE in eine eigene Tabelle der ISTS-DB geschrieben. Ist die Datenbank voll oder kann nicht angesprochen werden, so wird die aktuelle Funktion mit einem technischen Fehler abgebrochen. Dieses Ereignis wird anschließend in einem technischen Log-File der DataPower Firmware festgehalten, um entsprechende administrative Aktionen anzustoßen. Jede Anfrage an den ISTS bedeutet einen „Start-up" des TOE und wird entsprechend geloggt.

[18] Die Identifizierungs- und Authentisierungsversuche werden im technischen Log durch die DataPower Firmware geloggt.

[19] Eine Änderung dieser Parameter geschieht durch das Einspielen der Konfiguration über die DataPower Firmware. Diese Ereignisse und die dafür notwendige Login-Vorgänge werden durch die Firmware im technischen Log festgehalten.

Security Functional Requirement	Auditable Event(s)	Additional recorded information
EXT_STS_CAN.1/SSO	Each attempt to cancel a security token	Token ID, Partner ID
EXT_STS_ISS.1/SRV	Each attempt to generate a security token	Token ID, Partner ID
EXT_STS_ISS.1/SSO	Each attempt to generate a security token	Token ID, Partner ID
EXT_STS_VAL.1/SRV	Each attempt to validate a security token	Token ID, Partner ID
EXT_STS_VAL.1/SSO	Each attempt to validate a security token	Token ID, Partner ID

Anwendungshinweis:

Es erfolgt kein explizites Loggen des Starts-/Stopps der Auditfunktionen, da diese Funktionalität aufgrund des zustandslosen Entwurfs nicht existiert und ein entsprechendes Ereignis nicht eintreten kann.

FAU_GEN.2 User identity association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.2 Class FIA – Identification and authentication

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [*the identification of the user, the validation of the transmitted security token*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Anwendungshinweis:

Es gilt zu beachten, dass die Authentisierung nur für die Webservice-Nutzer, repräsentiert durch das Subjekt User Agent, mit Hilfe des TOE durchgeführt wird. Die Authentisierung des Webservice-Betreibers repräsentiert durch das Subjekt TGIC-Service kann innerhalb des TOE ausschließlich via X.509-Zertifikaten durchgeführt werden (vgl. FIA_UAU.5), während die Authentisierung der Administratoren ausschließlich durch die operative Umgebung des TOE realisiert wird.

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide [
the possibility to use the following authentication mechanisms:
- *Authentication via X.509-certificates,*
- *Authentication via nPA,*
- *Authentication via mTAN*
- *Authentication via TOTP*

] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [*following rules:*
- *if the web service requires an authentication via X.509-certificates the authentication mechanism via X.509-certificates shall be used,*
- *if the web service requires an authentication via nPA the authentication mechanism via nPA shall be used,*
- *if the web service requires an authentication via mTAN the authentication mechanism via mTAN shall be used*
- *if the web service requires an authentication via TOTP the authentication mechanism via TOTP shall be used*].

Anwendungshinweis:

Es gilt zu beachten, dass Teile der Authentisierungsmechanismen von der operativen Umgebung des TOE umgesetzt werden. Im Detail werden die folgenden Operationen für die jeweiligen Authentisierungsverfahren von der Umgebung durchgeführt:

- Authentifizierung via X.509-Zertifikat
  Im Rahmen der Authentifikation via X.509-Zertifikat wird die zu signierende Zufallszahl von der operativen Umgebung des TOE geliefert. Des Weiteren erfolgt die Signaturprüfung durch die operative Umgebung des TOE.
- Authentifizierung via neuen Personalausweis (nPA)
  Die Authentifizierung via nPA erfolgt mit Hilfe eines eID-Servers aus der operativen Umgebung des TOE. Der ISTS stößt lediglich den Prozess zur Authentifizierung an. Die Ergebnisse der nPA-Authentifikation werden durch den eID-Server anschließend dem ITC ISTS-eID-Connector bereitgestellt und stehen dann über letzteren dem ISTS zur Verfügung.
- Authentifizierung via mobiler Transaktionsnummer (mTAN)
  Im Rahmen der Authentifikation via mTAN wird die zur TAN-Generierung benötigte Zufallszahl von der operativen Umgebung des TOE geliefert. Des Weiteren nutzt das ISTS einen SMS-Server aus der Umgebung, um die generierte mTAN an den

Webservice-Nutzer zu senden. Das zusätzlich übermittelte Kennwort wird durch das externe ITC LDAP validiert.

- Authentifizierung via Time-based One-time Password (TOTP)
  Im Rahmen der Authentifikation via TOTP wird die benötigte Zufallszahl von der operativen Umgebung des TOE geliefert. Dafür wird das TOTP-Seed samt Secret aus dem LDAP bezogen. Der Nutzer erhält demselben TOTP-Seed bei der Registrierung in TGIC per separate E-Mail in Form des QR-Codes. Das zusätzlich übermittelte Kennwort wird durch das externe ITC LDAP validiert.

Alle übrigen Operationen werden vom TOE durchgeführt.

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1	The TSF shall allow [*the validation of the transmitted security token*] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Anwendungshinweis:

Es gilt zu beachten, dass die Identifizierung nur für die Webservice-Nutzer repräsentiert durch das Subjekt User Agent und Webservice-Betreiber repräsentiert durch das Subjekt TGIC-Service mit Hilfe des TOE durchgeführt wird. Die Identifizierung der Administratoren wird ausschließlich durch die operative Umgebung des TOE realisiert.

6.1.3 Class FMT – Security Management

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No Dependencies

FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions [*see Tabelle 14*].

