MICROMATA

Sicherheitsvorgaben für das Online-Wahlprodukt

POLYAS

CORE

Version: 1.12

basierend auf:

BSI-Schutzprofil BSI-CC-PP-0037

Polyas GmbH
Marie-Calm-Str. 1-5
D-34131 Kassel
Tel: +49 561 / 503 7864 – 0

Version	Datum	Autor	Kapitel	Grund der Änderungen
0.2	30.06.2009	Niels Menke, Kai Reinhard, Melanie Volkamer (Micromata)	alle	Ersterstellung
0.3	08.07.2011	Sönke Maseberg (datenschutz cert) Wolfgang Jung, Florian Heinecke (Micromata)	alle	Wiederaufnahme der CC-Zertifizierung
0.4	20.07.2012	Sönke Maseberg (datenschutz cert) Wolfgang Jung, Florian Heinecke (Micromata)		Berücksichtigung von Anmerkungen der Prüfstelle im ASE-Prüfbericht, v1.0 vom 18.06.2012
0.5	02.11.2012	Sönke Maseberg (datenschutz cert)		Ergebnisse Kick-Off-Meeting vom 10.10.2012
0.6	25.01.2013	Sönke Maseberg (datenschutz cert) Michael Elbers (Micromata)		Berücksichtigung von Anmerkungen der Prüfstelle im ASE-Prüfbericht, v1.1 vom 16.11.2012
0.7	08.02.2013	Sönke Maseberg (datenschutz cert) Michael Elbers (Micromata)		Berücksichtigung von Anmerkungen der Prüfstelle
0.8	25.03.2013	Sönke Maseberg (datenschutz cert) Michael Elbers (Micromata)		Berücksichtigung von Anmerkungen der Prüfstelle
0.9	09.04.2013	Sönke Maseberg (datenschutz cert) Michael Elbers (Micromata)		Berücksichtigung von Anmerkungen der Prüfstelle
0.91	25.04.2013	Sönke Maseberg (datenschutz cert) Michael Elbers (Micromata)		Berücksichtigung von Anmerkungen der Prüfstelle
0.92	21.10.2013	Sönke Maseberg (datenschutz cert)		Berücksichtigung von Anmerkungen der Prüfstelle (A.Endgerät und OE.Endgerät) Ergänzung bei Abs. 1.4.1.3
0.93	22.10.2013	Sönke Maseberg (datenschutz cert)		Tomcat durch TomEE ersetzt
0.94	15.10.2014	Sönke Maseberg (datenschutz cert)		Versionsnummer auf 2.2.0 geändert
0.95	24.02.2015	Florian Heinecke (Micromata GmbH)		Versionsnummer auf 2.2.3 geändert
0.96	06.03.2015	Florian Heinecke und Ibrahim Rabah (Micromata GmbH)		Einige Stellen geändert (gelb markiert)
0.97	21.04.2015	Sönke Maseberg		Graphik überarbeitet

Version	Datum	Autor	Kapitel	Grund der Änderungen
		(datenschutz cert)		
1.0	26.08.2015	Florian Heinecke (Micromata GmbH)		Finalisierung
1.1	25.09.2015	Jan Schirrmacher (datenschutz cert), Florian Heinecke (Micromata GmbH)	Kap. 1	Überarbeitung aufgrund des Site Visits vom 15.09.2015
1.2	12.11.2020	Florian Heinecke (Micromata GmbH) Wolfgang Jung (Polyas GmbH)		Kleine Anpassungen für die Antragsstellung zur Re-Zertifizierung 2021 Versionsnummern aktualisiert Ab dieser Version ist die Polyas GmbH der Herausgeber
1.3	02.12.2020	Florian Heinecke (Micromata GmbH) Wolfgang Jung (Polyas GmbH) Tobias Pressel (Micromata GmbH)		Versionsnummer aktualisiert Herausgeber angepasst Kap. 1.4.2 Authentifizierungsmerkmale durch Authentifizierungsdaten ersetzt Durchgehende Ersetzungen: Identifizierungsmerkmal durch Identifikationsdaten; Identifikationsmerkmal durch Identifikationsdaten; Authentifizierung durch Authentisierung; authentifiziert durch authentisiert
1.4	08.12.2020	Wolfgang Jung (Polyas GmbH)	1.4	Versionsnummern der Handreichungen
1.5	17.03.2021	Wolfgang Jung (POLYAS GmbH), Florian Heinecke (Micromata GmbH)		Anpassungen aufgrund des Review-Protokolls
1.6	20.04.2021	Wolfgang Jung (POLYAS GmbH)		Weitere Anpassungen aufgrund des Review-Protokolls
1.7	26.04.2021	Wolfgang Jung (POLYAS GmbH)		Versionsnummern aktualisiert
1.8	30.04.2021	Wolfgang Jung (POLYAS GmbH)		Review Protokoll eingearbeitet
1.9	26.05.2021	Wolfgang Jung (POLYAS GmbH) & Florian Heinecke (Micromata GmbH)	Kaptel 6, 5.1, 1.3.4	Protokollierung bei Beendigung, JDK-Version
1.10	27.05.2021	Wolfgang Jung (POLYAS GmbH)	Kapitel 1.2, Kapitel 1.4.1	Versionsnummern und Sequenzdiagramm aktualisiert
1.11	04.11.2021	Wolfgang Jung (POLYAS GmbH)	Kapitel 1.2	Aktualisierung der Versionsnummern und Prüfsummen
1.12	17.01.2022	Wolfgang Jung (POLYAS GmbH)	Kapitel 1.2	Aktualisierung der Versionsnummern und Prüfsummen auf Version 2.5.4

Tabelle 1: Dokumentenhistorie

Präambel

Erläuterungen zur Darstellung des folgenden Textes:

- Text in schwarzer Schrift stammt aus dem Schutzprofil „Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte“ (BSI-CC-PP-0037) [7].
- Text in blauer Schrift ist ggü. den Schutzprofil [7] im vorliegenden Sicherheitsvorgaben inhaltlich geändert, ergänzt bzw. in Einzelfällen auch gelöscht worden.

Anhang C enthält ein Abkürzungsverzeichnis und Glossar der verwendeten Begriffe.

Inhaltsverzeichnis

1 ST Einführung

POLYAS CORE ist ein Softwareprodukt zur Durchführung von Online-Wahlen. Die Sicherheitsanforderungen sind geeignet, Vereinswahlen, Gremienwahlen - etwa in den Hochschulen, im Bildungs- und Forschungsbereich - und insbesondere nicht-politische Wahlen mit geringem Angriffspotential sicher auszuführen.

Die Anforderungen des zugrunde liegenden Schutzprofils [7] basieren auf der Empfehlung des Europarates für Online-Wahlen [1], auf dem von der Physikalisch-Technischen Bundesanstalt (PTB) erarbeiteten Anforderungskatalog für Online-Wahlen [3] und auf dem Anforderungskatalog für Vereinswahlen von der Expertenrunde der Gesellschaft für Informatik e.V. [2].

1.1 ST Referenz

Titel: Sicherheitsvorgaben für das Online-Wahlprodukt POLYAS CORE

Herausgeber ab Version 1.2: Polyas GmbH, Marie-Calm-Str. 1-5, 34131 Kassel

Autoren: Niels Menke, Kai Reinhard, Melanie Volkamer, Dr. Sönke Maseberg, Florian Heinecke, Ibrahim Rabah, Jan Schirrmacher, Wolfgang Jung, Tobias Pressel

ST-Versionsnummer: 1.12

Fertigstelldatum: 17.01.2022

Zertifizierungsnummer: BSI-DSZ-CC-0862-V2-2021-MA-02

Schlüsselwörter: Remote Voting, eVoting, Online-Wahlen, elektronische Wahlen

1.2 EVG Referenz

Das Online-Wahlsystem POLYAS CORE stellt den Evaluierungsgegenstand (EVG) dieser Sicherheitsvorgaben dar. Dieser EVG ist, abweichend vom, aber konform zum zugrundeliegenden Schutzprofil (vgl. Anwendungsnotiz 3 [7]), nicht in eine clientseitige und eine serverseitige EVG-Komponente unterteilt, sondern besteht nur aus dem serverseitigen EVG.
Dieser serverseitige EVG setzt sich aus vier Komponenten zusammen:

- serverseitiger Urnen EVG (kurz Urne),
- serverseitiger Wählerverzeichnis EVG (kurz: Wählerverzeichnis),
- serverseitiger Validator EVG (kurz: Validator) und
- serverseitiger Wahlvorstandsinterface EVG (kurz: Wahlvorstandsinterface)

Jede dieser vier Komponenten besteht aus dem entsprechenden CORE-Bestandteil und einem gemeinsamen Bestandteil.
Die eindeutigen Referenzen des EVG und seiner Bestandteile sind:

- POLYAS CORE Software: Version 2.5.4 (interne Versionsnummer: `r@d7454b3961435e422c00a4d228d4efb2b290ed07`) mit folgenden fünf Bestandteilen:
  - Urnen EVG (polyas-vote): Version 2.5.4, SHA256 Prüfsumme: `db2b3a19091c7d9b4d1362c94093eb7fe19ef11290496cc057f91eef47e327af`
  - Wählerverzeichnis EVG (polyas-registry): Version 2.5.4, SHA256 Prüfsumme: `799359111720a5f6406665273ebd76158ed73065f612355630d87c954eed113d`
  - Validator EVG (polyas-validator): Version 2.5.4, SHA256 Prüfsumme: `8a36fc0f1fa84437e4f79a94383aebb20b991f620838df371b3a758efd2afc30`
  - Wahlvorstandsinterface EVG (polyas-management): Version 2.5.4, SHA256 Prüfsumme: `682c45a571529b26de8d9e150ccfa6329a5463a97717bf77dff7f6effb16961f`

- Gemeinsame Funktionen aller EVG Komponenten (polyas-common): Version 2.5.4, SHA256 Prüfsumme:
  `594da7391f171ffc1086175b167cfd29c3b9eb1eff3bcb376febd82fe43da107`

  Diese EVG-Bestandteile werden als JAR-Dateien in installationsfähige WAR-Archive eingebettet, wobei die WAR-Dateien kundenspezifisch erstellt werden und damit nicht als Teil des EVGs zu betrachten sind.
- POLYAS CORE Benutzerdokumentation:
  - Handreichung für den Wähler, Version 1.6
  - Handreichung für den Wahlvorstand, Version 1.5
  - Handreichung für den Wahlveranstalter, Version 1.9

1.3 EVG-Übersicht

In diesem Abschnitt sind die Art des EVG und wichtige Begriffe festgelegt. Der Gebrauch des EVG und seine wesentlichen Sicherheitsmerkmale sind zusammenfassend dargelegt. Abgeschlossen wird die EVG-Übersicht mit Angaben zu benötigter Hardware / Software / Firmware, die nicht Bestandteil des EVG ist.

1.3.1 Art des EVG

Der betrachtete Evaluationsgegenstand (EVG) – POLYAS CORE – ist ein Produkt zur Durchführung von Online-Wahlen (kurz: Online-Wahlprodukt). Er ist in ein Phasenmodell für den Ablauf einer Wahl eingebettet. Eine Wahl besteht aus drei Phasen: Wahlvorbereitung, Wahldurchführung inkl. Stimmauszählung und Archivierung.

Die in diesem ST definierten Anforderungen an den EVG beziehen sich nur auf die Phase Wahldurchführung inkl. der Stimmauszählung, nicht aber auf die Wahlvorbereitung (wie beispielsweise die Erstellung der Wahlberechtigungsliste) und die Archivierung der Wahldurchführungs- und Ergebnisdaten. Anforderungen an den Übergang zu den angrenzenden Phasen werden in Sicherheitszielen für die Umgebung zum Ausdruck gebracht.

Der EVG ist Teil des modularen Produktportfolios „POLYAS Online Voting Solutions“, welches den EVG um weitere Module erweitert. Diese weiteren Module sind für die Phasen Wahlvorbereitung und Archivierung relevant und nicht Gegenstand der Evaluierung.

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.

Der EVG ist ein verteiltes System, das aus mehreren serverseitigen EVG-Komponenten, aber keinem clientseitigen EVG besteht. Der serverseitige EVG besteht aus den folgenden Komponenten:

- serverseitigem Wählerverzeichnis EVG (kurz: Wählerverzeichnis),
- serverseitigem Validator EVG (kurz: Validator),
- serverseitigem Urnen EVG (kurz: Urne) und
- serverseitigem Wahlvorstandsinterface EVG (kurz: Wahlvorstandsinterface).
- einer gemeinsamen Bibliothek, die von allen vier zuvor genannten Komponenten eingebunden wird.

Im Rahmen der Auslieferung werden die serverseitigen Komponenten zusammen mit der gemeinsamen Bibliothek in jeweils einem WAR-Archiv mit den kundenspezifischen Anpassungen

zusammengefasst, welches durch einen Applikationsserver ausgeführt werden kann. Diese Anpassungen und auch die Laufzeitumgebung des Applikationsservers sind nicht Bestandteil des EVGs.

Die ersten drei Komponenten werden auf unterschiedlichen Wahlservern installiert; entsprechend:

- Wahlserver 1 für das Wählerverzeichnis
- Wahlserver 2 für den Validator und
- Wahlserver 3 für die Urne.
- Der serverseitige Wahlvorstandsinterface EVG kann wahlweise auf einem der drei Wahlserver oder einem vierten Wahlserver installiert werden.

Der serverseitige Wählerverzeichnis EVG verwaltet die Wahlberechtigungsliste, der serverseitige Validator EVG dient als Kontrollinstanz und der serverseitige Urnen EVG speichert die abgegebenen Stimmen. Der serverseitige 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. Für das Endgerät des Wählers sind die korrekte Anzeige des Stimmzettels und die korrekte Übertragung der Eingaben des Wählers in den empfohlenen Browsern (siehe hierzu Abschnitt 1.3.4) gewährleistet. Der Server erkennt dazu ggf. anhand der Browserkennung im HTTP-Request-Header den Typ des Wählerbrowsers. Eine separate Information des Wählers, wenn er einen Browser außerhalb der vorgesehenen Konfiguration verwendet, ist nicht erforderlich. Eine Speicherung der abgegebenen Stimme bzw. dem Stimmdatensatz auf dem empfohlenen Endgerät (vgl. Abschnitt 1.3.4) findet nicht statt. Da eine Zwischenspeicherung von empfangenen Daten bei anderen Konfigurationen des Endgerätes bzw. des Web-Browsers in Einzelfällen erfolgen kann, kann der EVG so konfiguriert werden, dass der Wähler nach Abschluss der Wahlhandlung mit einem entsprechenden konfigurierbaren Hinweis auf der letzten Webseite informiert wird, wie diese temporären Dateien zu löschen sind.

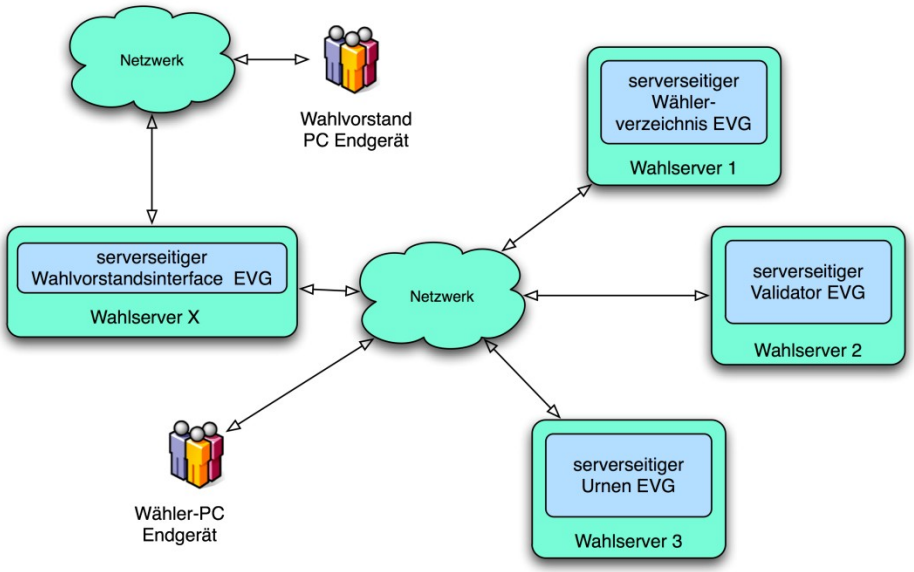

Abbildung 1: EVG-Übersicht

Der EVG ist für Online-Wahlen verwendbar, die über folgende Merkmale verfügen:

- Die Zuordnung einer abgegebenen Stimme zur Identität des Wählers muss geheim sein (Wahlgeheimnis), d.h. jede Stimme ist nur dem zugehörigen Wähler bekannt.

- Es muss nicht geheim gehalten werden, welche Wähler gewählt haben.
- Kein Wähler darf in der Lage sein, seine Wahlentscheidung zu beweisen.
- Nur registrierte Wähler dürfen eine Stimme abgeben
- Jeder Wähler darf nur eine Stimme abgeben.
- Während der Wahldurchführung darf kein Zwischenergebnis ermittelt werden.

1.3.2 Generelle Sicherheitserwartungen an den EVG

Die generellen Sicherheiterwartungen werden von den allgemeinen Wahlrechtsgrundsätzen (frei, gleich, geheim, allgemein und unmittelbar) abgeleitet. Die Sicherheitserwartungen lassen sich wie folgt zusammenfassen (vgl. [5] und [6]):

- 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).

Der EVG stellt während der geheimen Wahl sicher, dass mit der endgültigen Stimmabgabe und der Speicherung dieser Stimme in der Urne keine Verbindung mehr zwischen Wähler und Stimme existiert. Daher besteht nicht nur nach Ende der Wahldurchführung, sondern bereits nach Abschluss der Wahlhandlung keine Möglichkeit mehr, den Zusammenhang zwischen Wähler und Stimme herzustellen.

1.3.3 Gebrauch und wesentliche Sicherheitsmerkmale

1.3.3.1 Zustand des EVG vor der Wahldurchführung inkl. Stimmauszählung

In der Phase Wahlvorbereitung werden die Wahldaten angelegt, ggf. korrigiert und vom Wahlveranstalter verabschiedet. Jeder registrierte Wähler verfügt über seine Identifikationsdaten (PIN), sein Authentisierungsmerkmal ("Transaktionsnummer" in Form eines für eine abgeschlossene Wahlhandlung verwendbaren Passworts) sowie die URL, unter der das Wählerverzeichnis auf Wahlserver 1 verfügbar ist. Das Verfahren zur Erzeugung und Verteilung des Authentisierungsmerkmals ist so gestaltet, dass eine hinreichend, d.h. den Vorgaben des Wahlveranstalters entsprechend, zuverlässige und eindeutige Authentisierung jedes Wählers gewährleistet ist.

Vor dem Beginn der Wahldurchführung werden die Wahldaten in der genehmigten, d.h. in der vom Wahlveranstalter verabschiedeten Fassung, auf dem Wahlserver 1 (für das Wählerverzeichnis) für die Verwendung durch den serverseitigen Wählerverzeichnis EVG bereitgestellt. Die Signaturen der Einträge im Wählerverzeichnis werden dem Validator zur Verfügung gestellt. Die Installation und Konfiguration des serverseitigen EVG ist vom Wahlveranstalter durchgeführt und erfolgreich abgeschlossen [...].

1.3.3.2 Prozessbeschreibung für die Wahldurchführung inkl. Stimmauszählung

Die Wahldurchführung beginnt am serverseitigen EVG mit dem Starten der Wahldurchführung durch den Wahlvorstand. Beim Start der Wahldurchführung sorgt der serverseitige Urnen EVG dafür, dass die Urne leer ist.

Ausschließlich während der Wahldurchführung kann ein Wähler seine individuelle Wahlhandlung ausführen. Nur von Wählern mit Stimmberechtigung können Stimmen abgegeben, also in der Urne gespeichert werden. Es ist nicht möglich, Stimmen aus der Urne zu lesen oder in der Urne gespeicherte Stimmen zu verändern. Solange Stimmen noch korrigiert werden können, bleiben diese den Wählern zugeordnet und werden nicht in der Urne gespeichert. [...]

Während der Wahldurchführung kann am serverseitigen Wahlvorstandsinterface EVG vom Wahlvorstand ein Wiederanlauf durchgeführt werden, falls es zu Störungen oder Abstürzen kam. Der Wahlvorstand kann sich außerdem zu jeder Zeit durch einen Selbsttest von der korrekten Funktion des serverseitigen EVG überzeugen. Der Wahlveranstalter muss festlegen, unter welchen Bedingungen vom Wahlvorstand ein Wiederanlauf oder ein Selbsttest durchzuführen ist.

Zur Beendigung der Wahldurchführung leitet der Wahlvorstand am serverseitigen Wahlvorstandsinterface EVG das Wahlende ein. Falls er die Wahldurchführung vor dem vom Wahlveranstalter vorgegebenen Wahlende-Zeitpunkt beenden möchte, führt dies zu einem entsprechenden Hinweis. Die Beendigung der Wahldurchführung ist dennoch möglich. Ein Wiederanlauf oder jede andere Form der Rückkehr in die Wahldurchführung ist nicht mehr möglich.

Nach dem Wahlende kann der Wahlvorstand die Stimmauszählung veranlassen. Dazu wird dem Wahlvorstand zuvor angezeigt, wie viele Stimmen bereits in der Urne eingegangen sind, so dass er die Stimmenauszählung dann veranlassen kann, wenn eine – gemäß der Wahlordnung – ausreichende Anzahl von Stimmen vorliegt. Durch Auszählung aller in der Urne gespeicherten Stimmen werden die Anzahl der ungültigen und die Anzahl der gültigen Stimmen ermittelt. Durch Auszählung aller gültigen Stimmen wird die summarische Stimmverteilung für die einzelnen Wahlvorschläge ermittelt. Schließlich wird das Ergebnis festgestellt. Mit der Feststellung des Ergebnisses der Stimmauszählung werden die Wahldurchführungsdaten und das Ergebnis vom serverseitigen Urnen EVG so gespeichert, dass sie vor nachträglichen unbemerkten Manipulationen, also unbefugten Modifikationen außerhalb der Kontrolle des serverseitigen EVG, geschützt sind.

Der EVG ermittelt die Gültigkeit oder Ungültigkeit von Stimmen während der Auszählung. Die Stimme wird dazu entschlüsselt und, falls gültig, in eine Menge hinzugefügt, die anschließend ausgezählt wird. Falls die Stimme ungültig ist, wird sie als ungültig gezählt und nicht weiter ausgewertet.

Vom serverseitigen EVG werden während der Wahldurchführung inkl. Stimmauszählung sicherheitsrelevante Ereignisse protokolliert. Die Protokollaufzeichnungen werden auf dem Wahlserver vor unberechtigten Manipulationen geschützt gespeichert und können vom Wahlvorstand jederzeit durchgesehen werden.

