Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

BSI-DSZ-CC-0862-2016

zu

POLYAS CORE, Version 2.2.3

der

Micromata GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Telefon: +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-0862-2016 (*)

Online-Wahlprodukt

POLYAS CORE
Version 2.2.3

von	Micromata 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. 4 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

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, 10. März 2016
Bundesamt für Sicherheit in der Informationstechnik
Im Auftrag

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

Bernd Kowalski
Abteilungspräsident

L.S.

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

Dies ist eine eingefügte Leerseite.

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.

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

Gliederung

A. Zertifizierung

1. Grundlagen des Zertifizierungsverfahrens

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

- BSI-Gesetz[2]
- BSI-Zertifizierungs- und - Anerkennungsverordnung[3]
- BSI-Kostenverordnung[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]
- 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)

2. 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.

2.1. Europäische Anerkennung von ITSEC/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

---

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

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

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 EAL1 bis EAL4 und ITSEC Vertrauenswürdigkeitsstufen E1 bis E3 (niedrig) 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.

Das Abkommen wurde von den nationalen Stellen von Deutschland, Finnland, Frankreich, Großbritannien, Italien, Niederlande, Norwegen, Österreich, Schweden und Spanien unterzeichnet. Eine aktuelle Liste der Unterzeichnerstaaten bzw. der anerkannten Zertifizierungsstellen, Details zur Anerkennung sowie zur Historie des Abkommens können auf der Internetseite http://www.sogisportal.eu eingesehen werden.

Das SOGIS-MRA-Logo auf dem Zertifikat zeigt, dass das Zertifikat unter den Bedingungen des Abkommens von den oben genannten Nationen anerkannt wird.

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

2.2. Internationale Anerkennung von CC - Zertifikaten

Da 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).

Das CCRA-2014 ersetzt das frühere CCRA, das im Mai 2000 unterzeichnet worden war (CCRA-2000). CC-Zertifikate, die vor dem 8. September 2014 nach den Regelungen des CCRA-2000 erteilt wurden, fallen weiterhin unter die gegenseitige Anerkennung. Für Zertifizierungsverfahren, die am 8. September 2014 bereits angefangen hatten, sowie für Verfahren zur Aufrechterhaltung alter Zertifikate (Maintenance und Re-Zertifizierungen) wurde eine Übergangsfrist zur Anerkennung nach den Regelungen des CCRA-2000 bis bis 8. September 2017 vereinbart (d.h. für Vertrauenswürdigkeitsstufen bis einschließlich EAL 4 oder die Vertrauenswürdigkeitsfamilie Fehlerbehebung (Flaw Remediation, ALC_FLR).

Im September 2014 wurde das Abkommen CCRA-2014 von den nationalen Stellen von Australien, Dänemark, Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Indien, Israel, Italien, Japan, Kanada, Malaysia, Pakistan, Republik Korea, Neuseeland, Niederlande, Norwegen, Österreich, Schweden, Spanien, Republik Singapur, Tschechische Republik, Türkei, Ungarn und USA unterzeichnet.

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

Das CCRA-Logo auf dem Zertifikat zeigt, dass das Zertifikat unter den Bedingungen des Abkommens von den oben genannten Nationen anerkannt wird.

Da das Zertifizierungsverfahren vor dem 8. September 2014 begonnen hatte, fällt dieses Zertifikat unter die Anerkennungsregeln des CCRA-2000 für alle ausgewählten Vertrauenswürdigkeitskomponenten.

3. 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 2.2.3 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Produkts POLYAS CORE, Version 2.2.3 wurde von Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI) GmbH durchgeführt. Die Evaluierung wurde am 18. Dezember 2015 abgeschlossen. Das Prüflabor DFKI ist eine vom BSI anerkannte Prüfstelle (ITSEF)[6].

Der Sponsor und Antragsteller ist: Micromata GmbH.

Das Produkt wurde entwickelt von: Micromata GmbH.

Die Zertifizierung wurde damit beendet, dass das BSI die Übereinstimmung mit den Kriterien überprüft und den vorliegenden Zertifizierungsreport erstellt hat.

4. Gültigkeit des Zertifikats

Dieser Zertifizierungsreport bezieht sich nur auf die angegebene Version des Produktes.

Das Produkt ist nur 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 Vertrauenswürdigkeitsstufen werden in den Auszügen aus dem technischen Regelwerk am Ende des Zertifizierungsreports und in den CC selbst erläutert.

