Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

BSI-DSZ-CC-1189-2022

zu

RISE Konnektor, V5.0

der

Research Industrial Systems Engineering (RISE)

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-1189-2022 (*)

Gesundheitswesen: Konnektoren

RISE Konnektor V5.0

von	Research Industrial Systems Engineering (RISE)
PP-Konformität:	Common Criteria Schutzprofil (Protection Profile) Schutzprofil 2: Anforderungen an den Konnektor, Version 1.5.9, BSI-CC-PP-0098-V3-2021 vom 15.04.2021
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_IMP.1, ADV_TDS.3, ALC_TAT.1, AVA_VAN.3 und ALC_FLR.2

SOGIS
Recognition Agreement

Common Criteria

Das in diesem Zertifikat genannte IT-Produkt wurde von einer anerkannten Prüfstelle nach der Gemeinsamen Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 3.1 ergänzt um Interpretationen des Zertifizierungsschemas und Anweisungen der Zertifizierungsstelle 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, 14. April 2022

Bundesamt für Sicherheit in der Informationstechnik

Im Auftrag

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

Sandro Amendola L.S.
Abteilungspräsident

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 BSIG[1] die Aufgabe, für Produkte (Systeme oder Komponenten) der Informationstechnik, Sicherheitszertifikate zu erteilen.

Die Zertifizierung eines Produktes wird auf Veranlassung des Herstellers oder eines Vertreibers - im folgenden Antragsteller genannt - durchgeführt.

Bestandteil des Verfahrens ist die technische Prüfung (Evaluierung) des Produktes gemäß den vom BSI öffentlich bekannt gemachten oder allgemein anerkannten Sicherheitskriterien.

Die Prüfung wird in der Regel von einer vom BSI anerkannten Prüfstelle oder vom BSI selbst durchgeführt.

Das Ergebnis des Zertifizierungsverfahrens ist der vorliegende Zertifizierungsreport. Hierin enthalten sind u. a. das Sicherheitszertifikat (zusammenfassende Bewertung) und der detaillierte Zertifizierungsbericht.

Der Zertifizierungsbericht enthält die sicherheitstechnische Beschreibung des zertifizierten Produktes, die Einzelheiten der Bewertung und Hinweise für den Anwender.

2. Grundlagen des Zertifizierungsverfahrens

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

- BSI-Gesetz[2]
- BSI-Zertifizierungs- und - Anerkennungsverordnung[3]
- Besondere Gebührenverordnung BMI (BMIBGebV)[4]
- besondere Erlasse des Bundesministeriums des Innern
- die Norm DIN EN ISO/IEC 17065
- BSI-Zertifizierung: Verfahrensdokumentation zum Zertifizierungsprozess (CC-Produkte) [3]
- BSI Zertifizierung: Verfahrensdokumentation zu Anforderungen an Prüfstellen, deren Anerkennung und Lizenzierung (CC-Stellen) [3]

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

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

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

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

- Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria for Information Technology Security Evaluation/CC), Version 3.1[5] [1], auch als Norm ISO/IEC 15408 veröffentlicht
- Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Methodology for Information Technology Security Evaluation/CEM), Version 3.1 [2] auch als Norm ISO/IEC 18045 veröffentlicht
- BSI-Zertifizierung: Anwendungshinweise und Interpretationen zum Schema (AIS) [4]

3. Anerkennungsvereinbarungen

Um die Mehrfach-Zertifizierung des gleichen Produktes in verschiedenen Staaten zu vermeiden, wurde eine gegenseitige Anerkennung von IT-Sicherheitszertifikaten - sofern sie auf ITSEC oder Common Criteria (CC) beruhen - unter gewissen Bedingungen vereinbart.

3.1. Europäische Anerkennung von CC – Zertifikaten (SOGIS-MRA)

Das SOGIS-Anerkennungsabkommen (SOGIS-MRA) Version 3 ist im April 2010 in Kraft getreten. Es legt die Anerkennung von Zertifikaten für IT-Produkte auf einer Basisanerkennungsstufe und zusätzlich für IT-Produkte aus bestimmten Technischen Bereichen (SOGIS Technical Domain) auf höheren Anerkennungsstufen fest.

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

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

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

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

3.2. Internationale Anerkennung von CC - Zertifikaten

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

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

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

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

Dieses Zertifikat fällt unter die Anerkennungsregeln des CCRA-2014, 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, V5.0 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Produkts RISE Konnektor, V5.0 wurde von SRC Security Research & Consulting GmbH durchgeführt. Die Evaluierung wurde am 23. März 2022 abgeschlossen. Das Prüflabor SRC ist eine vom BSI anerkannte Prüfstelle (ITSEF)[6].

Der Sponsor und Antragsteller ist: Research Industrial Systems Engineering (RISE).

Das Produkt wurde entwickelt von: Research Industrial Systems Engineering (RISE).

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

[6] 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 14. April 2022, ist gültig bis 13. April 2027. 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, V5.0 ist in die BSI-Liste der zertifizierten Produkte, die regelmäßig veröffentlicht wird, aufgenommen worden (siehe auch Internet: https://www.bsi.bund.de und [5]). Nähere Informationen sind über die BSI-Infoline 0228/9582-111 zu erhalten.

Weitere Exemplare des vorliegenden Zertifizierungsreports können beim Hersteller des Produktes angefordert werden[7]. Der Zertifizierungsreport kann ebenso in elektronischer Form von der oben angegebenen Internetadresse heruntergeladen werden.

[7] Research Industrial Systems Engineering (RISE)
Forschungs-, Entwicklungs- u. Großprojektberatung GmbH
Concorde Business Park F
2320 Schwechat
Austria

B. Zertifizierungsbericht

Der nachfolgende Bericht ist eine Zusammenfassung aus

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

1. Zusammenfassung

Der Evaluierungsgegenstand (EVG) ist das Softwareprodukt Konnektor bestehend aus dem Netzkonnektor und dem Anwendungskonnektor.

Der Netzkonnektor umfasst die Sicherheitsfunktionen einer Firewall und eines VPN-Clients sowie einen NTP-Server, einen Namensdienst (DNS) und einen DHCP-Dienst. Er enthält auch die Grundfunktionen zum Aufbau sicherer TLS-Verbindungen zu anderen IT-Produkten.

Die Sicherheitsfunktionalität des Anwendungskonnektors umfasst die Signaturanwendung, die Ver- und Entschlüsselung von Dokumenten, den Kartenterminaldienst und den Chipkartendienst. Zusammen mit dem Netzkonnektor ermöglicht der Anwendungskonnektor zudem die gesicherte Kommunikation zwischen dem Konnektor und dem Clientsystem sowie zwischen Fachmodulen und Fachdiensten. Insbesondere setzt der Konnektor Kommunikationsprotokolle für die sichere Anbindung an das ePA-Aktensystem der Telematikinfrastruktur um.

Die Sicherheitsvorgaben [6] stellen die Grundlage für die Zertifizierung dar. Sie basieren auf dem zertifizierten Protection Profile [9].

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_IMP.1, ADV_TDS.3, ALC_TAT.1, AVA_VAN.3 und 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	Beschreibung
Netzkonnektor	
VPN-Client	Der EVG stellt einen sicheren Kanal zur zentralen Telematikinfrastruktur-Plattform (TI-Plattform) sowie zum Sicheren Internet Service 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

	Telematikinfrastruktur-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_ONLIONE=Enabled) führt der EVG in regelmäßigen Abständen eine Zeitsynchronisation mit Zeitservern durch. Siehe auch Sicherheitsdienst Zeitdienst. Kann eine Zeitsynchronisation 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 Managementinterface 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 Sitzungsschlüssel 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 deren Resistenz gegen Seitenkanalangriffe geschützt. Der EVG verhindert darüber hinaus den Abfluss von geheimen Informationen wirkungsvoll, etwa die Sitzungsschlüssel der VPN-Verbindung oder zu schützende Daten der TI und der Bestandsnetze.
Selbstschutz: Sicherheits-Log	Der EVG führt ein Sicherheits-Log gemäß Konnektor-Spezifikation.
Administration	Der EVG bietet die Möglichkeit zum lokalen 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 gewisser Filterregeln für den dynamischen Paketfilter sowie das Aktivieren und Deaktivieren des VPN-Tunnels. Die Administration gewisser Filterregeln für den dynamischen Paketfilter ist den Administratoren vorbehalten. Der EVG unterstützt keine Funktionalität für entferntes (remote) Management.
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-Schnittstelle 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 des SIS.
TLS-Kanäle unter Nutzung sicherer kryptographischer	Der Netzkonnektor stellt TLS-Kanäle zur sicheren Kommunikation mit anderen IT-Produkten zur Verfügung.