Tabelle 14 – Management der Sicherheitsattribute

Operation	Security Attribute
Change	Term of validity of a mTAN session
Change	Term of validity of a nPA session
Change	Term of validity of a X.509 session
Change	Term of validity of a TOTP session

Anwendungshinweis:

Konfigurationsanpassungen werden mit Hilfe einer Konfigurationsdatei durchgeführt. Der TOE prüft, ob die Konfiguration (eine XML-Datei) dem erwarteten XML-Schema entspricht und liest diese ein. Diese Prüfung erfolgt zustandslos jedes Mal, wenn die Datei eingelesen wird.

6.1.4 Class EXT_STS – Security Token Service

EXT_STS_CAN.1/SRV Security Token Cancelation

Hierarchical to: No other components.

Dependencies: EXT_STS_ISS.1/SRV Security Token Issuance

EXT_ STS_CAN.1.1/SRV	The TSF shall be able to cancel an issued **Service** ~~security~~ token upon the request of [*the user Webservice-Nutzer via the subject User Agent and the user Webservice-Betreiber via the subject TGIC-Service*].

Anwendungshinweis:

Es gilt zu beachten, dass der Widerruf von Service Tokens nur durch Benutzer erfolgen darf, die eindeutig diesem Service Token zugeordnet werden können. Dies sind entweder der Webservice-Nutzer, der das Token beantragt hat, oder der Webservice-Betreiber für den das Token ausgestellt wurde.

EXT_STS_CAN.1/SSO Security Token Cancelation

Hierarchical to: No other components.

Dependencies: EXT_STS_ISS.1/SSO Security Token Issuance

EXT_ STS_CAN.1.1/SSO	The TSF shall be able to cancel an issued **SSO** ~~security~~ token upon the request of [*the authenticated user Webservice-Nutzer via the subject User Agent and the authenticated user Webservice-Betreiber via the subject TGIC-Service*].

Anwendungshinweis:

Es gilt zu beachten, dass der Widerruf des SSO[20] Tokens nur durch Benutzer erfolgen darf, die eindeutig diesem SSO Token zugeordnet werden können. Dies sind entweder der Webservice-Nutzer, der das Token beantragt hat, oder der Webservice-Betreiber für den das Token ausgestellt wurde.

[20] SSO – Single Sign-On Token, ein Token welches dazu verwendet wird ein weiteres Token auszustellen.

EXT_STS_ISS.1/SRV Security Token Issuance

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

EXT_STS_ISS.1.1/SRV	The TSF shall be able to generate a **Service** ~~security~~ token upon a request of an authenticated user.
EXT_STS_ISS.1.2/SRV	The TSF shall include at least the following information to the **Service** ~~security~~ token within the generation process: [• *Token ID* • *Ausstellungsdatum und -uhrzeit* • *Partner ID* • *Webservice ID* • *XML-Signatur und Hash des Tokens* • *X.509 Zertifikat*].
EXT_STS_ISS.1.3/SRV	The TSF shall sent the **Service** ~~security~~ token via [*WS-Trust*[21] *via SOAP over HTTPS*] only to the authenticated user, who causes the generation of the **Service** ~~security~~ token.

Anwendungshinweis:

Es gilt zu beachten, dass der vertrauenswürdige Kanal und die notwendigen kryptografischen Operationen werden von der operativen Einsatzumgebung bereitgestellt werden.

[21] Hierbei handelt es sich um eine ISTS-spezifische aber Standard-konforme Erweiterung von WS-Trust 1.4

EXT_STS_ISS.1/SSO Security Token Issuance

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

EXT_STS_ISS.1.1/SSO	The TSF shall be able to generate a **SSO** ~~security~~ token upon a request of an authenticated user.
EXT_STS_ISS.1.2/SSO	The TSF shall include at least the following information to the **SSO** ~~security~~ token within the generation process: [• *Token ID* • *Ausstellungsdatum und -uhrzeit* • *Partner ID* • *Webservice ID* • *XML-Signatur und Hash des Tokens* • *X.509 Zertifikat*].
EXT_STS_ISS.1.3/SSO	The TSF shall send the **SSO** ~~security~~ token via [*WS-Trust*[22] *via SOAP over HTTPS*] only to the authenticated user, who causes the generation of the security token.

Anwendungshinweis:

Der Nutzer kann beim TOE über WS-Trust ein „SSO“ (single sign-on) Token beantragen. Mit diesem Token können beim TOE Service Token zur Authentifikation gegenüber dem TGIC-Service angefordert werden.

Es gilt zu beachten, dass der vertrauenswürdige Kanal und die notwendigen kryptografischen Operationen werden von der operativen Einsatzumgebung bereitgestellt werden.

[22] Hierbei handelt es sich um eine ISTS-spezifische aber Standard-konforme Erweiterung von WS-Trust 1.4

EXT_STS_VAL.1/SRV Security Token Validation

Hierarchical to: No other components

Dependencies: No dependencies

EXT_STS_VAL.1.1/SRV	The TSF shall perform the following actions to verify the validity of a **Service** ~~security~~ token [*validation whether the security token was cancelled or not*].

Anwendungshinweis:

Es gilt zu beachten, dass alle übrigen Aktionen, die zur Validierung des Service Tokens beitragen von der operativen Einsatzumgebung des TOE durchgeführt werden. Dies umfasst insbesondere die folgenden Handlungen:

- Entschlüsselung des Security Tokens,
- Prüfung der Security Token-Syntax via XML-Schema,
- Prüfung der Security Token-Signatur.

EXT_STS_VAL.1/SSO Security Token Validation

Hierarchical to: No other components

Dependencies: No dependencies

EXT_STS_VAL.1.1/SSO	The TSF shall perform the following actions to verify the validity of a **SSO** ~~security~~ token [*validation whether the security token was cancelled or not*].

Anwendungshinweis:

Es gilt zu beachten, dass alle übrigen Aktionen, die zur Validierung des SSO Tokens beitragen von der operativen Einsatzumgebung des TOE durchgeführt werden. Dies umfasst insbesondere die folgenden Handlungen:

- Entschlüsselung des Security Tokens,
- Prüfung der Security Token-Syntax via XML-Schema,
- Prüfung der Security Token-Signatur.

