Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

BSI-DSZ-CC-1052-2018

zu

RISE-Konnektor V1.0

der

Research Industrial Systems Engineering (RISE) Forschungs-, Entwicklungs- und Großprojektberatung 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-1052-2018(*)

RISE-Konnektor V1.0

von	Research Industrial Systems Engineering (RISE) Forschungs-, Entwicklungs- und Großprojektberatung GmbH
PP-Konformität:	Common Criteria Schutzprofil (Protection Profile) Schutzprofil 1: Anforderungen an den Netzkonnektor, V1.5, 27.04.2018, BSI-CC-PP-0097-2018
Funktionalität:	PP konform plus produktspezifische Ergänzungen Common Criteria Teil 2 erweitert
Vertrauenswürdigkeit:	Common Criteria Teil 3 konform EAL 3 mit Zusatz von ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1, AVA_VAN.5, ALC_FLR.2

SOGIS
Recognition Agreement
für Komponenten bis
EAL 4

Common Criteria

Das in diesem Zertifikat genannte IT-Produkt wurde von einer anerkannten Prüfstelle nach der Gemeinsamen Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 3.1 ergänzt um Interpretationen des Zertifizierungsschemas und Anweisungen der Zertifizierungsstelle für Komponenten oberhalb von EAL 5 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.

Common Criteria
Recognition Arrangement
Anerkennung nur für
Komponenten bis EAL 2
und ALC_FLR

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, 8. Januar 2019

Bundesamt für Sicherheit in der Informationstechnik

Im Auftrag

Joachim Weber
Fachbereichsleiter

L.S.

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

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

Dies ist eine eingefügte Leerseite.

Gliederung

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-Gesetz[1]
- BSI-Zertifizierungs- und - Anerkennungsverordnung[2]
- BSI-Kostenverordnung[3]
- besondere Erlasse des Bundesministeriums des Innern
- die Norm DIN EN ISO/IEC 17065
- BSI-Zertifizierung: Verfahrensdokumentation zum Zertifizierungsprozess (CC-Produkte) [3]
- BSI Zertifizierung: Verfahrensdokumentation zu Anforderungen an Prüfstellen, deren Anerkennung und Lizenzierung (CC-Stellen) [3]
- Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria for Information Technology Security Evaluation/CC), Version 3.1[4] [1], auch als Norm ISO/IEC 15408 veröffentlicht

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 Kostenverordnung für Amtshandlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Kostenverordnung-BSI-KostV) vom 3. März 2005, Bundesgesetzblatt I S. 519

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

- 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 http://www.sogisportal.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 unter die Anerkennung nach den Regeln des SOGIS-MRA, d.h. bis einschließlich der Komponenten nach CC Teil 3 EAL 4. Die Evaluierung beinhaltete die Komponente AVA_VAN.5, die nicht nach den Regelungen des SOGIS-MRA anerkannt ist. Für die Anerkennung ist hier die jeweilige EAL 4 Komponente maßgeblich.

3.2. Internationale Anerkennung von CC - Zertifikaten

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

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

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

Dieses Zertifikat fällt unter die Anerkennungsregeln des CCRA-2014, d.h. Anerkennung bis einschließlich CC Teil 3 EAL 2+ ALC_FLR Komponenten.

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 RISE-Konnektor V1.0 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Produkts RISE-Konnektor V1.0 wurde von SRC Security Research & Consulting GmbH durchgeführt. Die Evaluierung wurde am 31. Oktober 2018 abgeschlossen. Das Prüflabor SRC Security Research & Consulting GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[5].

Der Antragsteller ist: Research Industrial Systems Engineering (RISE) Forschungs-, Entwicklungs- und Großprojektberatung GmbH.

Das Produkt wurde entwickelt von: Research Industrial Systems Engineering (RISE) Forschungs-, Entwicklungs- und Großprojektberatung 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 Ergebnisse aus dem Zertifizierungsverfahren in einem nachfolgenden Evaluierung- und Zertifizierungsverfahren oder in einer Systemintegration verwendet werden oder wenn das Risikomanagement eines Anwenders eine regelmäßige Aktualisierung verlangt, wird

[5] Information Technology Security Evaluation Facility

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 8. Januar 2019, ist gültig bis 7. Januar 2024. Die Gültigkeit kann im Rahmen einer Re-Zertifizierung erneuert werden.

Der Inhaber des Zertifikates ist verpflichtet,

1. bei der Bewerbung des Zertifikates oder der Tatsache der Zertifizierung des Produktes auf den Zertifizierungsreport hinzuweisen sowie jedem Anwender des Produktes den Zertifizierungsreport und die darin referenzierten Sicherheitsvorgaben und Benutzerdokumentation für den Einsatz oder die Verwendung des zertifizierten Produktes zur Verfügung zu stellen,
2. die Zertifizierungsstelle des BSI unverzüglich über Schwachstellen des Produktes zu informieren, die nach dem Zeitpunkt der Zertifizierung durch Sie oder Dritte festgestellt wurden,
3. die Zertifizierungsstelle des BSI unverzüglich zu informieren, wenn sich sicherheitsrelevante Änderungen am geprüften Lebenszyklus, z. B. an Standorten oder Prozessen ergeben oder die Vertraulichkeit von Unterlagen und Informationen zum Evaluierungsgegenstand oder aus dem Evaluierungs- und Zertifizierungsprozess, bei denen die Zertifizierung des Produktes aber von der Aufrechterhaltung der Vertraulichkeit für den Bestand des Zertifikates ausgegangen ist, nicht mehr gegeben ist. Insbesondere ist vor Herausgabe von vertraulichen Unterlagen oder Informationen zum Evaluierungsgegenstand oder aus dem Evaluierungs- und Zertifizierungsprozess, die nicht zum Lieferumfang gemäß Zertifizierungsreport Teil B gehören oder für die keine Weitergaberegelung vereinbart ist, an Dritte, die Zertifizierungsstelle des BSI zu informieren.

