Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

BSI-DSZ-CC-0862-V2-2021

zu

POLYAS Core, Version 2.5.0

der

POLYAS 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-0862-V2-2021 (*)

Online-Wahlprodukt

POLYAS Core
Version 2.5.0

von	POLYAS GmbH
PP-Konformität:	Common Criteria Schutzprofil für Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte, Version 1.0, 18. April 2008, BSI-CC-PP-0037-2008
Funktionalität:	PP konform Common Criteria Teil 2 konform
Vertrauenswürdigkeit:	Common Criteria Teil 3 konform EAL 2 mit Zusatz von ALC_CMC.3, ALC_CMS.3, ALC_DVS.1 und ALC_LCD.1

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 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

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, 25. Juni 2021
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[1]
- BSI-Zertifizierungs- und - Anerkennungsverordnung[2]
- Besondere Gebührenverordnung BMI (BMIBGebV)[3]
- besondere Erlasse des Bundesministeriums des Innern
- die Norm DIN EN ISO/IEC 17065
- BSI-Zertifizierung: Verfahrensdokumentation zum Zertifizierungsprozess (CC-Produkte) [3]
- BSI Zertifizierung: Verfahrensdokumentation zu Anforderungen an Prüfstellen, deren Anerkennung und Lizenzierung (CC-Stellen) [3]
- Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria for Information Technology Security Evaluation/CC), Version 3.1 [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]

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

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

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

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 (CCRA)

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 POLYAS Core, Version 2.5.0 hat das Zertifizierungsverfahren beim BSI durchlaufen. Es handelt sich um eine Re-Zertifizierung basierend auf BSI-DSZ-CC-0862-2016. Für diese Evaluierung wurden bestimmte Ergebnisse aus dem Evaluierungsprozess BSI-DSZ-CC-0862-2016 wiederverwendet.

Die Evaluation des Produkts POLYAS Core, Version 2.5.0 wurde von der Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI) GmbH durchgeführt. Die Evaluierung wurde am 1. Juni 2021 abgeschlossen. Das Prüflabor Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI) GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[4].

Der Sponsor und Antragsteller ist: POLYAS GmbH.

Das Produkt wurde entwickelt von: POLYAS 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 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 25.06.2021, ist gültig bis 24.06.2026. Die Gültigkeit kann im Rahmen einer Re-Zertifizierung erneuert werden.

[4] Information Technology Security Evaluation Facility

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 POLYAS Core, Version 2.5.0 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[5]. Der Zertifizierungsreport kann ebenso in elektronischer Form von der oben angegebenen Internetadresse heruntergeladen werden.

[5] POLYAS GmbH
Marie-Calm Str. 1-5
34131 Kassel

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 Produkt POLYAS CORE, Version 2.5.0 zur Durchführung von Online-Wahlen (kurz: Online-Wahlprodukt) bestehend aus:

- POLYAS CORE Software
  - Urnen EVG (polyas-vote), Version 2.5.0
  - Wählerverzeichnis EVG (polyas-registry), Version 2.5.0
  - Validator EVG (polyas-validator), Version 2.5.0
  - Wahlvorstandsinterface EVG (polyas-management), Version 2.5.0
  - Gemeinsame Funktionsbibliothek aller EVG-Komponenten (polyas-common), Version 2.5.0
- POLYAS CORE Benutzerdokumentation
  - Handreichung für den Wähler, Version 1.4 [9]
  - Handreichung für den Wahlvorstand, Version 1.3 [10]
  - Handreichung für den Wahlveranstalter, Version 1.7 [11]

Entsprechend den Sicherheitsanforderungen ist POLYAS CORE, Version 2.5.0 geeignet, Vereinswahlen, Gremienwahlen – etwa in den Hochschulen, im Bildungs- und Forschungsbereich – und insbesondere nicht-politische Wahlen mit geringem Angriffspotential sicher auszuführen.

Die Stimmabgabe ist die zentrale Funktion wahrend der Wahldurchführung. Sie erfolgt aus der Ferne, über ein offenes Netzwerk und von einem Endgerät, das in der Lage ist, den gesamten Inhalt des Stimmzettels darzustellen und die Vorgaben des Wahlveranstalters für die Art der Darstellung, insb. die Reihenfolge der Wahlvorschläge, umzusetzen. Die abgegebenen Stimmen werden in der Urne auf dem Wahlserver gespeichert. Durch Stimmauszahlung aller abgegebenen Stimmen wird nach Wahlende auf dem Wahlserver das Ergebnis ermittelt und festgestellt.

POLYAS CORE, Version 2.5.0 ist, abweichend von, aber trotzdem konform mit dem zugrundeliegenden Schutzprofil BSI-CC-PP-0037 [8], nicht in clientseitige und serverseitige EVG-Komponenten unterteilt, sondern besteht nur aus serverseitigen EVG-Komponenten.

Der Wählerverzeichnis EVG verwaltet die Wahlberechtigungsliste, der Validator EVG dient als Kontrollinstanz und der serverseitige Urnen EVG speichert die abgegebenen Stimmen. Der Wahlvorstandsinterface EVG wird für den Remote-Zugriff durch den Wahlvorstand und zur Auszählung der Stimmen benötigt, auf den der Wahlvorstand über ein Endgerät zugreift. An einem weiteren Endgerät führt der Wähler die Wahlhandlung aus, um seine Stimme abzugeben.

Auf dem Endgerät (sowohl für den Wähler als auch den Wahlvorstand) ist keine spezifische Software auszuführen. Ein clientseitiger EVG auf dem Endgerät existiert damit nicht und der komplette Funktionsumfang wird vom serverseitigen EVG zur Verfügung gestellt.

Die Sicherheitsvorgaben [6] stellen die Grundlage für die Zertifizierung dar. Sie basieren auf dem zertifizierten Protection Profile [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 2 mit Zusatz von ALC_CMC.3, ALC_CMS.3, ALC_DVS.1 und ALC_LCD.1.

Die funktionalen Sicherheitsanforderungen (Security Functional Requirements SFR) an den EVG werden in den Sicherheitsvorgaben [6], Kapitel 5.1 beschrieben. Sie wurden komplett dem Teil der Common Criteria entnommen. Der EVG ist daher konform zum Teil 2 der Common Criteria.