6.2 Security assurance requirements (Anforderungen an die Vertrauenswürdigkeit)

Die Anforderungen an die Vertrauenswürdigkeit des TOEs sind die Vertrauenskomponenten der Evaluation Assurance Level 2 (EAL2). Sie wurden alle Teil 3 der Common Criteria entnommen. Die Vertrauenskomponenten sind in Tabelle 15 aufgeführt.

Tabelle 15 – EAL2 Vertrauenskomponenten

Vertrauens-komponente	Name
ADV_ARC.1	Security architecture description
ADV_FSP.2	Security-enforcing functional specification
ADV_TDS.1	Basic design
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.2	Use of a CM system
ALC_CMS.2	Parts of the TOE CM coverage
ALC_DEL.1	Delivery procedures
ASE_CCL.1	Conformance claims
ASE_ECD.1	Extended components definition
ASE_INT.1	ST introduction
ASE_OBJ.2	Security objectives
ASE_REQ.2	Derived security requirements
ASE_SPD.1	Security problem definition
ASE_TSS.1	TOE summary specification
ATE_COV.1	Evidence of coverage
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_VAN.2	Vulnerability analysis

6.3 Security requirement rationale

6.3.1 Rational for the security functional requirements

Tabelle 16 – Umsetzung der Sicherheitsziele

Security Objectives vs. Security Requirements	O.ACCOUNT	O.AUDREC	O.I&A	O.STS
FAU_GEN.1	X	X		
FAU_GEN.2	X	X		
FIA_UAU.1			X	
FIA_UAU.5			X	
FIA_UID.1			X	
FMT_SMF.1				X
EXT_STS_CAN.1/SRV				X
EXT_STS_CAN.1/SSO				X
EXT_STS_ISS.1/SRV				X
EXT_STS_ISS.1/SSO				X
EXT_STS_VAL.1/SRV				X
EXT_STS_VAL.1/SSO				X

O.ACCOUNT wird umgesetzt durch

- FAU_GEN.1, indem ein Logfile für sicherheitsrelevante Ereignisse erstellt wird und
- FAU_GEN.2, indem jedem Logeintrag eine Person zugeordnet wird.

O.AUDREC

- FAU_GEN.1, indem ein Logfile für sicherheitsrelevante Ereignisse erstellt wird und
- FAU_GEN.2, indem jedem Logeintrag eine Person zugeordnet wird.

O.I&A

- FIA_UAU.1, indem sich ein Webservice-Nutzer authentisieren muss, nachdem er sich zuvor identifiziert hat.[23]
- FIA_UAU.5, indem mehrere Mechanismen zur Authentifizierung zur Verfügung gestellt werden.
- FIA_UID.1, indem sich ein Benutzer identifizieren muss, bevor von ihm eine sicherheitsrelevante Funktion ausgeführt werden kann.[24]

O.STS

- FMT_SMF.1, indem die STS-Funktionalität verlässlich konfiguriert wird,
- EXT_STS_CAN.1/SRV und EXT_STS_CAN.1/SSO, indem der STS SAML-Token zurückrufen kann,
- EXT_STS_ISS.1/SRV und EXT_STS_ISS.1/SSO, indem der STS SAML-Token nur dann ausstellt, wenn der Benutzer sich vorher authentisiert hat,
- EXT_STS_VAL.1/SRV und EXT_STS_VAL.1/SSO, indem der STS SAML-Token validieren kann.

6.3.2 Dependencies of security functional requirements (Abhängigkeiten der funktionalen Sicherheitsanforderungen)

Tabelle 17 – Abhängigkeiten der funktionalen Sicherheitsanforderungen

SFR	Abhängigkeit	Erfüllt
FAU_GEN.1	FPT_STM.1	FPT_STM.1 ist nicht enthalten, da zuverlässige Zeitstempel von der operativen Umgebung des ISTS zur Verfügung gestellt werden. Diese Anforderung wird durch ein entsprechendes Sicherheitsziel an die operative Umgebung repräsentiert.
FAU_GEN.2	FIA_UID.1	Ja.
	FAU_GEN.1	Ja.
FIA_UAU.1	FIA_UID.1	Ja.
FIA_UAU.5	Keine Abhängigkeiten.	N/A
FIA_UID.1	Keine Abhängigkeiten.	N/A
FMT_SMF.1	Keine Abhängigkeiten.	N/A
EXT_STS_CAN.1/SRV	EXT_STS_ISS.1/SRV	Ja.

[23] Die Aktion Validierung eines Security Tokens darf ohne Authentisierung durchgeführt werden.

[24] Die Aktion Validierung eines Security Tokens darf ohne Identifizierung durchgeführt werden.

SFR	Abhängigkeit	Erfüllt
EXT_STS_CAN.1/SSO	EXT_STS_ISS.1/SSO	Ja.
EXT_STS_ISS.1/SRV	FIA_UAU.1	Ja.
EXT_STS_ISS.1/SSO	FIA_UAU.1	Ja.
EXT_STS_VAL.1/SRV	Keine Abhängigkeiten.	N/A
EXT_STS_VAL.1/SSO	Keine Abhängigkeiten.	N/A

6.3.3 Rational for the assurance requirements (Erklärung zu den Anforderungen an die Vertrauenswürdigkeit)

Die Vertrauenswürdigkeitsstufe EAL2 wurde deshalb gewählt, da diese einen für das Einsatzgebiet angemessenen Schutz der TOE Sicherheitsfunktionalitäten bietet. Aus diesem Grund und um die Evaluierungsaufwände in einem angemessenen Rahmen zu halten, wurde entschieden, dass der TOE Maßnahmen gegen niedriges Angriffspotential bieten muss.