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

6. Veröffentlichung

Das Produkt RISE-Konnektor V1.0 ist in die BSI-Liste der zertifizierten Produkte, die regelmäßig veröffentlicht wird, aufgenommen worden (siehe auch Internet: https://www.bsi.bund.de und [5]). Nähere Informationen sind über die BSI-Infoline 0228/9582-111 zu erhalten.

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

[6] Research Industrial System Engineering (RISE)
Forschungs-, Entwicklungs- und Großprojektberatung GmbH
Argentinierstraße 21, Innenhof
1040 Wien
Austria

B. Zertifizierungsbericht

Der nachfolgende Bericht ist eine Zusammenfassung aus

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

1. Zusammenfassung

Der Evaluierungsgegenstand (EVG) ist der Netzkonnektor RISE-Konnektor V1.0. Dieser bildet die Plattform für die Ausführung von Fachmodulen für den Anwendungskonnektor. Der EVG stellt Paketfilter- und VPN-Funktionalität für die Kommunikation mit der zentralen Telematikinfrastruktur-Plattform und dem Sicheren Internet Service (SIS), eine gesicherte Kommunikation zwischen dem Netzkonnektor und dem Clientsystem sowie zwischen Fachmodulen und fachanwendungsspezifischen Diensten (Fachdiensten bzw. Intermediären) bereit.

Die Sicherheitsvorgaben [6] stellen die Grundlage für die Zertifizierung dar. Sie basieren auf dem zertifizierten Protection Profile Common Criteria Schutzprofil (Protection Profile), Schutzprofil 1: Anforderungen an den Netzkonnektor, BSI-CC-PP-0097, Version 1.5 vom 27.04.2018, Bundesamt für Sicherheit in der Informationstechnik (BSI) [8].

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 3 mit Zusatz von ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1, AVA_VAN.5, ALC_FLR.2.

Die funktionalen Sicherheitsanforderungen (Security Functional Requirements SFR) an den EVG werden in den Sicherheitsvorgaben [6] Kapitel 6 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**
VPN-Client	Der EVG stellt einen sicheren Kanal zur zentralen Telematikinfrastruktur-Plattform (TI-Plattform) sowie zum Sicheren Internet Service (SIS) bereit, der nach gegenseitiger Authentisierung die Vertraulichkeit und Datenintegrität der Nutzdaten sicherstellt. Der Trusted Channel wird auf Basis des IPsec-Protokolls aufgebaut. Dabei wird IKEv2 unterstützt.
Informationsflusskontrolle	Regelbasiert verwenden alle schützenswerten Informationsflüsse die etablierten VPN-Tunnel. Nur Informationsflüsse, die vom Konnektor initiiert wurden, sowie Informationsflüsse von Clientsystemen in Bestandsnetze, dürfen den VPN-Tunnel in die Telematikinfrastruktur benutzen und erhalten damit überhaupt erst Zugriff auf die zentrale TI-Plattform. Andere Informationsflüsse, die den Zugriff auf Internet-Dienste aus den lokalen Netzen der Leistungserbringer betreffen, verwenden den VPN-Tunnel zum Sicheren Internet Service.
Dynamischer Paketfilter	Der EVG implementiert einen dynamischen Paketfilter. Die Filterregeln (packet filtering rules) sind mit geeigneten Default-Werten vorbelegt und können vom Administrator verwaltet werden.
Netzdienste: Zeitsynchronisation	Bei aktiviertem „Leistungsumfang Online“ (MGM_LU_ONLINE=Enabled) führt der EVG in regelmäßigen Abständen eine Zeitsynchronisation mit Zeitservern durch. Siehe auch Sicherheitsdienst Zeitdienst. Kann eine Zeitsynchronisation