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

Sicherheits-funktionalität des EVG	**Thema**
FAU_GEN.1	Der EVG protokolliert pro Teilsystem die in FAU_GEN.1 aufgeführten Ereignisse in einer jeweils separaten Logdatei.
FAU_SAR.1	Im Wahlvorstandsinterface können die Protokolldateien vom Wahlvorstand in verständlicher und lesbarer Form eingesehen werden.
FDP_DAU.1	Im Rahmen der Auszählung/Archivierung wird eine Archivprüfsumme als Manipulationsschutz erzeugt.
FDP_IFC.1A	Diese funktionale Anforderung wird durch den Ablauf zur Wahlhandlung realisiert: Die TSF realisieren die Wahlhandlung so, dass die funktionalen Anforderungen umgesetzt werden.
FDP_IFF.1A	Diese funktionale Anforderung stellt die Verwendung der Wahlattribute (zur Stimmberechtigung, Wahlhandlung etc.) während der Wahlhandlung
FDP_IFC.1B	Diese funktionale Anforderung wird durch den Ablauf bzgl. der Aktivitäten des Wahlvorstands realisiert – insb. durch Separation of Duty.
FDP_IFF.1B	Diese funktionale Anforderung stellt die Verwendung der Sicherheitsattribute zum Ablauf der Aktivitäten des Wahlvorstands sicher.
FDP_IFF.5	Diese funktionale Anforderung wird durch den Ablauf zur Wahlhandlung und bzgl. der Aktivitäten des Wahlvorstands realisiert.
FDP_SDI.2	Datenintegritätsfehler lösen im EVG Fehlermeldungen aus, die protokolliert und per E-Mail an den Wahlvorstand gemeldet werden.
FDP_RIP.1A und FDP_RIP.1B	Der Zwischenspeicher verwaltet die Stimme während des Wahlvorgangs eines Wählers im Arbeitsspeicher der Anwendung, welcher bei Abbruch der Wahlhandlung vor Einleitung der endgültigen Abgabe sowie bei der endgültigen Abgabe aktiv aus diesem entfernt wird. Hierbei geht die Zuordnung von Wählertoken und Stimme verloren. Darüber hinaus werden die Datenbanken der Urne, des Wählerverzeichnisses und des Validators beim Wahlstart – nicht jedoch beim Wiederanlauf – zurückgesetzt, und es wird der Zwischenspeicher vor der Verwendung bereinigt, damit dem Wähler ein leerer Stimmzettel angezeigt wird.
FDP_UCT.1A und FDP_UCT.1B	Der EVG stellt sicher, dass eine Kommunikation nur mittels https mit TLS-Zertifikaten gesichert erfolgt.
FDP_UIT.1A und	Der EVG stellt sicher, dass eine Kommunikation nur mittels https mit TLS-Zertifikaten

Sicherheits-funktionalität des EVG	Thema
FDP_UIT.1B	gesichert erfolgt. Der EVG stellt auch beim Empfang sicher, dass die Kommunikation nur mittels https mit TLS-Zertifikaten gesichert erfolgt. Sofern die verschlüsselte Kommunikation dies überhaupt zulässt, wird darüber hinaus durch das Protokoll sichergestellt, dass ein Löschen, Einfügen oder Wiedereinspielen von Nachrichten festgestellt wird.
FIA_ATD.1	Stimmberechtigungs- und Wahlhandlungsattribut werden mit Eröffnung jeder Wahlhandlung erzeugt, mit dem Wähler verbunden und bei Abbruch bzw. Ende der Wahlhandlung gelöscht.
FIA_UAU.1/.2 und FIA_UID.1/.2	Diese funktionale Anforderung wird durch den Ablauf zur Wahlhandlung bzw. bzgl. der Aktivitäten des Wahlvorstands realisiert.
FIA_UAU.6	Für jede der für SFP für Online-Wahlen kontrollierten Operation – dies gilt insb. für den Wahlstart, den Wahlstopp, die Auszählung sowie den Wahlwiederanlauf – wird sichergestellt, dass eine hinreichende Anzahl von Autorisierungen des Wahlvorstands vorliegt. Der Wahlvorstand muss sich dazu jeweils (neu) authentisieren.
FIA_USB.1A	Diese funktionale Anforderung wird durch den Ablauf zur Wahlhandlung realisiert, insofern als dass bei Eröffnung der Wahlhandlung das Stimmberechtigungsattribut den Wert „unbekannt“ und das Wahlhandlungsattribut den Wert „vor“ erhält.
FIA_USB.1B	Diese funktionale Anforderung wird durch den Ablauf bzgl. der Aktivitäten des Wahlvorstands realisiert, insb. durch die Separation of Duty.
FMT_SMR.2	Der EVG agiert nur mit zwei Rollen: die Rollen Wähler und Wahlvorstand sind von den Funktionen her strikt getrennt, so dass es keine Verknüpfung gibt.
FPR_ANO.1	Diese funktionale Anforderung wird durch den Ablauf zur Wahlhandlung implizit realisiert: Die Wahlberechtigungsliste (Wählerverzeichnis), welche die Identität der Wähler kennt, und die Wahlurne, die die Stimmen der Wähler speichert, sind getrennte Instanzen.
FPR_UNL.1A	Die Kommunikation zwischen Wähler und Wahlurne ist verschlüsselt, so dass nur der eigentliche Wähler Zugriff nehmen kann. Die Stimme selbst wird wiederum verschlüsselt und gemeinsam mit einem zufälligen Wert gespeichert.
FPR_UNL.1B	Die Stimmen werden bei der Abgabe nicht mit einem Zeitstempel versehen. Da in der Wahlberechtigungsliste (Wählerverzeichnis) keine Informationen zum Zeitpunkt oder der Reihenfolge der Stimmabgabe in irgendeiner Form gespeichert werden, ist eine nachträgliche Zuordnung der Stimme zum Wähler nicht mehr möglich.
FPT_ITT.1	Der EVG stellt sicher, dass eine Kommunikation nur mittels https mit TLS-Zertifikaten gesichert erfolgt.
FPT_RCV.1 und FPT_RCV.4	Nach einer Unterbrechung der Wahldurchführung durch Absturz/ Herunterfahren oder durch Ausfall der Kommunikation oder der Speichermedien wird ein Erhaltungsmodus realisiert.
FPT_TST.1	Beim Wahlstart laufen die Selbsttests automatisch ab. Das Ergebnis der Selbsttests ist im Wahlvorstandsinterface einsehbar. Darüber hinaus kann er manuelle Selbsttests durchführen.
FTA_SSL.3	Über einen konfigurierbaren Parameter der Wahlserver wird erreicht, dass eine Wahlhandlung nach einer konfigurierbaren Frist abgebrochen wird.