Der Prozessablauf für die individuelle Wahlhandlung jedes Wählers genügt folgenden Prinzipien:

- [...] Vor der Stimmabgabe ist der Wähler identifiziert und authentisiert worden. Die Auswertung seines Stimmabgabevermerks bestätigt ihn als Wähler mit Stimmberechtigung.
- Nach der Einleitung der Stimmabgabe zeigt der EVG dem Wähler seine Stimme erneut an, bevor er seine Stimme abgeben kann (Übereilungsschutz).

- Der Wähler kann zu jedem Zeitpunkt, bis zur Stimmabgabe, seine Wahlhandlung abbrechen, ohne seine Stimmberechtigung zu verlieren. Auch bei einem technisch bedingten Abbruch, etwa wegen Zeitablauf oder Fehlern bei der Kommunikation, muss die Stimmberechtigung erhalten bleiben.
- Es erfolgt eine Rückmeldung vom serverseitigen Urnen EVG an den Wähler, dass seine Stimme erfolgreich abgegeben, also in der Urne gespeichert, wurde.
- Der Vermerk der Stimmabgabe ist untrennbar mit der Speicherung der Stimme in der Urne verbunden.

1.3.3.3 Darstellung des Ablaufs der Wahlhandlung

Die Variante, die der EVG realisiert, wird mit „Anmelden bei Start der Wahlhandlung“ bezeichnet und ist ohne Berücksichtigung von Fehlern und Unterbrechungen in Abbildung 2 dargestellt. Der Wähler eröffnet die Wahlhandlung am [...] EVG mittels Browser. Er identifiziert und authentisiert sich gegenüber dem serverseitigen EVG. Der serverseitige EVG prüft die Stimmberechtigung des registrierten Wählers. Im nächsten Schritt wird einem Wähler mit Stimmberechtigung der Stimmzettel angezeigt, alle anderen Wähler werden vom serverseitigen EVG abgewiesen.

Der Wähler mit Stimmberechtigung kann seinen Stimmzettel ausfüllen, beliebig oft ändern und mit der Einleitung der Stimmabgabe seine Wahlentscheidung treffen. Anschließend wird dem Wähler mit Stimmberechtigung seine Stimme erneut angezeigt. Er hat nun die Möglichkeit, die Stimme abzugeben oder die Einleitung der Stimmabgabe zu widerrufen um die Stimme zu korrigieren. Nach der erfolgreichen Stimmabgabe, d.h. Speicherung der Stimme durch den serverseitigen EVG in der Urne, und dem damit verbundenen Vermerk der Stimmabgabe, erhält der registrierte Wähler eine Rückmeldung, dass seine Stimme gespeichert wurde.

Abbildung 1: Ablauf der Wahlhandlung aus Sicht des Wählers

[…]

1.3.3.4 Zustand des EVG nach der Wahldurchführung inkl. Stimmauszählung

Die Wahldurchführungsdaten und das Ergebnis werden zusammen mit dem EVG selbst für eine ggf. erforderliche Wahlprüfung aufbewahrt. Jede Manipulation, also unbefugte Modifikation, der Wahldurchführungsdaten oder des Wahlergebnisses liegt außerhalb der unmittelbaren Kontrolle des EVG. Jegliche Veränderungen sind erkennbar, weil der serverseitige EVG bei der Feststellung des Ergebnisses einen Manipulationsschutz erzeugt hat, der auch außerhalb des Wahlservers wirksam ist.

Die Art und Weise der Archivierung sowie deren Dauer wird vom Wahlveranstalter festgelegt. Die Bereinigung (Deinstallation, Löschen von Daten) des serverseitigen EVG liegt in der Verantwortung des Wahlveranstalters.

Die Veröffentlichung der Wahlergebnisse liegt im Verantwortungsbereich der Wahlveranstalter.

1.3.3.5 Bedienung durch den Wähler

[...] Dem Wähler stehen am Endgerät die folgenden Aktionen für die Ausführung der Wahlhandlung zur Verfügung:

- Identifizieren und Authentisieren des Wählers,
- Ausfüllen und Korrigieren des Stimmzettels,
- Einleiten der Stimmabgabe,
- Abgeben der Stimme und Löschen des ausgefüllten Stimmzettels,
- Abbrechen der Wahlhandlung und
- Überprüfen der Rückmeldung, ob die Stimme gespeichert wurde.

Alle Funktionen werden dabei vom serverseitigen EVG bereitgestellt. Der Wähler nutzt zur Kommunikation mit diesem einen Webbrowser auf einem Endgerät unter Nutzung von TLS ab Version 1.2 (vgl. Abschnitt 1.3.1).

Da mit dem EVG nur die Kernfunktionalitäten eines Online-Wahlsystems bereitgestellt werden, welche für eine konkrete Wahl noch konfiguriert werden müssen, lässt sich die graphische Darstellung des EVGs durch Informationen zur Wahl oder zur Bedienung ergänzen, was allerdings keinen Einfluss auf die Sicherheitsfunktionalität oder Sicherheit des EVG nimmt. Die konkrete graphische Darstellung der Bedienungsoberfläche des EVG liegt außerhalb der Evaluierung.

1.3.3.6 Bedienung durch den Wahlvorstand

Der Wahlvorstand wird am serverseitigen EVG identifiziert und authentisiert, bevor ihm die Ausführung jeglicher anderer Aktion erlaubt wird. Dies erfolgt per Remote-Zugang über TLS-geschützte Kommunikation mit dem serverseitigen Wahlvorstandsinterface EVG (Einsatzumgebung). Der Wahlvorstand nutzt hierfür, wie der Wähler, einen Webbrowser auf einem Endgerät.

Dem Wahlvorstand stehen dann Funktionen für die Durchsicht der vorhandenen Protokollaufzeichnungen und für die Ausführung einer Testfolge als Nachweis für den korrekten Betrieb des EVG (Selbsttest) zur Verfügung.

Mit dem Selbsttest kann der Wahlvorstand Störungen der Integrität der EVG-Sicherheitsfunktionen (TSF) oder der Benutzer- und TSF-Daten, die den korrekten Betrieb des EVG gefährden, erkennen.

Für die Prozesssteuerung des serverseitigen EVG werden dem Wahlvorstand folgende Operationen zur Verfügung gestellt:

- Starten der Wahldurchführung,
- Wiederanlaufen der Wahldurchführung nach Absturz oder Störung,
- Beenden der Wahldurchführung,
- Starten der Stimmauszählung mit Feststellung des Wahlergebnisses.

Vor der Ausführung jeder dieser Operationen wird der Wahlvorstand erneut identifiziert und authentisiert [...]. Die Anforderung der Operation wird durch die Identifikation und Authentisierung eines anderen Mitglieds des Wahlvorstands bestätigt [...] (Separation of Duty).

Darüber hinaus gehende Funktionen können durch Zusatzmodule aus dem Portfolio „POLYAS Online Voting Solutions“ bewusst ergänzt werden, sind im EVG jedoch nicht vorgesehen.

1.3.3.7 Störungen, Selbsttests und Wiederanlauf

Es wird davon ausgegangen, dass die Verfügbarkeit des Netzwerks, des Wahlservers und des serverseitigen EVG sowie die Integrität und Verfügbarkeit aller gespeicherten Benutzer- und TSF-Daten mit einer vom Wahlveranstalter festgelegten Service-Qualität gegeben ist. Dennoch muss mit Unterbrechungen der Netzwerkanbindung, mit Ausfällen des Wahlservers bzw. des serverseitigen EVG und mit beschädigten Speichermedien bzw. Schreibfehlern beim Speichern von Stimmdatensätzen und Stimmabgabevermerken gerechnet werden. Diese Störungen dürfen die Sicherheit der Wahldurchführung inkl. Stimmauszählung nicht gefährden.

Über Störungen der Netzwerkanbindung oder der Speicherung von Daten, die dem serverseitigen EVG gemeldet werden, wird der Wahlvorstand per E-Mail informiert. In solchen Fällen soll der Wahlvorstand eine vom serverseitigen EVG bereitgestellte Testfolge als Nachweis für den korrekten Betrieb des EVG (Selbsttest) ausführen. Aus den Resultaten des Selbsttests soll der Wahlvorstand gemäß den Vorgaben des Wahlveranstalters geeignete Korrekturmaßnahmen ableiten und ggf. einen geschützten Wiederanlauf durchführen um einen sicheren Zustand des serverseitigen EVG zu erhalten.

Der EVG stellt einen Mechanismus zur Verfügung [...], um die Wahldurchführung nach festgestellten Störungen der Netzwerkanbindung oder der Speicherung von Daten bzw. nach Ausfällen des Wahlservers oder des serverseitigen EVG wiederanlaufen zu lassen.

Durch den geschützten Wiederanlauf bleibt der sichere Betrieb des EVG gewährleistet. Dabei wird sichergestellt, dass kein Wähler mehr als eine Stimme abgeben kann oder trotz erfolgloser Stimmabgabe seine Stimmberechtigung verliert.

Die Benutzung des Wiederanlaufmechanismus nach Wahlende [...] wird vom EVG [...] verhindert. Eine Rückkehr zur Wahldurchführung ist somit nicht möglich.

1.3.3.8 Protokollierung

Mindestens die folgenden Ereignisse und Aktionen inkl. der Zeitpunkte des Auftretens der Ereignisse [...] werden vom serverseitigen EVG protokolliert [...]:

- Erfolgreiche Identifikation und Authentisierung des Wahlvorstands
- Starten und Wiederanlaufen und Beenden der Wahldurchführung
- Starten der Stimmauszählung mit Feststellung des Wahlergebnisses
- Durchführung und Resultate jedes Selbsttests
- Festgestellte Störungen bei der Verwendung unterstützender Mechanismen der IT-Umgebung, die die Betriebsfähigkeit der serverseitigen EVG beeinträchtigen

Die Protokollaufzeichnungen sind Teil der zu schützenden Werte. Sie müssen auf dem Wahlserver gespeichert werden und es wird dem Wahlvorstand ermöglicht [...], sie durchzusehen.

Die IT-Umgebung des serverseitigen EVG muss die vor unberechtigten Manipulationen geschützte Speicherung der Protokollaufzeichnungen gewährleisten.

1.3.4 Benötigte nicht-EVG Hardware/Firmware/Software

Wähler und Wahlvorstand nutzen jeweils einen Webbrowser auf ihrem Endgerät, mit dem sie mit dem Wahlserver bzw. dem serverseitigen EVG kommunizieren. Zur IT-Umgebung des […] Endge-

rätes zählen […] die Hardware, Betriebs- und Applikationssoftware und das lokale Netzwerk in einer PC-Umgebung.

Das Endgerät muss in der Lage sein, den gesamten Inhalt des Stimmzettels darzustellen und die Vorgaben des Wahlveranstalters für die Art der Darstellung, insb. die Reihenfolge der Wahlvorschläge umzusetzen.

Der EVG arbeitet endgeräteunabhängig, da er nur aus einem serverseitigen EVG besteht, und kann mit jedem Endgerät, welches über Internetzugang, einen Webbrowser, der HTTPS-Seiten anzeigen kann und einen Zugang zu Port 443 des Netzwerkes verfügt, ausgeführt werden. Die Identifikationsdaten des Wählers sind an keine spezifische Hardware, Firmware oder Software gebunden, da ein PIN/TAN-Verfahren eingesetzt wird.
Der serverseitige EVG wird auf mehreren Wahlservern betrieben. Zur IT-Umgebung des serverseitigen EVG zählen die Teile der Wahlserver, die zur Verwendung des EVG notwendig sind, also z.B. die Hardware, das Betriebssystem und das lokale Netzwerk in einer Rechenzentrumsumgebung. Die IT-Umgebung ist für alle serverseitigen EVG identisch. Jeder serverseitige EVG, mit Ausnahme des Wahlvorstandsinterface sollte auf einem eigenen Server – mit jeweils differierenden Zugangsdaten – betrieben werden.

Das Netzwerk zur Verbindung von Endgerät und Wahlserver wird als beliebiges Weitbereichsnetzwerk ohne spezifische Leistungsmerkmale angenommen.

Für die Anpassung der Mindestanforderungen an die Rahmenbedingungen von konkreten Wahlen bitte den Hersteller kontaktieren!

Der EVG ist prinzipiell betriebssystemunabhängig und benötigt als Grundlage auf dem Wahlserver eine Java Laufzeitumgebung und einen Java Application Webserver (Apache Tomcat). Diese sind explizit nicht Bestandteil des EVG.

Im Folgenden ist die empfohlene weitere Software für den Betrieb des EVG aufgelistet, die nicht Bestandteil des EVG ist (s. auch A.Wahlserver):

- Betriebssystem Debian Linux 10 oder neuer (Buster)
- Installiertes Java Open JDK 11.0.11 oder neuer
- Apache Tomcat Server 9.0.x oder höher
- PostgreSQL-Datenbank 11 oder höher
- SMTP-Server zum Versand der E-Mail-Benachrichtigungen (postfix 3.4 oder neuer)

Vom verwendeten Betriebssystem wird in Einklang mit A.Wahlserver ein Schutz vor unbefugtem Zugriff auf die Wahlserver sowie einen Schutz vor Datenverlust im Rahmen der technischen Möglichkeiten erwartet. Dies setzt voraus, dass keine nicht benötigten Services auf den jeweiligen Wahlservern laufen und das Betriebssystem dem aktuellen Patch-Level entspricht.

Die jeweilige, auf einem Wahlserver installierte PostgreSQL-Datenbank, soll nur für die jeweilige EVG-Komponente und nicht über das Netz zugreifbar sein. Auf dem Server soll die Wahlapplikation als einzige installierte Anwendung laufen.

- Es wird empfohlen, die einzelnen Komponenten auf redundanten Servern in einem Master-Slave Verbund zu betreiben.
- Der Einsatz eines verschlüsselten Dateisystems ist zur Einhaltung der Konformität zum vorliegenden ST nicht notwendig.
- Eine Firewall sollte nach den üblichen Best-practices so konfiguriert sein, dass aus dem öffentlichen Netzwerk nur die Verbindungen zu der Weboberfläche erlaubt sind. Zusätzlich kann der Zugang auf das Wahlvorstandsinterface nach Bedarf auf bestimmte Rechner (IP-Basiert) eingeschränkt oder weiter über den Einsatz einer VPN-Verbindung abgesichert werden.

- Ein RAID1 oder 5–Verbund der Datenträger wird zur erhöhten Zuverlässigkeit empfohlen.

1.4 EVG-Beschreibung

1.4.1 EVG Bestandteile

Der EVG besteht aus folgenden Komponenten:

- Wählerverzeichnis EVG (kurz: Wählerverzeichnis) als Java-Archiv (JAR)
- Urnen EVG (kurz: Urne) als Java-Archiv (JAR)
- Validator EVG (kurz: Validator) als Java-Archiv (JAR)
- Wahlvorstandsinterface EVG (kurz: Wahlvorstandsinterface) als Java-Archiv (JAR)
- Einer gemeinsamen Bibliothek für die zuvor genannten 4 Komponenten (polyas-common) als Java-Archiv (JAR)

Zum EVG gehört die folgende Dokumentation:

- Handreichung für den Wähler
- Handreichung für den Wahlvorstand
- Handreichung für den Wahlveranstalter

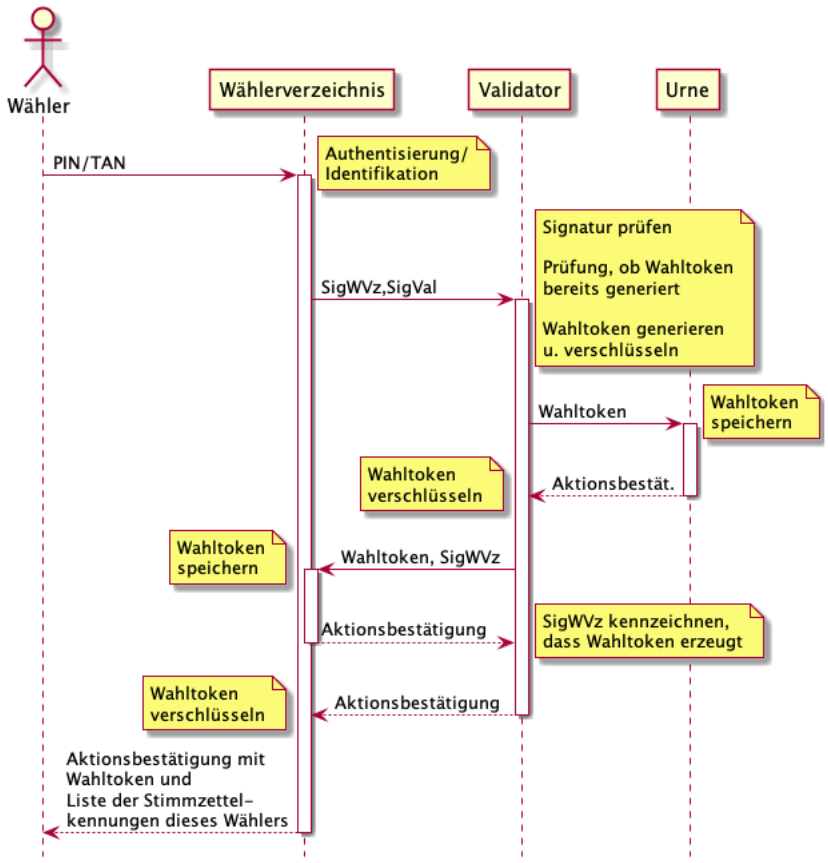

Abbildung 2: Darstellung der Stimmabgabe im Sequenzdiagramm I

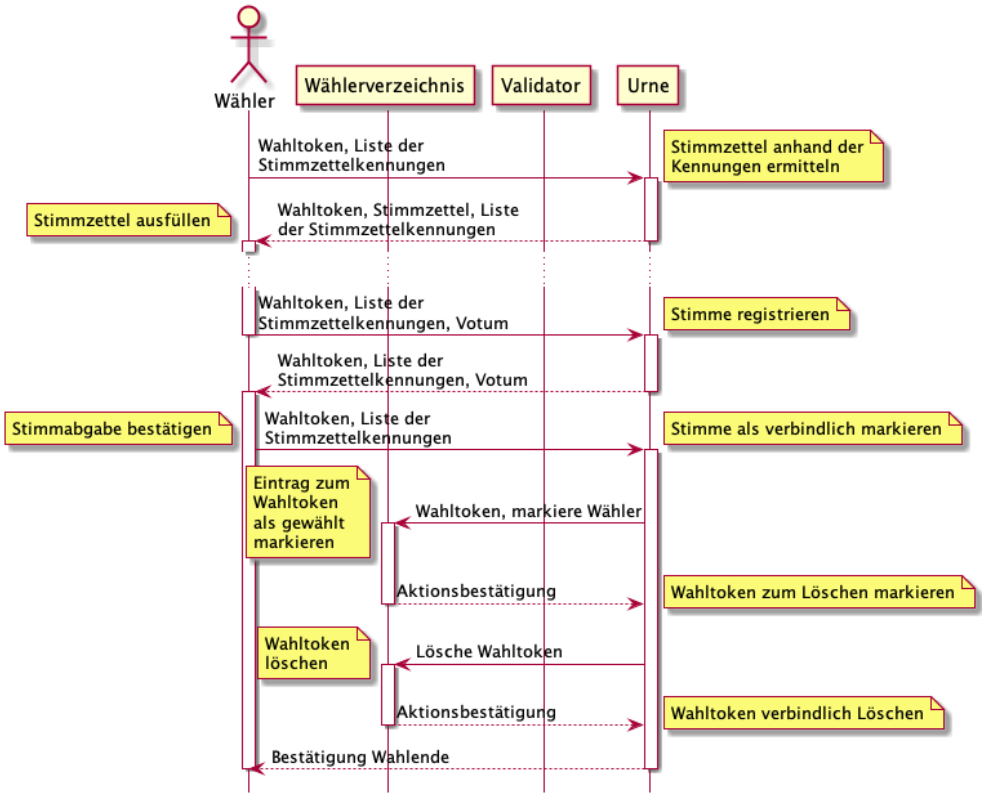

Abbildung 3: Darstellung der Stimmabgabe im Sequenzdiagramm II

1.4.1.1 Wählerverzeichnis EVG

Diese Komponente ist auf dem gleichen Wahlserver installiert, auf dem sich auch die Wahlberechtigungsliste mit den Authentisierungsdaten und den Stimmabgabevermerken (Datenbank) befindet. Der Wähler identifiziert und authentisiert sich gegenüber dem Wählerverzeichnis EVG. Anhand dieser Liste entscheidet der Wählerverzeichnis EVG, ob ein anfragender Wähler in der Wahlberechtigungsliste registriert ist, sich authentisieren kann und ob er ein Wähler mit bzw. ohne Stimmberechtigung ist. So wird sichergestellt, dass nur registrierte Wähler eine Stimme abgeben können. Im negativen Fall schickt der Wählerverzeichnis EVG eine entsprechende Fehlermeldung an den Wähler zurück. Im positiven Fall und falls sich der Wähler nie zuvor am Wählerverzeichnis EVG erfolgreich angemeldet hat, schickt das Wählerverzeichnis EVG die Wahlberechtigungsanfrage an den Validator EVG weiter, der ein anonymes, zufälliges Wählertoken generiert und dem Wählerverzeichnis EVG sowie dem Urne EVG für diese Wähler mitteilt. Dieses ordnet sie dem Wähler (temporär) zu und gibt es an den Wähler weiter. Sollte dieser Wähler schon einmal angemeldet sein, bekommt er die Möglichkeit zum Urne EVG zu gelangen ohne den Validator EVG abzufragen. Wenn ein Wähler seine Stimme abgegeben hat, teilt der Urnen EVG dem Wählerverzeichnis EVG dies mit, indem er ihm das entsprechende Wählertoken schickt. Der Wählerverzeichnis EVG setzt den Stimmabgabevermerk für den entsprechenden Wähler und löscht das Wählertoken.

1.4.1.2 Validator EVG

Diese Komponente kontrolliert den Wählerverzeichnis EVG. Eine solche Kontrolle ist im zugrundeliegenden Schutzprofil nicht vorgesehen. Um dennoch Wahlen mit größerem Angriffspotential adressieren zu können, setzt der EVG bereits eine Separation of Duty auf Architekturebene um. Die Idee dabei ist, dass einzelne Komponenten manipuliert sein können, diesen es aber nicht gelingt, die Wahl unbemerkt zu manipulieren. Der Validator EVG stellt sicher, dass ein manipulierter Wählerverzeichnis EVG nicht unbemerkt Wähler hinzufügen kann bzw. einzelne Wähler mehrfach zur Wahl zulassen kann. Dazu sind auf dem Wahlserver, auf dem der Validator EVG installiert ist, Signaturen der Wähler-Identifikationsdaten gespeichert. Erhält er eine Wahlberechtigungsnachfrage vom Wählerverzeichnis EVG, kann er prüfen, ob der entsprechende Wähler legitimiert existiert.