Die Vertrauenswürdigkeitsstufe EAL2 umfasst eine Analyse der Sicherheitsanforderungen, in der die funktionale Spezifikation mit der Interface-Beschreibung zusammen mit den Handbüchern zum Verständnis des Sicherheitsverhaltens betrachtet wird.

AVA_VAN.2 bietet Schutz gegen Angreifer mit geringem Angriffspotential und gewährleistet, dass bekannte, potentielle Schachstellen analysiert und unabhängig getestet werden. Die Analyse wird gestützt durch eine Auswahl an getesteten TOE Sicherheitsfunktionalitäten, Nachweisen in Form von Entwicklerunterlagen basierend auf einer funktionalen Spezifikation, einem grundlegenden Design der sicherheitsumsetzenden Funktionen, der unabhängigen Überprüfung einer Auswahl von Herstellertests und eine Schwachstellenanalyse, die den Schutz gegen Penetrationsangriffe mit geringen Angriffspotential darlegt.

7 TOE summary specification (TOE Übersichtsspezifikation)

7.1 SF1 – Security Audit

Die Secure Audit Funktionalität ermöglicht es dem TOE sicherheitsrelevante Ereignisse gemäß Tabelle 13 zu protokollieren. Eine Protokollierung des Startens und Beenden der Audit Funktion erfolgt nicht, da eine Abschaltung der Audit Funktion während des Betriebs des TOE nicht möglich ist. Die sicherheitsrelevanten Ereignisse werden vom TOE in eine eigene Tabelle der ITC DB geschrieben. Ist die Datenbank voll oder kann nicht angesprochen werden, so wird die aktuelle Funktion mit einem technischen Fehler abgebrochen. Dieses Ereignis wird anschließend in einem technischen Log-File der DataPower Firmware festgehalten, um entsprechende administrative Aktionen anzustoßen. Jeder Eintrag im Logfile umfasst zumindest die folgenden Informationen (vgl. FAU_GEN.1 und FAU_GEN.2):

- Zeitstempel, der Datum und Uhrzeit enthält,
- Art des Ereignisses,
- Ergebnis: Erfolg / Fehler (mit Fehlercode),
- ID des Webservice-Nutzers,
- ID des TGIC-Services (für den das Token ausgestellt wurde).

Im Fehlerfall sind die beiden IDs ggf. nicht verfügbar und werden offen gelassen. Es können dann zur Fehleranalyse die technischen Logdaten mit Hilfe von Zeitstempel und Fehlercode heran gezogen werden[25].

Die Audit-Einträge werden in der Datenbank mit einem Hashcode über den aktuellen Eintrag und dem Hashcode des letzten Eintrags ergänzt, damit über diese Hash-Bäume die Integrität der Auditdaten geprüft werden kann. Diese Funktionalität wird durch die ITC DB gewährleistet und ist nicht Bestandteil des TOE.

Die Informationen werden außerhalb des TOE in der ISTS-Datenbank gespeichert[26].

7.2 SF2 – Identification & Authentication

Der ISTS unterstützt vier Authentisierungsmechanismen (vgl. FIA_UAU.5):

- X.509-Zertifikat,
- eID des neuen Personalausweises (nPA),
- mobile Transaktionsnummer (mTAN)
- Time-based One-time Password Algorithmus (TOTP).

Dabei wird die Identifikation der Webservice-Nutzer und Webservice-Betreiber grundsätzlich vom TOE durchgeführt. Der Webservice-Nutzer fordert über seinen User Agent beim TOE ein

[25] Diese Fehleranalyse ist aber nicht Teil der vom TOE erbrachten Audit-Funktionalität, sondern ein technisches Betriebsthema.

[26] Zur Integritätssicherung werden innerhalb der Datenbank SHA-256 Prüfsummen mit Hilfe von Stored Procedures verwendet.

Service Token an und übermittelt dafür im Request seine Partner-ID sowie die Service-ID des TGIC-Services (jeweils als eindeutige Identifikatoren) (vgl. FIA_UID.1).

Aufgrund der Service-ID ermittelt der TOE über die XML-Datenbank im Filesystem den TGIC-Service, inkl. der von TGIC-Service geforderten Authentifikationsmechanismen und ggf. zusätzliche Claims, sowie auf Basis der Partner-ID über die ITC Nutzerverwaltung, den Webservice-Nutzer mit den für ihn aktivierten Authentifikationsmechanismen und Zugehörigkeiten zu Nutzergruppen. Eine Authentisierung und die darauf basierte Generierung des Service Tokens kann nur erfolgen, wenn der Webservice-Nutzer im ITC registriert ist und für diesen Nutzer mindestens ein vom TGIC-Service geforderter Authentifikationsmechanismus aktiviert ist. Ebenso müssen die vom TGIC-Service geforderten Claims für den Nutzer vorhanden sein. Andernfalls wird der Vorgang abgebrochen und eine entsprechende Fehlermeldung im technischen Log durch die DataPower Firmware generiert.

Nach erfolgreichem Abgleich dieser Daten fordert der TOE eine geeignete Authentifikation (in Form einer Challenge, generiert durch die Umgebung) durch den Webservice-Nutzer an. Die Authentifizierungen mit Hilfe des mTAN- und TOTP-Verfahrens werden hauptsächlich durch den TOE durchgeführt, alle übrigen Authentisierungsmechanismen erfolgen durch die operative Einsatzumgebung (vgl. FIA_UAU.1, FIA_UAU.5).

Folgende Authentifizierungsmechanismen sehen zur Auswahl:

- Authentifizierung mit X.509-Zertifikat (durch die operative Umgebung)

  Der Nutzer weist gegenüber dem TOE seine Authentizität nach, indem er die vom ISTS in der Challenge gesandten Daten[27] signiert[28] und an den ISTS zurückschickt. Die Signaturprüfung wird durch die operative Umgebung durchgeführt; das dafür notwendigen CA-Zertifikat stammt aus der ITC PKI und wird durch einen administrativen Prozess in der operativen Umgebung bereitgestellt.