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

[6] Information Technology Security Evaluation Facility

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 10. März 2016, ist gültig bis 9. März 2021. 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 sicherzustellen, dass auf den Zertifizierungsreport hingewiesen wird, sowie jedem Anwender des Produktes der Zertifizierungsreport und die darin referenzierten Sicherheitsvorgaben und die Benutzerdokumentation für den Einsatz oder die Verwendung des zertifizieren Produktes zur Verfügung gestellt wird,
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.

5. Veröffentlichung

Das Produkt POLYAS CORE, Version 2.2.3 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] Micromata GmbH
Marie-Calm-Straße 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 2.2.3 zur Durchführung von Online-Wahlen (kurz: Online-Wahlprodukt) bestehend aus:

- Urnen EVG, Version 2.2.3
- Wählerverzeichnis EVG, Version 2.2.3
- Validator EVG, Version 2.2.3
- Wahlvorstandsinterface EVG, Version 2.2.3
- Handreichung für den Wähler, Version 1.0
- Handreichung für den Wahlvorstand, Version 1.0
- Handreichung für den Wahlveranstalter, Version 1.0

Entsprechend den Sicherheitsanforderungen ist POLYAS CORE V2.2.3 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 während 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 Stimmauszählung aller abgegebenen Stimmen wird nach Wahlende auf dem Wahlserver das Ergebnis ermittelt und festgestellt.

POLYAS CORE V2.2.3 ist, abweichend von der generellen Darstellung im zugrundeliegenden Schutzprofil BSI-CC-PP-0037 [8], nicht in clientseitige und serverseitige EVG-Komponenten unterteilt, sondern besteht konform zu Anwendungsnotiz 3 des Schutzprofils nur aus serverseitigen EVG-Komponenten.

Der Wählerverzeichnis EVG verwaltet die Wahlberechtigungsliste, der Validator EVG dient als Kontrollinstanz und der 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 den Endgeräten (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. Für das Endgerät des Wählers sind die korrekte Anzeige des Stimmzettels und die korrekte Übertragung der Eingaben des Wählers in den empfohlenen Browsern (siehe Handreichung für den Wähler [10], Kapitel 3) getestet.

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 2 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 sicherheitsrelevanten 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 und verwendet.
FDP_IFC.1A	Diese funktionale Anforderung stellt den vorgesehenen Ablauf der Wahlhandlung sicher.
FDP_IFF.1A	Diese funktionale Anforderung stellt die Verwendung der Wahlattribute (zur Stimmberechtigung, Wahlhandlung etc.) während der Wahlhandlung sicher.
FDP_IFC.1B	Diese funktionale Anforderung realisiert den Ablauf bzw. die Aktivitäten des Wahlvorstands – 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 realisiert den Ablauf zur Wahlhandlung und die Aktivitäten des Wahlvorstands.
FDP_SDI.2	Datenintegritätsfehler lösen im EVG Fehlermeldungen aus, die protokolliert und per E-Mail an den Wahlvorstand gemeldet werden.
FDP_RIP.1A FDP_RIP.1B	Der Zwischenspeicher verwaltet die Stimme während des Wahlvorgangs eines Wählers im Arbeitsspeicher der Anwendung. Es 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.
FDP_UCT.1A FDP_UCT.1B	Der EVG stellt sicher, dass eine Kommunikation nur mittels https mit SSL-Zertifikaten gesichert erfolgt.
FDP_UIT.1A FDP_UIT.1B	Der EVG stellt sicher, dass eine Kommunikation nur mittels https mit SSL-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.

Sicherheits-funktionalität des EVG	Thema
	Ende der Wahlhandlung gelöscht.
FIA_UAU.1/.2 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 wird sichergestellt, dass eine hinreichende Anzahl von Autorisierungen des Wahlvorstands vorliegt.
FIA_USB.1A	Bei Eröffnung der Wahlhandlung erhält das Stimmberechtigungsattribut den Wert „unbekannt“ und das Wahlhandlungsattribut den Wert „vor“.
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: Wähler und Wahlvorstand sind von den Funktionen her strikt getrennt, so dass es keine Verknüpfung gibt.
FPR_ANO.1	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 SSL-Zertifikaten gesichert erfolgt.
FPT_RCV.1 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.
FTA_SSL.4	Dem Wähler wird bei der Kandidatenauswahl und Bestätigung der Stimmabgabe ein Logout-Button dargestellt, über den sich der Wähler abmelden kann.
FTA_TSE.1.	Für die Wahlhandlung müssen die Systeme gestartet und dürfen nicht gestoppt sein, damit eine Wahlhandlung eröffnet werden kann.
FTP_TRP.1A	Der EVG stellt sicher, dass eine Kommunikation nur mittels https mit

Sicherheits-funktionalität des EVG	Thema
FTP_TRP.1B	SSL-Zertifikaten gesichert erfolgt.