Falls für diesen Wähler noch keine Anfrage eingegangen ist, erzeugt der Validator EVG einen anonymes, zufälliges Wählertoken. Dies übermittelt er sowohl an den Urnen EVG (ohne Information über den anfragenden Wähler) und an den Wählerverzeichnis EVG. Außerdem vermerkt er, dass für diesen Wähler bereits ein Wählertoken erzeugt und erfolgreich an den Wählerverzeichnis EVG und den Urne EVG geschickt wurde. Auf diese Weise wird auch eine doppelte Stimmabgabe durch Manipulationen am Wählerverzeichnis EVG verhindert.

1.4.1.3 Urnen EVG

Diese Komponente ist auf dem Wahlserver installiert, auf dem die Stimmen in der Urne (einer Datenbank) gespeichert werden. Der Urnen EVG entscheidet über die Annahme bzw. Ablehnung einer eingehenden Stimme anhand der Tatsache, ob die Stimme von einer Person mit gültigem Wählertoken kommt. Hierzu erhält die Urne vom Validator gültige Wählertoken. Empfängt der Urnen EVG eine Stimme zusammen mit einem solchen gültigen Wählertoken vom Wähler, speichert er diese Stimme bei der verbindlichen Abgabe in der Urne, teilt dem Wählerverzeichnis EVG dieses Wählertoken mit, damit dieser den Wähler auf "hat gewählt" setzen kann, und löscht anschließend das Wählertoken. So ist sichergestellt, dass jeder registrierte Wähler nur eine Stimme abgeben kann. Die Speicherung erfolgt dabei in einer zufälligen Reihenfolge und ohne Zeitstempel.

Diese Separation hat also zur Folge, dass der Wählerverzeichnis EVG und der Validator EVG den Link zwischen Wähler und Wählertoken kennen und der Urnen EVG den Link zwischen Wählertoken und Stimme.

Da für den Moment des Wahlganges über das Wählertoken für einen Teilschritt des Wahlvorganges ein Abgleich zwischen Wähler und Stimme stattfinden und somit die Anonymität aufgehoben werden könnte, wird das Wählertoken stets zusätzlich für die jeweilige Komponente (Wählerverzeichnis, Urne) über RSA verschlüsselt. Somit müsste ein Angreifer nicht nur Zugriff auf beide Komponenten, Wählerverzeichnis und Urne, und deren Datenbanken haben, sondern auch in den Besitz der privaten Schlüssel mit zugehörigen Passphrases kommen. Das Wissen um die Zuordnung zwischen Wähler und Stimme mittels Wählertoken ist aber ohnehin nur temporär und ist nach Abschluss der Wahlhandlung nicht mehr im EVG gespeichert. Nach der Phase Wahlhandlung inklusive der Stimmauszählung ist daher kein Link mehr zwischen Wähler und seiner Stimme herzustellen.

1.4.1.4 Wahlvorstandsinterface EVG

Diese Komponente kann entweder auf einem eigenen System oder auf einem der anderen drei Wahlserver installiert werden. Über den Wahlvorstandsinterface EVG identifiziert und authentisiert sich der Wahlvorstand von seinem Endgerät und kann dann einen Selbsttest starten oder sich die Protokolle ansehen. Der Wahlvorstand kann außerdem eine der folgenden Operationen starten: Starten der Wahldurchführung, Beenden der Wahldurchführung und Starten der Stimmauszählung. Diese Operationen werden allerdings erst ausgeführt, wenn zwei Mitglieder des Wahlvorstands die entsprechende Operation gestartet haben (hierzu müssen sich die entsprechenden Mitglieder erneut mit zwei verschiedenen Sessions identifizieren und authentisieren). Der Wahlvorstandsinterface EVG informiert die anderen EVG Komponenten über die Zustandsänderungen und fordert ggf. Daten an, wie beispielsweise Protokolldaten und die Stimmen zur Auszählung. Der Wahlvorstandsinterface EVG stellt keine weitere Funktionalität zur Verfügung, wie etwa das Lesen von Stimmen während der Wahldurchführung oder das Hinzufügen, Löschen oder Verändern von Daten.

1.4.2 Phase Wahlvorbereitung (nicht Gegenstand der Evaluierung)

Folgende Aspekte müssen im Rahmen der Wahlvorbereitung, die nicht Teil der Evaluierung ist, erfüllt sein, damit der EVG seine Sicherheitsfunktionalität im vollen Umfang erfüllen kann:

- PIN/TAN wurde dem Wähler/Wahlvorstand sicher übermittelt
- Wähler/Wahlvorstand kennt URLs
- Wähler/Wahlvorstand kennt Fingerprints der Serverzertifikate

- Es existieren, zusätzlich zu den Schlüsseln für die https-Verbindung, zwei Schlüsselpaare pro EVG Komponente (Signaturschlüssel und Kommunikationsschlüssel). Die öffentlichen Schlüssel müssen dem jeweils anderen System bekannt sein. Die Signaturschlüssel werden für die Signatur und Ver-/Entschlüsselung der Datenbankeinträge verwendet, die Kommunikationsschlüssel stellen – nach derzeitigem Stand der Technik – eine zusätzliche vertrauliche und integre Verbindung zwischen den serverseitigen EVG-Komponenten her. Die Passphrasen für diese Schlüssel wurden dem Wahlvorstand sicher übermittelt.
- Das Wählerverzeichnis wird mit folgenden Daten befüllt: Identifikationsdaten der Wähler, Authentisierungsdaten der Wähler, Signaturen der Wählerverzeichniseinträge, Signaturen des Validators der Wählerverzeichniseinträge.
- Weder der Validator noch die Urne darf zu diesem Zeitpunkt Daten enthalten, dies wird durch das Wahlvorstandsinterface geprüft.
- Das Wahlvorstandsinterface wird mit folgenden Daten befüllt: Identifikationsdaten des Wahlvorstandes, Authentisierungsdaten des Wahlvorstandes, E-Mail-Adressen des Wahlvorstandes.

1.4.3 Ablauf der Wahlhandlung

Schritt 1 (Authentifizierung):

Der Wähler gibt die Wahl URL in seinem Webbrowser ein. Anhand des Fingerprints überprüft er, ob er mit dem richtigen Server des Wählerverzeichnis‘ (Wahlserver 1) kommuniziert. Anschließend gibt er seine Identifikationsdaten und sein Authentisierungsmerkmal ein. Der serverseitige Wählerverzeichnis EVG prüft, ob diese Kombination gültig ist und ob der Wähler bereits gewählt hat. Wenn die Kombination ungültig ist oder der Wähler bereits seine Stimme abgegeben hat, wird der Wähler zurück gewiesen. Wenn die anfragende Person allerdings ein Wähler in der Wahlberechtigungsliste, der am Wahlsystem nie zuvor angemeldet war, leitet das Wählerverzeichnis die Wahlberechtigungsanfrage an den serverseitigen Validator EVG weiter, der seinerseits prüft, ob der entsprechende Wähler zum ersten Mal am System angemeldet ist. Ist dies der Fall, generiert der Validator ein zufälliges Wählertoken. Dieses Wählertoken teilt er dem serverseitigen Urnen EVG mit und, falls dies erfolgreich war, anschließend dem Wählerverzeichnis. Das Wählerverzeichnis speichert dieses Wählertoken zu dem anfragenden Wähler in der Wahlberechtigungsliste und teilt dem Wähler sein Wählertoken mit. Ansonsten wird der Validator EVG nicht abgefragt, weil der Wähler bereits ein Wahltoken hat. Hat er seine Stimme abgegeben, wird er zurückgewiesen. Ansonsten kann er den Wahlvorgang durchführen.

Schritt 2 (Übermittlung des Wählertokens):

Mit diesem Wählertoken wird der Wähler automatisch mit dem Wahlserver 3 (für die Urnen) verbunden. Der serverseitige Urnen EVG prüft, ob das vom Wähler übertragene Wählertoken gültig ist und schickt dem Wähler ggf. den (leeren) Stimmzettel zurück. Dieser wird ihm in seinem Browser angezeigt. Nun prüft der Wähler erneut anhand des zweiten Fingerprints, ob er mit dem richtigen Urnenserver kommuniziert.

Schritt 3 (Stimmzettel ausfüllen):

Der Wähler kann in dem angezeigten Stimmzettel seinen Kandidaten/seine Kandidaten auswählen. Diese Auswahl kann er beliebig oft ändern bzw., falls er bei der Stimmabgabe gestört wird, den Vorgang sogar abbrechen. Im Fall, das der Wähler seine Auswahl getroffen hat, leitet er die Stimmabgabe ein. Hierbei wird der ausgefüllte Stimmzettel zusammen mit dem Wählertoken an den serverseitigen Urnen EVG übertragen.

Schritt 4 (Stimme bestätigen):

Die Urne prüft, ob das Wählertoken gültig ist und speichert ggf. den ausgefüllten Stimmzettel im Zwischenspeicher. Gleichzeitig wird dieser, zur Abgabe registrierte Stimmzettel, zusammen mit dem Wählertoken zurück an den Wähler geschickt. Dieser ausgefüllte Stimmzettel wird dem Wäh-

ler zur Bestätigung noch einmal angezeigt. Nun kann der Wähler den ausgefüllten Stimmzettel als seine Stimme verbindlich abgeben oder seine Stimme korrigieren.

Schritt 5 (Ende der Wahlhandlung):

Mit der verbindlichen Abgabe der Stimme ist das Ende der Wahlhandlung erreicht. Hierzu übermittelt der Wähler die Bestätigung zusammen mit dem Wählertoken an den serverseitigen Urnen EVG. In diesem letzten Schritt wird der im vorherigen Schritt gespeicherte ausgefüllte Stimmzettel unumkehrbar als Stimme in der Urne gespeichert. Der serverseitige Urnen EVG teilt dem serverseitigen Wählerverzeichnis EVG mit, dass das entsprechende Wählertoken verbraucht ist, und damit der zugehörige Wähler in der Wahlberechtigungsliste auf „hat gewählt" gesetzt werden muss. Ist dies erfolgt, löschen beide (serverseitiger Wählerverzeichnis EVG und serverseitiger Urnen EVG) das entsprechende Wählertoken. Damit ist keine Zuordnung der abgegebenen Stimmen zu dem Wähler mehr möglich.

Darüber hinaus wird dem Wähler bei der Kandidatenauswahl und Bestätigung der Stimmabgabe ein Logout-Button dargestellt, über den sich der Wähler abmelden kann.

Die eben abgegebene Stimme wird einem Stimmblock zugeordnet. Sobald dieser Stimmblock 30 Einträge enthält, wird automatisch eine Blockprüfsumme berechnet.

1.4.4 Ablauf des Wahlstarts

Schritt 1 (Authentisierung):

Der Wahlvorstand gibt die URL des Wahlvorstandsinterface in seinen Webbrowser ein. Anhand des Fingerprints überprüft er, ob er mit dem richtigen Server kommuniziert. Anschließend gibt er seine Identifikationsdaten und sein Authentisierungsmerkmal ein. Der serverseitige Wahlvorstandsinterface EVG prüft, ob diese Kombination gültig ist. Wenn die Kombination ungültig ist, wird der Wahlvorstand zurückgewiesen. Ist die Kombination gültig, leitet der Wahlvorstandsinterface EVG den Wahlvorstand an die Oberfläche des Wahlvorstandsinterface weiter.

Schritt 2 (Operationsanwahl):

Der Wahlvorstand wählt den Button "Wahlvorgang starten".

Schritt 3 (Separation of Duty (SoD)-Auskunft und Autorisierung):

Der Wahlvorstand erhält eine Auskunft, ob bereits genügend Autorisierungen für die Operation "Start des Wahlvorgangs" vorliegen. Ist dies nicht der Fall, kann er seine Autorisierung erteilen. Jeder Wahlvorstand kann die Operation während einer Wahldurchführung nur einmal autorisieren. Sollte das Attribut Wahlstatus bereits den Wert "Beendet" besitzen, wird dies dem Wahlvorstand in diesem Schritt mitgeteilt und er wird abgewiesen. Der EVG setzt die Datenbanken der Urne, des Wählerverzeichnisses und des Validators zurück. Liegen bereits genügend Autorisierungen vor, wird der Wahlvorstand zum nächsten Schritt geleitet. Hat der Wahlvorstand seine Autorisierung für diese Operation bereits erteilt, aber es liegen noch nicht genug weitere Autorisierungen vor, wird ihm dies mitgeteilt. Bei Abmeldung des Wahlvorstands verringert sich die Anzahl der Autorisierungen entsprechend.

Schritt 4 (Freischaltung):

Die sichere Kommunikation zwischen den serverseitigen EVG-Komponenten wird initiiert, und es werden die EVG-Komponenten freigeschaltet. Der Wahlvorstand gelangt zurück zu Schritt 3, oder wenn alle Applikationen gestartet wurden zu Schritt 5.

Schritt 5 (Wahldurchführungsattribut):

Sind alle Wahlapplikationen gestartet, nimmt das Attribut Wahlstatus im Wahlvorstandsinterface den Wert "UP" an.

1.4.5 Ablauf des Wiederanlaufs der Wahl

Der Wiederanlauf gestaltet sich analog zum Wahlstart mit folgender Ausnahme des Zurücksetzens der Datenbanken für Urne, Wählerverzeichnis und Validator. Hier wird der Hinweis ausgegeben, dass dies beim Wiederanlauf zulässig ist.

1.4.6 Ablauf des Wahlstopps

Schritt 1 (Authentisierung):

Äquivalent zu 1.4.4

Schritt 2 (Operationsanwahl):

Der Wahlvorstand wählt den Button "Wahlvorgang stoppen". Dieser ist nur anwählbar, wenn das Attribut Wahlstatus den Wert "UP" besitzt.

In der Konfiguration kann der Wahlendezeitpunkt hinterlegt werden. Wird die Aktion Wahlstopp zeitlich vor dem konfigurierten Wahlendezeitpunkt ausgelöst, erscheint ein Warnhinweis. Dennoch ist durch ein explizites Bestätigen des Wahlvorstandes ein Wahlstopp möglich. Wird kein Wahlendezeitpunkt in der Konfiguration hinterlegt, erscheint in diesem Fall der folgende Hinweis: „Achtung: Bevor Sie die Wahl endgültig beenden, prüfen Sie zuerst, ob der offizielle Wahlende-Zeitpunkt bereits erreicht ist!“

Schritt 3 (SoD-Auskunft und Autorisierung):

Der Wahlvorstand erhält eine Auskunft, ob bereits genügend Autorisierungen für die Operation "Stoppen des Wahlvorgangs" vorliegen. Ist dies nicht der Fall, kann er seine Autorisierung erteilen. Liegen bereits genug Autorisierungen vor, wird der Wahlvorstand zum nächsten Schritt geleitet. Hat der Wahlvorstand seine Autorisierung für diese Operation bereits erteilt, aber es liegen noch nicht genügend weitere Autorisierungen vor, wird ihm dies mitgeteilt. Bei Abmeldung des Wahlvorstands verringert sich die Anzahl der Autorisierungen entsprechend.

Schritt 4 (Auslösen des Wahlendes):

Dem Wahlvorstand wird der Button "Wahlvorgang stoppen" präsentiert. Ein Klick des Wahlvorstands auf diesen Button führt zum nächsten Schritt.

Schritt 5 (Inaktivieren der Wahlapplikationen):

Mittels verschlüsselter Kommunikation wird vom Wahlvorstandsinterface EVG zunächst der Validator EVG deaktiviert, damit sich keine neuen Wähler mehr anmelden können. Solange Wählerverzeichnis EVG und Urnen EVG noch aktiv sind, ist ein Abschluss der Wahlhandlung für bereits angemeldete Wähler noch möglich. Nach einer vorgegebenen, durch Wahlvorstand bestimmten Zeit werden dann auch Wählerverzeichnis EVG und Urnen EVG deaktiviert. Damit sind die Wahlserver in einem Modus, der keine Anmeldung von Wählern mehr erlaubt. Das Attribut Wahlstatus nimmt den Wert "DISABLED" an.

1.4.7 Ablauf der Protokolldateieinsicht

Schritt 1 (Authentisierung):

Äquivalent zu 1.4.4

Schritt 2 (Operationsanwahl):

Der Wahlvorstand wählt den Button "Protokolldateien".

Schritt 3 (Holen der Protokolldateien):

Das Wahlvorstandsinterface verbindet sich per https verschlüsselt an Wählerverzeichnis-, Urnen-, und Validator EVG an und fordert die Protokolldateien an. Diese werden als komprimierter Zeichenstrom verschlüsselt an das Wahlvorstandsinterface gesendet.

Schritt 4 (Anzeige der Protokolldateien):

Der Wahlvorstand erhält die Protokolldateien des Wählerverzeichnis EVG, Urnen EVG und Validator EVG und des Wahlvorstand EVG auf dem Bildschirm angezeigt.

1.4.8 Ablauf der Selbsttests

Schritt 1 (Authentisierung):

Äquivalent zu 1.4.4

Schritt 2 (Operationsanwahl):

Der Wahlvorstand wählt den Button "Selbsttest".

Schritt 3 (Holen der Selbsttestdaten):

Bei der Durchführung des Selbsttest wird auf die in Abschnitt 1.4.3 erwähnten Blockprüfsummen der Wählerstimmblöcke zurückgegriffen. Zuerst holt das Wahlvorstandsinterface per authentisierter und verschlüsselter Verbindung die aktuelle Blockprüfsumme aus der Datenbank des Wählerverzeichnis EVG. Anschließend wird die aktuell in die Datenbank geschriebene Blockprüfsumme des Urnen EVG abgerufen. Zeitgleich wird auf dem Urnen EVG die aktuelle Blockprüfsumme berechnet und ebenfalls zurückgeliefert. Der Validator EVG wird mittels eines verschlüsselten Aufrufs auf Verfügbarkeit geprüft.

Schritt 4 (Prüfung der Datenintegrität):

Mit dem Ankommen der Daten am Wahlvorstandsinterface EVG ist die Funktion der Infrastruktur gewährleistet. Nun werden die drei gelieferten Blockprüfsummen verglichen. Bei problemlos funktionierenden Datenträgern müssen die im Wählerverzeichnis EVG gespeicherte, die im Urnen EVG gespeicherte sowie die ad hoc berechnete Blockprüfsumme exakt übereinstimmen. Ist dies der Fall, wird der Selbsttest als ohne Fehler durchgeführt angesehen.

Schritt 5 (Ergebnisverarbeitung):

Lief der Selbsttest ohne Fehler wird dies dem Wahlvorstand auf der nächsten Seite mitgeteilt. Wurde beim Selbsttest ein Fehler festgestellt, wird dies ebenfalls mitgeteilt. Zusätzlich wird im Fehlerfall an alle E-Mail-Adressen der Wahlvorstände eine Warnung über die erkannte Fehlfunktion des EVG versandt.

1.4.9 Ablauf der Auszählung/Archivierung

Schritt 1 (Authentisierung):

Äquivalent zu 1.4.4

Schritt 2 (Operationsanwahl):

Der Wahlvorstand wählt den Button "Auszählung und Archivierung". Dieser ist nur anwählbar, wenn das Attribut Wahlstatus den Wert "DISABLED" besitzt.

Schritt 3 (SoD-Auskunft und Autorisierung):

Dem Wahlvorstand werden angezeigt, wie viele Stimmen für jeden Stimmzettel bereits in der Urne eingegangen sind. Der Wahlvorstand erhält außerdem eine Auskunft, ob bereits genug Autorisierungen für die Operation "Auszählung und Archivierung" vorliegen. Ist dies nicht der Fall kann er seine Autorisierung erteilen. Liegen bereits genug Autorisierungen vor, wird der Wahlvorstand zum nächsten Schritt geleitet. Liegen noch nicht genug Autorisierungen vor, wird der Wahlvorstand abgewiesen. Hat der Wahlvorstand seine Autorisierung für diese Operation bereits erteilt aber es lie-

gen noch nicht genug weitere Autorisierungen vor, wird ihm dies mitgeteilt. Bei Abmeldung des Wahlvorstands verringert sich die Anzahl der Autorisierungen entsprechend.

Schritt 4 (Anzeige der eingegangenen Stimmen):

Der Wahlvorstand bekommt erneut angezeigt wie viele Stimmen zu den einzelnen Stimmzetteln in der Urne eingegangen sind.

Schritt 5 (Auszählung):

Der Wahlvorstandsinterface EVG holt mittels authentisierter und verschlüsselter Kommunikation die Stimmen vom Urnen EVG. Nachdem die Stimmdatensätze vollständig übermittelt wurden, werden diese ausgezählt.

Schritt 6 (Holen der Archivierungsdaten):

Mittels authentisierter und verschlüsselter Kommunikation holt sich der Wahlvorstandsinterface EVG vom Wählerverzeichnis-, Urnen-, und Validator EVG sämtliche Protokolldateien und schreibt diese in eine Datei. Danach verbindet sich der Wahlvorstandsinterface EVG mittels authentisierter und verschlüsselter Kommunikation sowohl mit dem Wählerverzeichnis- als auch dem Urnen-EVG und fordert ein komplettes Abbild der Datenbank an. Dies wird jeweils verschlüsselt und komprimiert an das Wahlvorstandsinterface übertragen und enthält insbesondere die Wahlberechtigungsliste wie auch die einzelnen Stimmen in verschlüsseltem Format. Diese Datenbankabbilder werden ebenfalls jeweils in eine Datei geschrieben.

Schritt 7 (Erstellen des Archivs):

Die geschriebenen Dateien werden vom Wahlvorstandsinterface EVG in einem ZIP-Archiv zusammengefasst. Die ursprünglichen Dateien werden dabei gelöscht.

Schritt 8 (Erzeugung des Manipulationsschutz):

Das erstellte Archiv wird mit einer Archivprüfsumme versehen und im Hexadezimal-Format in eine Textdatei geschrieben, die den Dateinamen des Archivs mit der Endung `.sig` trägt. Anhand dieser Archivprüfsumme können Manipulationen an den Archivdaten später festgestellt werden.

Schritt 9: (Ergebnisdarstellung):

Dem Wahlvorstand werden die Ergebnisse der Auszählung mitgeteilt. Gleichzeitig bedeutet dies, dass die Archivierung und Erzeugung des Manipulationsschutzes erfolgreich abgeschlossen wurden.

1.4.10 Weitere Aspekte

Der EVG protokolliert, wie in Abs. 1.3.3.8 dargestellt.
Der EVG reagiert auf Störungen, wie in Abs. 1.3.3.7 dargestellt.

2 Postulate zur Übereinstimmung

Dieses ST postuliert Übereinstimmung mit CC Version 3.1 Revision 5
Dieses ST ist CC **Part 2 konform**.
Dieses ST ist CC **Part 3 konform**.
Dieses ST ist **augmentiert EAL 2** um die Komponenten

- ALC_CMC.3 (ersetzt ALC_CMC.2),
- ALC_CMS.3 (ersetzt ALC_CMS.2),
- ALC_DVS.1 und
- ALC_LCD.1.