Sicherheitsfunktionalität des EVG	Thema
	innerhalb eines bestimmten Zeitraums nicht erfolgreich durchgeführt werden oder überschreitet die Zeitabweichung zwischen Systemzeit und Zeit des Zeitservers zum Zeitpunkt der Zeitsynchronisierung einen bestimmten Wert, so wird der kritische Betriebszustand an der Signaleinrichtung des Konnektors angezeigt. Der Administrator kann die Zeit des Konnektors auch über das Management-Oberfläche einstellen, falls MGM_LU_ONLINE nicht aktiv ist.
Netzdienste: Zertifikatsprüfung	Der EVG überprüft die Gültigkeit der Zertifikate, die für den Aufbau der VPN-Kanäle verwendet werden. Die erforderlichen Informationen zur Prüfung der Gerätezertifikate werden dem EVG in Form einer (signierten) Trust-service Status List (TSL) und einer Sperrliste (CRL) bereitgestellt. Der EVG prüft die Zertifikate kryptographisch vermöge der aktuell gültigen TSL und CRL.
Stateful Packet Inspection	Der EVG kann nicht wohlgeformte IP-Pakete erkennen und verwirft diese. Er implementiert eine sogenannte „zustandsgesteuerte Filterung“. Dies ist eine dynamische Paketfiltertechnik, bei der jedes Datenpaket einer aktiven Session zugeordnet und der Verbindungsstatus in die Entscheidung über die Zulässigkeit eines Informationsflusses einbezogen wird.
Selbstschutz: Speicheraufbereitung	Der EVG löscht nicht mehr benötigte kryptographische Schlüssel (insbesondere session keys für die VPN-Verbindung) nach ihrer Verwendung durch aktives Überschreiben mit Nullen oder festen Werten. Der EVG speichert medizinische Daten nicht dauerhaft. Ausnahmen sind die Speicherung von Daten während ihrer Ver- und Entschlüsselung; auch diese werden sobald wie möglich nach ihrer Verwendung gelöscht.
Selbstschutz: Selbsttests	Bei Programmstart wird eine Prüfung der Integrität der installierten ausführbaren Dateien und sonstigen sicherheitsrelevanten Dateien (Konfigurationsdateien, TSF-Daten) durch Verifikation von Signaturen durchgeführt. Schlägt die Prüfung der Integrität fehl, so wird der start up Prozess abgebrochen. Nach einem Neustart wird der Prozess erneut durchlaufen.
Selbstschutz: Schutz von Geheimnissen, Seitenkanalresistenz	Der EVG schützt Geheimnisse während ihrer Verarbeitung gegen unbefugte Kenntnisnahme. Dies gilt grundsätzlich für kryptographisches Schlüsselmaterial. Der private Authentisierungsschlüssel für das VPN wird bereits durch die gSMC-K und dessen Resistenz gegen Seitenkanalangriffe geschützt. Der EVG verhindert darüber hinaus den Abfluss von geheimen Informationen wirkungsvoll, etwa die Session Keys der VPN-Verbindung oder zu schützende Daten der TI und der Bestandsnetze.
Selbstschutz: SicherheitsLog	Der EVG führt ein Sicherheits-Log gemäß Konnektor-Spezifikation.
Administration	Der EVG bietet die Möglichkeit zum lokalen und zum entfernten Management an. Dabei wird immer eine gesicherte Verbindung zum Konnektor aufgebaut. Zu den administrativen Tätigkeiten bzw. Wartungstätigkeiten gehören neben der Konfiguration des Konnektors u.a. die Verwaltung der Filterregeln für den dynamischen Paketfilter, sowie das Aktivieren und Deaktivieren des

Sicherheitsfunktionalität des EVG	Thema
	VPN-Tunnels. Die Administration der Filterregeln für den dynamischen Paketfilter ist den Administratoren vorbehalten.
Software Update	Der EVG bietet die Möglichkeit an Systemaktualisierungen durchzuführen. Der Update-Dienst des EVG kann beim zentralen Konfigurationsdienst der TI Informationen über verfügbare Update-Pakete erhalten und automatisch oder manuell (durch den Administrator) in den vorgesehenen Speicherbereich zur späteren Installation laden. Alternativ kann auch über die lokale Management-Oberfläche ein Update-Paket bezogen werden.
Kryptographische Basisdienste	Der Konnektor implementiert gemäß den Vorgaben des Dokuments „Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur [gemSpec_Krypt]“ die Kryptographische Basisdienste für den Aufbau von sicheren VPN Verbindungen zu den VPN Konzentratoren der TI und der SIS.
TLS-Kanäle unter Nutzung sicherer kryptographischer Algorithmen	Der Netzkonnektor stellt TLS-Kanäle zur sicheren Kommunikation mit anderen IT-Produkten zur Verfügung. Dabei wird die TLS-Funktionalität dem Anwendungskonnektor zur Verfügung gestellt, der auch das Management der TLS Verbindung übernimmt.

Tabelle 1: Sicherheitsfunktionalität des EVG

Mehr Details sind in den Sicherheitsvorgaben [6] Kapitel 6 und 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 3.3, 3.4 und 3.5 dar.

Die Konfigurationen des EVG werden in Kap. 8 dieses Berichts beschrieben.

Die Ergebnisse der Schwachstellenanalyse, wie in diesem Zertifikat bestätigt, erfolgte ohne Einbeziehung der für die Ver- und Entschlüsselung eingesetzten krypthographischen Algorithmen (vgl. §9 Abs. 4 Nr. 2 BSIG). Für Details siehe Kap. 9 dieses Berichts.

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:

RISE-Konnektor V1.0

Die folgende Tabelle beschreibt den Auslieferungsumfang:

Nr	Typ	Identifikator	Version	Auslieferungsart
1	HW	RISE-Konnektor Hardware (nicht Teil des EVG)	1.0.0	Das Gerät wird über eine sichere Lieferkette dem Endkunden zugestellt.
2	SW	RISE Netzkonnektor Software	1.5.7	Die Software wird im Zuge der Fertigung auf die Hardware aufgebracht.
3	DOC	RISE Konnektor Bedienungsanleitung, 24.10.2018 Hashwert (SHA256): bdd8f1625caa38ae900d34610eeac6ba40c4c7f25c9ea32da76a011f68aedb33	1.0.14	Die Handbücher, deren Integrität über den genannten Hashwert überprüft werden kann, können auf der Herstellerwebseite heruntergeladen werden.
		RISE Konnektor Bedienungsanleitung für Remote-Administration, 30.10.2018 Hashwert (SHA256): 0c1b28d1bd1093c3527b51be1c73db0d6d1463e3d64112d4d7158d7b0135fb25	1.0.1	

Tabelle 2: Auslieferungsumfang des EVG

Die Software wird zusammen mit der Hardware Version 1.0.0 als eine Einbox-Lösung implementiert. Die Hardware ist nicht Teil des EVG.