Tabelle 1: Sicherheitsfunktionalität des EVG

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

Die Werte, die durch den TOE 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 – 3.3 dar.

Dieses Zertifikat umfasst die folgenden Konfigurationen des EVG:

Der EVG besteht aus Software (JAR-Dateien) und Benutzerdokumentation (PDF-Dateien).

Die Komponenten der Benutzerdokumentation sind über den Titel und die eindeutige Versionsnummer identifiziert.

Die Komponenten der Software bestehen aus verschiedenen JAR-Dateien, die über den Dateinamen, die eindeutige Versionsnummer des EVG und die jeweilige Prüfsumme (SHA-256) der Dateien identifiziert sind:

- Urnen EVG polyas-vote-2.2.3.jar mit Prüfsumme:
  D46D3334CFA0EB8C1D1F1EB8DC25B2259D7B6F7D4D2BA1096A50ADE453C57CF1
- Wählerverzeichnis EVG polyas-registry-2.2.3.jar mit Prüfsumme:
  6200E9E782BED46552455295A10B1C37EE6C658E2B7D95BFA7B50F4105199554
- Validator EVG polyas-validator-2.2.3.jar mit Prüfsumme:
  5D10EDD8AF057FDC549D1794C031D99EF7EAA1A595FAE1511F5C87B79817028F
- Wahlvorstandsinterface EVG polyas-management-2.2.3.jar mit Prüfsumme:
  658AA3B304EC37DF224D65A34A539994AD2BAED6F67FFCB751AAB571EDEBBA91
- Gemeinsamer Bestandteil aller vier EVG-Komponenten polyas-common-2.2.3.jar mit Prüfsumme:
  FCBBEFC7705419793F1159B3119D09E727BA0F68749080D6BD99E2D2D15CDC4F

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 2.2.3

Die folgende Tabelle beschreibt den Auslieferungsumfang:

Nr.	Typ	Bezeichnung	Version / SHA-256-Prüfsumme	Auslieferungsart
1	SW	Urnen EVG: polyas-vote-2.2.3.jar	D46D3334CFA0EB8C1D1F1EB8DC25B2259D7B6F7D4D2BA1096A50ADE453C57CF1	Eingebettet in WAR-Datei polyas-vote-web-2.2.3-KUNDENNAME.war (s. lfd. Nr. 9)
2	SW	Wählerverzeichnis EVG: polyas-registry-2.2.3.jar	6200E9E782BED46552455295A10B1C37EE6C658E2B7D95BFA7B50F4105199554	Eingebettet in WAR-Datei polyas-registry-web-2.2.3-KUNDENNAME.war (s. lfd. Nr. 10)
3	SW	Validator EVG: polyas-validator-2.2.3.jar	5D10EDD8AF057FDC549D1794C031D99EF7EAA1A595FAE1511F5C87B79817028F	Eingebettet in WAR-Datei polyas-validator-web-2.2.3-KUNDENNAME.war (s. lfd. Nr. 11)
4	SW	Wahlvorstandsinterface EVG: polyas-management-2.2.3.jar	658AA3B304EC37DF224D65A34A539994AD2BAED6F67FFCB751AAB571EDEBBA91	Eingebettet in WAR-Datei polyas-management-gui-2.2.3- KUNDENNAME.war (s. lfd. Nr. 12)
5	SW	Gemeinsamer Bestandteil aller vier EVG-Komponenten: polyas-common-2.2.3.jar	FCBBEFC7705419793F1159B3119D09E727BA0F68749080D6BD99E2D2D15CDC4F	Eingebettet in jede WAR-Datei (s. lfd. Nr. 9, 10, 11, 12)
6	DOC	Benutzerdokumentation POLYAS CORE 2.2.3 Handreichung Wähler [10]	1.0	Elektronische Auslieferung
7	DOC	Benutzerdokumentation POLYAS CORE 2.2.3 Handreichung Wahlvorstand [11]	1.0	Elektronische Auslieferung
8	DOC	Benutzerdokumentation POLYAS CORE 2.2.3 Handreichung Wahlveranstalter [12]	1.0	Elektronische Auslieferung