Algorithmen	Dabei wird die TLS-Funktionalität dem Anwendungskonnektor zur Verfügung gestellt, der auch das Management der TLS Verbindung übernimmt.
Anwendungskonnektor	
Identifikation und Authentisierung	Der Konnektor implementiert unterschiedliche Mechanismen zur Identifikation und Authentisierung von Benutzern. Die Management-Schnittstelle des Konnektors erfordert eine Passworteingabe, die vor unberechtigtem Zugriff schützt. Die Kriterien, die vom Konnektor an die Benutzerpasswörter gestellt werden, entstammen [gemSpec_Kon], TIP1-A_4808. Im Rahmen des Pairing eines Kartenterminals generiert der Konnektor das „pairing secret“ mit hinreichend großer Entropie. Wird ein angeschlossenes Kartenterminal für Stapelsignaturen verwendet, fordert der Konnektor die Übertragung der DTBS über einen sicheren Kanal, der mittels card-to-card authentication mit dem HBA ausgehandelt wird.
Zugriffsberechtigungsdienst	Der Zugriffsberechtigungsdienst ist ein interner Dienst des Konnektors, der automatisch bei Aufruf einer Operation des Konnektors durch das Clientsystem ausgeführt wird. Durch den Zugriffsberechtigungsdienst wird eine Prüfung auf Zugriffsberechtigung für die angeforderten Ressourcen durchgeführt. Die erlaubten Zugriffsmöglichkeiten werden über ein Informationsmodell (kurz Infomodell) definiert. Durch das Infomodell werden Mandanten definiert und Clientsysteme sowie die vom Konnektor verwalteten externen Ressourcen (Kartenterminal mit Slots, Arbeitsplatz, SMC-Bs) zugeordnet. Die entsprechenden Zuordnungen werden durch einen Administrator eingestellt und beinhalten die erlaubten Zugriffswege vom Clientsystem über Arbeitsplatz zum Kartenterminal und dessen Slots.
Kartenterminaldienst	Der Kartenterminaldienst des Konnektors verwaltet alle adressierbaren Kartenterminals. Dabei werden die Zugriffe auf Kartenterminals durch Basisdienste und Fachmodule gekapselt. Über den Kartenterminaldienst können TLS-Kanäle zu den Kartenterminals auf- und abgebaut werden sowie SICCT-Kommandos gesendet und empfangen werden. Der Konnektor kommuniziert mit den angebundenen Kartenterminals über TLS-Kanäle. Der Netzkonnektor stellt diese Kommunikationskanäle für den Anwendungskonnektor zur Verfügung, vgl. „TLS-Kanäle unter Nutzung sicherer kryptographischer Algorithmen“.

	Informationen über die Arbeitsplatzkonfiguration eines angeschlossenen Kartenterminals können vom Kartenterminaldienst ausgegeben werden. Ausschließlich der Administrator darf diese Konfiguration verändern.
Kartendienst	Die Kartenterminals, die am Konnektor angebunden sind, können verschiedene Chipkartentypen (KVK, eGK, SMC-B und HBA) aufnehmen. Die in den Kartenterminals eines Arbeitsplatzes gesteckten Chipkarten mit ihren logischen Kanälen bilden einen dynamischen Kontext (siehe [gemSpec_Kon]). Die Identifikation dieser Chipkarten erfolgt durch Kartenhandles. Der EVG stellt Sicherheitsfunktionen des Chipkartendienstes anderen Diensten, dem Clientsystem oder den Fachmodulen bereit. Dazu gehören der Aufbau und die Verwaltung logischer Kanäle und die Kommunikation mit den Karten unter Verwendung spezieller Chipkartenkommandos. Der Chipkartendienst regelt dabei den Zugriff auf die Chipkarten für die verschiedenen Dienste und Anwender. Zudem wird durch den Chipkartendienst die lokale und entfernte PIN-Eingabe an den Kartenterminals umgesetzt und die unterschiedlichen Anforderungen an lokale und entfernte PIN-Eingabe und der damit verbundene Umgang mit den Authentisierungsverifikationsdaten (VAD) geregelt.
Signaturdienst	Der Signaturdienst des Konnektors unterstützt verschiedene Signaturtypen und –varianten und bietet Clientsystemen und Fachmodulen die Möglichkeit, Dokumente zu signieren und Dokumentensignaturen zu prüfen. Dabei kann bei Bedarf die Signaturrichtlinie für NFDM berücksichtigt werden. Der Signaturdienst umfasst die Funktionalität der nicht-qualifizierten elektronischen Signatur (nonQES) sowie der qualifizierten elektronischen Signatur (QES). Er unterstützt das folgende Signaturformat für QES: • XAdES für XML Dokumente nach NFDM-Signturrichtlinie. Außerdem unterstützt der EVG die folgenden Signaturformate für QES und nonQES: • CAdES für XML, PDF/A, Text und TIFF Dokumente, • PAdES für PDF/A Dokumente. Darüber hinaus werden für nonQES die folgenden Signaturformate unterstützt • CAdES für Binärdateien, • S/MIME für Multipurpose Internet Mail Extensions. Die Dokumentensignaturen werden mit Unterstützung der Signaturkarten (z.B. HBA) erzeugt. Die DTBS wird mit

	SHA-256 vom EVG erzeugt. Die Signaturerzeugung erfolgt durch die Signaturkarte mit RSASSA-PSS oder ECDSA. Für die Signaturprüfung werden darüber hinaus für nonQES und QES die Signaturformate PKCS#1 RSASSA-PSS und RSASSA-PKCS1-v1_5 mit verschiedenen SHA-2 Hash-Algorithmen unterstützt. Außerdem wird für QES und nonQES auch ECDSA mit SHA-256 unterstützt. Der Benutzer des Clientsystems muss seine Signatur-PIN an einem Kartenterminal eingeben. Das Prüfen von Dokumentensignaturen erfolgt auf Basis von Zertifikaten. Die Feststellung einer ungültig erzeugten Signatur wird dem Benutzer durch eine Warnmeldung angezeigt.
Verschlüsselungsdienst	Der Verschlüsselungsdienst bietet Schnittstellen zum hybriden und symmetrischen Ver- und Entschlüsseln von Dokumenten an. Der Verschlüsselungsdienst bietet für XML, PDF/A, Text, TIFF und Binärdaten die hybride Ver- /Entschlüsselung nach dem CMS Standard [12], [RFC 5652] bzw. die symmetrische Ver- /Entschlüsselung mittels AES-GCM an. Zudem wird für XML-Dokumente die hybride Ver-/Entschlüsselung nach [12], [XMLEnc] unterstützt und für MIME-Dokumenten die hybride Ver-/Entschlüsselung nach [12], [RFC 5751] unterstützt. Das Clientsystem übergibt die zu verschlüsselnden bzw. zu entschlüsselnden Dokumente. Vor dem Verschlüsseln eines Dokuments wird die Gültigkeit der zu benutzenden Verschlüsselungszertifikate geprüft.
TLS-Kanäle	Der Netzkonnektor stellt dem Anwendungskonnektor TLS-Kanäle zur Verfügung, vgl. „TLS-Kanäle unter Nutzung sicherer kryptographischer Algorithmen. Die Verwaltung von TLS-Kanälen wird duch den Anwendungskonnektor durchgeführt. Der Anwendungskonnektor initiiert dabei den Auf- und Abbau der TLS-Kanäle und stellt den Endpunkt für das Senden und Empfangen der Nutzdaten dar. Für das VSDM Fachmodul wird zudem TLS Session Resumption unterstützt. Der Administrator kann konfigurieren, ob für Verbindungen zum Clientsystem TLS-Kanäle verwendet werden müssen (ANCL_TLS_MANDATORY, ANCL_CAUT_MANDATORY) und einen Zertifikatsbasierten oder Passwortbasierten Authentisierungsmechanismus (ANCL_CAUT_MODE) festlegen. Für den Dienstverzeichnisdienst kann explizit die verpflichtende Nutzung von TLS deaktiviert werden (ANCL_DVD_OPEN).