Auslieferungsprozess des EVG

Die sichere Lieferkette wird im Dokument RISE Konnektor Sichere Lieferkette [9] beschrieben. Die Anweisungen an den Nutzer, wie die Einhaltung der sicheren Lieferkette überprüft werden kann, sind im Benutzerhandbuch genannt.

Das Gerät, das den EVG beinhaltet, ist in einem quaderförmigen Gehäuse untergebracht und verfügt über die Hardwareanschlüsse, die für den Betrieb des Konnektors nötig sind. Die gSMC-Ks befinden sich ebenfalls in diesem Gehäuse.

Identifizierung des EVG

Die Version des EVG kann über die grafische Benutzeroberfläche ermittelt werden. Eine Beschreibung dazu findet sich in [11]. Auf der Statusseite dieser Benutzeroberfläche finden sich Produktinformationen wie die Firmware Version (EVG Version), die Hardware Version der unterliegenden Hardware sowie die Seriennummer des Geräts.

3. Sicherheitspolitik

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

- VPN-Client,
- Dynamischer Paketfilter,
- Netzdienste,
- Stateful Packet Inspection,
- Selbstschutz,

- Administration,
- Kryptographische Basisdienste,
- TLS-Kanäle unter Nutzung sicherer kryptographischer Algorithmen.

4. Annahmen und Klärung des Einsatzbereiches

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

OE.NK.RNG	Externer Zufallszahlengenerator
OE.NK.Echtzeituhr	Echtzeituhr
OE.NK.Zeitsynchro	Zeitsynchronisation
OE.NK.gSMC-K	Sicherheitsmodul gSMC-K
OE.NK.KeyStorage	Sicherer Schlüsselspeicher
OE.NK.AK	Korrekte Nutzung des EVG durch Anwendungskonnektor
OE.NK.CS	Korrekte Nutzung des Konnektors durch Clientsysteme und andere aktive Komponenten im LAN
OE.NK.Admin_EVG	Sichere Administration des Netzkonnektors
OE.NK.PKI	Betrieb einer Public-Key-Infrastruktur und Verteilung der TSL
OE.NK.phys_Schutz	Physischer Schutz des EVG
OE.NK.sichere_TI	Sichere Telematikinfrastruktur-Plattform
OE.NK.kein_DoS	Keine denial-of-service-Angriffe
OE.NK.Betrieb_AK	Sicherer Betrieb des Anwendungskonnektors
OE.NK.Betrieb_CS	Sicherer Betrieb der Clientsysteme
OE.NK.Ersatzverfahren	Sichere Ersatzverfahren bei Ausfall der Infrastruktur
OE.NK.SIS	Sicherer Internet Service
OE.NK.SW-Update	Prozesse für sicheres Software-Update

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

5. Informationen zur Architektur

Die Architektur des EVG wird in den Sicherheitsvorgaben [6], Kapitel 1.3.4, beschrieben.

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

Die Sicherheitsfunktionen des EVG wurden durch die Anwendung der folgenden Methoden bestätigt:

- Automatisiertes Testen aller TSFI,
- Manuelles Testen aller TSFI,
- Sourcecode-Reviews und
- Netzwerktests einschließlich gezielter Tests der Protokolle IPsec und TLS.

In den folgenden Abschnitten werden die Herstellertests, die unabhängigen Prüfstellentests sowie die Penetrationstests im Rahmen der Schwachstellenanalyse erläutert.

Herstellertests

Bei den Herstellertests wurde der Evaluierungsgegenstand RISE-Konnektor V1.0 mit der Firmware-Version 1.5.7 getestet.

Der Hersteller hat alle TSFI und die zugehörigen SFR getestet. Alle relevanten Testfälle wurden auf die TSFIs abgebildet und jedes TSFI wurde von mehreren Testfällen abgedeckt. Weiterhin hat der Hersteller die Testfälle direkt auf die SFRs abgebildet, um sicher zu stellen, dass die Sicherheitsfunktionalität des EVG, im Rahmen der funktionalen Spezifikation von den Testfällen abgedeckt werden.

Bei den Herstellertests wurden die folgenden drei Testkategorien definiert:

- Automatisierte Tests: Testfall ist vollkommen in der Test-Suite implementiert
- Manuelle Tests: Testfall muss völlig oder teilweise manuell ausgeführt werden (Einsatz von zusätzlichen Tools wie bspw. Network Sniffer)
- Manuelle Testintegration: Manuelle Tests, die in der Referenzumgebung der Gematik durchgeführt werden

Nahezu alle Testfälle wurden im Modus „InReihe“ und einige bestimmte Testfälle wurden im Modus “Parallel“ durchgeführt, letztere werden entsprechend gekennzeichnet.

Bei den Herstellertests umfassen die Testfälle die folgenden Netzwerk-Szenarien:

- ANLW_ANBINDUNGS_MODUS = InReihe oder Parallel
- ANLW_INTERNET_MODUS = SIS, IAG oder Keiner

Weiterhin hat der Hersteller die Testfälle in der Konfiguration LU_ONLINE=DISABLED wiederholt.

Testergebnis

Die tatsächlichen Ergebnisse der Herstellertests entsprachen den erwarteten und spezifizierten Ergebnissen.

Unabhängige Prüfstellentests

Bei den unabhängigen Prüfstellentests wurde der Evaluierungsgegenstand RISE-Konnektor V1.0 überwiegend mit der Firmware-Version 1.5.7 getestet.

Für das Testen durch die Prüfstelle wurden sowohl die Ausprägungen “PROD” als auch “DEBUG” verwendet. Diese Ausprägungen sind konsistent mit den Angaben im Security Target [6].