Sicherheits-funktionalität des EVG	Thema
FTA_SSL.4	Diese funktionale Anforderung wird durch den Ablauf zur Wahlhandlung realisiert. Insbesondere wird dem Wähler bei der Kandidatenauswahl und Bestätigung der Stimmabgabe ein Logout-Button dargestellt, über den sich der Wähler abmelden kann.
FTA_TSE.1	Diese funktionale Anforderung wird durch den Ablauf zur Wahlhandlung implizit realisiert, d.h. die Systeme müssen gestartet und dürfen nicht gestoppt sein, damit eine Wahlhandlung eröffnet werden kann.
FTP_TRP.1A und FTP_TRP.1B	Der EVG stellt sicher, dass eine Kommunikation nur mittels https mit TLS-Zertifikaten gesichert erfolgt.

Tabelle 1: Sicherheitsfunktionalität des EVG

Mehr Details sind in den Sicherheitsvorgaben [6], Kapitel 6 dargestellt.

Die Werte, die durch den EVG geschützt werden, sind in den Sicherheitsvorgaben [6], Kapitel 3, definiert. Basierend auf diesen Werten stellen die Sicherheitsvorgaben die Sicherheitsumgebung in Form von Annahmen, Bedrohungen und organisatorischen Sicherheitspolitiken in Kapitel 3.1, 3.2 und 3.3 dar.

Dieses Zertifikat umfasst die folgenden Konfigurationen des EVG:

Die evaluierte Konfiguration des EVG POLYAS Core Version 2.5.0 beinhaltet IT-Komponenten (Software) und Benutzerdokumentation.

Die Software besteht aus fünf JAR-Dateien (Java Archiven). Jede JAR-Datei wird über die eindeutige Version 2.5.0 des EVG, den Dateinamen und die Prüfsumme (SHA-256) der Datei eindeutig identifiziert:

- Urnen EVG

  polyas-vote-2.5.0.jar mit Prüfsumme:

  E96BB2C12F8CA1EC959947FE960E0AE0BEC2598283D92D2BB8CDA951AB43050B

- Wählerverzeichnis EVG

  polyas-registry-2.5.0.jar mit Prüfsumme:

  212CD26A665501D98300A56BD72C761FD0BBE6B874527808A57AAE67212DB928

- Validator EVG

  polyas-validator-2.5.0.jar mit Prüfsumme:

  000AB52331DB0702EB72215DE3CF207F175B7320E345BDBFBF0AE17FCD291B52

- Wahlvorstandsinterface EVG

  polyas-management-2.5.0.jar mit Prüfsumme:

  2F8658FC1F026FB3D5EDACB5C861704CA72E31C8A3A73522F1EAFA54E573304A

- Gemeinsamer Bestandteil

  polyas-common-2.5.0.jar mit Prüfsumme:

  8BFAFFA3AE7DC2EAAD4B872A67D35D3FD1F37B0F2E5C37E6D9E8D74B894079DE

Die Benutzerdokumentation besteht aus verschiedenen PDF-Dateien, die über den Titel und die Version eindeutig identifiziert sind:

- Handreichung für den Wähler, Version 1.4 [9]
- Handreichung für den Wahlvorstand, Version 1.3 [10]
- Handreichung für den Wahlveranstalter, Version 1.7 [11]

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

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

2. Identifikation des EVG

Der Evaluierungsgegenstand (EVG) heißt

POLYAS Core, Version 2.5.0

Die folgende Tabelle beschreibt den Auslieferungsumfang:

Nr	Typ	Identifier	Version / SHA-256-Prüfsumme	Auslieferungsart
1	SW	polyas-vote-2.5.0.jar	E96BB2C12F8CA1EC959947FE960E0AE0BEC2598283D92D2BB8CDA951AB43050B	Eingebettet in WAR-Datei polyas-vote-web-2.5.0-KUNDENNAME.war (s. lfd. Nr. 9)
2	SW	polyas-registry-2.5.0.jar	212CD26A665501D98300A56BD72C761FD0BBE6B874527808A57AAE67212DB928	Eingebettet in WAR-Datei polyas-registry-web-2.5.0-KUNDENNAME.war (s. lfd. Nr. 10)
3	SW	polyas-validator-2.5.0.jar	000AB52331DB0702EB72215DE3CF207F175B7320E345BDBFBF0AE17FCD291B52	Eingebettet in WAR-Datei polyas-validator-web-2.5.0-KUNDENNAME.war (s. lfd. Nr. 11)
4	SW	polyas-management-2.5.0.jar	2F8658FC1F026FB3D5EDACB5C861704CA72E31C8A3A73522F1EAFA54E573304A	Eingebettet in WAR-Datei polyas-management-gui-2.5.0- KUNDENNAME.war (s. lfd. Nr. 12)
5	SW	polyas-common-2.5.0.jar	8BFAFFA3AE7DC2EAAD4B872A67D35D3FD1F37B0F2E5C37E6D9E8D74B894079DE	Eingebettet in jede WAR-Datei (s. lfd. Nr. 9, 10, 11, 12)
6	DOC	Benutzerdokumentation POLYAS CORE 2.5.0 Handreichung Wähler [9]	1.4	Elektronische Auslieferung

Nr	Typ	Identifier	Version / SHA-256-Prüfsumme	Auslieferungsart
7	DOC	Benutzerdokumentation POLYAS CORE 2.5.0 Handreichung Wahlvorstand [10]	1.3	Elektronische Auslieferung
8	DOC	Benutzerdokumentation POLYAS CORE 2.5.0 Handreichung Wahlveranstalter [11]	1.7	Elektronische Auslieferung
9	SW (non-TOE)	Wahlurne polyas-vote-web-2.5.0-KUNDENNAME.war vote.sql	n/a	Elektronische Auslieferung
10	SW (non-TOE)	Wählerverzeichnis polyas-registry-web-2.5.0-KUNDENNAME.war registry.sql	n/a	Elektronische Auslieferung
11	SW (non-TOE)	Validator polyas-validator-web-2.5.0-KUNDENNAME.war validator.sql	n/a	Elektronische Auslieferung
12	SW (non-TOE)	Wahladministration polyas-management-gui-2.5.0-KUNDENNAME.war management.sql	n/a	Elektronische Auslieferung
13	SW (non-TOE)	Java-Bibliothek (Vorbereitung) polyas-registry-admin-2.5.0.jar	n/a	Elektronische Auslieferung
14	SW (non-TOE)	Java-Bibliothek (Vorbereitung) polyas-validator-admin-2.5.0.jar	n/a	Elektronische Auslieferung
15	SW (non-TOE)	Java-Bibliothek (Vorbereitung) polyas-management-admin-2.5.0.jar	n/a	Elektronische Auslieferung

Nr	Typ	Identifier	Version / SHA-256-Prüfsumme	Auslieferungsart
16	SW config (non-TOE)	Konfigurationsdateien – Muster für EVG und WWW-Server vote.xml registry.xml validator.xml management.xml server.xml	n/a	Elektronische Auslieferung

Tabelle 2: Auslieferungsumfang des EVG

Die Software-Teile des EVG (JAR-Dateien) sind zusammen mit der umgebenden WWW-Applikation in WAR-Dateien eingebettet. Die WAR-Dateien werden zusammen mit der Benutzerdokumentation des EVG und allen anderen Bestandteilen der Auslieferung auf elektronischem Weg an den Wahlveranstalter ausgeliefert.