	TLS Kanäle werden unter anderem für die Kommunikation mit Fachdiensten, mit dem zentralen Verzeichnisdienst, dem KSR, dem TSL-Dienst, bei ANCL_TLS_MANDATORY = Enabled mit den Clientsystemen im LAN und mit den angebundene eHealth Kartenterminals verwendet.
Sicherer Datenspeicher	Der Konnektor besitzt einen sicheren Datenspeicher, in dem alle sicherheitsrelevanten, veränderlichen Daten dauerhaft gespeichert werden. Dieser Datenspeicher sichert die Integrität, Authentizität und Vertraulichkeit der Daten, die dort hinterlegt bzw. abgerufen werden. Der Konnektor stellt den vorhandenen Fachmodulen ebenfalls die Nutzung eines sicheren Datenspeichers für ihre sensiblen Daten zur Verfügung.
Fachmodul VSDM	Das Fachmodul VSDM ist fester Bestandteil des Konnektors und ermöglicht es, Versichertenstammdaten einer eGK zu lesen, zu schreiben oder um neue Einträge zu ergänzen. Die eGK wird dabei über den Kartenterminaldienst und den Kartendienst angesprochen. Das Fachmodul VSDM kann über die Management-Oberfläche administriert werden.
Sicherheitsmanagement	Der Konnektor verwaltet verschiedene Rollen, wie Administrator, Clientsystem, Kartenterminals und Chipkarten. Auf die Managementschnittstelle hat nur ein autorisierter Administrator Zugriff. Dieser kann zum Beispiel Kartenterminals managen, Arbeitsplätze konfigurieren und TLS-Kanäle verwalten. Dazu gehört auch das Verwalten von Software-Updates für den EVG und angebundene Kartenterminals, Verwalten von Zertifikaten und Durchführen eines Werksresets. Insbesondere kann der Administrator die Online-Anbindung des Konnektors im Netz des Leistungserbringers konfigurieren (MGM_LU_ONLINE) und die QES Funktionalität des Signaturdienstes aktivieren und deaktivieren (MGM_LU_SAK). Die öffentlichen Schlüssel der CVC root CA sind in der gSMC-K gespeichert und können nur durch das CMS System der gSMC-K gelöscht werden. Über cross CVC Zertifikate können durch den Anwendungskonnektor aber weitere öffentlichen Schlüssel der CVC root CA eingebracht werden.
Schutz der TSF	Der Konnektor kann die für QES und nonQES benötigten Zertifikate interpretieren, sowie Verschlüsselungszertifikat und CV-Zertifikate. Zudem werden Information gültiger TSL und CRL Listen in die Prüfungen einbezogen sowie BNetzA-VL bzw. die entsprechenden Hashwerte. Die Zulässigkeit importierter zu signierenden bzw. zu prüfender signierten Daten wird bei Bedarf gemäß NFDM Signaturrichtlinie geprüft. Vor der regulären Kommunikation mit einem eHealth

	Kartenterminal wird geprüft, ob dieses gepairt ist und im Infomodell des Konnektors korrekt zugeordnet wurde. Ebenso werden gesteckte Chipkarten identifiziert und auf Gültigkeit geprüft. Bei entfernter PIN-Eingabe wird geprüft ob Kartenterminal und HBA für diesen Verwendungsfall zugelassen sind. Der Konnektor führt beim Anlauf und regelmäßig während des Normalbetriebs Selbsttests durch, siehe dazu auch die Sicherheitsfunktion „Selbstschutz: Selbsttests“ des NK. Durch den sicheren Start-Up Prozess wird die Integrität des EVG auf einen sicheren Vertrauensanker im BIOS zurückgeführt. Durch Neustart des Konnektors können die damit verbundenen Prüfungen durch einen Benutzer jederzeit wiederholt werden. Die vom Anwendungskonnektor erzeugten Protokolleinträge des Sicherheitsprotokolls werden mit einem zuverlässigen Zeitstempel versehen. Der Anwendungskonnektor greift dabei auf die Echtzeituhr zurück, die in regelmäßigen Abständen und auf Anforderung des Administrators vom Netzkonnektor mit einem vertrauenswürdigen Zeitdienst synchronisiert wird, siehe auch die Sicherheitsfunktion „Netzdienste: Zeitsynchronisation“ des NK. Der Konnektor setzt die in [gemSpec_Kon], TAB_KON_503, definierten Fehlbetriebszustände (Error Condition) um. Wird ein sicherheitsrelevanter Betriebszustand erreicht, schränkt der Konnektor seine Funktionalität gemäß [gemSpec_Kon], TAB_KON_504, ein.
Sicherheitsprotokollierung	Der Konnektor führt zusammen mit dem Netzkonnektor ein Sicherheits-Log gemäß Konnektor-Spezifikation [gemSpec_Kon], siehe auch die Sicherheitsfunktion „Selbstschutz: Sicherheits-Log“. Nur der Administrator kann Protokolleinträge einsehen. Protokolleinträge können nicht verändert werden und nicht explizit gelöscht werden. Ältere Einträge werden rollierend überschrieben.
VAU-Anbindung	Der Konnektor unterstützt das Fachmodul ePA, indem er eine sichere Verbindung zur vertrauenswürdigen Ausführungsumgebung (VAU) gemäß VAU-Kommunikationsprotokoll aufbaut. Dabei wird ein sicherer Kanal auf HTTP-Anwendungsschicht zwischen dem Konnektor als Client und der VAU (Server) aufgebaut.
SGD-Anbindung	Der Konnektor unterstützt das Fachmodul ePA bei der Nutzung der Schlüsselableitungsfunktionalität im Zusammenhang mit der Fachanwendung ePA. Der Gesamtablauf der Schlüsselableitungsfunktionalität für den Konnektor als Client ist aufgeteilt zwischen Basiskonnektor (als Teil des Anwendungskonnektors) und Fachmodul. Die

	kryptographischen Vorgaben (u.a. Durchführung des ECDH key exchange, Schlüsselerzeugung, Ver- und Entschlüsselung, Signaturerzeugung und -prüfung) werden dabei durch den Konnektor umgesetzt.

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 den Kapitel 3.2, 3.3 und 3.4 dar.

Die Konfiguration des EVG wird in Kap. 8 dieses Berichtes 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 Berichtes.

Dieses Zertifikat gilt nur für die angegebene Version des Produktes in der evaluierten Konfiguration und nur in Verbindung mit dem vollständigen Zertifizierungsreport. Dieses Zertifikat ist keine generelle Empfehlung des IT-Produktes durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte. Eine Gewährleistung für das IT-Produkt durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte, ist weder enthalten noch zum Ausdruck gebracht.

2. Identifikation des EVG

Der Evaluierungsgegenstand (EVG) heisst:

RISE Konnektor, V5.0

Die folgende Tabelle beschreibt den Auslieferungsumfang:

Nr	Typ	Identifier	Version	Auslieferungsart
1	HW	RISE-Konnektor Hardware (nicht Teil des EVG)	1.0.0	Das Gerät wird dem Endkunden über eine sichere Lieferkette zugestellt.
2	SW	RISE-Konnektor V5.0	4.2.8	Die Software wird im Zuge der Fertigung auf die Hardware aufgebracht oder als Software-Update Paket über KSR verteilt.
3	HW	gSMC-Ks (nicht Teil des EVG)	STARCOS 3.6 Health SMCK R1	Die gSMC-Ks sind in der Konnektor Hardware verbaut.

4	SW	ePA, AMTS und NFDM Fachmodul Firmware (nicht Teil des EVG)	RISE Konnektor Fachmodul ePA v2.0.0 RISE Konnektor Fachmodul AMTS v1.1.1 RISE Konnektor Fachmodul NFDM v1.1.1	Die Fachmodule sind integraler Bestandteil des Anwendungskonnektors.
5	DOC	RISE Konnektor Bedienungsanleitung Hashwert (SHA-256): ce8939f1a2e801db5396f6c7487509e98a87123bd4526e73c2602c6940c26d03	Version 1.6.3, 17.12.2021	Download von Herstellerwebseite.
6	DOC	RISE Konnektor Security Guidelines für Fachmodule Hashwert (SHA-256): 805e206d29dde67e7e684df013d88d9deafbade75d485d934d2f1fc8f357713e	Version 1.2, 07.12.2021	Die Security Guidance für Fachmodule wird nur intern den Fachmodul-Entwicklern zur Verfügung gestellt.

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 oder den Dienstverzeichnisdienst des Konnektors ermittelt werden. Beschreibungen dazu finden 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:

Netzkonnektor:

- VPN-Client
- Dynamischer Paketfilter mit zustandsgesteuerter Filterung
- Netzdienste (Zeitsynchronisation und Zertifikatsprüfung)
- Stateful Packet Inspection
- Selbstschutz (Speicheraufbereitung, Selbsttests, Schutz von Geheimnissen/ Seitenkanalresistenz, Sicherheits-Log)
- Administration (Administrator-Rollen, Management-Funktionen, Authentisierung der Administratoren, gesicherte Wartung, Software Update)
- Kryptographische Basisdienste
- TLS-Kanäle unter Nutzung sicherer kryptographischer Algorithmen

Anwendungskonnektor:

- Identifikation und Authentisierung
- Zugriffsberechtigungsdienst
- Kartenterminaldienst
- Chipkartendienst
- Signaturdienst
- Verschlüsselungsdienst
- TLS-Kanäle
- Sicherer Datenspeicher
- Fachmodul VSDM
- Sicherheitsmanagement (inkl. Software-Update)
- Schutz der TSF
- Sicherheitsprotokollierung
- VAU-Kanal
- SGD-Kanal

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 unter anderem die folgenden Punkte relevant:

Netzkonnektor:

- OE.NK.Admin_EVG Sichere Administration des Netzkonnektors
- OE.NK.PKI Betrieb einer PKI und Verteilung der TSL
- OE.NK.phys_Schutz Physischer Schutz des EVG
- OE.NK.Betrieb_AK Sicherer Betrieb des Anwendungskonnektors
- OE.NK.Betrieb_CS Sicherer Betrieb der Clientsysteme

Anwendungskonnektor:

- OE.AK.Admin_EVG Sichere Administration des Anwendungskonnektors
- OE.AK.Admin_Konsole Sichere Administratorkonsole
- OE.AK.Kartenterminal Sicheres Kartenterminal
- OE.AK.SecAuthData Schutz der Authentisierungsdaten
- OE.AK.Clientsystem Sichere Clientsysteme
- OE.AK.ClientsystemKorrekt Clientsysteme arbeiten korrekt und unterstützen das Informationsmodell
- OE.AK.phys_Schutz Physischer Schutz des EVG

OE.AK.Personal Qualifiziertes und vertrauenswürdiges Personal

Weitere Anforderungen an die Umgebung und Details finden sich in den Sicherheitsvorgaben [6], Kapitel 4.3 und 4.4.