Die Evaluatoren haben alle Herstellertests wiederholt, eigene unabhängige Testfälle definiert und diese durchgeführt. Dabei haben sich die Evaluatoren auf die Sicherheitsfunktionen VPN-Client, Packet Filter, Net Services, Self Protection, Administration und TLS des EVG fokussiert.

Bei den unabhängigen Prüfstellentests und den Penetrationstests wurden die folgenden Gesichtspunkte besonders betrachtet:

Testbeschreibung	Firmware-Version
Testen aller TSFI via automatisierter Testfälle	fwVersion 1.5.7
Testen aller TSF via manueller Testfälle	fwVersion 1.5.4
Sourcecode-Analyse durch Evaluatoren	fwVersion 1.5.7
Statische Sourcecode-Analyse von der Java-Implementierung	fwVersion 1.5.7
RFC-Analyse von der TLS-Implementierung	fwVersion 1.5.7
RFC-Analyse von der VPN-Implementierung	fwVersion 1.5.7
Lasttests von VPN Verbindungen (Verbindungsaufbau und Verbindungsabbau)	fwVersion 1.5.7
Testen der TLS-Implementierung mit dem Prüfstellentool TLS test suite	fwVersion 1.5.7
Testen der VPN-Implementierung mit dem Prüfstellentool IPsec test suite	fwVersion 1.5.7
Netzwerk-Penetrationstests auf alle Netzwerk-Schnittstellen und relevanten Protokollen	fwVersion 1.5.4 und dedizierte Testwiederholungen mit fwVersion 1.5.7
Analyse und Testen der Firewall-Regeln	fwVersion 1.5.7

Tabelle 3: Übersicht der unabhängigen Prüfstellen- und Penetrationstests

Wie in Tabelle 3 geschildert, wurden einige Tests in der Firmware-Version 1.5.4 durchgeführt. Die Evaluatoren haben bei den jeweiligen Testfällen, die Unterschiede zwischen den beiden Firmware-Versionen 1.5.4 und 1.5.7 analysiert und kamen zu dem Ergebnis, dass die Wiederholung dieser Testfälle für die Firmware-Version 1.5.7 nicht notwendig sei. Somit sind die Testergebnisse, die in der Firmware-Version 1.5.4 aufgezeigt wurden, ebenso für die evaluierte Konfiguration gültig.

Testergebnis

Die tatsächlichen Ergebnisse der unabhängigen Prüfstellentests entsprachen den erwarteten und spezifizierten Ergebnissen.

Penetrationstests

Bei Penetrationstests wurde der EVG systematisch dem Angriffspotential “hoch”, high attack potential AVA_VAN.5, unterstellt.

Bei der Schwachstellenanalyse wurden zuerst veröffentlichte Schwachstellen auf ihre Relevanz in der Einsatzumgebung des EVG untersucht und ggfls. weiteren Tests und Analysen unterzogen.

Der folgende Abriss liefert eine Zusammenfassung der Herangehensweise bei Penetrationstests im Rahmen der Schwachstellenanalyse:

- Part I: Es wurde sichergestellt, dass alle relevanten Informationen und Dokumente einbezogen wurden. Die "Generic vulnerability guidance" in CEM [2] kam zur Anwendung.
- Part II: Es wurde untersucht, dass die Auslieferung keine ausnutzbaren Schwachstellen hat.
- Part III: In Anlehnung an die Angriffsmethoden für POIs [14] wurden entsprechende Angriffe auf den operativen EVG berücksichtigt.
- Part IV: Die Lebenszyklusphasen Entwicklung, Fertigung, Installation, Personalisierung und regulärer Betrieb wurden auf mögliche Schwachstellen untersucht.
- Part V: Identifikation und Bewertung von Angriffspunkten auf verschiedenen technischen Ebenen und Protokollebenen.
- Part VI: Schwachstellenanalyse basierend auf den zu schützenden Werte, die im zugrundeliegenden Schutzprofil identifiziert sind.

Testergebnis

Es wurde unter Berücksichtigung des unterstellten Angriffsniveaus keine ausnutzbare Schwachstelle identifiziert.

8. Evaluierte Konfiguration

Dieses Zertifikat bezieht sich auf die folgende Konfiguration des EVG:

- RISE-Konnektor V1.0
  - Firmware-Version
    - fwVersion: 1.5.7
    - fwVersionInfo: RISE Konnektor
  - Hardware-Version
    - hwVersion: 1.0.0
    - serialNumber: product specific
- Dokumente
  - RISE Konnektor Bedienungsanleitung [11],
  - RISE Konnektor Bedienungsanleitung für Remote Administratoren [11].

Der Administrator kann über die Benutzeroberfläche die Version des EVG auslesen. Mehr Details zur evaluierten Konfiguration des EVG sind in den Sicherheitsvorgaben [6] beschrieben.

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 für die Komponenten bis zur Vertrauenswürdigkeitsstufe EAL 5 erweitert durch Vorgaben der Zertifizierungsstelle für Komponenten höher EAL 5 verwendet.

Für die Analyse des Zufallszahlengenerators wurde AIS 20 verwendet (siehe [4]).

Die Verfeinerungen der Anforderungen an die Vertrauenswürdigkeit, wie sie in den Sicherheitsvorgaben beschrieben sind, wurden im Verlauf der Evaluation beachtet.