Eine Auslieferung an Wähler oder Wahlvorstand findet nicht statt, denn Benutzer in diesen Rollen können den EVG aus der Ferne über einen WWW-Browser verwenden.

Der Umfang der Übergabe an einen Wahlveranstalter hängt vom Betriebsmodus beim Wahlveranstalter ab. Für diesen gibt es folgende Möglichkeiten:

- Der Wahlveranstalter betreibt POLYAS eigenständig:
  Die Übergabe beinhaltet alle Auslieferungsgegenstände.
- Der Wahlveranstalter und Polyas GmbH betreiben POLYAS gemeinsam, d.h. der Wahlveranstalter betreibt nur das Wählerverzeichnis:
  Die Übergabe beinhaltet die Benutzerdokumentation (Nr. 6, 7, 8) und die für Vorbereitung und Betrieb des Wählerverzeichnisses benötigten Auslieferungsgegenstände (Nr. 2, 5, 10 und 13-16).
- Polyas GmbH betreibt POLYAS als Dienstleistung für den Wahlveranstalter:
  Die Übergabe beinhaltet nur die Benutzerdokumentation (Nr. 6, 7, 8).

Für den Transport werden alle Bestandteile der Auslieferung entweder auf einem Datenträger verschickt oder über einen WebDAV-Server zum download bereitgestellt.

Um die Integrität und Authentizität der Auslieferung sicherzustellen, werden die ausgelieferten Dateien verschlüsselt (AES-256). Das für die Entschlüsselung benötigte Kennwort wird dem Wahlveranstalter telefonisch mitgeteilt.

Um die Integrität der ausgelieferten Software des EVG sicherzustellen, werden Prüfsummen (SHA-256) über die JAR-Dateien (EVG-Bestandteile) gebildet. Die Prüfsummen werden dem Wahlveranstalter telefonisch mitgeteilt, auch wenn POLYAS nur teilweise oder gar nicht vom Wahlveranstalter betrieben wird. Sie sind ebenfalls diesen Report zu entnehmen. Die Kontrolle der Prüfsummen erfolgt durch den Wahlveranstalter.

Die Identifizierung der Benutzerdokumentation erfolgt durch die Bezeichnungen und die Versionsnummern der Handreichungen, wie in der obigen Übersicht (Nr. 6-8) angegeben.

Die Identifizierung der Software durch den Wahlveranstalter erfolgt über die Bezeichnungen und die Prüfsummen der JAR-Dateien, wie in der obigen Übersicht (Nr. 1-5) angegeben.

Die Identifizierung der Software durch den Wähler bzw. den Wahlvorstand erfolgt über die ständige Anzeige des Verweisnamens (POLYAS Core, Version 2.5.0) und die Prüfsummen der JAR-Dateien im Browser.

3. Sicherheitspolitik

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

Die generellen Sicherheitserwartungen an ein Produkt zur Durchführung von Online-Wahlen werden von den allgemeinen Wahlrechtsgrundsätzen (frei, gleich, geheim, allgemein und unmittelbar) abgeleitet, wobei der Grundsatz der unmittelbaren Wahl unberücksichtigt bleibt. Sie lassen sich wie folgt zusammenfassen:

- Eine Zusammenführung der Identität des Wählers mit seiner abgegebenen Stimme darf nicht hergestellt werden können. (Anonymität: geheime und freie Wahl).
- Der EVG darf dem Wähler nicht die Möglichkeit geben, seine Wahlentscheidung gegenüber anderen zu beweisen (Quittungsfreiheit: geheime und freie Wahl).
- Eine eindeutige und zuverlässige Identifikation und Authentisierung der Wähler muss sicherstellen, dass nur registrierte Wähler eine Stimme abgeben dürfen. (Authentisierung: allgemeine und gleiche Wahl).
- Jeder Wähler darf nur einmal eine Stimme abgeben. (One voter – one vote: gleiche Wahl).
- Es darf bei der Übertragung im Netzwerk nicht möglich sein, Stimmdatensätze unbemerkt zu verändern, zu löschen oder hinzuzufügen (Integrität des Netzwerks: allgemeine und gleiche Wahl).
- Es darf in der Urne nicht möglich sein, unbemerkt Stimmen zu verändern, unbemerkt Stimmen zu löschen oder unberechtigt Stimmen hinzuzufügen (Integrität der Urne: allgemeine und gleiche Wahl).
- Die Berechnung von Zwischenergebnissen muss ausgeschlossen werden (Zugriffskontrolle: geheime und gleiche Wahl).

Die spezifischen Sicherheitspolitiken sind durch die ausgewählte Zusammenstellung der Sicherheitsanforderungen an die Funktionalität definiert und werden vom EVG implementiert. Sie bestehen aus folgenden Anteilen:

- Informationsflusskontrollpolitik für Wahlhandlungen (FDP_IFC.1A, FDP_IFF.1A, FDP_IFF.5, FDP_RIP.1A, FDP_UCT.1A, FDP_UIT.1A, FTP_TRP.1A,) zur Definition und Kontrolle der Transaktionen in der Rolle Wähler;
- Informationsflusskontrollpolitik für Wahldurchführung inkl. Stimmauszählung (FDP_DAU.1, FDP_IFC.1B, FDP_IFF.1B, FDP_IFF.5, FDP_RIP.1B, FDP_UCT.1B, FDP_UIT.1B, FTP_TRP.1B,) zur Definition und Kontrolle der Transaktionen in der Rolle Wahlvorstand;
- Identifikation (FIA_UID.1/.2) und Authentisierung (FIA_UAU.1/.2/.6) der Benutzer in den Rollen Wähler und Wahlvorstand (FMT_SMR.2) sowie die damit zusammenhängende Verwaltung von kontrollierten Subjekten (FIA_ATD.1, FIA_USB.1A/.1B) und Sitzungen (FTA_SSL.3/.4, FTA_TSE.1);

- Trennung der Identität von der Stimme des Wählers (FPR_ANO.1, FPR_UNL.1A FPR_UNL.1B);
- Robustheit ggü. störenden äußeren Einflüssen (FDP_SDI.2, FPT_ITT.1, FPT_RCV.1, FPT_RCV.4, FPT_TST.1);
- Protokollierung sicherheitsrelevanter Ereignisse (FAU_GEN.1) und Durchsicht der Protokolldaten (FAU_SAR.1).