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.

In den Fällen, in denen die Tests nicht auf Basis der fwVersion 4.2.8 durchgeführt wurden, untersuchten die Evaluatoren die Unterschiede zwischen der getesteten Version und der Version 4.2.8 in Bezug auf die Testfälle und kamen zu dem Schluss, dass eine Wiederholung dieser Tests auf fwVersion 4.2.8 nicht notwendig ist, da sich die in den Testfällen adressierte Funktionalität nicht geändert hat und von den Änderungen nicht beeinflusst wird. Die jeweiligen Testergebnisse sind daher auch für den finalen EVG in Version 4.2.8 gültig.

Herstellertests

Bei den Herstellertests wurde der Evaluierungsgegenstand RISE Konnektor V5.0 in diversen Firmware-Versionen (u.a. in der finalen Version 4.2.8 sowie 4.2.5, 4.2.3 und 4.2.1) getestet. Für die Herstellertests wurden, abhängig vom jeweiligen Testfall, ein produktiver Konnektor (PROD) und ein Debug-Konnektor (DEBUG) verwendet. Alle Testkonfigurationen sind konsistent zu den Angaben in den Sicherheitsvorgaben [6].

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

Bei den Herstellertests wurden die folgenden drei Testkategorien definiert:

- Automatisierter Test: Der Testfall ist vollständig in der Testsuite implementiert.
- Manuelle Tests: Der Testfall muss komplett oder teilweise (z. B. mit Zuhilfenahme von zusätzlichen Testwerkzeugen wie Netzwerk Sniffer etc.) manuell durchgeführt werden.
- Manueller Test/Integration RU: Manueller Test, der in der gematik Referenzumgebung (RU) durchgeführt werden muss.

Nahezu alle Testfälle wurden im Modus „In Reihe“ 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.

Testergebnisse

Alle Testfälle wurden erfolgreich ausgeführt und haben zum erwarteten Ergebnis geführt, oder für fehlgeschlagene Testfälle wurde eine angemessene Begründung gegeben.

Unabhängige Prüfstellentests

Bei den unabhängigen Prüfstellentests wurde der Evaluierungsgegenstand RISE Konnektor V5.0 in diversen Firmware-Versionen (u.a. in der finalen Version 4.2.8 sowie 4.2.5, 4.2.3 und 4.2.1) 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 DEBUG-Ausprägung des EVG kann eindeutig durch das Feld fwVersionInfo bzw. durch die entsprechenden Angabe der fwVersion in der GUI vom produktiven EVG (PROD) unterschieden werden.

Die Evaluatoren wiederholten alle automatisierten Testfälle des Herstellers, die in der Testumgebung der Prüfstelle durchführbar sind. Zudem wurden eigene manuelle Tests durchgeführt. Für letztere wurden unter anderem Testfälle von den Evaluatoren entwickelt, die auf Testideen basieren, die aus den Herstellertests unter Berücksichtigung der beschriebenen Sicherheitsfunktionen abgeleitet wurden.

Die unabhängigen Prüfstellentests fokussieren sich auf die TSF wie in den Sicherheitsvorgaben [6], Kapitel 7.1 und 7.3, insbesondere VPN-Client, Paketfilter, Netzdienste, Selbstschutz, Administration und TLS.

Für die spezifischen Tests der Verbindungen zur VAU bzw. zum SGD wurde eine leicht modifizierte Firmware eingesetzt, die den Datenverkehr zu VAU bzw. SGD an eine vordefinierte Ziel-IP leitet und davon abgesehen identisch zur Firmware der Ausprägung DEBUG ist.

Testergebnisse

Alle relevanten Testfälle konnten erfolgreich durchgeführt werden und haben zum erwarteten Ergebnis geführt (oder es konnte eine angemessene Begründung für abweichendes Verhalten des EVG gegeben werden).

Penetrationstests

Bei Tests und Schwachstellenanalyse wurde systematisch das Angriffspotential “enhanced basic” (AVA_VAN.3) angenommen.

Bei der Schwachstellenanalyse wurden öffentlich bekannte Schwachstellen anhand von CVE-Listen, Fachliteratur und wissenschaftlichen Veröffentlichungen auf ihre Relevanz inder Einsatzumgebung des EVG untersucht und ggfls. weiteren Tests und Analysen unterzogen.

Neben der finalen Version des EVG wurde für die Testdurchführung eine Debug-Version des Konnektors verwendet, die zusätzliche Testfunktionalität aufweist. Diese zusätzliche Funktionalität ermöglichte die Durchführung bestimmter Tests (z. B. Verifikation der sicheren Löschung von Schlüsseln), die im finalen Konnektor nicht durchführbar sind (und auch nicht durchführbar sein dürfen).

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 Kap. B.2.1 [2] kam zur Anwendung.
- Part II: Zusammentragen von Ergebnissen einzelner Evaluationstätigkeiten.
- Part III: Untersuchung der einzelnen Punkte des JIL Dokuments [14] als Anhaltspunkt für mögliche weitere Schwachstellen im EVG.
- Part IV: Die Lebenszyklusphasen Entwicklung, Fertigung, Installation, Personalisierung und operativer Betrieb wurden auf mögliche Schwachstellen untersucht.

- Part V: Identifikation und Bewertung von Angriffspunkten auf verschiedenen Ebenen (Hardwareebene oder verschiedene Protokollschichten der externen Schnittstellen).
- Part VI: Es wurde gezeigt, dass für die im Schutzprofil [8] definierten Assets keine weiteren Schwachstellen existieren, die nicht schon durch die vorangegangenen Analysen betrachtet wurden.

Testergebnisse

Es wurden keine Abweichungen zwischen erwarteten und erhaltenen Resultaten gefunden. Kein Angriffsszenario mit dem angenommenen Angriffspotential war in der operativen Umgebung des EVG, wie in den Sicherheitsvorgaben [6] definiert, tatsächlich erfolgreich, sofern alle durch den Entwickler geforderten Maßnahmen Anwendung finden.

8. Evaluierte Konfiguration

Dieses Zertifikat bezieht sich auf die folgenden Konfigurationen des EVG:

- RISE-Konnektor V5.0
  - Firmware-Version
    - fwVersion: 4.2.8
    - fwVersionInfo: RISE Konnektor
  - Hardware-Version
    - hwVersion: 1.0.0
    - serialNumber: product specific
- Dokumente
  - RISE Konnektor Bedienungsanleitung [11]

Der Administrator kann über die Benutzeroberfläche die Firmware-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 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 Vertrauenswürdigkeitskomponenten bestätigt:

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

Die Evaluierung hat gezeigt:

- PP Konformität: Common Criteria Schutzprofil (Protection Profile) Schutzprofil 2: Anforderungen an den Konnektor, Version 1.5.9, BSI-CC-PP-0098-V3-2021 vom 15.04.2021 [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_IMP.1, ADV_TDS.3, ALC_TAT.1, AVA_VAN.3 und 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 Tabelle in Anhang B in Teil D dieses Reportes gibt einen Überblick über die zur Durchsetzung der Sicherheitspolitik im EVG enthaltenen kryptographischen Funktionalitäten und verweist auf den jeweiligen Anwendungsstandard, in dem die Eignung festgestellt ist.

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

Gemäß [13] sind die Algorithmen für den jeweiligen Zweck geeignet. Die Gültigkeitsdauer für jeden Algorithmus ist im offiziellen Katalog [13][TR-03116-1] angegeben.

Etwaige Abweichungen von den Implementierungsstandards sind in [15] gesammelt und die Abschnitte von [15] sind, wo zutreffend, in der Spalte ‚Implementierungsstandards' von Tabelle 3 genannt.

10. Auflagen und Hinweise zur Benutzung des EVG

Die in Tabelle 2 genannte Betriebsdokumentation enthält die notwendigen Informationen zur Anwendung des EVG und alle darin enthaltenen Sicherheitshinweise sind zu beachten. Zusätzlich sind alle Aspekte der Annahmen, Bedrohungen und Politiken wie in den Sicherheitsvorgaben dargelegt, die nicht durch den EVG selbst, sondern durch die Einsatzumgebung erbracht werden müssen, zu berücksichtigen.