Dieses ST postuliert Konformität mit dem BSI-Schutzprofil BSI-CC-PP-0037 **[7]** (dieses verlangt strict conformance).

2.1 Übereinstimmung mit dem PP-Typ

Der EVG-Typ im ST entspricht dem EVG-Typ im PP bis auf die folgenden Erweiterungen:

I. Zur Gewährleistung des Wahlgeheimnisses wurde der serverseitige EVG auf unterschiedliche Systeme unterteilt (Validator, Wählerverzeichnis, Urne, Wahlvorstandsinterface). Dies ist vom PP-Autoren explizit vorgesehen (vgl. Anwendungsnotiz 3, [7]).
II. Das Einsatzszenario wurde erweitert, da ein Remote-Zugriff für den Wahlvorstand ermöglicht wird. Dies ist vom PP-Autoren explizit vorgesehen (vgl. Anwendungsnotiz 19, [7]).
III. Weiterhin nutzt der Wähler keinen dedizierten Client-EVG, sondern einen kompatiblen Browser (vgl. Abschnitt 1.3). Dies ist ebenfalls vom PP-Autoren explizit vorgesehen (vgl. Anwendungsnotiz 3, [7]).
IV. In T.UnbefugterWähler ist ein Fehler berichtigt worden: Das Authentisierungsmerkmal (des Wählers) gehört nicht zu den zu schützenden Werten. Der Angriff richtet sich vielmehr gegen die in der Bedrohung angeführte Authentisierungsnachricht.

Entsprechend fanden Anpassungen in der Definition des Sicherheitsproblems, der Sicherheitsziele, der funktionalen Sicherheitsanforderungen und der Sicherheitsfunktionen im Sinne des PP-Autors (auf der Grundlage der Anwendungsnotizen) statt.

2.2 Übereinstimmung mit der Definition des Sicherheitsproblems

Um die Erweiterungen des EVGs gegenüber dem PP abzubilden, wurden folgende Anpassungen in der Definition des Sicherheitsproblems durchgeführt:

- Die Bedrohungen T.IntegritätNachricht wurde um die Unterfälle e) und f) erweitert. Dies beruht auf Erweiterung I) und II).
- Die Bedrohung T.GeheimNachricht wurde im Unterfall a) und um den Unterfall c) erweitert. Dies beruht auf Erweiterung I) (samt Realisierung mit Wählertoken) und II).
- Die Bedrohung T.AuthentizitätServer wurde erweitert. Dies beruht auf Erweiterung I) und II).
- Die Bedrohung T.ArchivierungWahlgeheimnis wurde dahingehend präzisiert, dass keine Zusatzdaten erforderlich sind, vgl. Begründung zur Entfernung von A.ArchivierungWahlgeheimnis.
- Die organisatorische Sicherheitspolitik P.OneVoterOneVote wurde dahingehend spezifiziert, dass kein clientseitiger EVG eingesetzt wird.
- Die Annahme A.Wahlvorstand wurde dahingehend spezifiziert, dass auch das Endgerät des Wahlvorstands, welches dieser für seinen Remote-Zugriff nutzt, vertrauenswürdig ist. Dies beruht auf Erweiterung II).

- Die Annahme A.AuthDaten wurde dahingehend spezifiziert, dass in diesem Kontext auch der Wählertoken relevant ist. Dies beruht auf Erweiterung I).
- Die Annahme A.AuthentizitätServer wurde dahingehend spezifiziert, dass auch der Wahlvorstand überprüft, ob er mit dem korrekten EVG kommuniziert. Dies beruht auf Erweiterung II).
- Die Annahme A.Endgerät wurde dahingehend spezifiziert, dass kein clientseitiger EVG eingesetzt wird. Dies beruht auf Erweiterung III).
- Die Annahme A.ArchivierungWahlgeheimnis wird nicht benötigt, weil der EVG eine entsprechende Sicherheitsleistung erbringt. Inhaltlich wird diese Annahme aus dem PP durch das Sicherheitsziel für den EVG O.ArchivierungWahlgeheimnis adressiert.
- Die Annahme A.GeschützteKommunikation wurde dahingehend spezifiziert, dass der serverseitige EVG auf unterschiedliche Systeme unterteilt ist. Dies beruht auf Erweiterung I).

2.3 Übereinstimmung mit den Sicherheitszielen

Um die Erweiterungen des EVGs gegenüber dem PP abzubilden, wurden folgende Anpassungen in der Definition der Sicherheitsziele durchgeführt:

- Die Sicherheitsziele für den EVG O.IntegritätNachrichtWahlvorstand und O.IntegritätNachrichtServerServer wurden hinzugefügt, um die Erweiterung der Bedrohung T.IntegritätNachricht zu begegnen.
- Das Sicherheitsziel O.GeheimNachricht wurde um die Realisierung mit Wählertoken ergänzt.
- Die Sicherheitsziele für den EVG O.GeheimNachrichtWahlvorstand und O.GeheimNachrichtServerServer wurden hinzugefügt, um die Erweiterung der Bedrohung T.GeheimNachricht zu begegnen.
- Das Sicherheitsziel für den EVG O.AuthentizitätServerWahlvorstand wurde hinzugefügt, um die Erweiterung der Bedrohung T.AuthentizitätServer zu begegnen.
- O.ArchivierungIntegrität wurde im Sinne des PP-Autors (vgl. Anwendungsnotiz 20 [7]) angepasst. Der EVG erstellt keinen Manipulationsschutz für weitere Daten, die nicht Bestandteil der Wahldurchführung und Auszählung sind.
- OAuthentizitätServer ist an die Abgrenzung des EVG (kein clientseitiger EVG) angepasst worden.
- O.Störung wurde an die Unterteilung des serverseitigen EVG angepasst.

Die Sicherheitsziele für die Umgebung sind im ST verglichen mit dem PP entsprechend den geänderten Annahmen angepasst worden:

- OE.Wahlvorstand wurde entsprechend der Annahme A.Wahlvorstand erweitert.
- OE.AuthDaten wurde entsprechend der Annahme A.AuthDaten erweitert.
- OE.AuthentizitätServer wurde entsprechend der Annahme A.AuthentizitätServer gemäß Anwendungsnotiz 24 [7] erweitert.
- OE.Endgerät wurde entsprechend der Annahme A.Endgerät gemäß Anwendungsnotiz 21 [7] spezifiziert.
- OE.Wahlserver wurde gemäß Anwendungsnotiz 22 [7] spezifiziert.
- OE.ArchivierungWahlgeheimnis wurde analog zur Annahme A.ArchivierungWahlgeheimnis entfernt.
- OE.GeschützteKommunikation wurde entsprechend Annahme A.GeschützteKommunikation spezifiziert.
- OE.Zwischenspeicherung wurden gemäß Anwendungsnotiz 26 [7] spezifiziert.

2.4 Übereinstimmung mit den Sicherheitsanforderungen

Analog zu den hinzugefügten Sicherheitszielen für den EVG wurden entsprechende Sicherheitsanforderungen formuliert (außerdem sind alle Sicherheitsanforderungen aus dem PP auch im ST enthalten):

- FDP_UIT.1B wurde hinzugefügt, um das Sicherheitsziel O.IntegritätNachrichtWahlvorstand zu erreichen.
- FTP_TRP.1B wurde hinzugefügt, um das Sicherheitsziel O.AuthentizitätServerWahlvorstand zu erreichen.
- FPT_ITT.1 wurde hinzugefügt, um die Sicherheitsziele O.IntegritätNachrichtServerServer und O.GeheimNachrichtServerServer zu erreichen.
- FDP_UCT.1B wurde hinzugefügt, um das Sicherheitsziel O.GeheimNachrichtWahlvorstand zu erreichen.
- Die funktionalen Sicherheitsanforderungen wurden – sofern notwendig – an CC Version 3.1 Revision 5 angepasst.

3 Definition des Sicherheitsproblems

Die Darlegung des Sicherheitsproblems beschreibt die Sicherheitsaspekte der Umgebung, in der der EVG eingesetzt werden soll, und die erwartete Art des Gebrauchs. Sie umfasst all die organisatorischen Sicherheitspolitiken, die als relevant gelten. Zur Definition des Sicherheitsproblems gehören insbesondere die Bedrohungen der Sicherheit, die in der Umgebung vorhanden sind bzw. von deren Vorhandensein ausgegangen wird.
Bei der Definition des Sicherheitsproblems wurde Folgendes berücksichtigt:

- die materielle Umgebung des EVG, die alle für die Sicherheit relevanten Aspekte der EVG-Einsatzumgebung angibt, einschließlich bekannter materieller und personeller Sicherheitsvorkehrungen,
- die Werte, die Schutz durch die Bestandteile des EVG benötigen, für die die Sicherheitsanforderungen oder -politiken gelten werden.

Zu schützende Werte

- Authentisierungsnachricht (Benutzerdaten)
- Authentisierungsdaten (TSF-Daten)
- Identifikationsdaten (Benutzer- und TSF-Daten)
- Wählertoken (Benutzer- und TSF-Daten)
- Stimmzetteldaten (Benutzerdaten)
- Stimmzettel (Benutzerdaten)
- Stimme (Benutzerdaten)
- Stimmdatensatz (Benutzerdaten)
- Rückmeldung (Benutzerdaten)
- Wahldaten (Benutzerdaten)
- Wahldurchführungsdaten (Benutzerdaten)
- Protokollaufzeichnungen (Benutzerdaten)
- Ergebnis (Benutzerdaten)
- Serverkommunikationsdaten (TSF-Daten)

Subjekte

Die folgenden Subjekte sind Benutzer, die in die Wahldurchführung inkl. der Stimmauszählung einbezogen sind:

- Registrierter Wähler
- Wahlvorstand

Die folgenden Subjekte sind Angreifer, also Personen, die den ordnungsgemäßen Ablauf der Wahldurchführung zu stören, zu manipulieren oder zu verhindern versuchen:

- Netzwerkangreifer
- Registrierter Wähler
- Unbefugter Wähler
- Person, die nach der Phase „Wahldurchführung inkl. Stimmauszählung“ Zugriff auf die im EVG gespeicherten Daten hat.

3.1 Bedrohungen

Hier werden alle Bedrohungen gegen die zu schützenden Werte betrachtet, die bei der Bedrohungsanalyse als für den EVG relevant ermittelt werden. Die CC charakterisieren eine Bedrohung anhand ihrer Urheber, der Angriffe und der angegriffenen Werte. Urheber von Bedrohungen werden beschrieben, indem auf Aspekte wie Fachkenntnisse, verfügbare Betriebsmittel und Motivation ein-

gegangen wird. Angriffe werden beschrieben, indem Aspekte wie Angriffsmethode, Gelegenheiten und ausgenutzte Schwachstellen angesprochen werden.

3.1.1 Definitionen – Methode, Gelegenheit, Fachkenntnis

Methode – Ein Angriff wird als direkt bezeichnet, wenn der Angreifer durch dessen erfolgreiche Ausführung sein endgültiges Ziel (also entweder die Manipulation des Wahlergebnisses und/oder das Brechen des Wahlgeheimnisses) direkt erreicht.

Gelegenheit – Ein Angriff wird als aktiv bezeichnet, wenn der Angriffszeitpunkt durch den Angreifer bestimmt werden kann, indem er aktiv ins Geschehen eingreift, beispielsweise durch Erzeugen, Löschen oder Verändern von Nachrichten auf dem Übertragungsweg. Das reine Mitlesen von Nachrichten zählt zu den passiven Angriffen.

Fachkenntnis und Verfügbare Betriebsmittel des Angreifers

A) Netzwerkangreifer

- Fachkenntnis: Profi
- Verfügbare Betriebsmittel: Betriebsmittel, die leicht zu beschaffen sind.
- Es wird von einem Angriffspotential ausgegangen, das nach CC Profiwissen voraussetzt, aber mit üblichem Equipment auskommt und auf die Fähigkeit zur Durchführung von Netzwerkangriffen (z.B. Man-in-the-Middle Angriffe) beschränkt ist.
- Angreifer, der Daten auf dem Übertragungsweg mitliest, löscht, hinzufügt oder verändert. Der Netzwerkangreifer hat keinen physikalischen Zugang zum Endgerät des Wählers.

B) Registrierter Wähler

- Fachkenntnis: Laie
- Verfügbare Betriebsmittel: Endgerät [...]

C) Unbefugter Wähler

- Fachkenntnis: Laie
- Verfügbare Betriebsmittel: Endgerät [...] und Betriebsmittel, die leicht zu beschaffen sind.

D) Person, die nach der Phase „Wahldurchführung inkl. Stimmauszählung“ Zugriff auf die im EVG gespeicherten Daten hat

- Fachkenntnis: Laie
- Verfügbare Betriebsmittel: Betriebsmittel, die leicht zu beschaffen sind [...].

3.1.2 Definition von Bedrohungen

T.UnbefugterWähler Ein unbefugter Wähler oder ein Wähler ohne Stimmberechtigung gibt eine Stimme ab.

- Motivation: Er möchte das Wahlergebnis manipulieren. Dazu fälscht er die Identifikationsdaten und die Authentisierungsnachricht um sich unberechtigt als Wähler mit Stimmberechtigung auszugeben und im Namen des berechtigten Wählers eine Stimme abzugeben.
- Angriffsmethode: direkt
- Gelegenheiten: aktiv

- Ausgenutzte Schwachstelle: Authentisierungsverfahren
- Angegriffener Wert: Identifikations-/ Authentisierungsdaten, […] Authentisierungsnachricht, Ergebnis.

T.Beweis Ein Wähler mit Stimmberechtigung nutzt Daten auf seinem Endgerät, die während der Wahldurchführung vom EVG erzeugt werden, um seine Wahlentscheidung gegenüber einer anderen Person zu beweisen.

- Motivation: Der Beweis wird benötigt, um die Forderung einer Erpressung zu erfüllen oder die Gegenleistung für einen Stimmenkauf zu erbringen.
- Angriffsmethode: direkt
- Gelegenheiten: aktiv
- Ausgenutzte Schwachstelle: Dateien, Nachrichten, Meldungen oder ähnliches, das der EVG auf dem Endgerät zur Verfügung stellt.
- Angegriffener Wert: Stimme.

T.IntegritätNachricht Ein Netzwerkangreifer greift direkt in das Netzwerk ein, um Daten auf dem Übertragungsweg unbemerkt zu löschen, hinzuzufügen, wiedereinzuspielen oder zu verändern.

- Motivation: Das Wahlergebnis wird manipuliert
  (a) Die betroffenen Nachrichten können Stimmdatensätze enthalten, und durch Löschen, Hinzufügen, Wiedereinspielen oder Verändern kann der Angreifer das Wahlergebnis direkt manipulieren.

  (b) Die betroffenen Nachrichten können Stimmdatensätze oder Identifikationsdaten enthalten. Authentisierungsnachrichten können auch betroffen sein. Bestimmte Wähler können dadurch von der Online-Wahl ausgeschlossen werden.

  (c) Die betroffenen Nachrichten können Stimmzetteldaten enthalten. Der Stimmzettel wird dem Wähler in veränderter Form angezeigt.

  (d) Die betroffene Nachricht könnte die Rückmeldung enthalten, um dem Wähler vorzutäuschen, dass seine Stimme erfolgreich abgegeben, also in der Urne gespeichert, wurde.

  (e) Die betroffenen Nachrichten können das Ergebnis enthalten. Dem Wahlvorstand wird ein verändertes Wahlergebnis angezeigt.

  (f) Die betroffenen Nachrichten können solche sein, die zwischen den einzelnen serverseitigen EVGs bzw. zwischen den entsprechenden Wahlservern ausgetauscht werden. Hierdurch kann der Ablauf der Wahl gestört werden. Durch Störung des Prozessablaufs der Wahlhandlung kann der Wähler sein Wahlrecht verlieren oder mehrfach eine Stimme abgeben. Durch Störung der Prozesssteuerung kann der Wahlvorstand die Kontrolle über die Wahldurchführung inkl. Stimmauszählung verlieren.
- Angriffsmethode: direkt
- Gelegenheiten: aktiv
- Ausgenutzte Schwachstelle: Netzwerk
- Angegriffener Wert: Ergebnis und (a) Stimmdatensatz; (b) Stimmdatensatz, Identifikationsdaten, Authentisierungsnachricht des Wählers; (c) Stimmzetteldaten; (d) Rückmeldung. (e) Ergebnis, (f) Wählertoken, Serverkommunikationsdaten

T.GeheimNachricht Ein Netzwerkangreifer greift direkt in das Netzwerk ein, um die mit der Wahldurchführung zusammenhängenden Daten auf dem Übertragungsweg mitzulesen.

- Motivation:
  (a) Er kann personenbezogene Identifikationsdaten, Wählertoken und Stimmdatensätze nutzen, um eine Zuordnung zwischen Stimme und Wähler herzustellen und damit das Wahlgeheimnis zu brechen.

  (b) Er kann Zwischenergebnisse berechnen, wenn er die einzelnen Stimmdatensätze mitliest und die darin enthaltenen Stimmen aufsummiert.

  (c) Die betroffenen Nachrichten können Identifikationsdaten und Authentisierungsnachrichten des Wahlvorstands enthalten. Kennt man diese Daten, ist man in der Lage sämtliche Operationen des Wahlvorstands auszuführen; unter anderem ist es möglich, den Wahlablauf durch Stoppen der Wahl zu stören.
- Angriffsmethode: direkt
- Gelegenheiten: passiv
- Ausgenutzte Schwachstelle: Kommunikationsnetz
- Angegriffener Wert: (a) Identifikationsdaten, Wählertoken, Stimmdatensatz, Stimme; (b) Stimmdatensatz, Stimme, Ergebnis; (c) Identifikationsdaten und Authentisierungsnachrichten des Wahlvorstand

T.AuthentizitätServer Ein Netzwerkangreifer leitet den Wähler/Wahlvorstand auf einen gefälschten Wahlserver um. Der Wähler/Wahlvorstand kommuniziert in der Folge nicht mit dem authentischen Wahlserver.
- Motivation: Alle Punkte von T.IntegritätNachricht und T.GeheimNachricht
- Angriffsmethode: indirekt
- Gelegenheiten: aktiv
- Ausgenutzte Schwachstelle: Netzwerk
- Angegriffener Wert: Alle Werte von T.IntegritätNachricht und T.GeheimNachricht

T.ArchivierungIntegrität Eine Person, die nach der Phase „Wahldurchführung inkl. der Stimmauszählung“ Zugriff auf die vom EVG gespeicherten Daten hat, fälscht oder verändert das gespeicherte Wahlergebnis, die gespeicherten Wahldurchführungsdaten und, falls erforderlich, die Protokollaufzeichnungen oder weitere Daten, um bei einer Nach- bzw. Neuzählung zu einem anderen Wahlergebnis zu kommen.
- Motivation: Das Wahlergebnis wird manipuliert.
- Angriffsmethode: direkt
- Gelegenheiten: aktiv
- Ausgenutzte Schwachstelle: kein Schutz der Daten durch den EVG nach Ende der Wahldurchführung inkl. der Stimmauszählung.
- Angegriffener Wert: Wahldurchführungsdaten, Stimme, Ergebnis

T.ArchivierungWahlgeheimnis Eine Person, die nach der Phase „Wahldurchführung inkl. der Stimmauszählung“ Zugriff auf die im EVG gespeicherten Daten hat […], kann an Hand der im EVG gespeicherten Daten eine Zuordnung zwischen dem Wähler und seiner Stimme (im Klartext oder in verschlüsselter Form) herstellen.
- Motivation: Das Wahlgeheimnis brechen.
- Angriffsmethode: direkt
- Gelegenheiten: aktiv
- Ausgenutzte Schwachstelle: kein Schutz der Daten durch den EVG nach Ende der Wahldurchführung inkl. der Stimmauszählung.
- Angegriffener Wert: Wahldurchführungsdaten, Stimme

3.2 Organisatorische Sicherheitspolitik

Die Beschreibung organisatorischer Sicherheitspolitiken gibt die Politiken und Regeln an, mit denen der EVG übereinstimmen muss. Individuelle Aussagen sind so dargelegt, dass sie zu einer klaren Festlegung von Sicherheitszielen genutzt werden können.

P.Abbruch Der Wähler muss vor der Stimmabgabe jederzeit die Möglichkeit haben, die Wahlhandlung abzubrechen, ohne dabei seine Stimmberechtigung zu verlieren.

P.WahlBeenden Das versehentliche vorzeitige Beenden der Wahldurchführung muss verhindert werden. Der Wahlvorstand hat aber die Möglichkeit, die Wahldurchführung dennoch vor dem geplanten Wahlende-Zeitpunkt zu beenden.

P.Wahlende Nach dem Beenden der Wahldurchführung kann keine Wahlhandlung eröffnet oder weitergeführt werden, insbesondere können keine Stimmen mehr abgegeben werden.

P.WahlgeheimnisWahlvorstand Der Wahlvorstand ist während der Wahldurchführung nicht in der Lage mit Hilfe des EVG das Wahlgeheimnis zu brechen.

P.IntegritätWahlvorstand Der Wahlvorstand ist nicht in der Lage mit Hilfe des EVG Stimmen in die Urne hinzuzufügen. Er ist außerdem nicht in der Lage, die Stimmen in der Urne zu löschen oder gezielt zu verändern. Insbesondere existiert keine Funktion, mit deren Hilfe der Wahlvorstand in der Lage ist, den EVG nach dem Start der Wahldurchführung in seinen Anfangszustand zurücksetzen.

P.Zwischenergebnis Es muss sichergestellt werden, dass der Wahlvorstand keine Zwischenergebnisse berechnen kann.

P.Übereilungsschutz Der EVG darf nur Stimmdatensätze in der Urne speichern, die der Wähler nach expliziter Kontrolle seiner Stimme endgültig abgegeben hat.

P.Korrektur Der Wähler muss die Möglichkeit haben, seine Stimme bis zur endgültigen Abgabe beliebig oft zu korrigieren. Auch nach der expliziten Kontrolle der Stimme ist eine Korrektur möglich.

P.Rückmeldung Der registrierte Wähler erhält eine zutreffende Rückmeldung über die Erlaubnis bzw. Verweigerung und den Erfolg bzw. Misserfolg seiner Stimmabgabe.

P.Störung Der Wahlvorstand muss beim Erstanlauf und auf Anforderung durch Ausführung eines Selbsttests am serverseitigen EVG erkennen können, wenn eine technische Störung der Integrität der EVG-Sicherheitsfunktionen (TSF) oder der Benutzer- und TSF-Daten, die den korrekten Betrieb des EVG gefährden, vorliegt. Nach einem Absturz/Herunterfahren des serverseitigen EVG, des Wahlservers oder einem Ausfall der Kommunikation oder der Speichermedien muss der Wahlvorstand einen Wiederanlauf der Wahldurchführung ausführen können. Dabei muss der EVG die Integrität der Wahldurchführungsdaten gewährleisten.