Weitere Details der EVG-Sicherheitspolitiken sind in den Abschnitten 5.1 und 6 des Security Target [6] dargelegt.

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:

Sicherheitsziel für die Einsatzumgebung	**Art der Maßnahmen**	**Sicherheitsmaßnahmen mit Bezug zur Benutzerdokumentation**
OE.Wahlvorbereitung	technisch organisatorisch	Die technischen Aspekte dieses Sicherheitsziels, d.h. die Vorbereitung der Wahlserver, die Installation der Wahldaten (Stimmzettel und Wählerverzeichnis) und die Konfiguration und Installation des serverseitigen EVG, werden von den einzelnen Schritten der Installation des EVG und der Vorbereitung der Einsatzumgebung, wie in der Handreichung Wahlveranstalter beschrieben, angemessen adressiert. Die organisatorischen Aspekte dieses Sicherheitsziels, d.h. die Festlegung und Bekanntgabe von Zeitplänen für die Phasen der Online-Wahl, die Vermeidung von Konflikten mit anderen Wahlformen (Präsenzwahl, Briefwahl) und die Registrierung der Wähler sind für die EVG-Sicherheitsfunktionalität nicht von Bedeutung.
OE.Beobachten	organisatorisch	Die Handreichung Wähler beschreibt angemessene Sicherheitsmaßnahmen für die unbeobachtete Stimmabgabe.
OE.Wahlvorstand	materiell technisch organisatorisch	Die Aspekte für den Zugang/Zugriff auf den EVG bzw. die Server werden im Rahmen der Vorbereitung der Serverinfrastruktur und der Erzeugung der Schlüssel und Zugangsdaten, wie in der Handreichung Wahlveranstalter beschrieben, angemessen adressiert. Die Handreichung Wahlveranstalter beschreibt angemessene Sicherheitsmaßnahmen für die Überwachung der Verfügbarkeit von Netzwerk bzw. Server durch den Wahlvorstand. Die Handreichung Wahlvorstand beschreibt angemessene Sicherheitsmaßnahmen (Verpflichtungen) ● für den alleinigen Zugriff auf die Benutzer- und

Sicherheitsziel für die Einsatzumgebung	Art der Maßnahmen	Sicherheitsmaßnahmen mit Bezug zur Benutzerdokumentation
		TSF-Daten unter Verwendung der EVG-Funktionalität; ● für die Schulung zum sicheren Betrieb und zum beabsichtigten Gebrauch des EVG; ● für den Schutz der Identifikationsdaten und Authentisierungsmerkmale; und ● auf welche Weise der Wahlvorstand seine Verantwortung für die Vertrauenswürdigkeit des Endgeräts wahrnehmen kann.
OE.AuthDaten	organisatorisch	Die Handreichung Wähler beschreibt angemessene Sicherheitsmaßnahmen für den Schutz der Identifikationsdaten und Authentisierungsmerkmale.
OE.Endgerät	materiell technisch organisatorisch	Die Handreichung Wähler beschreibt angemessene Sicherheitsmaßnahmen, auf welche Weise der Wähler seine Verantwortung für die Vertrauenswürdigkeit des Endgeräts wahrnehmen kann.
OE.Wahlserver	materiell technisch organisatorisch	Die Sicherung der Wahlserver wird im Rahmen der Vorbereitung der Serverinfrastruktur und der Erzeugung der Schlüssel und Zugangsdaten, wie in der Handreichung Wahlveranstalter beschrieben, angemessen adressiert.
OE.Verfügbarkeit	—	Maßnahmen zur Gewährleistung der Verfügbarkeit des Netzwerks und der Wahlserver sind für die EVG-Sicherheitsfunktionalität nicht von Bedeutung. Relevante organisatorische Hinweise zur Beachtung durch den Wahlvorstand sind im Zusammenhang mit dem Sicherheitsziel OE.Wahlvorstand berücksichtigt.
OE.Serverraum	materiell organisatorisch	Die Handreichung Wahlveranstalter beschreibt angemessene Sicherheitsmaßnahmen für die Beschränkung des Zutritts/Zugangs zu den Wahlservern.
OE.Speicherung	technisch organisatorisch	Die Handreichung Wahlveranstalter enthält angemessene Hinweise auf die Meldung von Fehlern bei der Speicherung im Wahlsystem.
OE.Systemzeit	technisch organisatorisch	Die Handreichung Wahlveranstalter enthält angemessene Hinweise für die Festlegung der Genauigkeit der Systemzeit.
OE.Protokollschutz	technisch	Die Handreichung Wahlveranstalter enthält angemessene Hinweise auf die geschützte Speicherung der Protokolldaten durch die Wahlserver.

Sicherheitsziel für die Einsatzumgebung	Art der Maßnahmen	Sicherheitsmaßnahmen mit Bezug zur Benutzerdokumentation
OE.AuthentizitätServer	technisch organisatorisch	Die Handreichung Wähler beschreibt angemessene Sicherheitsmaßnahmen für die Kontrolle der Authentizität des Wählerverzeichnisses und der Urne. Die Handreichung Wahlvorstand beschreibt angemessene Sicherheitsmaßnahmen für die Kontrolle der Authentizität der Wahladministration.
OE.ArchivierungIntegrität	technisch organisatorisch	Die Handreichung Wahlveranstalter enthält angemessene Hinweise auf die Erzeugung eines Manipulationsschutzes für die archivierten Daten.
OE.GeschützteKommunikation	technisch	Die Handreichung Wahlveranstalter enthält angemessene Hinweise auf die Fähigkeiten für den Betrieb einer geschützten Kommunikationsverbindung. Die entsprechende Konfiguration wird im Rahmen der Erzeugung der Schlüssel angemessen adressiert.
OE.Zwischenspeicherung	technisch organisatorisch	Die Handreichung Wähler beschreibt angemessene Sicherheitsmaßnahmen zur Löschung der privaten Daten des Browsers nach dem Ende der Wahlhandlung. Sie enthält auch eine angemessene Empfehlung zur Vermeidung der Speicherung privater Daten durch Verwendung eines privaten Betriebsmodus, sofern der Browser einen solchen Modus anbietet.