Der Anwender des Produktes muss die Ergebnisse dieser Zertifizierung in seinem Risikomanagementprozess berücksichtigen. Um die Fortentwicklung der Angriffsmethoden und -techniken zu berücksichtigen, sollte er ein Zeitintervall definieren, in dem eine Neubewertung des EVG erforderlich ist und vom Inhaber dieses Zertifikates verlangt wird.

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

Zertifizierte Aktualisierungen des EVG, die die Vertrauenswürdigkeit betreffen, sollten verwendet werden, sofern sie zur Verfügung stehen. Stehen nicht zertifizierte

Aktualisierungen oder Patches zur Verfügung, sollte er den Inhaber dieses Zertifikates auffordern, für diese eine Re-Zertifizierung bereitzustellen. In der Zwischenzeit sollte der Risikomanagementprozess für das IT-System, in dem der EVG eingesetzt wird, prüfen und entscheiden, ob noch nicht zertifizierte Aktualisierungen und Patches zu verwenden sind oder zusätzliche Maßnahmen getroffen werden müssen, um die Systemsicherheit aufrecht zu erhalten.

Der EVG kann seine Sicherheitsleistung nur unter den folgenden Bedingungen erbringen:

- Die EVG-Konfiguration sieht eine verpflichtende Nutzung von TLS sowie eine verpflichtende Client-System-Authentisierung vor;
- Die angeschlossenen Client-Systeme verifizieren die Authentizität des Konnektors, wenn sie dessen Dienste nutzen oder Ereignisse empfangen;
- Der Benutzer ist in der Lage zu identifizieren, dass die Verbindung zu einem Client-System sicher ist.

Der EVG Benutzer soll (***shall***) den EVG nur dann betreiben, wenn die oben genannten Bedingungen erfüllt sind. Ein Verstoß oder eine Nichterfüllung dieser Bedingungen wird als eine Schwachstelle des EVG bezüglich der Einsatzumgebung verstanden. In diesem Fall ist der EVG Benutzer dafür verantwortlich Gegenmaßnahmen gegen diese Schwachstelle zu ergreifen.

Der EVG unterstützt unterschiedliche Betriebskonfigurationen. Die wesentlichen Konfigurationen sind: “Parallel”-, “inReihe”- und „Offline“-Modus. Die empfohlene Konfiguration ist “in-Reihe”, da diese eine höhere Sicherheit der angeschlossenen LAN-seitigen Netzwerke bietet.

Für aktive VPN Verbindungen, die IPSec nutzen, sind im EVG keine Gegenmaßnahmen gegen die statistische Datenverkehrsanalyse implementiert.

11. Sicherheitsvorgaben

Die Sicherheitsvorgaben [6] werden zur Veröffentlichung in einem separaten Dokument im Anhang A bereitgestellt.

12. Definitionen

12.1. Abkürzungen

AES Advanced Encryption Standard

AIS Anwendungshinweise und Interpretationen zum Schema

AK Anwendungskonnektor

AMTS Arzneimitteltherapiesicherheit

BIOS Basic Input/Output System

BnetzA-VL Vertrauensliste der Bundesnetzagentur

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
CRL	Certificate Revocation List
DTBS	Data To Be Signed
EAL	Evaluation Assurance Level – Vertrauenswürdigkeitsstufe
eGK	Elektronische Gesundheitskarte
ePA	Elektronische Patientenakte
ESP	Encapsulating Security Payload
ETR	Evaluation Technical Report
EVG	Evaluierungsgegenstand
GCM	Galois/Counter Mode
gSMC-K	Sicherheitsmodul für den Konnektor
HBA	Heilberufsausweis
HMAC	Keyed-Hash Message Authentication Code
ICCSN	Integrated Circuit Card Serial Number
IKE	Internet Key Exchange
IPsec	Internet Protocol Security
IT	Information Technology - Informationstechnologie
ITSEF	Information Technology Security Evaluation Facility - Prüfstelle für IT-Sicherheit
KSR	Konfigurations- und Software-Repository
LAN	Local Area Network
NFDM	Notfalldatenmanagement
NK	Netzkonnektor
NTP	Network Time Protocol
PKI	Public Key Infrastructure
PP	Protection Profile – Schutzprofil
PTV	Produkttyp Version
QES	Qualifizierte Elektronische Signatur
SAR	Security Assurance Requirement - Vertrauenswürdigkeitsanforderungen
SF	Security Function - Sicherheitsfunktion
SFP	Security Function Policy - Politik der Sicherheitsfunktion
SFR	Security Functional Requirement - Funktionale Sicherheitsanforderungen

SGD	Schlüsselgenerierungsdienst
SHA	Secure Hash Algorithm
SIS	Secure Internet Service
ST	Security Target – Sicherheitsvorgaben
SW	Software
TCP/IP	Transmission Control Protocol/Internet Protocol
TI	Telematikinfrastruktur
TOE	Target of Evaluation - Evaluierungsgegenstand
TSC	TSF Scope of Control - Anwendungsbereich der TSF-Kontrolle
TSF	TOE Security Functionality – EVG-Sicherheitsfunktionalität
TSFI	TOE Security Functionality Interface – TSF Schnittstelle
TSL	Trust-service Status List
UDP	User Datagram Protocol
VPN	Virtual Private Network
VAU	Vertrauenswürdige Ausführungsumgebung
VSDM	Versichertenstammdatenmanagement
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.

Evaluationsgegenstand – Software, Firmware und / oder Hardware und zugehörige Handbücher.

EVG-Sicherheitsfunktionalität - Eine Menge, die die gesamte Hardware, Software, und Firmware des EVG umfasst, auf die Verlass sein muss, um die SFR durchzusetzen.

Formal - Ausgedrückt in einer Sprache mit beschränkter Syntax und festgelegter Semantik, die auf bewährten mathematischen Konzepten basiert.

Informell - Ausgedrückt in natürlicher Sprache.

Objekt - Eine passive Einheit im EVG, die Informationen enthält oder empfängt und mit der Subjekte Operationen ausführen.

Schutzprofil - Eine implementierungsunabhängige Menge von Sicherheitsanforderungen für eine Kategorie von EVG.

Semiformal - Ausgedrückt in einer Sprache mit beschränkter Syntax und festgelegter Semantik.

Sicherheitsfunktion - Ein Teil oder Teile eines EVG, auf die zur Durchsetzung einer hierzu in enger Beziehung stehenden Teilmenge der Regeln der EVG-Sicherheitspolitik Verlass sein muss.

Sicherheitsvorgaben - Eine implementierungsabhängige Menge von Sicherheitsanforderungen für eine Kategorie von EVG.

Subjekt - Eine aktive Einheit innerhalb des EVG, die die Ausführung von Operationen auf Objekten bewirkt.

Zusatz - Das Hinzufügen einer oder mehrerer Anforderungen zu einem Paket.

13. Literaturangaben

[1] Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria for Information Technology Security Evaluation/CC), Version 3.1
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

[2] Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017, https://www.commoncriteriaportal.org

[3] BSI-Zertifizierung: 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[8] 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-1189-2022, Version 3.1, 17.01.2022, Security Target für RISE Konnektor V5.0, Research Industrial Systems Engineering (RISE)

[8] specifically

- AIS 1, Version 14, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 14, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 19, Version 9, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria) und ITSEC
- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 23, Version 4, Zusammentragen von Nachweisen der Entwickler
- AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 38, Version 2, Reuse of evaluation results
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren

[7] Evaluierungsbericht, Version 3.4, 23.03.2022, Evaluation Technical Report (ETR) – Summary, SRC Security Research & Consulting GmbH (vertrauliches Dokument)

[8] Common Criteria Protection Profile, Schutzprofil 2: Anforderungen an den Konnektor, BSI-CC-PP-0098-V3-2021, Version 1.5.9 vom 15.04.2021, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[9] RISE Konnektor Sichere Lieferkette, Version 0.9.8, 20.03.2020, Research Industrial Systems Engineering (RISE)

[10] Konfigurationsliste des EVG bestehend aus folgenden vertraulichen Dokumenten:

configuration list, collection of csv-files for each source code repository, Version 4.2.8

RISE Konnektor Implementierung, Version 1.19.0, Stand 15.12.2021

RISE Konnektor Referenzverzeichnis, Version 5.3, 15.02.2022

[11] Guidance Dokumentation für den EVG

RISE Konnektor Bedienungsanleitung, Version 1.6.3, 17.12.2021

RISE Konnektor Security Guidelines für Fachmodule, Version 1.2, 07.12.2021

[12] Implementation standards:

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

[FIPS 186-4] NIST: FIPS 186-4 Digital Signature Standard (DSS), July 2013

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

[FIPS 202] NIST: FIPS PUB 202: SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, August 2015

[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

[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 forTransport 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 KeyInfrastructure 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

[RFC 4055] Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Schaad, et al., June 2005 [RFC 5280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Cooper, et al., May 2008

[RFC 7292] PKCS #12: Personal Information Exchange Syntax v1.1, Moriarty, et al., July 2014