- Authentifizierung mit neuem Personalausweis (nPA) (durch die operative Umgebung)

  Die Authentifizierung via nPA erfolgt mit Hilfe eines eID-Servers in der operativen Umgebung des TOE. Der TOE stößt lediglich den Prozess zur Authentifizierung an. Die Ergebnisse der nPA-Authentifikation werden durch den eID-Server anschließend dem ITC ISTS-eID-Connector bereitgestellt und stehen dann über letzteren dem ISTS zur Verfügung.

- Authentifizierung mit mobiler Transaktionsnummer (mTAN)

  Im Rahmen der Authentifikation via mTAN wird die zur TAN-Generierung benötigte Zufallszahl von der operativen Umgebung des TOE geliefert. Der TOE nutzt einen SMS-Server in der Umgebung, um die generierte TAN an die Mobilfunknummer aus dem hinterlegten Benutzerprofil des Webservice-Nutzers zu versenden.

[27] Bei den Daten handelt es sich um eine Zufallszahl, die von der Firmware des IBM DataPower Gateway X2 zur Verfügung gestellt wird.

[28] Es wird der er gesamte SOAP-Body im Rahmen der X.509-Authentifikation signiert. Im Rahmen der SignChallengeResponse-Nachricht ist nur eine Signatur im WS-Security-Element im SOAP-Header erlaubt, entweder eine Signatur über den gesamten SOAP-Body (zu bevorzugen) oder wie in den Vorversionen über das SignChallengeResponse-Element (ab sofort deprecated).

Der Nutzer übergibt die empfangende Transaktionsnummer aus der SMS und ein dem Nutzer durch die (externe) ITC Nutzerverwaltung zugewiesenes Kennwort über eine Interaktionsmöglichkeit an den darauf wartenden User Agent, der die Transaktionsnummer und das Kennwort im Rahmen der mTAN-Authentifikation an den TOE zurück sendet. Der TOE vergleicht schließlich die zuvor generierte mit der durch den User Agent des Nutzers übermittelten Transaktionsnummer. Das übermittelte Passwort wird durch das ITC LDAP verifiziert, um eine Aussage über die Authentizität des Nutzers machen zu können.

Der Webservice-Nutzer darf ein beliebiges, SMS fähiges Mobiltelefon einsetzen. Das Mobiltelefon sollte aus Sicherheitsgründen nicht das Endgerät sein, auf dem sich auch der User Agent befindet. Die Anforderungen an das eigentliche User Agent Endgerät in Bezug auf den Austausch der mobilen Transaktionsnummer sind weitgehend irrelevant. Allerdings muss der User Agent des Webservice-Nutzers eine Interaktions-Möglichkeit bieten, um die manuell übertragene Transaktionsnummer und das Kennwort zu übernehmen und an den Insurance Service Token Service (ISTS) zu übertragen.

- Time-based One-time Password Algorithms (TOTP)

  Die Authentifikation via TOTP wird verwendet, wenn dieses Verfahren durch den Nutzer und den Service-Betreiber unterstützt und als einzige gemeinsame Authentifikation für beide Kommunikationspartner ist, oder dediziert durch den Servicenutzer gefordert wird.

  Grundsätzliche Vorbedingungen für den Einsatz des TOTP zur Authentifikation durch eine natürliche Person als Webservice-Nutzer sind folgende:

  - Der Nutzer besitzt durch den ITC generierten Geheimschlüssel zusammen mit Konfigurationsparametern (auch Seed genannt). Das TOTP-Seed wird samt Secret aus dem LDAP bezogen.
  - Der Nutzer besitzt einen TOTP-Client für die Berechnung des Einmalkennwortes mit der Unterstützung des SHA512-Algorithms[29].
  - Zeitsynchronisation mit einem NTP-Server

  Damit die TOTP-Berechnung auf beiden Seiten gleiche Werte produziert, soll die Uhr auf dem dafür vorgesehenen Gerät mit einem NTP-Server synchronisiert sein und der TOTP-Client soll in der Lage sein, die SHA512-Authentifikation zu unterstützen. Das auf Basis des HMAC-Algorithmus unter der Verwendung der Systemzeit sowie des Geheimschlüssels generierte Einmalkennwort kann je Konfiguration eine 6- bzw. 8-stellige Zahl sein. Das übermittelte Passwort wird durch das ITC LDAP verifiziert, um eine Aussage über die Authentizität des Nutzers machen zu können.
  Der generierte Schlüssel ist immer einem TGIC-Konto zugeordnet. Aus diesem wird ein QR-Code generiert, der per E-Mail bei der Registrierung an den Webservice-Nutzer versendet wird. TGIC-Nutzerverwaltung nutzt hierzu ein Mail Gateway in der operativen Umgebung. Die Übertragung des QR-Codes erfolgt dabei per unverschlüsselter E-Mail in einem durch den MTA gesicherten Kanal. Die Sicherheit des Verfahrens ergibt sich aus dem TOTP-Secret in Verbindung mit dem TOTP-Benutzer-Kennwort.

[29] Der Hash-Algorithmus ist für jeden Benutzer konfigurierbar.

Die Authentisierung der Webservice-Betreiber kann nur mit Hilfe von X.509-Zertifikaten, wie oben beschrieben, erfolgen.

7.3 SF3 – Security Token Service

Der Insurance Security Token Service (ISTS) in Form eines WS-Trust-konformen STS [WS-Trust] stellt nach erfolgreicher Authentifikation SAML-Token [SAML] aus (Anwendungsfall: Ausgabe eines Service Tokens (Issuance Binding)) (vgl. EXT_STS_ISS.1/SRV).