Tabelle 3: Sicherheitsziele für die EVG-Einsatzumgebung

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

5. Informationen zur Architektur

Der EVG besteht aus vier Teilsystemen:

- S1 – Wählerverzeichnis
- S2 – Validator
- S3 – Urne
- S4 – Wahlvorstandsinterface

Die drei Teilsysteme S1, S2 und S3 sollen jeweils auf einem eigenen System (Wahlserver) betrieben werden, während das Teilsystem S4 auf einem der anderen drei Wahlserver oder einem separaten Wahlserver betrieben werden kann. Auf jedem Wahlserver sind die von dem jeweiligen Teilsystem benötigten Datenbanken lokal bereitzustellen.

Die Benutzer greifen über das Internet von einem Endgerät mit einem Browser auf den EVG zu (vergleiche Abb. 1 in den Sicherheitsvorgaben [6]):

- Benutzer in der Rolle Wähler greifen auf S1 (Wählerverzeichnis) und S3 (Urne) zu;
- Benutzer in der Rolle Wahlvorstand greifen auf S4 (Wahlvorstandsinterface) zu.

Die Schnittstellen der Teilsysteme zu den Benutzern entsprechen den TSF-Schnittstellen. Darüber hinaus benutzen die Teilsysteme des EVG Schnittstellen der Laufzeitumgebung, d.h. zur jeweiligen Datenbank, zum jeweiligen Betriebssystem und zum Mail-Server.

Die Trennung der Teilsysteme und die Transaktionsprotokolle gewährleisten in Verbindung mit der Rollentrennung, dass die Informationsflusskontrollpolitiken für Wahlhandlungen und Wahldurchführung inkl. Stimmauszählung und damit die Trennung der Identität von der Stimme der Wählers wirksam durchgesetzt werden.

6. Dokumentation

Die evaluierte Dokumentation, die in Tabelle 2 aufgeführt ist, wird zusammen mit dem Produkt zur Verfügung gestellt. Hier sind die Informationen enthalten, die zum sicheren Umgang mit dem EVG in Übereinstimmung mit den Sicherheitsvorgaben benötigt werden.

Zusätzliche Hinweise und Auflagen zum sicheren Gebrauch des EVG, die im Kapitel 10 enthalten sind, müssen befolgt werden.

7. Testverfahren

7.1. Testkonfiguration

Die Testkonfiguration, mit der der Entwickler den EVG getestet hat, entspricht der evaluierten Konfiguration und besteht aus folgenden Komponenten:

- Betriebssystem (Linux): Debian 10.9
- Java Laufzeitumgebung (JDK-11): openjdk 11.0.11
- Software build management: Apache Maven 3.6.3
- Docker engine (server) 19.03.12
- Datenbanksystem: PostgreSQL 11.12
- WWW Application Server: Apache Tomcat 9.0.41
- PostgreSQL JDBC driver 42.2.14
- JavaMail API 1.4
- SMTP Server greenmail 1.6.2

Als Plattform für die unabhängigen Tests der Prüfstelle sind drei Server (Hardware) mit integrierter Festplatte und dort installiertem Betriebs-, Datei- und Datenbanksystem verwendet worden, um einen materiell getrennten Betrieb von Wählerverzeichnis, Validator und Urne zu ermöglichen.

Die für die Tests verwendete Laufzeitumgebung des EVG besteht aus folgenden Komponenten:

- Betriebssystem (Linux): Debian 10.7 (Codename Buster)
- Datenbanksystem (PostgeSQL 11): postgresql-11 11.9-0+deb10u1 (Debian Paket)
- Java Laufzeitumgebung: OpenJDK SE 11
- WWW-Server: Apache Tomcat 9.0.39
- JDBC-Treiber (Teil der Auslieferung): PostgreSQL JDBC Driver 42.2.14

- Java Mail API (Teil der Auslieferung): JavaMail API (compat) 1.4.7
- E-Mail Server Exim (v4): exim4-daemon-light 4.92-8+deb10u4 (Debian Paket)

Diese Laufzeitumgebung entspricht der vorgesehenen Laufzeitumgebung, wie in der Handreichung für den Wahlveranstalter beschrieben.

7.2. Funktionale Entwicklertests

Der Entwickler hat 21 Testszenarios in drei Gruppen ausgearbeitet.

Die Testszenarien und der Testablauf sind auf die Transaktionen der Benutzer in den Rollen Wähler und Wahlvorstand ausgerichtet. Sie umfassen sowohl den eigentlichen Zweck jeder Transaktion als auch deren Randbedingungen (Sitzungen und ihr Ablauf) und Seiteneffekte (Protokollierung, Zwischenspeicherung).

Die Testergebnisse entsprachen in allen Fällen den Erwartungen und ergeben keine Hinweise auf eine fehlerhafte Implementierung der TSF.

7.3. Unabhängige Evaluatortests

Zur Ergänzung der Entwicklertests hat der Evaluator 12 Testszenarios ausgearbeitet. Damit wird die Abdeckung der SFR-Komponenten durch Tests verbessert sowie die Existenz und ggf. Ausnutzbarkeit von potentiellen Schwachstellen überprüft.

Die Tests des Evaluators betrachten auch Wechselwirkungen von Randbedingungen und Seiteneffekten bei nebenläufig ausgeführten Transaktionen.

Von der Prüfstelle sind die Tests aus allen 33 Szenarien ausgeführt worden. Für die Ausführung der Entwickler- und der Evaluatortests sind grundsätzlich die TSF-Schnittstellen verwendet worden. Für einige Tests sind zusätzlich die Konfiguration des WWW-Servers und/oder der Inhalt der Datenbanken von Wählerverzeichnis und Urne gezielt manipuliert worden.

Im Testverlauf ist kein fehlerhaftes Verhalten des EVG und kein fehlerhaftes Ergebnis beobachtet worden.

7.4. Schwachstellenanalyse

Der Evaluator hat sowohl öffentlich verfügbare Quellen als auch die zur Verfügung stehende Herstellerdokumentation auf Hinweise für potentielle Schwachstellen durchsucht.

Ausgehend von der Analyse der Schwachstellen hat der Evaluator Penetrationstests ausgearbeitet.

Aus den Testergebnissen und der Analyse aller potentieller Schwachstellen ergeben sich keine Schwachstellen, die mit Angriffspotential Basic ausnutzbar wären.