P.Protokoll Vom serverseitigen EVG müssen mindestens für die in Kapitel 1.3.3.8 aufgelisteten Ereignisse inkl. der Zeitpunkte des Auftretens der Ereignisse Protokollaufzeichnungen erzeugt und

in der IT-Umgebung des serverseitigen EVG vor unberechtigten Manipulationen geschützt gespeichert werden. Dem Wahlvorstand muss die Durchsicht der Protokollaufzeichnungen ermöglicht werden.

P.OneVoterOneVote Es muss sichergestellt werden, dass ein Wähler nicht mehr als eine Stimme abgeben kann und ein registrierter Wähler seine Stimmberechtigung nicht verliert, ohne eine Stimme abgegeben zu haben. Dies muss insbesondere bei Abbrüchen der Wahlhandlung, die durch den Wähler, den [...] EVG, die IT-Umgebung des EVG sowie durch das Netzwerk verursacht werden, und bei jedem Wiederanlauf der Wahldurchführung gegeben sein.

P.AuthWahlvorstand Der EVG muss den Wahlvorstand vor jeder anderen Aktion identifizieren und authentisieren. Die Authentisierungsfunktion muss eine Separation of Duty unter den Mitgliedern des Wahlvorstandes unterstützen. Die Operationen zum Starten, Wiederanlaufen und Beenden der Wahldurchführung sowie zum Starten der Stimmauszählung mit Feststellung des Wahlergebnisses werden erst ausgeführt, wenn sie jeweils von mindestens zwei authentisierten Mitgliedern des Wahlvorstands unabhängig autorisiert wurden.

P.StartStimmauszählung Der Wahlvorstand kann die Stimmauszählung erst nach dem Beenden der Wahldurchführung starten.

P.Stimmauszählung Alle Stimmdatensätze, die nach Wahlende in der Urne gespeichert sind, gehen in die Stimmauszählung mit Feststellung des Wahlergebnisses ein.

3.3 Annahmen

Im Abschnitt Annahmen werden die Sicherheitsauflagen an die Umgebung angeführt, in der der EVG eingesetzt werden soll und deren Umsetzung angenommen wird. Dazu gehören:

- Informationen über den beabsichtigten Gebrauch des EVG, einschließlich Aspekte wie beabsichtigte Anwendung, potentielle Bedeutung der Werte und mögliche Einschränkungen der Benutzung, und
- Informationen über die Umgebung, in der der EVG eingesetzt werden soll, einschließlich materieller, personeller und Vernetzbarkeitsaspekte.

Annahmen betreffen alle Maßnahmen, die etwas zur IT-Sicherheit beitragen, aber nicht vom EVG selbst erwartet werden können. Ohne die Annahmen ist die EVG-Sicherheitsleistung beeinträchtigt. Damit ist jede Annahme eine Voraussetzung für die Wirksamkeit der Sicherheitsfunktionen.

3.3.1 Informationen über den beabsichtigen Gebrauch

A.Wahlvorbereitung Die Wahldaten sind zu Beginn der Wahldurchführung ordnungsgemäß und in der genehmigten, d.h. vom Wahlveranstalter verabschiedeten, Fassung auf dem Wahlserver installiert worden und die Urne ist leer. Die Phase Wahlvorbereitung ist also korrekt abgeschlossen. Der serverseitige EVG ist inkl. der Identifikations- und Authentisierungsdaten für den Wahlvorstand korrekt konfiguriert und initialisiert. Es liegt in der Verantwortung des Wahlveranstalters, eindeutige Zeitpläne für alle drei Wahlphasen vorzugeben. Der Wahlveranstalter ist insbesondere für die Festlegung des Wahlende-Zeitpunktes der Phase Wahldurchführung verantwortlich.

A.Beobachten Der Wähler achtet darauf, dass ihn niemand bei seiner Stimmabgabe beobachtet. Der Wahlveranstalter ist dafür verantwortlich, dem Wähler angemessene Hinweise für die unbeobachtete Stimmabgabe zu geben.

A.Wahlvorstand Der Wahlvorstand greift nur über den serverseitigen EVG auf die Benutzer- und TSF-Daten zu, d.h. er nutzt nur die vom serverseitigen EVG zur Verfügung gestellte Funktionalität. Der Wahlvorstand ist ausreichend geschult, um den sicheren Betrieb des EVG zu verstehen und benutzt den EVG in der beabsichtigten Weise. Jedes Mitglied des Wahlvorstands hat seine Identifikationsdaten und sein Authentisierungsmerkmal erhalten und gibt diese nicht an andere Personen weiter. Bei der Bestimmung des Wahlvorstandes ist vom Wahlveranstalter zu beachten, dass Personen nicht alleine Zugang und Zugriff zum serverseitigen EVG gewährleistet wird. Der Wahlvorstand nimmt seine Verantwortung zur Sicherung des Endgerätes wahr. Es wird angenommen, dass der EVG vom Wahlvorstand so benutzt wird, dass das Endgerät den Vorgang weder beobachten noch beeinflussen kann. Dazu gehört auch, dass der Wahlvorstand sein Endgerät nicht absichtlich für solche Zwecke manipuliert. Das Endgerät ist in der Lage, die Ausgabe des EVG korrekt anzuzeigen und die Eingaben des Wahlvorstands korrekt an die Wahlserver zu übertragen.

A.AuthDaten Der registrierte Wähler hat alle zur Durchführung der Wahl erforderlichen Daten, insb. die Identifikationsdaten und das Authentisierungsmerkmal, erhalten. Es liegt in der Verantwortung des Wahlveranstalters die Wähler zu informieren, wie sie mit ihren Identifikationsdaten, Authentisierungsmerkmalen und Wählertoken umgehen sollen, damit ihre Stimme nur berechtigt abgegeben werden kann. Der registrierte Wähler beachtet die Vorgaben des Wahlveranstalters zum Umgang mit diesen Daten, d.h. er gibt sie insbesondere nicht an andere Wähler weiter.

3.3.2 Informationen über die Umgebung

A.Endgerät Der Wähler nimmt seine Verantwortung zur Sicherung des Endgerätes wahr. Es wird angenommen, dass der [...] EVG [...] vom Wähler so [...] benutzt wird, dass das Endgerät den Vorgang der Stimmabgabe weder beobachten noch beeinflussen kann. Dazu gehört auch, dass der Wähler sein Endgerät nicht absichtlich für solche Zwecke manipuliert. Das Endgerät ist in der Lage, den Stimmzettel korrekt anzuzeigen, die Eingaben des Wählers korrekt an den Wahlserver zu übertragen und die Stimme nach der Wahlhandlung zu löschen.

A.Wahlserver Der Schutz des Wahlservers gegenüber Angriffen aus dem Netzwerk ist durch die Umsetzung eines Sicherheitskonzeptes für die Netzwerkanbindung, das Zugriffe von Netzwerkangreifern auf den Wahlserver ausschließt, gewährleistet.

A.Verfügbarkeit Die Robustheit, die Servicequalität und die Verfügbarkeit des Netzwerkes und des Wahlservers sind gegeben.

A.ServerRaum Außer dem Wahlvorstand hat während der Wahldurchführung bis zur Stimmauszählung niemand Zutritt zum Server-Raum und Zugang zum Wahlserver.

A.Speicherung Die Speichermedien funktionieren korrekt, d.h. die Integrität und die Verfügbarkeit aller gespeicherten Benutzer- und TSF-Daten sind gewährleistet. Fehler während der Speicherung von Stimmdatensätzen in der Urne werden den EVG-Sicherheitsfunktionen gemeldet.

A.Systemzeit Die Systemzeit wird von der IT-Umgebung des Servers bereitgestellt und entspricht der aktuellen Uhrzeit. Die benötigte Genauigkeit der Systemzeit wird vom Wahlveranstalter festgelegt.

A.Protokollschutz Die IT-Umgebung des serverseitigen EVG gewährleistet die vor unberechtigten Manipulationen geschützte Speicherung der vom serverseitigen EVG erzeugten Protokollaufzeichnungen.

A.AuthentizitätServer Der Wähler und der Wahlvorstand überprüfen, ob sie mit dem richtigen serverseitigen EVG kommuniziert.

[…]

A.GeschützteKommunikation Die IT-Umgebung ermöglicht den Betrieb einer vor Modifikation und Preisgabe geschützten Kommunikationsverbindung zwischen Endgerät und Wahlserver sowie der Wahlserver untereinander.

A.Zwischenspeicherung Außerhalb der Kontrolle des EVG im Endgerät zwischengespeicherte Stimmzettel oder Stimmdatensätze sind nach der Wahlhandlung nicht mehr verfügbar.

4 Sicherheitsziele

Mit jeder Annahme, jeder organisatorischen Sicherheitspolitik oder Bedrohung muss mindestens ein Sicherheitsziel verknüpft werden. Die CC fordern damit, dass alle Vorgaben plausibel und nachvollziehbar sind. Die Darlegung der Sicherheitsziele ist unterteilt in die Sicherheitsziele für den EVG und dessen Umgebung. Sie gehen auf alle definierten Sicherheitsumgebungsaspekte ein. Sie spiegeln die dargelegte Absicht wider und sind geeignet, allen identifizierten Bedrohungen entgegenzuwirken, alle organisatorischen Sicherheitspolitiken durchzusetzen und alle Annahmen abzudecken.

4.1 Sicherheitsziele für den EVG

Die Sicherheitsziele für den EVG sind eine prägnante Darlegung der beabsichtigten Reaktion des EVG auf das Sicherheitsproblem. Die dargelegten Ziele behandeln das Sicherheitsproblem angemessen. Die Sicherheitsziele für den EVG sind auf Aspekte derjenigen identifizierten Bedrohungen, denen der EVG entgegenwirken soll, und auf die vom EVG zu erfüllenden organisatorischen Sicherheitspolitiken zurückverfolgbar. Die Sicherheitsziele beziehen sich auf die Phase Wahldurchführung inkl. Stimmauszählung.

O.StimmberechtigterWähler Am EVG können nur Wähler mit Stimmberechtigung, die vom EVG eindeutig identifiziert und authentisiert werden, eine Stimme abgeben und damit einen Stimmdatensatz in der Urne speichern.

O.Beweis Der EVG darf dem Wähler keine Informationen zur Verfügung stellen, die ihm die Möglichkeit geben würden, seine Wahlentscheidung gegenüber anderen zu beweisen.

O.IntegritätNachricht Der EVG verwendet einen geschützten Kommunikationspfad, um sicherzustellen, dass Identifikationsdaten, Authentisierungsnachrichten, Stimmzettel, Stimmdatensätze, Stimmzetteldaten und Rückmeldungen auf dem Übertragungsweg zwischen Wähler und serverseitigem EVG nicht unbemerkt verändert, gelöscht, hinzugefügt oder wiedereingespielt werden können.

O.IntegritätNachrichtWahlvorstand Der serverseitige EVG verwendet einen geschützten Kommunikationspfad, um sicherzustellen, dass das Ergebnis auf dem Übertragungsweg zwischen Wahlvorstand und serverseitigem Wahlvorstandsinterface EVG nicht unbemerkt verändert, gelöscht, hinzugefügt oder wiedereingespielt werden können.

O.IntegritätNachrichtServerServer Die serverseitigen EVG Komponenten (Wählerverzeichnis, Validator, Urne und Wahlvorstandsinterface) gewährleisten den Gebrauch eines vertrauenswürdigen Kanals, um die übertragenen Wählertoken und Serverkommunikationsdaten gegen unberechtigtes Verändern, Löschen, Hinzufügen oder Wiedereinspielen zu schützen.

O.Wahlgeheimnis Der EVG stellt unter Verwendung eines geschützten Kommunikationspfads das Wahlgeheimnis auf dem Übertragungsweg sicher, d.h. es darf nicht möglich sein, dem Wähler seine Stimme im Klartext zuzuordnen. Insbesondere können über die Anzahl oder die Größe der Nachrichten keine Rückschlüsse auf die Anzahl der Kreuze und/oder die Position und/oder auf die ungültige Stimme gezogen werden.

O.GeheimNachricht Der EVG stellt unter Verwendung eines geschützten Kommunikationspfads die Vertraulichkeit der Wählertoken, Identifikationsdaten und der Authentisierungsnachricht sicher.

O.GeheimNachrichtWahlvorstand Der EVG stellt unter Verwendung eines geschützten Kommunikationspfads die Vertraulichkeit der Identifikationsdaten und Authentisierungsnachrichten des Wahlvorstands sicher.

O.GeheimNachrichtServerServer Die serverseitigen EVG Komponenten (Wählerverzeichnis, Validator, Urne und Wahlvorstandsinterface) gewährleisten den Gebrauch eines vertrauenswürdigen Kanals, um die Vertraulichkeit der Wählertoken zu gewährleisten.

O.AuthentizitätServer Für die Wahlhandlung des Wählers gewährleistet der serverseitige EVG den Gebrauch eines vertrauenswürdigen Pfads, der logisch von anderen Kommunikationspfaden getrennt ist und eine gesicherte gegenseitige Identifikation von Wähler und serverseitigem EVG bereitstellt. Der Wähler kann am Endgerät [..] eine Kommunikation mit dem serverseitigen EVG über den vertrauenswürdigen Pfad einleiten.

O.AuthentizitätServerWahlvorstand Für die Operationen des Wahlvorstands gewährleistet der serverseitige EVG den Gebrauch eines vertrauenswürdigen Pfads, der logisch von anderen Kommunikationspfaden getrennt ist und eine gesicherte gegenseitige Identifikation von Wahlvorstand und serverseitigem EVG bereitstellt. Der Wahlvorstand kann an seinem Endgerät eine Kommunikation mit dem serverseitigen EVG über den vertrauenswürdigen Pfad einleiten.

O.ArchivierungIntegrität Der serverseitige EVG stellt sicher, dass nach der Stimmauszählung mit Feststellung des Wahlergebnisses für die Wahldurchführungsdaten, für das Wahlergebnis und [..] für die Protokollaufzeichnungen [..] ein Manipulationsschutz erzeugt wird, der außerhalb der Kontrolle des EVG und außerhalb des Wahlservers wirksam ist. Nachträgliche Fälschungen oder betrügerische Manipulationen sind feststellbar.

O.ArchivierungWahlgeheimnis Die nach Feststellung des Wahlergebnisses noch auf dem Wahlserver gespeicherten Daten lassen keine Zuordnung zwischen dem Wähler und seiner Stimme (im Klartext oder in verschlüsselter Form) zu. Eine Zuordnung darf insbesondere nicht über die Reihenfolge und/oder den Zeitpunkt der Speicherung der Stimmdatensätze in der Urne geschehen.

O.Abbruch Der EVG bietet dem Wähler vor der Stimmabgabe jederzeit die Möglichkeit, seine Wahlhandlung zu beenden, ohne seine Stimmberechtigung dabei zu verlieren.

O.WahlBeenden Der EVG stellt sicher, dass der Wahlvorstand einen Hinweis erhält, falls er die Wahldurchführung vorzeitig beenden möchte. Nach einer expliziten Bestätigung ist das Beenden durch den Wahlvorstand aber auch vor dem geplanten Wahlende-Zeitpunkt möglich.

O.Wahlende Der EVG stellt sicher, dass nach dem Beenden der Wahldurchführung keine Wahlhandlung eröffnet oder weitergeführt werden kann, und insbesondere keine Stimmen mehr abgegeben werden können.

O.WahlgeheimnisWahlvorstand Der EVG stellt das Wahlgeheimnis am Wahlserver während der Wahldurchführung inkl. der Stimmauszählung sicher. Eine Zuordnung zwischen Wähler und seiner Stimme ist für den Wahlvorstand nicht möglich.

O.IntegritätWahlvorstand Der EVG stellt sicher, dass Stimmdatensätze in der Urne nicht durch den Wahlvorstand hinzugefügt, gelöscht oder verändert werden. Insbesondere stellt er sicher, dass der Wahlvorstand den EVG nach dem Start der Wahldurchführung auch durch einen Wiederanlauf nicht in seinen Anfangszustand zurücksetzen kann.

O.Zwischenergebnis Der EVG stellt sicher, dass weder direkt, d.h. durch Stimmauszählung, noch indirekt, d.h. durch Preisgabe des Inhalts von Stimmdatensätzen, Zwischenergebnisse ermittelt werden.

O.Übereilungsschutz Der EVG erlaubt die Stimmabgabe nur, wenn der Wähler seine Stimme explizit kontrolliert und bestätigt hat. Dazu wird ihm diese vor der endgültigen Abgabe erneut angezeigt.

O.Korrektur Der EVG bietet dem Wähler die Möglichkeit, seine Stimme bis zur endgültigen Abgabe beliebig oft zu korrigieren. Auch nach der expliziten Kontrolle der Stimme ist eine Korrektur möglich.

O.Rückmeldung Der registrierte Wähler erhält eine zutreffende Rückmeldung über die Erlaubnis bzw. Verweigerung und den Erfolg bzw. Misserfolg seiner Stimmabgabe. Der EVG gibt dem registrierten Wähler nach erfolgreicher Identifikation und Authentisierung die Möglichkeit zu prüfen, ob er bereits eine Stimme abgegeben hat. Dies bedeutet, dass ein Wähler mit Stimmberechtigung nach der Stimmabgabe eine Meldung über deren Erfolg bzw. Misserfolg erhält. Ein Wähler ohne Stimmberechtigung erhält eine Meldung, dass er sein Stimmrecht bereits ausgeübt hat.

O.Störung Der serverseitige EVG ermöglicht dem Wahlvorstand beim Erstanlauf und auf Anforderung die Ausführung eines Selbsttests um technische Störungen der Integrität der EVG-Sicherheitsfunktionen (TSF) oder der Benutzer- und TSF-Daten, die den korrekten Betrieb des EVG gefährden, zu erkennen. Nach einem Absturz / Herunterfahren des serverseitigen EVG, des Wahlservers oder einem Ausfall der Kommunikation oder der Speichermedien ermöglicht der serverseitige Wahlvorstandsinterface EVG dem Wahlvorstand die Ausführung eines Wiederanlaufs der Wahldurchführung. Dabei gewährleistet der EVG die Integrität der Wahldurchführungsdaten.

O.Protokoll Der serverseitige EVG erzeugt mindestens für die in Kapitel 1.3.3.8 aufgelisteten Ereignisse inkl. der Zeitpunkte des Auftretens der Ereignisse Protokollaufzeichnungen. Der serverseitige EVG ermöglicht dem Wahlvorstand die Durchsicht der Protokollaufzeichnungen.

O.OneVoterOneVote Der serverseitige EVG stellt sicher, dass ein Wähler nicht mehr als eine Stimme abgeben kann und ein registrierter Wähler seine Stimmberechtigung nicht verliert, ohne eine Stimme abgegeben zu haben. Die Erhaltung der Stimmberechtigung wird vom serverseitigen EVG insbesondere auch bei einem Abbruch durch den Wähler oder einem technisch bedingten Abbruch, etwa wegen Zeitablauf oder Fehlern bei der Kommunikation sichergestellt. Außerdem stellt der serverseitige EVG sicher, dass bei einem Wiederanlauf der Wahldurchführung kein Wähler seine Stimmberechtigung verliert oder mehr als eine Stimme abgeben kann.

O.AuthWahlvorstand Der EVG muss den Wahlvorstand vor jeder anderen Aktion identifizieren und authentisieren. Die Authentisierungsfunktion muss eine Separation of Duty unter den Mitgliedern des Wahlvorstandes unterstützen. Die Operationen zum Starten, Wiederanlaufen und Beenden der Wahldurchführung sowie zum Starten der Stimmauszählung mit Feststellung des Wahlergebnisses werden erst ausgeführt, wenn sie jeweils von mindestens zwei authentisierten Mitgliedern des Wahlvorstands unabhängig autorisiert wurden. Dadurch wird sichergestellt, dass sich immer mindestens zwei Mitglieder des Wahlvorstandes gegenseitig kontrollieren können.

O.StartStimmauszählung Der EVG stellt sicher, dass der Wahlvorstand die Stimmauszählung erst nach dem Beenden der Wahldurchführung starten kann.

O.Stimmauszählung Der EVG stellt sicher, dass zu Beginn der Wahldurchführung die Urne keine Stimmdatensätze enthält und dass alle Stimmdatensätze, die nach Wahlende in der Urne gespei-

chert sind, ausgezählt (ggf. zuvor auch entschlüsselt) werden und in die Stimmauszählung mit Feststellung des Wahlergebnisses eingehen.

4.2 Sicherheitsziele für die Einsatzumgebung

Die Sicherheitsziele für die Umgebung sind eine erneute Darlegung des Annahmenteils der Darlegung der EVG-Sicherheitsumgebung. Sie sind auf Aspekte derjenigen identifizierten Bedrohungen, denen durch den EVG nicht vollständig entgegengewirkt wird, und auf die organisatorischen Sicherheitspolitiken, die vom EVG nicht vollständig erfüllt werden, zurückverfolgbar.

OE.Wahlvorbereitung Die Wahldaten sind zu Beginn der Wahldurchführung ordnungsgemäß und in der genehmigten, d.h. vom Wahlveranstalter verabschiedeten, Fassung auf dem Wahlserver installiert worden und die Urne ist leer. Die Phase Wahlvorbereitung ist also korrekt abgeschlossen. Der serverseitige EVG ist inkl. der Identifikations- und Authentisierungsdaten für den Wahlvorstand korrekt konfiguriert und initialisiert. Wenn parallel zur Online-Wahl auch herkömmliche Wahlformen (Wahl im Wahllokal und/oder Briefwahl) angeboten werden, liegt es in der Verantwortung des Wahlveranstalters sicher zu stellen, dass Wähler nicht über unterschiedliche Wahlformen eine Stimme abgeben können. Dies kann beispielsweise dadurch geschehen, dass die Online-Wahldurchführung vor der Öffnung des Wahllokals liegt. Es liegt in der Verantwortung des Wahlveranstalters, eindeutige Zeitpläne für alle drei Wahlphasen vorzugeben. Der Wahlveranstalter ist insbesondere für die Festlegung des Wahlende-Zeitpunktes der Phase Wahldurchführung verantwortlich. Dabei sollen die Fristen rechtzeitig vor dem Start der Wahldurchführung öffentlich bekannt gegeben werden. Der Wahlveranstalter soll die Online-Wahl so gestalten, dass die Registrierung zur Teilnahme kein Hindernis für den Wähler darstellt. Es liegt in der Verantwortung des Wahlveranstalters, dass der Wähler die in der Wahlberechtigungsliste enthaltenen Einträge überprüfen und ggf. Berichtigung verlangen kann.