[RFC 5652] Cryptographic Message Syntax (CMS), R. Housley, September 2009

[RFC 5751] Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification, Ramsdell & Turner, January 2010

[RFC 5083] Cryptographic Message Syntax (CMS) Authenticated-Enveloped-Data Content Type, R. Housley, November 2007

[RFC 5084] Using AES-CCM and AES-GCM Authenticated Encryption in the Cryptographic Message Syntax (CMS), R. Housley, November 2007

[RFC 7027] Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS), J. Merkle, October 2013

[RFC 5869] H. Krawczyk, P Eronen: HMAC-based Extract-and-Expand Key Derivation Function (HKDF), RFC 5869, May 2010

[RFC 2898] B. Kaliski: PKCS #5: Password-Based Cryptography Specification Version 2.0, RFC 2898, September 2000

[SEC1] Standards for Efficient Cryptography, SEC 1: Elliptic Curve Cryptography, Certicom Research, May 21, 2009, Version 2.0

[HaC] A. Menezes, P. van Oorschot und O. Vanstone. Handbook of Applied Cryptography. CRCPress, 1996

[CAdES] ETSI TS 101 733 V1.7.4 (2008-07), Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)

[CAdES_BP] European Telecommunications Standards Institute (ETSI: Electronic Signatures and Infrastructure (ESI); CAdES Baseline Profile; ETSI Technical Specification TS 103 173, Version 2.1.1, 2012-03

[PAdES] ETSI TS 102 778-3 V1.2.1, PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced – PAdES-BES and PAdES-EPES ProfilesTechnical Specification, 2010

[PAdES_BP] European Telecommunications Standards Institute (ETSI): Electronic Signatures and Infrastructure (ESI); PAdES Baseline Profile; ETSI Technical Specification TS 103 172, Version 2.1.1, 2012-03

[XMLSig] XML Signature Syntax and Processing (Second Edition), W3C Recommendation 10 June 2008, https://www.w3.org/TR/2008/REC-xmldsig-core-20080610/

[XMLEnc] XML Encryption Syntax and Processing, Version 1.1 W3C Recommendation, 11 April 2013, https://www.w3.org/TR/2013/REC-xmlenc-core1-20130411/

[XAdES] XML Advanced Electronic Signatures (XAdES), European Telecommunications Standards Institute (ETSI): Technical Specication XML Advanced Electronic Signatures (XAdES). ETSI Technical Specication TS 101 903, Version 1.4.2, 2010

[XAdES_BP] European Telecommunications Standards Institute (ETSI): Electronic Signatures and Infrastructure (ESI); XAdES Baseline Profile; ETSI Technical Specification TS 103 171, Version 2.1.1, 2012-03

[SP800-133] NIST Special Publication 800-133 Revision 2, Recommendation for Cryptographic Key Generation, June 2020

[SP 800-90A] NIST Special Publication 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Revision 1, June 2015

[SP 800-56A] NIST Special Publication 800-56A, Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography, April 2018

[ANSSI-0241] Journal officiel de la république française , Avis relatif aux paramètres de courbes elliptiques définis par l'Etat français, 16. Oktober 2011

[ETSI_TS_119_612] ETSI TS 119 612, Electronic Signatures and Infrastructures (ESI); Trusted Lists, Version 2.1.1 (2015-07)

[ETSI_TS_119_312] ETSI TS 119 312, Electronic Signatures and Infrastructures (ESI); Cryptographic Suites, Version 1.2.1 (2017-05)

[TLS_Analysis] TLS-Analyse durch SRC, anhand der Anforderungen an TLS im deutschen CC-Zertifizierungsschema, Version 1.9, 29.10.2021, SRC Security Research & Consulting GmbH file name: 1189_TLS_Analyse_RISE_v19.pdf (vertrauliches Dokument)

[VPN_Analysis] VPN-Analyse bestehend aus:

IPsec-RFCs - MAY_SHOULD Anforderungen, Version: 1.1, 16.09.2020, SRC Security Research & Consulting GmbH, filename: 1132_RISE_RFCMS_v11_20200916.pdf (vertrauliches Dokument)

VPN Analyse, basierend auf Anforderungen an kryptographisch gesicherte VPN-Kanäle / Trusted Channels im deutschen CC-Zertifizierungsschema, Version 1.4, 25.10.2021, SRC Security Research & Consulting GmbH file name: 1189_VPN_Analyse_RISE_v14_20211025.pdf (vertrauliches Dokument)

[13] Application standards:

[gemSpec_Kon] Einführung der Gesundheitskarte: Spezifikation Konnektor, PTV5: Version 5.14.0, gematik GmbH

[gemSpec_Krypt] Einführung der Gesundheitskarte - Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, Version 2.20.0, gematik GmbH

[TR-03116-1] Technische Richtlinie BSI TR-03116-1 Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 1: Telematikinfrastruktur, Version 3.20, 21.09.2018, Bundesamt für Sicherheit in der Informationstechnik (BSI)

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

[15] Kryptographische Mechanismen des RISE Konnektor V5.0 (PTV5), Version 1.4, 12.10.2021 (vertrauliches Dokument)

C. Auszüge aus den Kriterien

Die Bedeutung der Vertrauenswürdigkeitskomponenten und -stufen kann direkt den Common Criteria entnommen werden. Folgende Referenzen zu den CC 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/cc/ veröffentlicht.

D. Anhänge

Liste der Anhänge zu diesem Zertifizierungsreport

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

Anhang B: Übersicht und Bewertung der im EVG enthaltenen kryptographischen Funktionalitäten

Anhang B zum Zertifizierungsreport BSI-DSZ-CC-1189-2022

Übersicht und Bewertung der im EVG enthaltenen kryptographischen Funktionalitäten

#	Zweck	Kryptographische Funktion	Implementierungsstandard	Schlüssellänge in Bits	Anwendungsstandard
1	Authentizität	Signaturverifikation für VPN und TLS sha256WithRSAEncryption (OID 1.2.840.113549.1.1.11) und (nur für TLS) ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)	[RFC 8017] (PKCS#1) [FIPS 180-4] (SHA-256) [TR-03111] (ECDSA)	Für RSA: 2048 bit Für ECDSA: Schlüsselgröße entsprechend der benutzten elliptischen Kurve brainpoolP256r1 ([RFC 7027])	[gemSpec_Krypt] Kap. 3.3.1 und Kap. 3.3.2
2		ECDSA Signaturverifikation für VAU Protokoll ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)	[gemSpec_Krypt], Kap. 6 (VAU) [TR-03111] (ECDSA) [FIPS 180-4] (SHA)	Schlüsselgrößen entsprechend der benutzten elliptischen Kurve brainpoolP256r1 ([RFC 5639])	[gemSpec_Krypt], Kap. 6
3		ECDSA Signaturerstellung mit Unterstützung von SMC-B oder eGK und Verifikation für SGD Client ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)	[TR-03111] (ECDSA) [RFC 5639] (brainpool) [FIPS 180-4] (SHA)	Schlüsselgrößen entsprechend der benutzten elliptischen Kurve brainpoolP256r1 ([RFC 5639])	[gemSpec_Krypt], Kap. 3.15 (SGD)
4		Verifikation von Signaturen des TSL-Signer-Zertifikats und CRL mit sha256WithRSAEncryption (OID 1.2.840.113549.1.1.11) und ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2) auf brainpoolP256r1	[RFC 8017] (PKCS#1) [FIPS 180-4] (SHA) [TR-03111] (ECDSA) [AVA_CCA], sec. 2.27	2048 bit für RSA Für ECDSA: Schlüsselgröße entsprechend der benutzten elliptischen Kurve brainpoolP256r1 ([RFC 5639])	[gemSpec_Krypt], Kap. 3.14
5	Authentisierung	Signaturerstellung mit Unterstützung von gSMC-K und Verifikation für VPN sha256withRSAEncryption (OID 1.2.840.113549.1.1.11)	[RFC 8017] (PKCS#1) [FIPS 180-4] (SHA)	2048 bit	[gemSpec_Krypt], Kap. 3.3.1