8. Evaluierte Konfiguration

Dieses Zertifikat bezieht sich auf die folgenden Konfigurationen des EVG:

Der EVG kann nur in einer Konfiguration betrieben werden. Sie entspricht dem Gegenstand der Evaluierung und beinhaltet alle ausgelieferten Bestandteile des EVG (Nr. 1-8 in der Übersicht der Auslieferungsgegenstände).

Weitere evaluierte Konfigurationen ergeben sich insb. auch nicht bei teilweisem bzw. vollständigem Betrieb von POLYAS durch die Polyas GmbH.

Die Einbettung des EVG in die umgebende WWW-Applikation erfolgt außerhalb des EVG. Insbesondere gehört die umgebende WWW-Applikation nicht zum EVG. In jede kundenspezifische Anpassung der WWW-Applikation ist die evaluierte Konfiguration des EVG eingebettet.

Für den Betrieb der evaluierten Konfiguration des EVG wird die Java-Laufzeitumgebung OpenJDK 11.0.11 oder eine höhere Version benötigt. Die Verwendung einer voherigen OpenJDK-Version ist in der evaluierten Konfiguration nicht zulässig.

Dem Benutzer wird für die Anmeldung eine HTML-Seite mit Eingabefeldern für PIN/TAN (Wähler) bzw. Benutzername/Passwort (Wahlvorstand) präsentiert. Im Rahmen der Gestaltung der umgebenden WWW-Applikation besteht grundsätzlich die technische Möglichkeit, die Anmeldung durch eine erweiterte Funktionalität anders zu gestalten, etwa durch vorgelagerte Schritte zur Authentisierung mit anderen Mechanismen (SmartCards, Biometrie, Single-Sign-On, Personalausweis). Derartige Erweiterungen sind in der zertifizierten Konfiguration nicht zulässig.

Die Bereitstellung zusätzlicher Funktionen für den Wahlvorstand für die Phase „Wahldurchführung“, insbesondere und bspw. die zulässige Veränderung des Wählerverzeichnisses (Sperrung, Löschung, Ergänzung eines Wählers) aufgrund von Anforderungen der Wahlordnung, hat unabsehbare Folgen für die Wirksamkeit der Sicherheitsfunktionalität des EVG. Eine Veränderung der Funktionen für die Phase „Wahldurchführung“ ist in der zertifizierten Konfiguration nicht zulässig.

In der kundenspezifischen Gestaltung der WWW-Applikation ist grundsätzlich die Auswahl einzelner von mehreren Stimmzetteln durch den Wähler möglich, sofern dem Wähler mehrere Stimmzettel zugeordnet sind. Diese optionale Gestaltung ist in der zertifizierten Konfiguration nicht zulässig.

9. Ergebnis der Evaluierung

9.1. CC spezifische Ergebnisse

Der Evaluierungsbericht (Evaluation Technical Report, ETR) [7] wurde von der Prüfstelle gemäß den Gemeinsamen Kriterien [1], der Methodologie [2], den Anforderungen des Schemas [3] und allen Anwendungshinweisen und Interpretationen des Schemas (AIS) [4] erstellt, die für den EVG relevant sind.

Die Evaluierungsmethodologie CEM [2] wurde verwendet.

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

- Alle Komponenten der Vertrauenswürdigkeitsstufe EAL 2 der CC (siehe auch Teil C des Zertifizierungsreports)
- Die zusätzlichen Komponenten
  ALC_CMC.3, ALC_CMS.3, ALC_DVS.1 und ALC_LCD.1

Da die Evaluierung eine Re-Evaluierung zum Zertifikat BSI-DSZ-CC-0862-2016 darstellt, konnten bestimmte Evaluierungsergebnisse wiederverwendet werden. Die Re-Evaluierung der EVG Version 2.5.0 diente der Erneuerung des bestehenden Zertifikats für Version 2.2.3 und einer Prüfung des EVG nach aktuellem Stand der Technik. Diese Re-

Evaluierung konzentrierte sich insbesondere auf folgende Bereiche: Aktualisierung der evaluierten Konfiguration des EVG und der Konformität zu CC 3.1R5, Unterstützung für mehrere Stimmzettel pro Wähler, Aktualisierung der Schwachstellenanalyse, Aktualisierung der Lebenzyklusunterstützung.

Die Evaluierung hat gezeigt:

- PP Konformität: Common Criteria Schutzprofil für Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte, Version 1.0, 18. April 2008, BSI-CC-PP-0037-2008 [8]
- Funktionalität: PP konform
  Common Criteria Teil 2 konform
- Vertrauenswürdigkeit: Common Criteria Teil 3 konform
  EAL 2 mit Zusatz von ALC_CMC.3, ALC_CMS.3, ALC_DVS.1 und ALC_LCD.1

Die Ergebnisse der Evaluierung gelten nur für den EVG gemäß Kapitel 2 und für die Konfigurationen, die in Kapitel 8 aufgeführt sind.

9.2. Ergebnis der kryptographischen Bewertung

Der EVG enthält keine kryptographischen Mechanismen. Folglich waren solche Mechanismen nicht Gegenstand der Evaluierung.

10. Auflagen und Hinweise zur Benutzung des EVG

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

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

Die Begrenzung der Gültigkeit der Verwendung der kryptographischen Algorithmen wie in Kapitel 9 dargelegt muss ebenso durch den Anwender und seinen 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.

Zusätzlich sind die folgenden Auflagen und Hinweise zu beachten:

Die Feststellungen der Evaluierung ergeben die nachfolgend aufgeführten Auflagen für den Einsatz des evaluierten Produkts.

- Um zu gewährleisten, dass jedem bereits angemeldeten Wähler genügend Zeit für die Abgabe und endgültige Bestätigung seiner Stimme bleibt, muss die Wartezeit für die Beendigung der Phase Wahldurchführung länger sein als die Zeitspanne für den Fristablauf einer Wählersitzung. Der Wahlveranstalter trägt im Rahmen der Wahlvorbereitung die Verantwortung für die Kontrolle und Einstellung der entsprechenden Parameter ElectionEndWaitingPeriod (Konfigurationsdatei polyas-manangent-web.xml) und session-timeout (Konfigurationsdatei web.xml). Dabei soll die Zeitspanne für den Fristablauf einer Wählersitzung zwischen 5 und 30 Min. liegen.
- Eine ungewöhnlich Häufung von Stimmabgaben innerhalb kurzer Zeit, insb. kurz vor Beendigung der Phase Wahldurchführung kann als Indiz für einen möglichen Sicherheitsvorfall (Kompromittierung der Datenbank des Urnen EVG) interpretiert werden. Der Wahlvorstand wird auf seine Verantwortung für die Feststellung und Bewertung einer solchen ungewöhnlichen Häufung von Stimmabgaben hingewiesen.