Nr.	Typ	Bezeichnung	Version / SHA-256-Prüfsumme	Auslieferungsart
9	SW (non-TOE)	Wahlurne polyas-vote-web-2.2.3-KUNDENNAME.war vote.sql	n/a	Elektronische Auslieferung
10	SW (non-TOE)	Wählerverzeichnis polyas-registry-web-2.2.3-KUNDENNAME.war registry.sql	n/a	Elektronische Auslieferung
11	SW (non-TOE)	Validator polyas-validator-web-2.2.3-KUNDENNAME.war validator.sql	n/a	Elektronische Auslieferung
12	SW (non-TOE)	Wahladministration polyas-management-gui-2.2.3-KUNDENNAME.war management.sql	n/a	Elektronische Auslieferung
13	SW (non-TOE)	Java-Bibliothek (Vorbereitung) polyas-registry-admin-2.2.3.jar	n/a	Elektronische Auslieferung
14	SW (non-TOE)	Java-Bibliothek (Vorbereitung) polyas-validator-admin-2.2.3.jar	n/a	Elektronische Auslieferung
15	SW (non-TOE)	Java-Bibliothek (Vorbereitung) polyas-management-admin-2.2.3.jar	n/a	Elektronische Auslieferung
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. Die Benutzerdokumentation kann auch in gedruckter Form ausgeliefert werden.

Eine Auslieferung an Wähler oder Wahlvorstand findet nicht statt, denn Benutzer in diesen Rollen können den EVG aus der Ferne über einen Internet-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 die Micromata GmbH betreiben POLYAS gemeinsam, d.h. der Wahlveranstalter betreibt nur das Wählerverzeichnis:
  Die Übergabe beinhaltet die Benutzerdokumentation (siehe Tabelle 2, Nr. 6 – 8) und die für die Vorbereitung und für den Betrieb des Wählerverzeichnisses benötigten Auslieferungsgegenstände (siehe Tabelle 2, Nr. 2, 5, 10 und 13-16).
- die Micromata GmbH betreibt POLYAS als technische Unterstützung für den Wahlveranstalter:
  Die Übergabe beinhaltet nur die Benutzerdokumentation (siehe Tabelle 2, Nr. 6 – 8).

Die beiden letztgenannten Betriebsmodi definieren die Micromata GmbH als technischen Betreiber der Dienstleistung unabhängig von der Vertragsgestaltung.

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

Um die Integrität der ausgelieferten Software sicherzustellen, werden Prüfsummen (SHA-256) über die WAR-Dateien und die darin eingebetteten JAR-Dateien (EVG-Bestandteile) gebildet. Die Prüfsummen werden dem Wahlveranstalter telefonisch mitgeteilt, auch wenn POLYAS nur teilweise oder gar nicht vom Wahlveranstalter betrieben wird. Die Kontrolle der Prüfsummen erfolgt durch den Wahlveranstalter.

Die Identifizierung der Benutzerdokumentation erfolgt durch die auf den Handreichungen angegebenen Bezeichnungen und Versionsnummern (siehe Tabelle 2 oben, Nr. 6 – 8).

Die Identifizierung des EVGs durch den Wahlveranstalter erfolgt über die Bezeichnungen und die Prüfsummen der JAR-Dateien (siehe Tabelle 2, Nr. 1 – 5).

Die Identifizierung des EVGs durch den Wähler bzw. den Wahlvorstand erfolgt über die ständige Anzeige des Verweisnamens (Polyas Core V2.2.3) durch die Software.

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. 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 der Sicherheitsvorgaben [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**	**Bezug zur Benutzerdokumentation**
OE.Wahlvorbereitung	technisch	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.
	organisatorisch	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 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

Sicherheitsziel für die Einsatzumgebung	Art der Maßnahmen	Bezug zur Benutzerdokumentation
		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.
OE.Authentizität Server	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.Archivierung	technisch	Die Handreichung Wahlveranstalter enthält

Sicherheitsziel für die Einsatzumgebung	Art der Maßnahmen	Bezug zur Benutzerdokumentation
Integrität	organisatorisch	angemessene Hinweise auf die Erzeugung eines Manipulationsschutzes für die archivierten Daten.
OE.Geschützte Kommunikation	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 Datenbank, zum 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

Als Plattform für die Entwicklertests und 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 (S1), Validator (S2) und Urne (S3) zu ermöglichen.