OE.Beobachten Der Wähler kann seine Stimme unbeobachtet abgeben. Hierfür muss der Wähler sorgen. Der EVG kann nicht verhindern, dass dem Wähler über die Schultern geschaut wird, während er seine Stimme abgibt. Der Wahlveranstalter ist dafür verantwortlich, dem Wähler angemessene Hinweise für die unbeobachtete Stimmabgabe zu geben.

OE.Wahlvorstand Der Wahlvorstand greift nur über den serverseitigen EVG auf die Benutzer- und TSF-Daten zu, d.h. er nutzt nur die vom serverseitigen EVG zur Verfügung gestellte Funktionalität. Der Wahlvorstand ist ausreichend geschult, um den sicheren Betrieb des EVG zu verstehen und benutzt den EVG in der beabsichtigten Weise. Er installiert insbesondere keine bösartige Software für den Zugriff auf diese Daten. Von der Möglichkeit, den EVG oder die Benutzer- und TSF-Daten zu verändern oder auszutauschen, macht der Wahlvorstand keinen Gebrauch. Jedes Mitglied des Wahlvorstands hat seine Identifikationsdaten und sein Authentisierungsmerkmal erhalten und gibt diese Daten nicht an andere Personen weiter. Bei der Bestimmung des Wahlvorstandes ist vom Wahlveranstalter zu beachten, dass Personen nicht alleine Zugang und Zugriff zum serverseitigen EVG gewährleistet wird. Der Wahlveranstalter soll dafür sorgen, dass über sämtliche Zugriffe auf den serverseitigen EVG oder den Wahlserver sowie der daran beteiligten Personen, Buch geführt wird. Der Wahlvorstand überwacht die Verfügbarkeit des Netzwerks und des Wahlservers entsprechend den Vorgaben des Wahlveranstalters und informiert den Wahlveranstalter über sämtliche festgestellten Störungen und Ausfälle.
Die Vertrauenswürdigkeit des Endgerätes liegt in der Verantwortung des Wahlvorstands, da der EVG nicht die Möglichkeit und die Berechtigung hat, das gesamte Endgerät nach Malware zu untersuchen und ggf. zu beseitigen. Der EVG wird, falls erforderlich, von dem Wahlvorstand so installiert bzw. benutzt, dass das Endgerät den Vorgang weder beobachten noch beeinflussen kann. Dazu gehört auch, dass der Wahlvorstand sein Endgerät nicht absichtlich für solche Zwecke manipuliert. Auf dem Endgerät wird vom Wahlvorstand Software eingesetzt, die in der Lage ist, die Ausgabe des EVG korrekt anzuzeigen und die Eingaben des Wahlvorstands korrekt an die Wahlserver zu übertragen.

Der Wahlvorstand muss sein Endgerät gemäß einer verfügbaren Handreichung in einem vertrauenswürdigen Zustand halten. In dieser Handreichung wird erläutert wie der Wahlvorstand sein Betriebssystem mittels gängiger Anti-Viren und Personal-Firewall-Software auf einem ausreichenden Sicherheitsstandard halten kann.

OE.AuthDaten Nur registrierte Wähler sind im Besitz der zur Teilnahme an der Wahl benötigten Daten, insb. Identifikationsdaten, Authentisierungsmerkmal und Wählertoken. Nur so kann der EVG sicherstellen, dass nur Wähler mit Stimmberechtigung ihre Stimme abgeben können. Falls Identifikationsdaten oder Authentisierungsmerkmale an die Wähler verteilt werden müssen, so liegt es in der Verantwortung des Wahlveranstalters diese rechtzeitig bereit zu stellen. Die Verteilung muss dabei authentisch und integer sowie ggf. auch vertraulich erfolgen.

OE.Endgerät Die Vertrauenswürdigkeit des Endgerätes liegt in der Verantwortung des Wählers, da der EVG nicht die Möglichkeit und die Berechtigung hat, das gesamte Endgerät nach Malware zu untersuchen und ggf. zu beseitigen. Der [...]EVG wird [...] von dem Wähler so [...] benutzt, dass das Endgerät den Vorgang der Stimmabgabe weder beobachten noch beeinflussen kann. Dazu gehört auch, dass der Wähler sein Endgerät nicht absichtlich für solche Zwecke manipuliert. Auf dem Endgerät wird vom Wähler Software eingesetzt, die in der Lage ist, den Stimmzettel korrekt anzuzeigen, die Eingaben des Wählers korrekt an den Wahlserver zu übertragen und die Stimme nach der Wahlhandlung zu löschen.
Der Wähler muss sein Endgerät gemäß einer verfügbaren Handreichung in einem vertrauenswürdigen Zustand halten. In dieser Handreichung wird erläutert, wie der Wähler sein Betriebssystem mittels gängiger Anti-Viren und Personal-Firewall-Software auf einem ausreichenden Sicherheitsstandard halten kann.

OE.Wahlserver Der Wahlvorstand nimmt seine Verantwortung zur Sicherung des Wahlservers wahr, um auszuschließen, dass ein Netzwerkangreifer Zugriff auf den Server erhält. Die Umsetzung eines entsprechenden Sicherheitskonzeptes für die Netzwerkanbindung wird über Sicherheitsmaßnahmen, die dem Stand der Technik entsprechen, erreicht. Der EVG soll neben den benötigten Ressourcen wie Datenbank und Application Server als einzige Anwendung auf dem Betriebssystem laufen (vgl. Abschnitt 1.3.4). Der Wahlserver selbst muss gegen unbefugten Zugriff mit ausreichend starken Nutzerpasswörtern/Zertifikaten gesichert sein.

OE.Verfügbarkeit Auf die Robustheit, Servicequalität und Verfügbarkeit des Netzwerks und des Wahlservers hat der EVG keinen Einfluss. Diese müssen ausreichend hoch sein, um die gesamte Wahldurchführung inkl. der Stimmauszählung zu ermöglichen. Die Wahl des Netzwerks liegt in der Verantwortung des Wahlveranstalters. Eine hohe Robustheit, Servicequalität und Verfügbarkeit des ausgewählten Netzwerks sollte sich in einer dem Online-Wahlverfahren vergleichbaren Praxis bestätigt haben. Die erforderliche Servicequalität des Netzwerks und des Wahlservers hängt vom vorgegebenen Zeitraum für die Wahldurchführung ab. Der Wahlveranstalter sorgt dafür, dass die Verfügbarkeit des Wahlservers und seiner Netzwerkanbindung bei Störungen und Ausfällen mit angemessenem Service Level wiederhergestellt wird. Der Wahlveranstalter legt fest, wie der Wahlvorstand das Netzwerk und den Wahlserver überwacht und Störungen oder Ausfälle feststellt, und mit welchen Maßnahmen der Wahlvorstand den Störungen oder Ausfällen begegnen soll. Der Wahlveranstalter wird über sämtliche Störungen und Ausfälle informiert. Für Probleme mit der Robustheit, Servicequalität und Verfügbarkeit des Netzwerks oder des Wahlservers, die nicht in angemessener Zeit behoben werden können, definiert der Wahlveranstalter geeignete Notfallszenarios.

OE.ServerRaum Ausschließlich der Wahlvorstand hat Zutritt und Zugang zum Wahlserver. Dies ist notwendig, um ausschließen zu können, dass der EVG verändert oder gar ausgetauscht wird. Solche Angriffe können vom EVG weder verhindert noch erkannt werden.

OE.Speicherung Der EVG benutzt Speichermedien zur Ablage der Stimmdatensätze in der Urne. Für den Schutz der Integrität und der Verfügbarkeit der gespeicherten Benutzer- und TSF-Daten ist der EVG auf das korrekte Funktionieren der Speichermedien angewiesen. Um die Integrität während der Speicherung von Stimmdatensätzen in der Urne überwachen zu können, werden dabei auftretende Fehler den EVG-Sicherheitsfunktionen gemeldet.

OE.Systemzeit Der serverseitige EVG kann sich auf die Übereinstimmung der Systemzeit des Wahlservers mit der aktuellen Uhrzeit verlassen. Dies ist notwendig, um verlässliche Protokolleinträge zu erzeugen und um feststellen zu können, ob der Wahlende-Zeitpunkt erreicht ist. Die benötigte Genauigkeit der Systemzeit wird vom Wahlveranstalter festgelegt.

OE.Protokollschutz Die IT-Umgebung des serverseitigen EVG speichert die vom serverseitigen EVG erzeugten Protokollaufzeichnungen und schützt sie vor unberechtigtem Löschen, Verändern und Hinzufügen.

OE.AuthentizitätServer Der Wähler sowie der Wahlvorstand überprüfen anhand des eingesetzten TLS-Zertifikates, ob sie mit dem richtigen serverseitigen EVG kommunizieren.

OE.ArchivierungIntegrität Die IT-Umgebung stellt alle benötigten Betriebsmittel für die Erzeugung eines Manipulationsschutzes für Informationen zur Verfügung.

[…]

OE.GeschützteKommunikation Die IT-Umgebung stellt kryptographische Operationen und Protokolle für den Betrieb einer vor Modifikation und Preisgabe geschützten Kommunikationsverbindung zwischen Endgerät und Wahlserver sowie der Wahlserver untereinander zur Verfügung Dazu gehören auch die Operationen und Protokolle für Erzeugung, Verteilung, Zugriff und Vernichtung der benötigten kryptographischen Schlüssel.

OE.Zwischenspeicherung Außerhalb der Kontrolle des EVG im Endgerät zwischengespeicherte Stimmzettel oder Stimmdatensätze sind nach der Wahlhandlung nicht mehr verfügbar. Dazu werden die benutzten Ressourcen bereinigt – insb. durch das Löschen des Zwischenspeichers im verwendeten Browser.

4.3 Erklärung der Sicherheitsziele

Die Erklärung der Sicherheitsziele weist nach, dass die dargelegten Sicherheitsziele auf alle Aspekte, die in der EVG-Sicherheitsumgebung identifiziert werden, zurückverfolgbar sind und dass sie geeignet sind, diese abzudecken.
Für jedes Sicherheitsziel für den EVG und für jedes Sicherheitsziel für die Umgebung wird angegeben, welche Bedrohungen abgewehrt, welche Sicherheitspolitik beachtet und welche Annahmen abgedeckt werden.
Aus den tabellarischen Übersichten ist ersichtlich, dass jede Bedrohung, jede Sicherheitspolitik und jede Annahme von mindestens einem Sicherheitsziel adressiert wird und jedes Sicherheitsziel mindestens eine Bedrohung oder eine Annahme adressiert.

	T.UnbefugterWähler	T.Beweis	T.IntegritätNachricht	T.GeheimNachricht	T.AuthentizitätServer	T.ArchivierungIntegrität	T.ArchivierungWahlgeheimnis	P.Abbruch	P.WahlBeenden	P.Wahlende	P.WahlgeheimnisWahlvorstand	P.IntegritätWahlvorstand	P.Zwischenergebnis	P.Übereilungsschutz	P.Korrektur	P.Rückmeldung	P.Störung
O.StimmberechtigterWähler	x																
O.Beweis		x															
O.IntegritätNachricht			x														
O.IntegritätNachrichtWahlvorstand			x														
O.IntegritätNachrichtServerServer			x														
O.Wahlgeheimnis				x													
O.GeheimNachricht				x													
O.GeheimNachrichtWahlvorstand				x													
O.GeheimNachrichtServerServer				x													
O.AuthentizitätServer			x	x	x												
O.AuthentizitätServerWahlvorstand			x	x	x												
O.ArchivierungIntegrität						x											
O.ArchivierungWahlgeheimnis							x										
O.Abbruch								x									
O.WahlBeenden									x								
O.Wahlende										x							
O.WahlgeheimnisWahlvorstand											x						
O.IntegritätWahlvorstand												x					
O.Zwischenergebnis				x									x				
O.Übereilungsschutz														x			
O.Korrektur															x		
O.Rückmeldung																x	
O.Störung																	x
O.Protokoll																	
O.OneVoterOneVote																	
O.AuthWahlvorstand																	
O.StartStimmauszählung																	
O.Stimmauszählung																	
OE.Wahlvorbereitung	x								x								
OE.Beobachten		x															
OE.Wahlvorstand	x								x		x	x	x				
OE.AuthDaten	x																
OE.Endgerät	x	x														x	
OE.Wahlserver	x				x	x	x		x	x		x	x				x
OE.Verfügbarkeit																x	x
OE.Serverraum	x				x		x		x	x		x	x				
OE.Speicherung																	
OE.Systemzeit									x								
OE.Protokollschutz																	
OE.AuthentizitätServer			x	x	x												
OE.ArchivierungIntegrität						x											
OE.GeschützteKommunikation			x	x	x												
OE.Zwischenspeicherung																	

Tabelle 2: Umsetzung des Sicherheitsproblems durch die Sicherheitsziele (1/2)

	P.Protokoll	P.OneVoterOneVote	P.AuthWahlvorstand	P.StartStimmauszählung	P.Stimmauszählung	A.Wahlvorbereitung	A.Beobachten	A.Wahlvorstand	A.AuthDaten	A.Endgerät	A.Wahlserver	A.Verfügbarkeit	A.Serverraum	A.Speicherung	A.Systemzeit	A.Protokollschutz	A.AuthentizitätServer	A.Geschützte Kommunikation	A.Zwischenspeicherung
O.StimmberechtigterWähler																			
O.Beweis																			
O.IntegritätNachricht																			
O.IntegritätNachrichtWahlvorstand																			
O.IntegritätNachrichtServerServer																			
O.Wahlgeheimnis																			
O.GeheimNachricht																			
O.GeheimNachrichtWahlvorstand																			
O.GeheimNachrichtServerServer																			
O.AuthentizitätServer																			
O.AuthentizitätServerWahlvorstand																			
O.ArchivierungIntegrität																			
O.ArchivierungWahlgeheimnis																			
O.Abbruch																			
O.WahlBeenden																			
O.Wahlende																			
O.WahlgeheimnisWahlvorstand																			
O.IntegritätWahlvorstand																			
O.Zwischenergebnis																			
O.Übereilungsschutz																			
O.Korrektur																			
O.Rückmeldung																			
O.Störung																			
O.Protokoll	x																		
O.OneVoterOneVote		x																	
O.AuthWahlvorstand			x																
O.StartStimmauszählung				x	x														
O.Stimmauszählung					x														
OE.Wahlvorbereitung						x													
OE.Beobachten							x												
OE.Wahlvorstand	x	x	x	x	x			x											
OE.AuthDaten									x										
OE.Endgerät										x									
OE.Wahlserver		x	x	x	x						x								
OE.Verfügbarkeit												x							
OE.Serverraum		x	x	x	x								x						
OE.Speicherung														x					
OE.Systemzeit	x														x				
OE.Protokollschutz	x															x			
OE.AuthentizitätServer																	x		
OE.ArchivierungIntegrität																			
OE.GeschützteKommunikation																		x	
OE.Zwischenspeicherung																			x

Tabelle 3: Umsetzung des Sicherheitsproblems durch die Sicherheitsziele (2/2)

4.3.1 Abwehr der Bedrohungen durch den EVG

T.UnbefugterWähler Die Bedrohung wird durch das Ziel O.StimmberechtigterWähler abgewehrt. Dabei wird es durch das Ziel OE.Wahlvorstand unterstützt, da dieses sicherstellt, dass der Wahlvorstand unbefugte Wähler nicht zur Stimmabgabe zulässt. Außerdem wird die Abwehr durch die folgenden Ziele der IT-Umgebung unterstützt:

- OE.Wahlvorbereitung (da hierdurch sichergestellt ist, dass keine Personen in der Wahlberechtigungsliste stehen, die keine Stimmberechtigung haben),

- OE.ServerRaum (da hierdurch außer dem Wahlvorstand niemand Zutritt und Zugang zum Wahlserver hat),
- OE.Endgerät (da hierdurch keine Schadsoftware auf dem Endgerät sein kann, die Zugangsdaten mitliest und einem unbefugten Wähler zuschickt, der damit seine Stimme im Namen eines Wählers abgeben kann),
- OE.Wahlserver (da hierdurch keine Schadsoftware auf dem Wahlserver ist, die unbefugte Wähler zur Wahlhandlung zulassen könnte, beispielsweise durch Ändern der Stimmberechtigung oder der Wahlberechtigungsliste),
- OE.AuthDaten (da hierdurch nur Wähler im Besitz von Identifikations- und Authentisierungsmitteln sind) und

T.Beweis Die Bedrohung wird durch das Ziel O.Beweis abgewehrt. Hierbei wird es durch die folgenden Ziele der IT-Umgebung unterstützt:

- OE.Beobachten (da hierdurch niemand den Wähler bei seiner Stimmabgabe beobachtet, um einen Beweis zu erhalten),
- OE.Endgerät (da hierdurch keine Schadsoftware auf dem Endgerät ist, die Daten generiert, mit deren Hilfe der Wähler seine Wahlentscheidung beweisen kann).
- […]

T.IntegritätNachricht Die Bedrohung wird durch die Ziele O.IntegritätNachricht (a-d), O.IntegritätNachrichtWahlvorstand (e) und O.IntegritätNachrichtServerServer (f) abgewehrt. Die Ziele O.AuthentizitätServer und O.AuthentizitätServerWahlvorstand gewährleisten die authentische Verbindung zwischen Wähler und Wahlserver bzw. Wahlvorstand und Wahlserver. Hierbei werden die EVG-Sicherheitsziele durch die folgenden Ziele der IT-Umgebung unterstützt:

- OE.AuthentizitätServer (da hierdurch der Wähler bzw. der Wahlvorstand die Authentizität des serverseitigen EVG kontrolliert) und
- OE.GeschützteKommunikation (da hierdurch eine vor Modifikation geschützte Verbindung zwischen Endgerät (des Wählers bzw. des Wahlvorstands) und Wahlserver sowie zwischen den Wahlserver bereitgestellt wird).

T.GeheimNachricht Die Bedrohung wird zum einen durch das Ziel O.Wahlgeheimnis abgewehrt, da hierdurch sichergestellt wird, dass der Netzwerkangreifer keine Zuordnung zwischen Wähler und seiner Stimme im Klartext herstellen kann und zum anderen durch die Ziele O.GeheimNachricht (a-b), O.GeheimNachrichtWahlvorstand (c) und O.GeheimNachrichtServerServer (a) abgewehrt. Durch O.GeheimNachricht und O.GeheimNachrichtWahlvorstand wird sichergestellt [..], dass ein Netzwerkangreifer weder Stimmdatensätze noch Identifikationsdaten des Wählers bzw. Identifikationsdaten und Authentisierungsnachricht des Wahlvorstands im Klartext erhält. Durch O.GeheimNachricht und O.GeheimNachrichtServerServer wird sichergestellt, dass ein Netzwerkangreifer die Wählertoken nicht im Klartext erhält. Das Ziel O.Zwischenergebnis gewährleistet, dass keine Zwischenergebnisse ermittelt werden können, weil die Stimme während der Übertragung nicht preisgegeben wird. Die Ziele O.AuthentizitätServer und O.AuthentizitätServerWahlvorstand gewährleisten die authentische Verbindung zum Wahlserver vom Endgerät. Hierbei werden die EVG-Sicherheitsziele durch die folgenden Ziele der IT-Umgebung unterstützt:

- OE.AuthentizitätServer (da hierdurch der Wähler bzw. der Wahlvorstand die Authentizität des serverseitigen EVG kontrolliert) und
- OE.GeschützteKommunikation (da hierdurch eine vor Preisgabe geschützte Verbindung zwischen Endgerät (von Wähler bzw. Wahlvorstand) und Wahlserver sowie zwischen den Wahlserver bereitgestellt wird).

T.AuthentizitätServer Die Bedrohung wird durch die Ziele O.AuthentizitätServer und O.AuthentizitätServerWahlvorstand abgewehrt. Hierbei wird es durch die folgenden Ziele der IT-Umgebung unterstützt:

- OE.AuthentizitätServer (da der Wähler bzw. der Wahlvorstand hierbei überprüft, ob er mit dem richtigen serverseitigen EVG kommuniziert)
- OE.ServerRaum (da hierdurch nur der Wahlvorstand Zutritt und Zugang zum Wahlserver hat)
- OE.Wahlserver (da hierdurch keine Schadsoftware auf dem Wahlserver ist, die den gesamten EVG verändert oder austauscht)
- OE.GeschützteKommunikation (da hierdurch eine authentische Verbindung zwischen Endgerät (von Wähler bzw. Wahlvorstand) und Wahlserver sowie zwischen den Wahlserver bereitgestellt wird).

T.ArchivierungIntegrität Die Bedrohung wird durch das Ziel O.ArchivierungIntegrität abgewehrt. Es wird durch die folgenden Ziele für die IT-Umgebung unterstützt:

- OE.ArchivierungIntegrität (da hierdurch die benötigten Betriebsmittel für die Erzeugung des Manipulationsschutzes zur Verfügung stehen); und
- OE.Wahlserver (da hierdurch keine Schadsoftware auf dem Wahlserver ist, die die authentische Erzeugung des Manipulationsschutzes gefährden könnte).

T.ArchivierungWahlgeheimnis Die Bedrohung wird durch das Ziel O.ArchivierungWahlgeheimnis abgewehrt. Hierbei wird es durch die folgenden Ziele der IT-Umgebung unterstützt:

- OE.ServerRaum (da hierdurch nur der Wahlvorstand Zutritt und Zugang zum Wahlserver hat) und
- OE.Wahlserver (da hierdurch keine Schadsoftware auf dem Wahlserver ist, die das Wahlgeheimnis gefährdende Daten speichern könnte).
- […]

4.3.2 Durchsetzung der organisatorischen Sicherheitspolitiken durch den EVG

P.Abbruch Die Politik wird vom Ziel O.Abbruch durchgesetzt.

P.WahlBeenden Die Politik wird vom Ziel O.WahlBeenden durchgesetzt. Hierbei wird es durch die folgenden Ziele der IT-Umgebung unterstützt:

- OE.Wahlvorbereitung (da hierdurch dem EVG der geplante Wahlende-Zeitpunkt bekannt ist),
- OE.ServerRaum (da hierdurch nur der Wahlvorstand Zutritt und Zugang zum Wahlserver hat),
- OE.Wahlserver (da hierdurch keine Schadsoftware auf dem Wahlserver ist, die den gesamten EVG verändert oder austauscht),
- OE.Wahlvorstand (da hierdurch der Wahlvorstand den EVG nicht aushebelt und seine Sicherheitsfunktionen umgeht) und
- OE.Systemzeit (da hierdurch eine zuverlässige Systemzeit zur Verfügung steht, anhand der überprüft werden kann, ob der geplante Wahlende-Zeitpunkt bereits erreicht ist).

P.Wahlende Die Politik wird vom Ziel O.Wahlende durchgesetzt. Hierbei wird es durch die folgenden Ziele der IT-Umgebung unterstützt:

- OE.ServerRaum (da hierdurch nur der Wahlvorstand Zutritt und Zugang zum Wahlserver hat) und
- OE.Wahlserver (da hierdurch keine Schadsoftware auf dem Wahlserver ist, die den gesamten EVG verändert oder austauscht).