Die Feststellungen der Evaluierung ergeben die nachfolgend aufgeführten Auflagen und Hinweise an den Entwickler / Hersteller.

- Die in der Handreichung für den Wähler beschriebene optionale Auswahl einzelner Stimmzettel wird in der Evaluierung nicht betrachtet. An einem entsprechenden Ablauf ist der EVG anscheinend nicht beteiligt.

  Die Ergebnisse der Evaluierung sind für die optionale Auswahl einzelner Stimmzettel durch den Wähler nicht gültig. Dem Entwickler / Hersteller wird auferlegt, die Auswahl einzelner Stimmzettel in der kundenspezifischen Gestaltung der WWW-Applikation entweder nicht zu verwenden oder deutlich auf die Ungültigkeit der Evaluierungsergebnisse und damit der Zertifizierung hinzuweisen .
- Dem Benutzer wird für die Anmeldung eine HTML-Seite mit Eingabefeldern für PIN/TAN (Wähler) bzw. Benutzername/Passwort (Wahlvorstand) präsentiert. Im Rahmen der Gestaltung der umgebenden WWW-Applikation besteht grundsätzlich die technische Möglichkeit, die Anmeldung durch eine erweiterte Funktionalität anders zu gestalten, etwa durch vorgelagerte Schritte zur Authentisierung mit anderen Mechanismen (SmartCards, Biometrie, Single-Sign-On, Personalausweis).

  Die Ergebnisse der Evaluierung sind für solche Erweiterungen nicht gültig. Dem Entwickler / Hersteller wird auferlegt, bei der Gestaltung der WWW-Applikation entweder auf solche Erweiterungen zu verzichten oder deutlich auf die Ungültigkeit der Evaluierungsergebnisse und damit der Zertifizierung hinzuweisen.
- Für den Fall, dass der Entwickler / Hersteller zusätzliche Funktionen für einzelne Schritte der Wahlvorbereitung in die umgebende WWW-Applikation integriert, wird dem Entwickler/Hersteller auferlegt, den Wahlveranstalter auf seine Verantwortung für die Erhaltung der Sicherheit, insb. den Schutz der Vertraulichkeit von TANs, Passwörtern und Schlüsseln hinzuweisen, und geeignete technisch-organisatorische Maßnahmen für die Wahrnehmung dieser Verantwortung anzubieten.
- Die Bereitstellung zusätzlicher Funktionen für den Wahlvorstand in der Phase „Wahldurchführung“, insb. und bspw. die zulässige Veränderung des Wählerverzeichnisses (Sperrung, Löschung, Ergänzung eines Wählers) aufgrund von Anforderungen der Wahlordnung, hat unabsehbare Folgen für die Wirksamkeit der Sicherheitsfunktionalität des EVG.

  In einem solchen Szenario sind die Ergebnisse der Evaluierung nicht gültig. Dem Entwickler / Hersteller wird auferlegt, entweder solche zusätzlichen Funktionen nicht

bereitzustellen oder deutlich auf die Ungültigkeit der Evaluierungsergebnisse und damit der Zertifizierung hinzuweisen.

- Für den Fall, dass die Phase Wahldurchführung vom Wahlvorstand vorzeitig, d.h. vor dem festgelegten Wahlendezeitpunkt, beendet wird, befindet sich der EVG in einem Zustand, der noch keine Auszählung zulässt. Dies ist erst mit Ablauf des Wahlzeitraums möglich.

  Dem Entwickler / Hersteller wird auferlegt, im Rahmen der Auslieferung des EVG dafür zu sorgen, dass der Wahlveranstalter einen Hinweis über den Einfluss des Wahlzeitraums auf die Wechselwirkung zwischen Beendigung und Auszählung erhält. Dieser Zusammenhang soll im Rahmen der Schulung an den Wahlvorstand vermittelt werden.

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
EAL	Evaluation Assurance Level - Vertrauenswürdigkeitsstufe
EVG	Evaluierungsgegenstand
ETR	Evaluation Technical Report
IT	Information Technology - Informationstechnologie
ITSEF	Information Technology Security Evaluation Facility - Prüfstelle für IT-Sicherheit
JAR	Java-Archiv
PIN	Persönliche Identifikationsnummer
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
SHA	Secure Hash Algorithm
ST	Security Target – Sicherheitsvorgaben
TAN	Transaktionsnummer
TLS	Transport Layer Security
TOE	Target of Evaluation - Evaluierungsgegenstand
TSF	TOE Security Functionality – EVG-Sicherheitsfunktionalität
WAR	Web Application Archive
WWW	World Wide Web

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.

WAR-Datei - Web Application Archive (gelegentlich auch Web Archive) ist ein Dateiformat, das beschreibt, wie eine vollständige Webanwendung nach der Java-Servlet-Spezifikation in eine Datei im JAR- bzw. ZIP-Format verpackt wird. Solche Dateien haben immer die Endung .war und werden daher umgangssprachlich auch „WAR-Datei“ genannt.

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[6] 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 für das Online-Wahlprodukt POLYAS CORE, BSI-DSZ-0862-V2, Version 1.10, 27.05.2021, POLYAS GmbH

[7] Evaluierungsbericht, Version 2.1, 01.06.2021, Evaluierung POLYAS Core V 2.5.0, Evaluation Technical Report Summary, DFKI (vertrauliches Dokument)

[8] Common Criteria Schutzprofil – Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte, BSI-CC-PP-0037, Version 1.0, 18.04.2008. Bundesamt für Sicherheit in der Informationstechnik (BSI)

[9] POLYAS GmbH: Benutzerdokumentation Polyas – Handreichung Wähler 2.5.0, Version 1.4, 21.05.2021

[10] POLYAS GmbH: Benutzerdokumentation Polyas – Handreichung Wahlvorstand 2.5.0, Version 1.3, 15.02.2021

[11] POLYAS GmbH: Benutzerdokumentation Polyas – Handreichung Wahlveranstalter 2.5.0, Version 1.7, 27.05.2021

[12] Konfigurationsliste für Security Target, Benutzer- und Evaluierungsdokumentation, Release Tag 2.5.0, 31.05.2021

[13] Konfigurationsliste für Software und Benutzerdokumentation, Release Tag 2.5.0, 31.05.2021

[6] specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 38, Version 2, Reuse of evaluation results

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.

Bemerkung: Ende des Reportes