Weiterhin kann der Nutzer beim TOE über WS-Trust ein „SSO“ (single sign-on) Token beantragen. Mit diesem Token können beim TOE weitere Service Token zur Authentifikation gegenüber dem TGIC-Service angefordert werden (vgl. EXT_STS_ISS.1/SSO). Durch den Einsatz eines SSO Token können Kosten bei Verwendung der mTAN Authentifizierung reduziert werden, indem eine Authentifizierung nur einmal für das SSO Token durchgeführt werden muss. Durch das SSO Konzept ist es möglich, ein zuvor beantragtes SSO Token ohne erneute Authentifikation des Nutzers in ein Service Token für einen konkreten TGIC-Service umzuwandeln.

Zusätzlich werden die folgenden Anwendungsfälle vom TOE unterstützt:

- Widerrufen eines Service Tokens (Cancel Binding) (vgl. EXT_STS_CAN.1/SRV),
- Widerrufen eines SSO Tokens (Cancel Binding) (vgl. EXT_STS_CAN.1/SSO),
- Validieren eines Service Tokens (Validate Binding) (vgl. EXT_STS_VAL.1/SRV) und
- Validieren eines SSO Tokens (Validate Binding) (vgl. EXT_STS_VAL.1/SSO).

Die drei Anwendungsfälle (Issuance, Cancel and Validate) des ISTS beruhen auf dem Nachrichtenprotokoll WS-Trust, das auf WS-Trust [WS-Trust] aufbaut. Als Netzwerkprotokoll für die Kommunikation zwischen User Agent und ISTS bzw. TGIC-Service und ISTS wird SOAP über HTTPS verwendet. Der vertrauenswürdige Kanal und die notwendigen kryptografischen Operationen werden dabei von der operativen Einsatzumgebung bereitgestellt. Die Spezifikation der Security Token, die durch den ISTS vergeben werden, baut auf dem SAML-Standard in Version 2.0 [SAML] auf.

Nach erfolgreicher Authentifikation erstellt der TOE ein Service Token auf den Namen des Webservice-Nutzers und zur Verwendung mit dem vom Webservice-Nutzer identifizierten TGIC-Service. Das Service Token besitzt eine in der XML-Datenbank pro TGIC-Service jeweils einzeln konfigurierbare Gültigkeit und enthält zusätzlich ggf. Bestätigungen für vom Webservice-Nutzer angeforderte oder vom TGIC-Service freigegebene Claims. Zudem ist das Service Token digital signiert und für den identifizierten TGIC-Service verschlüsselt worden.[30]

Das SAML-Token beinhaltet mindestens die folgenden Attribute:

- Token ID,
- Ausstellungsdatum und -uhrzeit,
- Partner ID,
- Webservice ID,

[30] Signatur und Verschlüsselung erfolgen durch die Firmware des IBM DataPower Gateway X2.

- XML-Signatur und Hash des Tokens,
- X.509 Zertifikat.

Optional können weitere Attribute je nach Anwendungsfall hinzugefügt werden, z.B.

- Vor- und Nachname,
- E-Mail-Adresse,
- Geschlecht,
- Anschrift,
- Geburtsdatum,
- Organisation,
- weitere freie Nutzergruppen,
- Gültigkeitsdauer des Tokens.

Fordert ein Webservice-Nutzer über seinen User Agent beim ISTS einen Service Token an (Issuance Binding), übermittelt er dafür im Request seine Partner-ID sowie die Service-ID des TGIC-Services (jeweils als eindeutige Identifikatoren). Aufgrund der Service-ID ermittelt der ISTS über die lokale XML-Datenbank den TGIC-Service, inkl. der von diesem geforderten Authentifikationsmechanismen und Claims, sowie auf Basis der Partner-ID über die ITC Nutzerverwaltung den Webservice-Nutzer mit den für ihn aktivierten Authentifikationsmechanismen und Zugehörigkeiten zu Nutzergruppen. Nach erfolgreichem Abgleich dieser Daten fordert der ISTS eine geeignete Authentifikation (in Form einer Challenge, siehe Kapitel 7.2) durch den Webservice-Nutzer an.

Stehen im Rahmen des Issuance Binding mit expliziter Nutzer-Authentifikation entsprechend der aktuellen Konfiguration des Service-Nutzers und des TGIC-Services mehrere Authentifikationsmechanismen zur Auswahl, wählt der ISTS implizit und deterministisch den zu nutzenden Authentifikationsmechanismen, mit Priorisierung in folgender Reihenfolge aus: X.509, mTAN, nPA, TOTP. Möchte der Aufrufer den zu nutzenden Authentifikationsmechanismus hingegen explizit auswählen, so ist dieses explizit möglich. Bei Issuance Binding mit SSO-Token ist diese Konfiguration nicht erlaubt. Hierdurch werden Freiheitsgrade, welche ggf. durch die implizit deterministische Auswahl des Authentifikationsmechanismus erlaubt sind, unterbunden.

Des Weiteren hat der Webservice-Betreiber die Möglichkeit ein erhaltenes Service Token zu prüfen (vgl. EXT_STS_VAL.1/SRV bzw. EXT_STS_VAL.1/SSO). Dazu muss dieser das Security Token mit dem öffentlichen Token-Zertifikat des ISTS erneut verschlüsselt und durch den TGIC-Service an das ISTS gesendet werden. Sobald der TOE das zu prüfende Security Token erhält, wird dieses von der Umgebung entschlüsselt und die mathematische Korrektheit sowie die Vertrauenswürdigkeit der Signatur von der dem TOE zugrundeliegenden Firmware geprüft. Anschließend prüft der TOE, ob das erhaltene Token nicht widerrufen wurde.