Das Urteil PASS der Evaluierung wird für die folgenden Vertrauenswürdigkeits-komponenten bestätigt:

- Alle Komponenten der Vertrauenswürdigkeitsstufe EAL 3 der CC (siehe auch Teil C des Zertifizierungsreports)
- Die zusätzlichen Komponenten ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1, AVA_VAN.5, ALC_FLR.2

Die Evaluierung hat gezeigt:

- PP Konformität: Common Criteria Schutzprofil (Protection Profile), Schutzprofil 1: Anforderungen an den Netzkonnektor, BSI-CC-PP-0097, Version 1.5 vom 27.04.2018, Bundesamt für Sicherheit in der Informationstechnik (BSI) [8]
- Funktionalität: PP konform plus produktspezifische Ergänzungen Common Criteria Teil 2 erweitert
- Vertrauenswürdigkeit: Common Criteria Teil 3 konform EAL 3 mit Zusatz von ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1, AVA_VAN.5, ALC_FLR.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

Die folgende Tabelle gibt einen Überblick über die zur Durchsetzung der Sicherheitspolitik im EVG enthaltenen kryptographischen Funktionalitäten:

#	Zweck	Kryptografische Funktion	Implementierungs-standard	Schlüssel-größe in Bit	Anwendungs-standard	Bemerkungen
1	Authenticity	RSA signature verification for VPN and TLS sha256withRSAEncryption (OID 1.2.840.113549.1.1.11)	[RFC 8017] (RSASSA-PKCS1-v1_5) [FIPS 180-4] (SHA)	2048 bit	[gemSpec_Krypt] chap. 3.3.1 and 3.3.2	FPT_TDC.1/NK.Zert FPT_TDC.1/NK.TLS.Zert
2		ECDSA signature verification for VPN and TLS ecdsaWithSha256 (OID 1.2.840.10045.4.3.2)	[RFC 3279] (ECDSA) [RFC 5639] (brainpool)	Key sizes corresponding to the used elliptic curve brainpoolP256r1 (RFC 5639)	[gemSpec_Krypt] chap. 3.3.1 and 3.3.2	FPT_TDC.1/NK.Zert FPT_TDC.1/NK.TLS.Zert
3	Authentication	RSA signature creation with support of gSMC-K and verification for VPN and TLS sha256withRSAEncryption (OID 1.2.840.113549.1.1.11)	[RFC 8017] (RSASSA-PKCS1-v1_5) [FIPS 180-4] (SHA)	2048 bit	[gemSpec_Krypt], chap. 3.3.1	FCS_COP.1/NK.Auth FCS_COP.1/NK.TLS.Auth
4	Key agreement	Diffie-Hellman key agreement for VPN (IPsec IKEv2, diffie-hellman group 14)	[RFC 3526] (DH Group) [RFC 7296] (IKEv2)	DH: group 14 2048 bit exponent length ≥ 384 bits	[gemSpec_Krypt], chap. 3.3.1	FCS_CKM.2/NK.IKE
5		Diffie-Hellman key agreement (DH)and Elliptic Curve Diffie-Hellman key agreement (ECDH) for TLS	[RFC 4346] (TLS v1.1) [RFC 5246] (TLS v1.2) [RFC 3268] (DHE_RSA) [RFC 4492] (ECDHE_RSA) [RFC 3526] (DH Group 14)	DH: group 14 2048 bit exponent length ≥ 2047 bits ECDH: Key sizes corresponding to the used elliptic curves secp{256,384}r1 (SEC2) and brainpoolP{256, 384}r1 (RFC 5639)	[gemSpec_Krypt], chap. 3.3.2	FCS_CKM.1/NK.TLS
6	Key	HMAC value generation for	[FIPS 180-4]	128 bit and	[gemSpec_Kry	FCS_COP.1/NK.HMAC

	Derivation	VPN (PRF) PRF-HMAC-SHA-1, PRF-HMAC-SHA-256	(SHA) [RFC 2404] (HMAC) [RFC 4868] (HMAC) [RFC 7296] (IKEv2)	256 bit	pt], chap. 3.3.1	Pseudo-Random-Function (PRF) for key agreement
7		Key Derivation for TLS 1.1 and 1.2	[RFC 4346] (TLS v1.1) [RFC 5246] (TLS v1.2) [FIPS180-4] (SHA), [RFC1321] (MD5), [RFC2104] (HMAC),	128 bit and 256 bit	[gemSpec_Krypt], chap. 3.3.2	FCS_CKM.1/NK.TLS
8	Integrity	HMAC value generation and verification for VPN HMAC with SHA-1, SHA-256	[FIPS 180-4] (SHA) [RFC 2104] (HMAC) [RFC 2404] (HMAC-SHA-1 with ESP) [RFC 4868] (HMAC-SHA-2 with IPsec) [RFC 7296] (IKEv2)]	160 bit and 256 bit	[gemSpec_Krypt], chap. 3.3.1	FCS_COP.1/NK.HMAC for integrity of IKE Messages and ESP packets
9		HMAC value generation and verification for TLS HMAC with SHA-1, SHA-256 and SHA-384	[FIPS 180-4] (SHA) [RFC 2104] (HMAC) [RFC 4346] (TLSv1.1) [RFC 5246] (TLS v1.2)	160 bit, 256 bit and 384 bit	[gemSpec_Krypt], chap. 3.3.2	FCS_COP.1/NK.TLS.HMAC
10	Confidentiality	symmetric encryption and decryption for VPN communication AES-CBC (OID 2.16.840.1.101.3.4.1.42)	[FIPS 197] (AES) [RFC 3602] (AES-CBC) [RFC 4303] (ESP) [RFC 4301] (IPsec)	256 bit	[gemSpec_Krypt], chap. 3.3.1	FCS_COP.1/NK.IPsec FCS_COP.1/NK.ESP for confidentiality of IKE Messages and ESP packets
11		symmetric encryption and decryption for TLS AES-128 and AES-256 in CBC Mode	[FIPS 197] (AES) [RFC 3602] (AES-CBC) [RFC 3268]	128 bit and 256 bit	[gemSpec_Krypt], chap. 3.3.2	FCS_COP.1/NK.TLS.AES