P.WahlgeheimnisWahlvorstand Die Politik wird vom Ziel O.WahlgeheimnisWahlvorstand durchgesetzt. Hierbei wird es durch das folgende Ziel der IT-Umgebung unterstützt:
- OE.Wahlvorstand (da hierdurch der Wahlvorstand den EVG nicht aushebelt und seine Sicherheitsfunktionen umgeht).

P.IntegritätWahlvorstand Die Politik wird von dem Ziel O.IntegritätWahlvorstand durchgesetzt. Hierbei werden sie durch die folgenden Ziele der IT-Umgebung unterstützt:
- OE.Wahlvorstand (da hierdurch der Wahlvorstand den EVG nicht aushebelt und seine Sicherheitsfunktionen umgeht),
- OE.ServerRaum (da hierdurch nur der Wahlvorstand Zutritt und Zugang zum Wahlserver hat) und
- OE.Wahlserver (da hierdurch keine Schadsoftware auf dem Wahlserver ist, die den gesamten EVG verändert oder austauscht)

P.Zwischenergebnis Die Politik wird vom Ziel O.Zwischenergebnis durchgesetzt. Hierbei wird es durch die folgenden Ziele der IT-Umgebung unterstützt:
- OE.Wahlvorstand (da hierdurch der Wahlvorstand den EVG nicht aushebelt und seine Sicherheitsfunktionen umgeht),
- OE.ServerRaum (da hierdurch nur der Wahlvorstand Zutritt und Zugang zum Wahlserver hat) und
- OE.Wahlserver (da hierdurch keine Schadsoftware auf dem Wahlserver ist, die den gesamten EVG verändert oder austauscht)

P.Übereilungsschutz Die Politik wird vom Ziel O.Übereilungsschutz durchgesetzt.

P.Korrektur Die Politik wird vom Ziel O.Korrektur durchgesetzt.

P.Rückmeldung Die Politik wird vom Ziel O.Rückmeldung durchgesetzt. Hierbei wird es durch die folgenden Ziele der IT-Umgebung unterstützt:
- OE.Verfügbarkeit (da hierdurch verschickte Rückmeldungen auch ankommen),
- OE.Endgerät (da hierdurch empfangene Rückmeldungen auch entsprechend angezeigt werden).

P.Störung Die Politik wird vom Ziel O.Störung durchgesetzt. Hierbei wird es durch das folgende Ziel der IT-Umgebung unterstützt:
- OE.Verfügbarkeit (da hierdurch dem Wahlvorstand Vorgaben für die Feststellung von Störungen zur Verfügung stehen),
- OE.Wahlserver (da hierdurch keine Schadsoftware auf dem Wahlserver ist, die den gesamten EVG verändert oder austauscht).

P.Protokoll Die Politik wird vom Ziel O.Protokoll durchgesetzt. Es wird durch die folgenden Ziele der IT-Umgebung unterstützt:

- OE.Systemzeit (da hierdurch eine zuverlässige Systemzeit zur Verfügung steht, die für die Protokollierung verwendet werden kann);
- OE.Protokollschutz (da hierdurch die gespeicherten Protokollaufzeichnungen unverändert bleiben); und
- OE.Wahlvorstand (da hierdurch gewährleistet ist, dass der Wahlvorstand die Erzeugung und geschützte Speicherung der Protokollaufzeichnungen nicht umgeht).

P.OneVoterOneVote Die Politik wird vom Ziel O.OneVoterOneVote durchgesetzt. Hierbei wird das Ziel durch die folgenden Ziele an die IT-Umgebung unterstützt:

- OE.ServerRaum (da hierdurch nur der Wahlvorstand Zutritt und Zugang zum Wahlserver hat),
- OE.Wahlvorstand (da hierdurch der Wahlvorstand den EVG nicht aushebelt und seine Sicherheitsfunktionen umgeht) und
- OE.Wahlserver (da hierdurch keine Schadsoftware auf dem Wahlserver ist, die den gesamten EVG verändert oder austauscht).

P.AuthWahlvorstand Die Politik wird vom Ziel O.AuthWahlvorstand durchgesetzt. Hierbei wird das Ziel durch die folgenden Ziele an die IT-Umgebung unterstützt:

- OE.ServerRaum (da hierdurch nur der Wahlvorstand Zutritt und Zugang zum Wahlserver hat),
- OE.Wahlvorstand (da hierdurch der Wahlvorstand den EVG nicht aushebelt und seine Sicherheitsfunktionen umgeht) und
- OE.Wahlserver (da hierdurch keine Schadsoftware auf dem Wahlserver ist, die den gesamten EVG verändert oder austauscht).

P.StartStimmauszählung Die Politik wird vom Ziel O.StartStimmauszählung durchgesetzt. Hierbei wird das Ziel durch die folgenden Ziele an die IT-Umgebung unterstützt:

- OE.ServerRaum (da hierdurch nur der Wahlvorstand Zutritt und Zugang zum Wahlserver hat),
- OE.Wahlvorstand (da hierdurch der Wahlvorstand den EVG nicht aushebelt und seine Sicherheitsfunktionen umgeht) und
- OE.Wahlserver (da hierdurch keine Schadsoftware auf dem Wahlserver ist, die den gesamten EVG verändert oder austauscht).

P.Stimmauszählung Die Politik wird von den Zielen O.Stimmauszählung und O.StartStimmauszählung durchgesetzt. Hierbei werden sie durch die folgenden Ziele an die IT-Umgebung unterstützt:

- OE.ServerRaum (da hierdurch nur der Wahlvorstand Zutritt und Zugang zum Wahlserver hat),
- OE.Wahlvorstand (da hierdurch der Wahlvorstand den EVG nicht aushebelt und seine Sicherheitsfunktionen umgeht) und
- OE.Wahlserver (da hierdurch keine Schadsoftware auf dem Wahlserver ist, die den gesamten EVG verändert oder austauscht).

4.3.3 Abdeckung der Annahmen

Die Abdeckung der Annahmen ist durch deren erneute Darlegung als Sicherheitsziele für die Einsatzumgebung offensichtlich (vgl. Tabelle 3). Die Bezeichner sind entsprechend gleich gewählt (A.* entspricht OE.*). Den Zielen ist im Vergleich zu den Annahmen in einzelnen Fällen eine Begründung für die Notwendigkeit des Sicherheitsziels für die Einsatzumgebung hinzugefügt. Jede Annahme wird direkt und vollständig durch das gleichnamige Sicherheitsziel aufrecht erhalten.

5 IT-Sicherheitsanforderungen

Die IT-Sicherheitsanforderungen sind die Verfeinerung der Sicherheitsziele in eine Menge von Sicherheitsanforderungen an den EVG und Sicherheitsanforderungen an die IT-Umgebung, die im Falle ihrer Erfüllung sicherstellen, daß der EVG seine Sicherheitsziele erfüllen kann. Die Sicherheitsanforderungen enthalten sowohl Anforderungen an das Vorhandensein des gewünschten Verhaltens als auch Anforderungen an die Abwesenheit des unerwünschten Verhaltens.

Vorbemerkung:

- **Zuweisungs**-Operationen sind **fett** gedruckt.
- *Auswahl*-Operationen sind *kursiv* gedruckt.
- VERFEINERUNGEN sind in GROSSBUCHSTABEN gedruckt.
- Werte von Sicherheitsattributen sind unterstrichen dargestellt.
- […]

5.1 Funktionale EVG-Sicherheitsanforderungen

Die Darlegung der funktionalen EVG-Sicherheitsanforderungen definiert die funktionalen Anforderungen an den EVG in Form funktionaler Komponenten aus Teil 2 der CC.
Der EVG enthält Betriebsmittel, die zur Verarbeitung und Speicherung von Informationen benutzt werden können. Das Hauptziel der TSF ist die vollständige und korrekte Durchsetzung der TSP für die Betriebsmittel und Informationen, die der EVG kontrolliert.
EVG-Betriebsmittel können auf vielfältige Weise gegliedert und genutzt werden. Teil 2 der CC führt jedoch eine spezielle Gliederung ein, die eine Spezifikation von gewünschten Sicherheitseigenschaften zulässt. Alle Einheiten, die aus Betriebsmitteln gebildet werden können, können zwei Kategorien zugeordnet werden. Die Einheiten können aktiv sein, d.h. diese sind Ursache von Aktionen, die EVG-intern ablaufen und lösen Operationen aus, die mit Informationen ausgeführt werden. Die Einheiten können andererseits passiv sein, d.h. diese sind entweder der Behälter, aus dem Informationen stammen oder der Behälter, in dem Informationen gespeichert werden.

Aktive Einheiten werden als Subjekte bezeichnet. Innerhalb des EVG gibt es folgende Arten von Subjekten, die von der Durchsetzung der in diesem Abschnitt spezifizierten TSP betroffen sind:

- ***Wähler:*** Alle aktiven Einheiten im […] EVG, die die Aktionen der Wahlhandlung auslösen. Weil alle Aktionen von der Person, die die Wahlhandlung ausführt, verursacht werden, wird für Subjekt und Benutzer der gleiche Begriff verwendet.
- ***Wahlvorstand:*** Alle aktiven Einheiten im serverseitigen EVG, die die Aktionen für den Ablauf der Wahldurchführung inkl. Stimmauszählung auslösen. Weil alle Aktionen von der Person, die für den ordnungsgemäßen Ablauf der Wahldurchführung inkl. Stimmauszählung zuständig ist, verursacht werden, wird für Subjekt und Benutzer der gleiche Begriff verwendet.

Passive Einheiten werden als Objekte bezeichnet. Objekte sind die Ziele von Operationen, die von Subjekten ausgeführt werden können. Sie sind Behälter, die Informationen enthalten. Innerhalb des EVG gibt es folgende Arten von Informationen:

- Authentisierungsnachrichten
- Identifikationsdaten
- Protokollaufzeichnungen

- Rückmeldungen
- Stimmabgabevermerke
- Stimmdatensätze
- Stimmen
- Stimmzettel
- Stimmzetteldaten
- Wahldurchführungsdaten
- Wahlende-Zeitpunkt
- Wählertoken
- Wahlergebnis
- Zwischenergebnis
- Serverkommunikationsdaten

Subjekte und Objekte besitzen bestimmte Sicherheitsattribute, die Informationen enthalten, welche ein korrektes Verhalten des EVG ermöglichen. Diese sind:

- ***Anzahl der Autorisierungen für die angeforderte Operation:*** Dieses Attribut wird zur Verweigerung kontrollierter Operation verwendet. Deren Ausführung wird verhindert solange nicht genügend viele Mitglieder des Wahlvorstands für die Autorisierung der angeforderten Operation authentisiert wurden.
- ***Wahlzeitraum:*** Dieses Attribut wird zur Kontrolle des Ablaufs der Wahldurchführung inkl. Stimmauszählung verwendet. Es besitzt vor dem Starten der Wahldurchführung den Wert Vorbereitung, nach dem Starten der Wahldurchführung den Wert Durchführung und nach dem Beenden der Wahldurchführung den Wert Auszählung.
- ***Stimmberechtigungsattribut:*** Dieses Attribut wird zur Kontrolle der Stimmberechtigung des Wählers verwendet. Es spiegelt den Stimmabgabevermerk wieder. Seine möglichen Werte sind unbekannt, mit oder ohne Stimmberechtigung. Bei der Eröffnung jeder Wahlhandlung wird das Attribut auf den Wert unbekannt gesetzt. Wenn der Wähler erfolgreich identifiziert und authentisiert wurde, wird der Wert des Attributs auf den Wert mit oder den Wert ohne geändert, je nach Stimmabgabevermerk. Nach der erfolgreichen Stimmabgabe und entsprechendem Vermerk erhält das Attribut den Wert ohne.
- ***Wahlhandlungsattribut:*** Dieses Attribut wird zur Kontrolle des Fortschritts der Wahlhandlung verwendet. Es kann die Werte vor oder nach Einleitung der Stimmabgabe annehmen. Bei der Eröffnung jeder Wahlhandlung wird das Attribut auf den Wert vor gesetzt. Die Einleitung der Stimmabgabe ändert das Attribut auf den Wert nach. Wird die Einleitung der Stimmabgabe widerrufen, erhält das Attribut wieder den Wert vor.

FAU_GEN.1 Generierung der Protokolldaten

Ist hierarchisch zu: Keinen anderen Komponenten.
Abhängigkeiten: FPT_STM.1 Verlässliche Zeitstempel

FAU_GEN.1.1 Die SERVERSEITIGE TSF muß in der Lage sein, für folgende protokollierbaren Ereignisse eine Protokollaufzeichnung zu generieren:

a Starten und Beenden der Protokollierungsfunktionen.

b Alle protokollierbaren Ereignisse für den Protokollierungsgrad *nicht angegeben*; und

c die Ereignisse aus Kapitel 1.3.3.8 sowie keine weiteren Ereignisse.

Anwendungshinweis: Nach dem Starten des serverseitigen EVG ist die TSF dauerhaft aktiv, und somit wird auch die Protokollierung als Bestandteil der TSF-Funktionalität nicht beendet. In diesem Sinne tritt das Ereignis „Beenden der Protokollierungsfunktionen“ nie ein.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

FAU_GEN.1.2 Die SERVERSEITIGE TSF muß innerhalb jeder Aufzeichnung mindestens die folgenden Informationen speichern:

a Datum und Uhrzeit des Ereignisses, Art des Ereignisses, Identität des Subjekts (OHNE INFORMATION ÜBER DIE IDENTITÄT DES WÄHLERS) und das Ergebnis (Erfolg oder Misserfolg) des Ereignisses; und

b basierend auf den Definitionen der in PP/ST eingebundenen protokollierbaren Ereignisse, für jede Art von Protokollierungsereignissen **keine weiteren protokollierungsrelevanten Informationen**.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

[VERFEINERUNG FÜR wenn anwendbar: OHNE INFORMATION ÜBER DIE IDENTITÄT DES WÄHLERS]

FAU_SAR.1 Durchsicht der Protokollierung

Ist hierarchisch zu: Keinen anderen Komponenten.
Abhängigkeiten: FAU_GEN.1 Generierung der Protokolldaten

FAU_SAR.1.1 Die SERVERSEITIGE TSF muß für **den Wahlvorstand** die Fähigkeit bereitstellen, die **in Kapitel 1.3.3.8 genannten Protokollinformationen und keine weiteren protokollierungsrelevanten Information** aus den Protokollaufzeichnungen zu lesen.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

FAU_SAR1.2 Die SERVERSEITIGE TSF muß die Protokollaufzeichnungen in einer für die Interpretation der Informationen durch den Benutzer geeigneten Art und Weise bereitstellen.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

FDP_DAU.1 Einfache Datenauthentisierung

Ist hierarchisch zu: Keinen anderen Komponenten.
Abhängigkeiten: Keine Abhängigkeiten.

FDP_DAU.1.1 Die SERVERSEITIGE TSF muß die Fähigkeit zur Generierung von Nachweisen als Gültigkeitsgarantie von **Wahldurchführungsdaten, Wahlergebnis und *Protokollaufzeichnungen*** bereitstellen.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

FDP_DAU.1.2 Die SERVERSEITIGE TSF muß **keinem Subjekt** mit der Fähigkeit zur Verifizierung des Gültigkeitsnachweises der angegebenen Information, D.H. ZUR FESTSTELLUNG, DASS DER INHALT DER ANGEGEBENEN INFORMATIONEN NICHT NACHTRÄGLICH GEFÄLSCHT ODER BETRÜGERISCH VERÄNDERT WURDE, bereitstellen.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

[VERFEINERUNG FÜR zur Verifizierung des Gültigkeitsnachweises der angegebenen Information: zur Verifizierung des Gültigkeitsnachweises der angegebenen Information, D.H. ZUR FESTSTELLUNG, DASS DER INHALT DER ANGEGEBENEN INFORMATIONEN NICHT NACHTRÄGLICH GEFÄLSCHT ODER BETRÜGERISCH VERÄNDERT WURDE.]

FDP_IFC.1A Teilweise Informationsflusskontrolle (Wahlhandlung)

Ist hierarchisch zu: Keinen anderen Komponenten.
Abhängigkeiten: FDP_IFF.1 Einfache Sicherheitsattribute

FDP_IFC.1A.1 Die TSF muß die **SFP für Wahlhandlungen** für **die folgenden Subjekte, Informationen und kontrollierten Operationen** durchsetzen:

- **Subjekte: Wähler**
- **Informationen: Stimmen, Stimmdatensätze, Identifikationsdaten, Authentisierungsnachrichten, Stimmzettel, Stimmzetteldaten, Rückmeldungen, Stimmabgabevermerke, Zwischenergebnis**
- **Kontrollierte Operationen: Identifikation / Authentisierung, Einleitung der Stimmabgabe, Widerruf der eingeleiteten Stimmabgabe, Endgültige Stimmabgabe**

DIE SFP FÜR WAHLHANDLUNGEN MUSS FOLGENDE SICHERHEITSPRINZIPIEN EINHALTEN [VERFEINERUNG FÜR Anwendungsbereich der Kontrolle]**:**

A DIE KONTROLLIERTEN OPERATIONEN DÜRFEN NUR WÄHREND DER WAHLDURCHFÜHRUNG AUSGEFÜHRT WERDEN;

B NUR WÄHREND DER WAHLDURCHFÜHRUNG DÜRFEN STIMMDATENSÄTZE IN DER URNE GESPEICHERT WERDEN;

C NUR REGISTRIERTE WÄHLER DÜRFEN EINE STIMME ABGEBEN;

D JEDER WÄHLER DARF NUR EINMAL EINE STIMME ABGEBEN;

E KEIN INFORMATIONSFLUSS DARF DEM WÄHLER INFORMATIONEN ZUR VERFÜGUNG STELLEN, DIE IHM DIE MÖGLICHKEIT GEBEN WÜRDEN, SEINE WAHLENTSCHEIDUNG GEGENÜBER ANDEREN ZU BEWEISEN;

F KEIN INFORMATIONSFLUSS ZWISCHEN DEM WÄHLER UND DEM INHALT DER URNE DARF DAZU FÜHREN, DASS GESPEICHERTE STIMMDATENSÄTZE VERÄNDERT ODER GELÖSCHT WERDEN; UND

G KEIN INFORMATIONSFLUSS ZWISCHEN DEM WÄHLER UND DEM INHALT DER URNE DARF DAZU FÜHREN, DASS DIREKT, D.H. DURCH STIMMAUSZÄHLUNG, ODER INDIREKT, D.H. DURCH PREISGABE DES INHALTS GESPEICHERTER STIMMDATENSÄTZE, ZWISCHENERGEBNISSE ERMITTELT WERDEN.

FDP_IFF.1A Einfache Sicherheitsattribute (Wahlhandlung)

Ist hierarchisch zu: Keinen anderen Komponenten.
Abhängigkeiten: FDP_IFC.1 Teilweise Informationsflusskontrolle
FMT_MSA.3 Initialisierung statischer Attribute

FDP_IFF.1A.1 Die TSF muß die **SFP für Wahlhandlungen** auf Grundlage folgender Arten von Subjekt- und Informations-Sicherheitsattributen durchsetzen:

·Stimmberechtigungsattribut
·Wahlhandlungsattribut
·Wahlzeitraum

FDP_IFF.1A.2 Die TSF muß einen über eine kontrollierte Operation erfolgenden Informationsfluss zwischen dem kontrollierten Subjekt und den kontrollierten Informationen erlauben, wenn die folgenden Regeln zutreffen:

[Regel 1] Der Wähler kann sich beim serverseitigen EVG identifizieren und authentisieren, wenn das Stimmberechtigungsattribut den Wert unbekannt besitzt. Falls die Identifikation und Authentisierung erfolgreich ist, erhält das Stimmberechtigungsattribut den Wert mit bzw. ohne, je nach Stimmabgabevermerk. Sonst behält es den Wert unbekannt.

[Regel 2] Der Wähler kann durch Auswahl der Wahlvorschläge seine Wahlentscheidung treffen und schließlich die Stimmabgabe einleiten, wenn das Wahlhandlungsattribut den Wert vor besitzt. Dabei wird dem ausgefüllten Stimmzettel der benötigte Zwischenspeicher zugeteilt und das Wahlhandlungsattribut erhält den Wert nach.

[Regel 3] Der Wähler kann die Einleitung der Stimmabgabe widerrufen, wenn das Wahlhandlungsattribut den Wert nach besitzt. Dabei wird der dem ausgefüllten Stimmzettel zugeteilte Zwischenspeicher wieder freigegeben und das Wahlhandlungsattribut erhält den Wert vor.

[Regel 4] Der Wähler kann seine Stimme abgeben, wenn das Stimmberechtigungsattribut den Wert mit und das Wahlhandlungsattribut den Wert nach besitzt. Dabei werden in einer untrennbar verbundenen Aktion der Stimmdatensatz in der Urne gespeichert und die Stimmabgabe des Wählers vermerkt. Nach erfolgreicher Ausführung der Aktion wird der dem ausgefüllten Stimmzettel zugeteilte Zwischenspeicher wieder freigegeben und das Stimmberechtigungsattribut erhält den Wert ohne. Sonst behält es den Wert mit.

FDP_IFF.1A.3 Die TSF muß die **folgenden zusätzlichen SFP-Regeln** durchsetzen**:**

[Regel 5] Dem registrierten Wähler wird eine zutreffende Rückmeldung über die Erlaubnis bzw. Verweigerung und den Erfolg bzw. Misserfolg seiner Stimmabgabe gegeben.

FDP_IFF.1A.4 Die TSF muß einen Informationsfluss auf Grundlage folgender Regeln explizit autorisieren: **keine**

FDP_IFF.1A.5 Die TSF muß einen Informationsfluss auf Grundlage folgender Regeln explizit verweigern:

[Regel 6] Die Ausführung der kontrollierten Operationen Identifikation / Authentisierung [Regel 1], Einleitung der Stimmabgabe [Regel 2], Widerruf der eingeleiteten Stimmabgabe [Regel 3] und endgültige Stimmabgabe [Regel 4] ist explizit zu verweigern, wenn das Attribut Wahlzeitraum nicht den Wert Durchführung besitzt.