Sowohl der Webservice-Nutzer (agierend durch den User Agent) als auch der Webservice-Betreiber (durch den TGIC-Service) haben nach einer erfolgreichen Authentisierung die Möglichkeit ein zuvor für sie erstelltes Service Token zu widerrufen (vgl. EXT_STS_CAN.1/SRV bzw. EXT_STS_CAN.1/SSO). Dazu sendet der User Agent bzw. der TGIC-Service eine Anfrage an den ISTS, die den zu widerrufenden Security Token enthält. Der zu widerrufende Security

Token liegt dabei in verschlüsselter Form vor. Sendet ein Webservice-Nutzer die Anfrage zum Widerruf, so bleibt das Security Token unverändert verschlüsselt durch das ISTS für den Webservice-Betreiber. Stammt die Anfrage vom Webservice-Betreiber, so muss dieser das Security Token vorher entschlüsseln und für den ISTS neu verschlüsseln.

Bevor das Service Token widerrufen wird, muss sich der Webservice-Nutzer bzw. Webservice-Betreiber wie oben beschrieben authentifizieren. Die Authentifizierung des Webservice-Betreibers darf jedoch lediglich unter Verwendung von X.509-Zertifikaten erfolgen. War die Authentifizierung erfolgreich, so erhält der Webservice-Nutzer bzw. der Webservice-Betreiber eine Bestätigung, dass das entsprechende Token widerrufen wurde. Sollte das Security Token nicht widerrufen werden, tritt ein SOAP Fault auf.

7.4 SF4 – Security Management

Der TOE verfügt über die Möglichkeit über eine Konfigurationsdatei einige Konfigurationsparameter einzustellen (vgl. FMT_SMF.1).

Folgende Konfigurationsparameter sind vorgesehen:

- Gültigkeitsdauer einer mTAN Session,
- Gültigkeitsdauer einer nPA Session,
- Gültigkeitsdauer einer X.509 Session,
- Gültigkeitsdauer einer TOTP Session.

Der TOE prüft, ob die Konfiguration (eine XML-Datei) dem erwarteten XML-Schema entspricht und liest diese ein. Diese Prüfung erfolgt zustandslos jedes Mal, wenn die Datei eingelesen wird.

Wird der Authentifikationsvorgang gegenüber dem ISTS nicht innerhalb dieser Zeit abgeschlossen, ist die Authentifikation nicht erfolgreich und muss wiederholt werden.

7.5 Rationale on TOE specification (Erklärung der TOE-Übersichtsspezifikation)

Die Spezifikation der TOE Sicherheitsfunktionalitäten bezieht sich direkt auf die TOE Sicherheitsanforderungen. Die folgende Tabelle zeigt die Beziehung zwischen Sicherheitsanforderungen und Sicherheitsfunktionalität.

Tabelle 18 – Sicherheitsanforderungen vs. Sicherheitsfunktionalität

Sicherheitsanforderungen vs. Sicherheitsfunktionalität	SF1 - Security Audit	SF2 - Identification and Authentication	SF3 - Security Token Service	SF4 - Security Management
FAU_GEN.1	X			
FAU_GEN.2	X			
FIA_UAU.1		X		
FIA_UAU.5		X		
FIA_UID.1		X		
FMT_SMF.1				X
EXT_STS_CAN.1/SRV			X	
EXT_STS_CAN.1/SSO			X	
EXT_STS_ISS.1/SRV			X	
EXT_STS_ISS.1/SSO			X	
EXT_STS_VAL.1/SRV			X	
EXT_STS_VAL.1/SSO			X	

8 Anhang

8.1 Kryptografische Verfahren innerhalb der TOE Einsatzumgebung

8.1.1 Authenticity

Anwendungsbereich im TOE:

a) EXT_STS_ISS: XML-Signatur des ausgestellten Tokens durch den ISTS
b) EXT_STS_ISS: XML-Signatur der Nachrichten für die Kommunikation zwischen ITC ISTS-eID-Connector und eID-Server im Rahmen der nPA-Authentifikation
c) EXT_STS_ISS: Prüfung der im Rahmen der X.509-Authentifikation durch den zu authentifzierenden Nutzer extern generierten XML-Signatur
d) EXT_STS_CAN: Verifikation der XML-Signatur des vom Aufrufer übergebenen Token durch den ISTS
e) EXT_STS_CAN: XML-Signatur der Nachrichten für die Kommunikation zwischen ITC ISTS-eID-Connector und eID-Server im Rahmen der nPA-Authentifikation
f) EXT_STS_CAN: Prüfung der im Rahmen der X.509-Authentifikation durch den zu authentifzierenden Nutzer extern generierten XML-Signatur
g) EXT_STS_VAL: Verifikation der XML-Signatur des vom Aufrufer übergebenen Token durch den ISTS

Kryptografischer Mechanismus:

- RSA-signature generation and verification (RSASSA-PKCS1-v1_5) using SHA256
- SHA512 hash used as OTP Seed for TOTP (configurable)

Standard:

- [XML-DSig], [RFC6931] http://www.w3.org/2001/04/xmldsig-more - rsa-sha256

Schlüssellänge:

- RSA: Modus length = 2048 bits

8.1.2 Key Encryption

Anwendungsbereich im TOE:

a) EXT_STS_ISS: Hybride XML-Verschlüsselung des ausgestellten Tokens durch den ISTS
b) EXT_STS_CAN: Hybride XML-Entschlüsselung des übergebenen Tokens durch den ISTS

Kryptografischer Mechanismus:

- RSA-encryption and decryption (RSASSA-PKCS1-v1_5)

Standard:

- [XML-Enc] http://www.w3.org/2001/04/xmlenc#rsa-1_5

Schlüssellänge:

- RSA: Modus length = 2048 bits

8.1.3 Confidentiality

Anwendungsbereich im TOE:

a) EXT_STS_ISS: Hybride XML-Verschlüsselung des ausgestellten Token durch den ISTS
b) EXT_STS_CAN: Hybride XML-Entschlüsselung des vom Aufrufer übergebenen Token durch den ISTS
c) EXT_STS_VAL: Hybride XML-Entschlüsselung des vom Aufrufer übergebenen Token durch den ISTS