#	Zweck	Kryptographische Funktion	Implementie-rungsstandard	Schlüssellänge in Bits	Anwendungs-standard
		Signaturerstellung mit Unterstützung von gSMC-K und -Verifikation für TLS sha256withRSAEncryption (OID 1.2.840.113549.1.1.11) und (nur Verifikation) ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)	[RFC 8017] (PKCS#1) [FIPS 180-4] (SHA) [RFC 5246] (TLS v1.2) [TR-03111] (ECDSA)	2048 bit für RSA Für ECDSA: Schlüsselgröße entsprechend der benutzten elliptischen Kurve brainpoolP256r1 ([RFC 7027])	[gemSpec_Krypt], Kap. 3.3.1
		ECDSA Signaturerstellung mit Unterstützung von SMC-B oder eGK und Verifikation für VAU Protokoll ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)	[gemSpec_Krypt], Kap. 6 (VAU) [TR-03111] (ECDSA) [RFC 5639] brainpool [FIPS 180-4] (SHA)	Schlüsselgrößen entsprechend der benutzten elliptischen Kurve brainpoolP256r1 ([RFC 5639])	[gemSpec_Krypt], Kap. 6
6	Schlüssel-austausch	Diffie-Hellman Schlüsselaustausch (DH) für VPN (IPsec IKEv2, DH Gruppe 14)	[HaC] (DH) [RFC 3526] (DH Group) [RFC 7296] (IKEv2) [AVA_CCA], sec. 2.10	DH: group 14 2048-bit Länge des privaten Exponenten >= 2047 bit	[gemSpec_Krypt], Kap. 3.3.1
7		Diffie-Hellman Schlüsselaustausch (DH) und Elliptic Curve Diffie-Hellman Schlüsselaustausch (ECDH) für TLS	[HaC] (DH) [SEC1] (ECDH), [RFC 5246] (TLS v1.2) [RFC 3268] (DHE_RSA) [RFC 4492] (ECDHE_RSA) [RFC 3526] (DH Group 14) [AVA_CCA], sec. 2.10	DH: group 14 2048 bit Länge des privaten Exponenten >= 2047 bit ECDH: Schlüsselgrößen entsprechend der benutzten elliptischen Kurven P-{256,384} ([FIPS 186-4]) und brainpoolP{256, 384}r1 ([RFC 7027])	[gemSpec_Krypt], Kap. 3.3.2
8		Elliptic-Curve-Diffie-Hellman Schlüsselaushandlung (ECDH) für VAU Protokoll	[gemSpec_Krypt], Kap. 6 (VAU) [SEC1] (ECDH) [RFC-5639] (brainpool)	Schlüssellänge entsprechend der verwendeten elliptischen Kurve brainpoolP256r1 ([RFC5639])	[gemSpec_Krypt], Kap. 6
9	Schlüsselab-leitung	HMAC Berechnung für VPN (PRF) PRF-HMAC-SHA-1, PRF-HMAC-SHA-256	[FIPS 180-4] (SHA) [RFC 2404] (PRF-HMAC-SHA-1) [RFC 4868] (PRF-HMAC-SHA-256)	128 bit und 256 bit	[gemSpec_Krypt], Kap. 3.3.1

#	Zweck	Kryptographische Funktion	Implementierungsstandard	Schlüssellänge in Bits	Anwendungsstandard
			[RFC 7296] (IKEv2)		
10		Schlüsselableitung für TLS 1.2	[RFC 5246] (TLS v1.2) [FIPS 180-4] (SHA) [RFC 2104] (HMAC),	128 bit und 256 bit	[gemSpec_Krypt], Kap. 3.3.2
11		Schlüsselableitung mit HKDF für VAU Protokoll	[gemSpec_Krypt], Kap. 6 (VAU) [FIPS 180-4] (SHA) [RFC 5869] (HKDF)	256 Bit	[gemSpec_Krypt], Kap. 6 (VAU)
12	Schlüsselgenerierung	RSA Schlüsselpaar Generierung im X.509 und PKCS#12 Format	[RFC 4055] (sup. [RFC 5280]), [RFC 7292] (PKCS#12) [FIPS 186-4] (Method B.3.3)	2048 bit	[TR-03116-1]
13	Integrität	HMAC Berechnung und Prüfung für VPN HMAC mit SHA-1, SHA-256	[FIPS 180-4] (SHA) [RFC 2104] (HMAC) [RFC 2404] (HMAC-SHA-1 mit ESP) [RFC 4868] (HMAC-SHA-2 mit IPsec) [RFC 7296] (IKEv2)	160 bit und 256 bit	[gemSpec_Krypt], Kap. 3.3.1
14		HMAC Berechnung und Prüfung für TLS HMAC mit SHA-1, SHA-256 und SHA-384	[FIPS 180-4] (SHA) [RFC 2104] (HMAC) [RFC 5246] (TLS v1.2)	160 bit, 256 bit und 384 bit	[gemSpec_Krypt], Kap. 3.3.2
15	Vertraulichkeit	Symmetrische Verschlüsselung und Entschlüsselung mit ESP und für VPN Kommunikation AES-CBC	[FIPS 197] (AES) [RFC 3602] (AES-CBC) [RFC 4303] (ESP) [RFC 4301] (IPsec)	256 bit	[gemSpec_Krypt], Kap. 3.3.1
16		Symmetrische Verschlüsselung und Entschlüsselung für TLS v1.2 AES-128 und AES-256 in CBC	[FIPS 197] (AES) [RFC 3602] (AES-CBC) [RFC 3268] (AES-TLS mit DH) [RFC 4492] (AES-TLS mit ECDH)	128 bit und 256 bit	[gemSpec_Krypt], Kap. 3.3.2
17	Vertraulichkeit mit Nachrichtenauthentizität (Authenticated Encryption)	AES-128 und AES-256 im GCM Modus für TLS 1.2	[FIPS 197] (AES) [RFC 3268] (AES-TLS) [SP 800-38D] (GCM) [RFC 5289] (AES-GCM-TLS) [RFC 5116] (AEAD)	128 bit und 256 bit	[gemSpec_Krypt], Kap. 3.3.2

#	Zweck	Kryptographische Funktion	Implementierungsstandard	Schlüssellänge in Bits	Anwendungsstandard
18		AES-256 im GCM Modus für VAU Kommunikation	[gemSpec_Krypt], Kap. 6 (VAU) [FIPS 197] (AES) [SP 800-38D] (GCM) [RFC 5116] (AEAD)	256 bit und 128 bit Tag-Länge	[gemSpec_Krypt], Kap. 6
19		ECIES-basierte hybride Ver- und Entschlüsselung mit Nachrichtenauthentizität und ECC Schlüsselgenerierung mittels ECIES mit brainpool256r1, HKDF mit SHA-256 und AES-256 im GCM Modus	[gemSpec_Krypt], Kap. 3.15 (SGD) [SEC1] (ECIES) [SP 800-56A#5.7.1.2] (ECDH) [RFC 5639] (brainpool) [FIPS 180-4] (SHA) [RFC 5869] (HKDF) [FIPS 197] (AES) [SP 800-38D] (GCM) [RFC 5116] (AEAD)	ECDH: Schlüsselgrößen entsprechend der benutzten elliptischen Kurve brainpoolP256r1 ([RFC 5639]) AES-GCM: 256 bit AES und 128 bit Tag-Länge	[gemSpec_Krypt], Kap. 3.15
20	Vertrauenswürdiger Kanal	TLS v1.2	[RFC 5246] (TLS v1.2) [TLS_Analysis]	-	[gemSpec_Krypt], Kap. 3.3.2
21		VPN IPsec (IKEv2) unter Verwendung zertifikatsbasierter Authentizierung	[RFC 4301] (IPsec) [RFC 4303] (ESP) [RFC 7296] (IKEv2) [VPN_Analysis]	-	[gemSpec_Krypt], Kap. 3.3.1
22		VAU Protokoll Kommunikation gemäß den Anforderungen des ePA-Aktensystems für den Austausch des Nachrichtenlimits der VAU	[gemSpec_Krypt], Kap. 6 (VAU)	-	[gemSpec_Krypt], Kap. 6
23		SGD Protokoll (ECIES) Kommunikation gemäß den Anforderungen des ePA-Aktensystems für den Nachrichtenaustausch mit dem SGD-HSM	[gemSpec_Krypt], Kap. 3.15 (SGD)	-	[gemSpec_Krypt], Kap. 3.15
24	Authentizität	PAdES basiert: QES Signaturgenerierung mit SHA-256 und Unterstützung von HBA und Verifikation mit	[RFC 8017] (PKCS#1) [TR-03111] (ECDSA) [PAdES] [PAdES_BP] [FIPS 180-4] (SHA) [AVA_CCA], sec. 2.27	1976 bit bis 4096 bit für RSA Für ECDSA: Schlüsselgröße entsprechend der benutzten elliptischen Kurve brainpoolP256r1 ([RFC 5639])	[gemSpec_Krypt], Kap. 3.12 [gemSpec_Krypt], Kap. 3.8