			(AES-TLS with DH) [RFC 4492] (AES-TLS with ECDH)			
12	Authenticated Encryption	AES-128 and AES-256 in GCM mode for TLS 1.2	[FIPS 197] (AES) [RFC 3268] (AES-TLS) [SP 800-38D] (GCM) [RFC 5289] (AES-GCM-TLS) [RFC5116] (AEAD)	128 bit and 256 bit	[gemSpec_Krypt], chap. 3.3.2	FCS_COP.1/NK.TLS.AES
13	Trusted Channel	TLS v1.1 and v1.2	[RFC 4346] (TLSv1.1) [RFC 5246] (TLS v1.2) [TLS_Analysis]	-	[gemSpec_Krypt], chap. 3.3.2	FTP_ITC.1/NK.TLS using the ciphersuites TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, and TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 FTP_TRP.1/NK.Admin (local and remote administration)
14		VPN IPsec (IKEv2) using certificate based authentication	[RFC 4301] (IPsec) [RFC 4303] (ESP) [RFC 7296] (IKEv2) [VPN_Analysis]	-	[gemSpec_Krypt], chap. 3.3.1	FTP_ITC.1/NK.VPN_TI FTP_ITC.1/NK.VPN_SIS FTP_TRP.1/NK.Admin (remote administration)

Tabelle 4: Kryptografische Funktionen des EVG

Die kryptografische Stärke dieser Algorithmen wurde in diesem Zertifizierungsverfahren nicht bewertet (siehe BSIG §9, Abs. 4, 2).

Gemäß [13] sind die in Tabelle 4 angegebenen kryptografischen Funktionen für den jeweiligen Zweck geeignet. Die Gültigkeitsdauer für jeden Algorithmus ist im offiziellen Katalog angegeben.

Jedoch können kryptografische Funktionen mit einem Sicherheitsniveau unterhalb von 100 Bit nicht länger als sicher angesehen werden ohne den Anwendungskontext zu beachten. Deswegen muss geprüft werden ob diese kryptografischen Funktionen für den vorgesehenen Verwendungszweck angemessen sind. Weitere Hinweise und Anleitungen können der 'Technischen Richtline BSI TR-02102' (https://www.bsi.bund.de) entnommen werden.

Jede kryptografische Funktion in der folgenden Tabelle 5, die in der Spalte 'Sicherheitsniveau mehr als 100 Bit' ein 'Nein' enthält erreicht ein Sicherheitsniveau unterhalb von 100 Bit (im allgemeinen Anwendungsfall).

Nr.	Zweck	Kryptografische Funktion	Implementierungsstandard	Schlüsselgröße in Bit	Sicherheitslevel über 100 Bit	Bemerkungen
1	Authenticity	RSA signature verification with encoding RSASSA-PKCS1-1.5 with SHA-256	[RFC 8017] (RSASSA-PKCS1-v1_5), [FIPS180-4] (SHA)	2048 bit	Ja	Firmware update signatures verification FDP_ITC.1/NK.Update
2		RSA signature verification with encoding RSASSA-PSS with SHA256	[RFC 8017] (RSASSA-PKCS1-v1_5), [FIPS180-4] (SHA)	2048 bit	Ja	UpdateInfo.xml and FirmwareGroupInfo.xml signatures verification FDP_ITC.1/NK.Update

Tabelle 5: Kryptografische Funktionen des EVG (Update Prozess)

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 Risikomanagement-prozess 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

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

EAL Evaluation Assurance Level - Vertrauenswürdigkeitsstufe

ETR Evaluation Technical Report

EVG Evaluierungsgegenstand

IKE Internet Key Exchange

IPsec Internet Protocol Security

IT Information Technology - Informationstechnologie

ITSEF Information Technology Security Evaluation Facility - Prüfstelle für IT-Sicherheit

PP Protection Profile - Schutzprofil

SAR Security Assurance Requirement - Vertrauenswürdigkeitsanforderungen

SF Security Function - Sicherheitsfunktion

SFP Security Function Policy - Politik der Sicherheitsfunktion

SFR Security Functional Requirement - Funktionale Sicherheitsanforderungen

SIS Secure Internet Service

ST Security Target - Sicherheitsvorgaben

TOE	Target of Evaluation – Evaluierungsgegenstand
SW	Software
TCP/IP	Transmission Control Protocol/Internet Protocol
TI	Telematikinfrastruktur
TOE	Target of Evaluation (EVG)
TSF	TOE Security Functionality – EVG-Sicherheitsfunktionalität
TSFI	TOE Security Functionality Interface – TSF Schnittstelle
UDP	User Datagram Protocol
WAN	Wide Area Network

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.