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

- Betriebssystem (Linux): Debian 6.0 (Codename Squeeze)
- Datenbanksystem: PostgreSQL 9.1
- Java Laufzeitumgebung: JDK 1.7.0_71 mit JCE Policy 7
- Java Datenbankanbindung: JDBC4 PostgreSQL driver 9.1-903
- WWW-Server: Apache Tomcat 7.0.5

Der EVG selbst wurde in der evaluierten Konfiguration (siehe Kapitel 8) betrieben.

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 weitere 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 B a s i c 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 (siehe Tabelle 2, Nr. 1 – 8).

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.

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).
Derartige Erweiterungen sind in der evaluierten 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 evaluierten 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 Vertrauenswürdigkeitskomponenten 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

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.

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, insbesondere 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.

- 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, insbesondere den Schutz der Vertraulichkeit von TANs, Passwörtern und Schlüsseln hinzuweisen, und geeignete technisch-organisatorische Maßnahmen für die Wahrnehmung dieser Verantwortung anzubieten.
- 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
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level - Vertrauenswürdigkeitsstufe
EVG	Evaluierungsgegenstand
ETR	Evaluation Technical Report
HTML	HyperText Markup Language
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
TOE	Target of Evaluation - Evaluierungsgegenstand
TSC	TSF Scope of Control - Anwendungsbereich der TSF-Kontrolle
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 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012
http://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. 4, September 2012, http://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 für das Online-Wahlprodukt POLYAS CORE, BSI-DSZ-0862-2016, Version 1.1, 25. 09. 2015, Micromata GmbH

[7] Evaluierungsbericht, Version 1.2, 17.12.2015, Evaluierung POLYAS CORE V2.2.3, 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] Konfigurationsliste für den EVG, Version 201510081550, Konfigurationsliste vom 08.10.2015 Polyas Core Version 2.2.3 (vertrauliches Dokument)

[10] Micromata GmbH: Benutzerdokumentation POLYAS CORE 2.2.3 – Handreichung Wähler, Version 1.0, 26.08.2015.

[11] Micromata GmbH: Benutzerdokumentation POLYAS CORE 2.2.3 – Handreichung Wahlvorstand, Version 1.0, 26.08.2015.

[12] Micromata GmbH: Benutzerdokumentation POLYAS CORE 2.2.3 – Handreichung Wahlveranstalter, Version 1.0, 26.08.2015.

[8] speziell

- AIS 32, CC-Interpretationen im deutschen Zertifizierungsschema, Version 7, 08.06.2011.

Dies ist eine eingefügte Leerseite.

C. Auszüge aus den Kriterien

Anmerkung: Die folgenden Auszüge aus den technischen Regelwerken wurden aus der englischen Originalfassung der CC Version 3.1 entnommen, da eine vollständige aktuelle Übersetzung nicht vorliegt.

CC Part 1:

Conformance Claim (chapter 10.4)

“The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - **CC Part 3 extended** - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model

Assurance Class	Assurance Components
	ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next Section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC Part 3. More precisely, each EAL includes no more than one

component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.

Evaluation assurance level 1 (EAL 1) - functionally tested (chapter 8.3)

“Objectives

EAL 1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL 1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL 1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL 1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.”

Evaluation assurance level 2 (EAL 2) - structurally tested (chapter 8.4)

“Objectives

EAL 2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL 2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL 3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL 3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL 3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering."

Evaluation assurance level 4 (EAL 4) - methodically designed, tested, and reviewed (chapter 8.6)

"Objectives

EAL 4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL 4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL 4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs."

Evaluation assurance level 5 (EAL 5) - semiformally designed and tested (chapter 8.7)

"Objectives

EAL 5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL 5 assurance. It is likely that the additional costs attributable to the EAL 5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL 5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques."

Evaluation assurance level 6 (EAL 6) - semiformally verified design and tested (chapter 8.8)

"Objectives

EAL 6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL 6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs."

Evaluation assurance level 7 (EAL 7) - formally verified design and tested (chapter 8.9)

"Objectives

EAL 7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL 7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis."

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

“Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

D. Anhänge

Liste der Anhänge zu diesem Zertifizierungsreport

Anhang A: Die Sicherheitsvorgaben [6] werden in einem eigenen Dokument zur Verfügung gestellt.

Dies ist eine eingefügte Leerseite.