Kryptografischer Mechanismus:

- AES-encryption (AES256-CBC) with 128bit IV

Standard:

- [XML-Enc], [RFC6931] http://www.w3.org/2001/04/xmlenc#aes256-cbc

Schlüssellänge:

- AES: |k| = 256

8.1.4 Trusted Channel

Anwendungsbereich im TOE:

a) EXT_STS_ISS: SSL-Client für die Verbindung zum SMS-Server zur Auslösung der mTAN-Authentifikation
b) EXT_STS_CAN: SSL-Client für die Verbindung zum SMS-Server zur Auslösung der mTAN-Authentifikation

Kryptografischer Mechanismus:

- TLS_RSA_WITH_AES_256_CBC_SHA

Standard:

- [RFC3268]

Schlüssellänge:

- RSA: Modus length = 2048
- AES: |k| = 256

8.1.5 Randon Number Generation

Anwendungsbereich im TOE:

a) Zur dynamischen Erzeugung von AES-Schlüsseln

b) Zur Erzeugung von mTANs zur mTAN-Authentifikation
c) Zur Erzeugung von zu signierenden Zufallszahlen zur X.509-Authentifikation

Kommentare:

- zu a)
  Die Funktionalität wird in der TOE-Umgebung implizit genutzt und vom TOE selbst nicht parametrisiert.
- zu b/c)
  Die Funktionalität der TOE-Umgebung zur Zufallszahlenerzeugung wird vom TOE explizit aufgerufen

8.1.6 Cryptographic Primitive

Anwendungsbereich im TOE:

Vergleiche die Anwendungsbereiche wie in den Abschnitten 8.1.3 und 8.1.4 aufgeführt.

Kryptografischer Mechanismus:

- AES

Standard:

- [FIPS-197]

Schlüssellänge:

- AES: |k| = 256

Anwendungsbereich im TOE:

Vergleiche die Anwendungsbereiche wie in Abschnitten 8.1.1 aufgeführt.

Kryptografischer Mechanismus:

- SHA-256, SHA-512

Standard:

- [FIPS-180-4]

Anwendungsbereich im TOE:

Vergleiche die Anwendungsbereiche wie in den Abschnitten 8.1.1, 8.1.2 und 8.1.4 aufgeführt.

Kryptografischer Mechanismus:

- RSA-encryption and -decryption

Standard:

- [PKCS#1]

Schlüssellänge:

- RSA: Modus length = 2048

8.2 Referenzen

[CC] *Common Criteria for Information Technology Security Evaluation*, version 3.1, revision 5
Part 1: Introduction and general model, CCMB-2017-04-001,
Part 2: Security functional requirements, CCMB-2017-04-002,
Part 3: Security Assurance Requirements, CCMB-2017-04-003.

[FIPS-180-4] Secure Hash Standard (SHS), *Federal Information Processing Standards (FIPS) Publication, FIPS PUB 180-4, August 2015*

[FIPS-197] *Advanced Encryption Standard (AES), Federal Information Processing Standards Publication, FIPS PUB 197, November 26, 2001*

[PKCS#1] *PKCS#1 v2.2 – RSA Cryptography Standard, Public-Key Cryptography Standards, PKCS#1, Version 2.2, October 27, 2012*

[RFC3268] *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS), IETF Request for Comments, RFC 3268, June 2002*

[RFC6234] *US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF), Request for Comments, IETF RFC 6234, Mai 2011*

[RFC6238] *TOTP: Time-Based One-Time Password Algorithm, Request for Comments, IETF RFC 6238, Mai 2011*

[RFC6931] *Additional XML Security Uniform Resource Identifiers (URIs), Request for Comments, IETF RFC 6931, April 2013*

[SAML] *Assertions and Protocols for the OASIS - Security Assertion Markup Language (SAML) V2.0*, Cantor et al., OASIS Standard, Version 1.2, March 15, 2005

[XML-Enc] *XML Encryption Syntax and Processing, Eastlake et al., W3C Recommendation, December 10, 2002*

[XML-DSig] *XML Signature Syntax and Processing, Eastlake et al., W3C Recommendation, Second Edition, June 10, 2008*

[WS-Trust] *WS-Trust 1.4*, Lawrence et al., OASIS-Standard, Version 1.4, February 2, 2009 mit Approved Errata 01 vom 25.04.2012

[WS-Security] *Web Services Security, SOAP Message Security 1.1 (WS-Security 2004)*, Lawrence et al., OASIS-Standard, Version 1.1, 01.02.2006

8.3 Abkürzungen

API	Application Programming Interface
BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria
DB	Database / Datenbank
EAL	Evaluation Assurance Level
eID	Elektronische Identifizierungsfunktion (des Personalausweises)
GDV	Gesamtverband der Deutschen Versicherungswirtschaft e.V.
IBM	International Business Machines (konkret: IBM Deutschland GmbH)
ISTS	Insurance Security Token Service
ITC	Insurance Trust Center (des GDV)
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
OSP	Organizational Security Policy
Partner ID	ID eines Nutzers oder einer Organisation
PKI	Public Key Infrastruktur
PP	Protection Profile
RFC	Request for Comments
SAML	Security Assertion Markup Language
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMS	Short Message Service
SSL	Secure Socket Layer
SSO	Single Sign-On
ST	Security Target
STS	Security Token Service
TGIC	Trusted German Insurance Cloud
TGIC-WS	TGIC-Service
TLS	Transport Layer Security

TOE	Target of Evaluation
TOTP	Time-Based One-Time Password Algorithm
TSF	TOE Security Functions
TSFI	TSF Interface
TÜViT	TÜV Informationstechnik GmbH
UA	User Agent
VM	Virtuelle Maschine
X.509	ITU-T-Standard für PKI-Zertifikate
XML	Extensible Markup Language