Evaluierungsgegenstand – 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: Verfahrendokumentation zum Zertifizierungsprozess (CC-Produkte) und Verfahrensdokumentation zu Anforderungen an Prüfstellen, die Anerkennung und Lizenzierung (CC-Stellen), https://www.bsi.bund.de/zertifizierung

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

[5] 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-CC-1052, Version 1.9, 31.10.2018, Security Target für RISE-Konnektor V1.0, Research Industrial Systems Engineering (RISE)

[7] Evaluierungsbericht, Version 1.0, 31.10.2018, Evaluation Report, SRC Security Research & Consulting GmbH (vertrauliches Dokument)

[8] Common Criteria Schutzprofil (Protection Profile), Schutzprofil 1: Anforderungen an den Netzkonnektor, BSI-CC-PP-0097, Version 1.5 vom 27.04.2018, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[9] RISE Konnektor Sichere Lieferkette, Version 0.9.7, 08.06.2018

[10] Konfigurationsliste für den EVG (vertrauliches Dokument):
configuration list, collection of csv-files for each source code repository, Version 1.5.7, 25.09.2018, file name: ConfigList_release_v-1.5.7.zip

[11] Guidance Dokumentation für den EVG

RISE Konnektor Bedienungsanleitung, 1.0.14, 24.10.2018

RISE Konnektor Bedienungsanleitung für Remote-Administration, Version 1.0.1, 30.10.2018

[12] Implementation standards:

[FIPS 180-4] NIST: FIPS PUB 180-4 Secure Hash Signature Standard (SHS), March 2012

[7] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren

[TR-02102-3] Technische Richtlinie TR-02102-3 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 3 – Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2), Version 2014-01

[SP 800-38D] NIST Special Publication 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November, 2007

[RFC 2404] C. Madson, R. Glenn: Use of HMAC-SHA-1-96 within ESP and AH, November 1998, RFC 2404, https://www.rfc-editor.org/rfc/rfc2404.txt

[RFC 4868] S. Kelly, S. Frankel: Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec. May 2007, RFC 4868, https://www.rfc-editor.org/rfc/rfc4868.txt

[RFC 7296] C. Kaufman, P.Hoffman, Y.Nir, P.Eronen, T. Kivinen: Internet Key Exchange Protocol Version 2 (IKEv2), October 2014, RFC 7296 (IKEv2), http://www.ietf.org/rfc/rfc7296.txt

[FIPS 197] NIST FIPS 197: Advanced Encryption Standard (AES). November 2001

[RFC 3602] S .Frankel, R. Glenn, S. Kelly: The AES-CBC Cipher Algorithm and Its Use with IPsec. September 2003, RFC 3602, https://www.rfc-editor.org/rfc/rfc3602.txt

[RFC 4303] S. Kent: IP Encapsulating Security Payload (ESP), December 2005, RFC 4303 (ESP), https://www.ietf.org/rfc/rfc4303.txt

[RFC 4301] S. Kent, K. Seo: Security Architecture for the Internet Protocol, December 2005, RFC 4301 (IPsec), https://www.ietf.org/rfc/rfc4301.txt

[RFC 3526] T. Kivinen, M.Kojo: More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE). May 2003, RFC 3526, https://www.rfc-editor.org/rfc/rfc3526.txt

[RFC 2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997

[RFC 3268] Chown, P., Advanced Encryption Standard (AES) Cipher suites for Transport Layer Security (TLS), RFC 3268, June 2002

[RFC 4492] Blake-Wilson, et al., Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS), RFC 4492, May 2006

[RFC 5289] E. Rescorla, TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM), RFC 5289, August 2008

[RFC 4346] RFC 4346 T. Dierks: The Transport Layer Security (TLS) Protocol, Version 1.1, April 2006

[RFC 5246] RFC 5246 T. Dierks: The Transport Layer Security (TLS) Protocol, Version 1.2, August 2008

[RFC 8017] K. Moriarty, B. Kaliski, J. Jonsson, A. Rusch: PKCS #1: RSA Cryptography Specifications Version 2.2. November 2016. RFC 8017, http://www.rfc-editor.org/rfc/rfc8017.txt

[RFC 5116] An Interface and Algorithms for Authenticated Encryption, D. McGrew, January 2008

[RFC 3279] Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, W. Polk, R. Housley, L. Bassham, April 2002

[RFC 5639] Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, M. Lochter, J. Merkle, March 2010

[RFC 1321] The MD5 Message-Digest Algorithm, R. Rivest, April 1992

[TLS_Analysis] TLS-Analyse durch SRC, anhand der Anforderungen an TLS im deutschen CC-Zertifizierungsschema, Version 1.2, 29.10.2018, SRC Security Research & Consulting GmbH (vertrauliches Dokument)

[VPN_Analysis] VPN-Analyse bestehend aus:

IPsec-RFCs - MAY_SHOULD Anforderungen, Version: 0.5, 01.10.2018, SRC Security Research & Consulting GmbH
file name: VPN_Analyse_RISE_RFCMS_v05_20181001.pdf (vertrauliches Dokument)

VPN Analyse, basierend auf Anforderungen an kryptographisch gesicherte VPN-Kanäle / Trusted Channels im deutschen CC-Zertifizierungsschema, Version 0.4, 01.10.2018, SRC Security Research & Consulting GmbH
file name: VPN_Analyse_RISE_v04_20181001.pdf (vertrauliches Dokument)

[13] Application standards:

[gemSpec_Kon] Einführung der Gesundheitskarte: Konnektorspezifikation, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, Version 4.11.1, 27.04.2017

[gemSpec_Krypt] Einführung der Gesundheitskarte: Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, Version 2.10.0, 14.05.2018

[TR-03116-1] Technische Richtlinie BSI TR-03116-1, Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 1: Telematikinfrastruktur, Bundesamt für Sicherheit in der Informationstechnik, Version 3.19, 03.12.2015, Technische Arbeitsgruppe TR-03116-1

[14] Joint Interpretation Library (JIL) Attack Methods for POIs, Version 1.95, February 2015

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 -kompomenten: 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/ veröffentlicht.

D. Anhänge

Liste der Anhänge zu diesem Zertifizierungsreport

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

Bemerkung: Ende des Reports