#	Zweck	Kryptographische Funktion	Implementierungsstandard	Schlüssellänge in Bits	Anwendungsstandard
		RSASSA-PKCS1-v1_5 und RSASSA-PSS mit Hashfunktionen SHA-{256,384,512} und ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2) auf brainpoolP256r1			
25		PAdES basiert: nonQES Signaturgenerierung mit SHA-256 und Unterstützung von SMC-B und Verifikation mit RSASSA-PSS mit Hashfunktionen SHA-256 und ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2) auf brainpoolP256r1	[RFC 8017] (PKCS#1) [TR-03111] (ECDSA) [PAdES] [PAdES_BP] [FIPS 180-4] (SHA) [AVA_CCA], sec. 2.27	2048bit für RSA Für ECDSA: Schlüsselgröße entsprechend der benutzten elliptischen Kurve brainpoolP256r1 ([RFC 5639])	[gemSpec_Krypt], Kap. 3.12 [gemSpec_Krypt], Kap. 3.8
26	Authentizität	CAdES basiert: QES Signaturgenerierung mit SHA-256 und Unterstützung von HBA und Verifikation mit RSASSA-PKCS1-v1_5 und RSASSA-PSS mit Hashfunktionen SHA-{256,384,512} und ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2) auf brainpoolP256r1	[RFC 8017] (PKCS#1) [TR-03111] (ECDSA) [RFC 5652] (CMS) [CAdES] [CAdES_BP] [FIPS 180-4] (SHA) [AVA_CCA], sec. 2.27	1976 bis 4096 bit für RSA Für ECDSA: Schlüsselgröße entsprechend der benutzten elliptischen Kurve brainpoolP256r1 ([RFC 5639])	[gemSpec_Krypt], Kap. 3.12 [gemSpec_Krypt], Kap. 3.7
27	Authentizität	CAdES basiert: nonQES Signaturgenerierung	[RFC 8017] (PKCS#1) [TR-03111] (ECDSA)	2048 bit für RSA Für ECDSA: Schlüsselgröße	[gemSpec_Krypt], Kap. 3.12 [gemSpec_Krypt],

#	Zweck	Kryptographische Funktion	Implementie-rungsstandard	Schlüssellänge in Bits	Anwendungs-standard
		mit SHA-256 und Unterstützung von SMC-B und Verifikation mit encoding RSASSA-PSS mit Hashfunktionen SHA-256 und ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2) auf brainpoolP256r1	RFC 5652] (CMS) [CAdES] [CAdES_BP] [FIPS 180-4] (SHA) [AVA_CCA], sec. 2.27	entsprechend der benutzten elliptischen Kurve brainpoolP256r1 ([RFC 5639])	Kap. 3.7
28	Authentizität	XAdES basiert: QES (NFDM) Signaturgenerierung mit SHA-256 und Unterstützung von HBA und Verifikation mit RSASSA-PKCS1-v1_5 und RSASSA-PSS mit Hashfunktionen SHA-{256,384,512} und ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2) auf brainpoolP256r1	[RFC 8017] (PKCS#1) [TR-03111] (ECDSA) [XMLSig] [XAdES] [XAdES_BP] [FIPS 180-4] (SHA) [AVA_CCA], sec. 2.27	1976 bit bis 4096 bit Für ECDSA: Schlüsselgröße entsprechend der benutzten elliptischen Kurve brainpoolP256r1 ([RFC 5639])	[gemSpec_Krypt], Kap. 3.12 [gemSpec_Krypt], Kap. 3.1
29	Authentizität	Verifikation von Zertifikaten, OCSP Antworten und OCSP Zertifikate: QES RSASSA-PKCS1-v1_5 und RSASSA-PSS mit Hashfunktionen SHA-{256,384,512} und ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2) auf brainpoolP256r1	[RFC 8017] (PKCS#1) [TR-03111] (ECDSA) [FIPS 180-4] (SHA) [AVA_CCA], sec. 2.27	1976 bit bis 4096 bit für RSA Für ECDSA: Schlüsselgröße entsprechend der benutzten elliptischen Kurve brainpoolP256r1 ([RFC 5639])	[gemSpec_Krypt], Kap. 3.12

#	Zweck	Kryptographische Funktion	Implementierungsstandard	Schlüssellänge in Bits	Anwendungsstandard
30		Verifikation von Zertifikaten, OCSP Antworten und OCSP Zertifikate: nonQES RSASSA-PKCS1-v1_5 mit Hashfunktion SHA-256 und ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2) auf brainpoolP256r1	[RFC 8017] (PKCS#1) [TR-03111] (ECDSA) [FIPS 180-4] (SHA) [AVA_CCA], sec. 2.27	2048bit für RSA Für ECDSA: Schlüsselgröße entsprechend der benutzten elliptischen Kurve brainpoolP256r1 ([RFC 5639])	[gemSpec_Krypt], Kap. 3.12
31		Verifikation von TSL.xml ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2) und RSASSA-PSS mit Hashfunktion SHA-256	[RFC 8017] (PKCS#1) [FIPS 180-4] (SHA) [TR-03111] (ECDSA) [AVA_CCA], sec. 2.27	2048bit für RSA Für ECDSA: Schlüsselgröße entsprechend der benutzten elliptischen Kurve brainpoolP256r1 ([RFC 5639])	[gemSpec_Krypt], Kap. 3.1.1
32		Verifikation von BNetzA-VL.xml RSASSA-PKCS1-v1_5 mit Hashfunktionen SHA-{256,384,512} und RSASSA-PSS mit Hashfunktionen SHA-{256,384,512} und SHA3-{256,384,512} und ECDSA mit Hashfunktionen SHA-{256,384,512}	[RFC 8017] (PKCS#1) [TR-03111] (ECDSA) [FIPS 180-4] (SHA) [FIPS 202] (SHA-3) [AVA_CCA], sec. 2.27	32768 bit >= Schlüssellänge >= 1900 bit für RSA Für ECDSA: Schlüsselgröße entsprechend der benutzten elliptischen Kurven brainpoolP{256,384,512}r1 ([RFC 5639]) NIST P-{256,384,521} ([FIPS 186-4]) FRP256v1 [ANSSI-0241]	[gemSpec_PKI], Kap. 8.5.2 [ETSI_TS_119_612]
33	Vertraulichkeit mit Nachrichtenauthentizität (Authenticated Encryption)	Hybride Dokumentver- und –Entschlüsselung (XML, MIME, CMS) mit RSAES-OAEP und Verwendung von AES-GCM	[FIPS 197] (AES) [SP 800-38D] (AES GCM) [RFC 8017] (RSAOAEP) [XMLEnc] (XML) [RFC 5751] (S/MIME) [RFC 5083] (CMS) [RFC 5084] (AES-GCM in CMS)	RSA ENC: 2048 bit (RSAOAEP) AES-GCM-ENC: 256 bit AES-GCM-DEC: 128, 192, 256 bit	[gemSpec_Krypt], Kap. 3.1.4 und 3.6 [gemSpec_Krypt], Kap. 3.1.5 und 3.5

#	Zweck	Kryptographische Funktion	Implementierungsstandard	Schlüssellänge in Bits	Anwendungsstandard
			[RFC 5652] (CMS)		
34		Hybride Dokumenten Ver- und Entschlüsselung (XML, CMS) mit ECIES und AES-GCM für Dokumenten Ver- und Entschlüsselung	[gemSpec_COS] Kap. 6.8.1.4 (ECIES) [RFC-5639] (brainpool) [FIPS 197] (AES) [SP 800-38D] (AES GCM) [XMLEnc] (XML) [RFC-5652] (CMS)	ECC: Schlüssellänge entsprechend der verwendeten elliptischen Kurve brainpoolP256r1 ([RFC5639]) AES-GCM-ENC: 256 Bit AES-GCM-DEC: 128, 192, 256 Bit	[gemSpec_Krypt], Kap. 5.7
35	Schlüsselgenerierung	AES Schlüsselgenerierung für hybride Verschlüsselung durch Verwendung eines sicheren Zufallszahlengenerators	[SP 800-133], Kap. 6.1 (Schlüsselgenerierung)	256	[gemSpec_Krypt], Kap. 3.1.5 und 3.5

Update und Backup

#	Zweck	Kryptographische Funktion	Implementierungsstandard	Schlüssellänge in Bits	Sicherheitsniveau mehr als 100 Bit	Bemerkungen
36	Authentizität	RSA Signaturverifikation mit RSASSA-PKCS1-v1_5 mit SHA-256	[RFC 8017] (RSASSA-PKCS1-v1_5), [FIPS 180-4] (SHA)	2048 bit	Ja	Firmwareupdate Signaturverifikation FDP_UIT.1/NK.Update
37		RSA Signaturverifikation mit RSASSA-PSS mit SHA-256	[RFC 8017] (RSASSA-PSS), [FIPS 180-4] (SHA)	2048 bit	Ja	UpdateInfo.xml und FirmwareGroupInfo.xml Signaturverifikation FDP_UIT.1/NK.Update
38	Vertraulichkeit mit Nachrichtenauthentizität (Authenticated Encryption)	Backup Passwortgenerierung mit sicherem Zufallszahlengenerator	[RISE-KON-TDS], Kap. 5.9.4.3.5	Passwortlänge 20, 90 Zeichen	Ja	FMT_MTD.1/ AK.eHKT_Abf
39		Verschlüsselung mit AES-GCM mit von dem Passwort abgeleitetem Schlüssel gemäß PBKDF2	[SP 800-38D] (AES-GCM) [RFC 2898] (PBKDF2)	256bit	Ja	FMT_MTD.1/ AK.eHKT_Abf

Tabelle 3: kryptografische Funktionen des EVG