FDP_IFC.1B Teilweise Informationsflusskontrolle (Wahldurchführung inkl. Stimmauszählung)

Ist hierarchisch zu: Keinen anderen Komponenten.
Abhängigkeiten: FDP_IFF.1 Einfache Sicherheitsattribute

FDP_IFC.1B.1 Die SERVERSEITIGE TSF muß die **SFP für Online-Wahlen** für **die folgenden Subjekte, Informationen und kontrollierten Operationen** durchsetzen:

- **Subjekte: Wahlvorstand**
- **Informationen: Stimmen, Stimmdatensätze, Protokollaufzeichnungen, Stimmzetteldaten, Wahldurchführungsdaten, Wahlende-Zeitpunkt, Wahlergebnis, Zwischenergebnis**
- **Kontrollierte Operationen: Starten der Wahldurchführung, Wiederanlaufen der Wahldurchführung, Beenden der Wahldurchführung, Starten der Stimmauszählung mit Feststellung des Wahlergebnisses**

DIE SFP FÜR ONLINE-WAHLEN MUSS FOLGENDE SICHERHEITSPRINZIPIEN EINHALTEN [VERFEINERUNG FÜR Anwendungsbereich der Kontrolle]**:**

A DIE KONTROLLIERTEN OPERATIONEN DÜRFEN NUR AUSGEFÜHRT WERDEN, WENN SIE VON MEHR ALS EINEM MITGLIED DES WAHLVORSTANDS AUTORISIERT WERDEN;

B KEIN INFORMATIONSFLUSS ZWISCHEN DEM WAHLVORSTAND UND DEM INHALT DER URNE DARF DAZU FÜHREN, DASS STIMMDATENSÄTZE GESPEICHERT ODER GESPEICHERTE STIMMDATENSÄTZE VERÄNDERT ODER GELÖSCHT WERDEN;

C KEIN INFORMATIONSFLUSS ZWISCHEN DEM WAHLVORSTAND UND DEM INHALT DER URNE DARF DAZU FÜHREN, DASS DIREKT, D.H. DURCH STIMMAUSZÄHLUNG, ODER INDIREKT, D.H. DURCH PREISGABE DES INHALTS GESPEICHERTER STIMMDATENSÄTZE, ZWISCHENERGEBNISSE ERMITTELT WERDEN;

D FÜR DIE STIMMAUSZÄHLUNG MÜSSEN ALLE ABGEGEBENEN STIMMEN, D.H. ALLE IN DER URNE GESPEICHERTEN STIMMDATENSÄTZE BERÜCKSICHTIGT WERDEN; UND

E NACH DER STIMMAUSZÄHLUNG MIT FESTSTELLUNG DES WAHLERGEBNISSES MUSS FÜR DIE WAHLDURCHFÜHRUNGSDATEN, DAS WAHLERGEBNIS UND DIE *PROTOKOLLAUFZEICHNUNGEN* EIN MANIPULATIONSSCHUTZ ALS GÜLTIGKEITSGARANTIE ERZEUGT WERDEN.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

FDP_IFF.1B Einfache Sicherheitsattribute (Wahldurchführung inkl. Stimmauszählung)

Ist hierarchisch zu: Keinen anderen Komponenten.
Abhängigkeiten: FDP_IFC.1 Teilweise Informationsflusskontrolle
FMT_MSA.3 Initialisierung statischer Attribute

FDP_IFF.1B.1 Die SERVERSEITIGE TSF muß die **SFP für Online-Wahlen** auf Grundlage folgender Arten von Subjekt- und Informations-Sicherheitsattributen durchsetzen:

- **Wahlzeitraum**
- **Anzahl der Autorisierungen für die angeforderte Operation**

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

FDP_IFF.1B.2 Die SERVERSEITIGE TSF muß einen über eine kontrollierte Operation erfolgenden Informationsfluss zwischen dem kontrollierten Subjekt und den kontrollierten Informationen erlauben, wenn die folgenden Regeln zutreffen:

[Regel 1] Der Wahlvorstand kann die Operation zum Starten der Wahldurchführung anfordern, wenn das Attribut Wahlzeitraum den Wert Vorbereitung besitzt. Bei Ausführung der Operation wird der Urne Speicherplatz für die Speicherung von Stimmdatensätzen zugeteilt. Das Attribut Wahlzeitraum erhält den Wert Durchführung.

[Regel 2] Der Wahlvorstand kann die Operation zum Wiederanlaufen der Wahldurchführung anfordern, wenn das Attribut Wahlzeitraum den Wert Durchführung besitzt. Bei Ausführung der Operation behält das Attribut Wahlzeitraum den Wert Durchführung.

[Regel 3] Nach dem Wahlende-Zeitpunkt kann der Wahlvorstand die Operation zum Beenden der Wahldurchführung anfordern, wenn das Attribut Wahlzeitraum den Wert Durchführung besitzt. Bei Ausführung der Operation erhält das Attribut Wahlzeitraum den Wert Auszählung.

[Regel 4] Der Wahlvorstand kann die Operation zum Starten der Stimmauszählung mit Feststellung des Wahlergebnisses anfordern, wenn das Attribut Wahlzeitraum den Wert Auszählung besitzt. Bei Ausführung der Operation wird durch Auszählung aller abgegebenen Stimmen, d.h. aller in der Urne gespeicherten Stimmdatensätze das Wahlergebnis ermittelt. Das Attribut Wahlzeitraum behält den Wert Auszählung.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

FDP_IFF.1B.3 Die SERVERSEITIGE TSF muß die **folgenden zusätzlichen SFP-Regeln** durchsetzen**:**

[Regel 5] Nach der Stimmauszählung mit Feststellung des Wahlergebnisses wird ein Manipulationsschutz als Gültigkeitsgarantie von Wahldurchführungsdaten, Wahlergebnis und *Protokollaufzeichnungen* erzeugt.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

FDP_IFF.1B.4 Die SERVERSEITIGE TSF muß einen Informationsfluss auf Grundlage folgender Regeln explizit autorisieren:

[Regel 6] Die Ausführung der Operation zum Beenden der Wahldurchführung vor dem Wahlende-Zeitpunkt wird vom Wahlvorstand durch Bestätigung des Wahlendes explizit autorisiert.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

FDP_IFF.1B.5 Die SERVERSEITIGE TSF muß einen Informationsfluss auf Grundlage folgender Regeln explizit verweigern:

[Regel 7] Die Ausführung der kontrollierten Operationen zum Starten der Wahldurchführung [Regel 1], Wiederanlaufen der Wahldurchführung [Regel 2], Beenden der Wahldurchführung [Regel 3] und Starten der Stimmauszählung mit Feststellung des Wahlergebnisses [Regel 4] ist explizit zu verweigern, wenn die Anzahl der Autorisierungen von unterschiedlichen Mitgliedern des Wahlvorstands für die angeforderte Operation kleiner als zwei ist.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

FDP_IFF.5 Keine unerwünschten Informationsflüsse

Ist hierarchisch zu: FDP_IFF.4 Teilweise Beseitigung der unerwünschten Informationsflüsse
Abhängigkeiten: FDP_IFC.1 Teilweise Informationsflußkontrolle

FDP_IFF.5.1 Die TSF muß sicherstellen, daß keine unerwünschten Informationsflüsse zur Umgehung von **SFP für Wahlhandlungen und SFP für Online-Wahl** existieren.

A Die TSF stellen dem Wähler keine Quittung oder andere Daten zur Verfügung, mit deren Hilfe der Wähler seine Wahlentscheidung beweisen könnte. Insbesondere enthält die Rückmeldung über die erfolgreiche Stimmabgabe keinen solchen Beweis;

B Kein Informationsfluss zwischen dem Wahlvorstand und dem Inhalt der Urne darf dazu führen, dass Stimmdatensätze gespeichert werden; und Kein Informationsfluss zwischen dem Wähler oder dem Wahlvorstand und dem Inhalt der Urne darf dazu führen, dass gespeicherte Stimmdatensätze verändert oder gelöscht werden; und

C Kein Informationsfluss zwischen dem Wähler oder dem Wahlvorstand und dem Inhalt der urne darf dazu führen, dass direkt, d.h. durch Stimmauszählung, oder indirekt, d.h. durch Preisgabe des Inhalts gespeicherter Stimmdatensätze, Zwischenergebnisse ermittelt werden;

D Die Eröffnung einer Wahlhandlung durch den Wähler darf bereits während der Ausführung der Operation zum Beenden der Wahldurchführung nicht mehr möglich sein. Die Ausführung der Operation soll so lange andauern, dass alle begonnenen Wahlhandlungen beendet werden können.

[Verfeinerung für keine unerwünschten Informationsflüsse:

a) …; b) …; c) …; d)…;]

FDP_SDI.2 Überwachung der Integrität der gespeicherten Daten und Reaktionen

Ist hierarchisch zu: FDP_SDI.1 Überwachung der Integrität der gespeicherten Daten
Abhängigkeiten: Keine Abhängigkeiten.

FDP_SDI.2.1 Die serverseitige TSF muß die in der Urne gespeicherten Stimmdatensätze auf **Schreibfehler beim Speichern in der Urne oder beim untrennbar damit verbundenen Vermerk der Stimmabgabe** bei allen Objekten auf Basis folgender Attribute: **Fehlermeldungen, die von der unterliegenden Software (bspw. Betriebssystem) signalisiert werden,** überwachen.

[Verfeinerung für TSF: serverseitige TSF]

[Verfeinerung für Container, welche von der TSF kontrolliert werden: der Urne]

[Verfeinerung für Benutzerdaten: Stimmdatensätze]

FDP_SDI.2.2 Bei Erkennen eines Datenintegritätsfehlers muß die serverseitige TSF **den Wahlvorstand informieren und keine weitere Aktionen ausführen.**

[Verfeinerung für TSF: serverseitige TSF]

FDP_RIP.1A Teilweiser Schutz bei erhalten gebliebenen Informationen (Stimmzettel)

Ist hierarchisch zu: Keinen anderen Komponenten.
Abhängigkeiten: Keine Abhängigkeiten

FDP_RIP.1A.1 Die SERVERSEITIGE TSF muß sicherstellen, daß der frühere Informationsinhalt VON ZWISCHENSPEICHER bei *Zuteilung VON ZWISCHENSPEICHER zu und Wiederfreigabe VON ZWISCHENSPEICHER von* folgenden Objekten: **Stimmzettel** nicht verfügbar ist.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

[VERFEINERUNG FÜR einer Ressource: VON ZWISCHENSPEICHER]

FDP_RIP.1B Teilweiser Schutz bei erhalten gebliebenen Informationen (Urne)

Ist hierarchisch zu: Keinen anderen Komponenten.
Abhängigkeiten: Keine Abhängigkeiten

FDP_RIP.1B.1 Die SERVERSEITIGE TSF muß sicherstellen, daß der frühere Informationsinhalt VON SPEICHERPLATZ FÜR DIE SPEICHERUNG VON STIMMDATENSÄTZEN bei *Zuteilung VON SPEICHERPLATZ FÜR DIE SPEICHERUNG VON STIMMDATENSÄTZEN zu* folgenden Objekten: **Urne** nicht verfügbar ist.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

[VERFEINERUNG FÜR einer Ressource: VON SPEICHERPLATZ FÜR DIE SPEICHERUNG VON STIMMDATENSÄTZEN]

FDP_UCT.1A Einfache Vertraulichkeit des Datenaustausches (Wähler)

Ist hierarchisch zu: Keinen anderen Komponenten.
Abhängigkeiten: [FTP_ITC.1 Inter-TSF Vertrauenswürdiger Kanal oder FTP_TRP.1 Vertrauenswürdiger Pfad]

[FDP_ACC.1 Teilweise Zugriffskontrolle oder FDP_IFC.1 Teilweise Informationsflusskontrolle]

FDP_UCT.1A.1 Die TSF muß die **SFP für Wahlhandlungen** durchsetzen, um […] WÄHLERTOKEN, IDENTIFIKATIONSDATEN, AUTHENTISIERUNGSNACHRICHTEN, STIMMZETTEL UND STIMMDATENSÄTZE vor nichtautorisierter Preisgabe geschützt zu *übertragen und empfangen*.

[VERFEINERUNG FÜR Benutzerdaten: WÄHLERTOKEN, IDENTIFIKATIONSDATEN, AUTHENTISIERUNGS-NACHRICHTEN, STIMMZETTEL UND STIMMDATENSÄTZE]

FDP_UCT.1B Einfache Vertraulichkeit des Datenaustausches (Wahlvorstand)

Ist hierarchisch zu: Keinen anderen Komponenten.

Abhängigkeiten: [FTP_ITC.1 Inter-TSF Vertrauenswürdiger Kanal oder FTP_TRP.1 Vertrauenswürdiger Pfad]

[FDP_ACC.1 Teilweise Zugriffskontrolle oder FDP_IFC.1 Teilweise Informationsflusskontrolle]

FDP_UCT.1B.1 Die TSF muß die **SFP für Online-Wahlen** durchsetzen, um IDENTIFIKATIONSDATEN UND AUTHENTISIERUNGSNACHRICHTEN DES WAHLVORSTANDES vor nichtautorisierter Preisgabe geschützt zu *übertragen und empfangen*.

[VERFEINERUNG FÜR Benutzerdaten: IDENTIFIKATIONSDATEN UND AUTHENTISIERUNGSNACHRICHTEN DES WAHLVORSTANDES]

FDP_UIT.1A Einfache Integrität des Datenaustausches (Wähler)

Ist hierarchisch zu: Keinen anderen Komponenten.

Abhängigkeiten: [FDP_ACC.1 Teilweise Zugriffskontrolle oder FDP_IFC.1 Teilweise Informationsflußkontrolle]

[FTP_ITC.1 Inter-TSF Vertrauenswürdiger Kanal oder FTP_TRP.1 Vertrauenswürdiger Pfad]

FDP_UIT.1A.1 Die TSF muß die **SFP für Wahlhandlungen** durchsetzen, um […] WÄHLERTOKEN, IDENTIFIKATIONSDATEN, AUTHENTISIERUNGSNACHRICHTEN, STIMMZETTEL, STIMMDATENSÄTZE, STIMMZETTELDATEN UND RÜCKMELDUNGEN vor *Modifizieren, Löschen, Einfügen und Wiedereinspielen* geschützt zu *übertragen und zu empfangen*.

[VERFEINERUNG FÜR Benutzerdaten: WÄHLERTOKEN, IDENTIFIKATIONSDATEN, AUTHENTISIERUNGS-NACHRICHTEN, STIMMZETTEL, STIMMDATENSÄTZE, STIMMZETTELDATEN UND RÜCKMELDUNGEN]

FDP_UIT.1A.2 Die TSF muß in der Lage sein, beim Empfang der WÄHLERTOKEN, IDENTIFIKATIONSDATEN, AUTHENTISIERUNGSNACHRICHTEN, STIMMZETTEL, STIMMDATENSÄTZE, STIMMZETTELDATEN UND RÜCKMELDUNGEN festzustellen, ob ein *Modifizieren, Löschen, Einfügen oder Wiedereinspielen* stattgefunden hat.

[VERFEINERUNG FÜR Benutzerdaten: WÄHLERTOKEN, IDENTIFIKATIONSDATEN, AUTHENTISIERUNGS-NACHRICHTEN, STIMMZETTEL, STIMMDATENSÄTZE, STIMMZETTELDATEN UND RÜCKMELDUNGEN]

FDP_UIT.1B Einfache Integrität des Datenaustausches (Wahlvorstand)

Ist hierarchisch zu: Keinen anderen Komponenten.

Abhängigkeiten: [FDP_ACC.1 Teilweise Zugriffskontrolle oder FDP_IFC.1 Teilweise Informationsflußkontrolle]

[FTP_ITC.1 Inter-TSF Vertrauenswürdiger Kanal oder FTP_TRP.1 Vertrauenswürdiger Pfad]

FDP_UIT.1B.1 Die TSF muß die **SFP für Online-Wahlen** durchsetzen, um DAS ERGEBNIS vor *Modifizieren, Löschen, Einfügen und Wiedereinspielen* geschützt zu *übertragen und zu empfangen*.

[VERFEINERUNG FÜR Benutzerdaten: ERGEBNIS]

FDP_UIT.1B.2 Die TSF muß in der Lage sein, beim Empfang DES ERGEBNIS‘ festzustellen, ob ein *Modifizieren, Löschen, Einfügen oder Wiedereinspielen* stattgefunden hat.

[VERFEINERUNG FÜR Benutzerdaten: ERGEBNIS]

FIA_ATD.1 Definition der Benutzerattribute

Ist hierarchisch zu: Keinen anderen Komponenten

Abhängigkeiten: Keine Abhängigkeiten

FIA_ATD.1.1 Die TSF muss die folgende Liste von Sicherheitsattributen, die zu einzelnen Benutzern gehören, erhalten:

- **Stimmberechtigungsattribut und Wahlhandlungsattribut (für Wähler):**
  Die Attribute werden mit Eröffnung jeder Wahlhandlung erzeugt und bleiben mit dem erzeugenden Wähler verbunden. Bei Abbruch (durch Fehler, Zeitablauf oder den Wähler) oder Ende der Wahlhandlung wird die Verbindung aufgelöst. Damit existieren die Attribute nicht mehr.
- **Anzahl der Autorisierungen für die angeforderte Operation (für den Wahlvorstand):**
  Das Attribut wird über die Anforderung einer kontrollierten Operation der SFP für Online-Wahlen mit dem Wahlvorstand verknüpft. Vor der ersten Anforderung der kontrollierten Operation besitzt es den Wert Null.

FIA_UAU.1 Zeitpunkt der Authentisierung (für Wähler)

Ist hierarchisch zu: keiner anderen Komponenten.

Abhängigkeiten: FIA_UID.1 Zeitpunkt der Identifikation

FIA_UAU.1.1 DIE SERVERSEITIGE TSF muß die Ausführung der **Eröffnung der Wahlhandlung und keine weiteren Aktionen** für den Wähler erlauben, bevor dieser authentisiert wird.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

[VERFEINERUNG FÜR Benutzer: WÄHLER]

FIA_UAU.1.2 Die SERVERSEITIGE TSF muß erfordern, daß jeder WÄHLER erfolgreich authentisiert wurde, bevor für diesen jegliche andere TSF-vermittelte Aktionen erlaubt werden.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

[VERFEINERUNG FÜR Benutzer: WÄHLER]

FIA_UAU.2 Benutzerauthentisierung vor jeglicher Aktion (für Wahlvorstand)

Ist hierarchisch zu: FIA_UAU.1
Abhängigkeiten: FIA_UID.1 Zeitpunkt der Identifikation

FIA_UAU.2.1 Die SERVERSEITIGE TSF muß erfordern, daß JEDES MITGLIED DES WAHLVORSTANDS erfolgreich authentisiert wurde, bevor diesem jegliche andere TSF-vermittelte Aktionen erlaubt werden.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

[VERFEINERUNG FÜR jeder Benutzer: JEDES MITGLIED DES WAHLVORSTANDS]

FIA_UAU.6 Wiederauthentisierung (für Wahlvorstand)

Ist hierarchisch zu: Keinen anderen Komponenten.
Abhängigkeiten: Keine Abhängigkeiten

FIA_UAU.6.1 Die SERVERSEITIGE TSF muß DAS MITGLIED DES WAHLVORSTANDS wiederauthentisieren, WENN **dieses Mitglied des Wahlvorstands die Ausführung einer von der SFP für Online-Wahlen kontrollierten Operation anfordert**.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

[VERFEINERUNG FÜR den Benutzer: DAS MITGLIED DES WAHLVORSTANDS]

[VERFEINERUNG FÜR unter den Bedingungen … wiederauthentisieren: wiederauthentisieren, WENN …]

FIA_UID.1 Zeitpunkt der Identifikation (für Wähler)

Ist hierarchisch zu: Keinen anderen Komponenten.
Abhängigkeiten: Keine Abhängigkeiten

FIA_UID.1.1 Die SERVERSEITIGE TSF muß die Ausführung der **Eröffnung der Wahlhandlung und keiner weiteren Aktionen** für den WÄHLER erlauben, bevor dieser identifiziert wird.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

[VERFEINERUNG FÜR Benutzer: WÄHLER]

FIA_UID.1.2 Die SERVERSEITIGE TSF muß erfordern, daß jeder WÄHLER erfolgreich identifiziert wurde, bevor für diesen jegliche andere TSF-vermittelte Aktionen erlaubt werden.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

[VERFEINERUNG FÜR Benutzer: WÄHLER]

FIA_UID.2 Benutzeridentifikation vor jeglicher Aktion (für Wahlvorstand)

Ist hierarchisch zu: FIA_UID.1
Abhängigkeiten: Keine Abhängigkeiten

FIA_UID.2.1 Die SERVERSEITIGE TSF muß erfordern, daß JEDES MITGLIED DES WAHLVORSTANDS erfolgreich identifiziert wurde, bevor für diesen jegliche andere TSF-vermittelte Aktionen erlaubt werden.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

[VERFEINERUNG FÜR jeder Benutzer: JEDES MITGLIED DES WAHLVORSTANDS]

FIA_USB.1A Benutzer-Subjekt-Bindung (für Wähler)

Ist hierarchisch zu: Keinen anderen Komponenten.
Abhängigkeiten: FIA_ATD.1 Definition der Benutzerattribute

FIA_USB.1A.1 Die TSF muß die folgenden Benutzersicherheitsattribute mit den Subjekten, die für den WÄHLER handeln, verknüpfen: **Stimmberechtigungsattribut und Wahlhandlungsattribut.**

[VERFEINERUNG FÜR Benutzer: WÄHLER]

FIA_USB.1A.2 Die TSF muß die folgenden Regeln für die initiale Verknüpfung der Benutzersicherheitsattribute mit den Subjekten, die für den WÄHLER handeln, durchsetzen: **Bei Eröffnung der Wahlhandlung erhält**

- **das Stimmberechtigungsattribut den Wert unbekannt; und**
- **das Wahlhandlungsattribut den Wert vor.**

[VERFEINERUNG FÜR Benutzer: WÄHLER]

FIA_USB.1A.3 Die TSF muß die folgenden Regeln bei Änderungen an den Benutzersicherheitsattributen, die mit den für die WÄHLER handelnden Subjekten verknüpft sind, durchsetzen: **Über die Regeln der SFP für Wahlhandlungen hinaus werden die Benutzersicherheitsattribute nicht geändert**.

[VERFEINERUNG FÜR Benutzer: WÄHLER]

FIA_USB.1B Benutzer-Subjekt-Bindung (für Wahlvorstand)

Ist hierarchisch zu: Keinen anderen Komponenten.
Abhängigkeiten: FIA_ATD.1 Definition der Benutzerattribute

FIA_USB.1B.1 Die SERVERSEITIGE TSF muß die folgenden Benutzersicherheitsattribute mit den Subjekten, die NACH ERFOLGREICHER WIEDERAUTHENTISIERUNG für den WAHLVORSTAND EINE VON DER SFP FÜR ONLINE-WAHLEN KONTROLLIERTE OPERATION ANFORDERN, verknüpfen: **Anzahl der Autorisierungen für die angeforderte Operation**.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

[VERFEINERUNG FÜR für den Benutzer: NACH ERFOLGREICHER WIEDERAUTHENTISIERUNG für den WAHLVORSTAND]

[VERFEINERUNG FÜR handeln: EINE VON DER SFP FÜR ONLINE-WAHLEN KONTROLLIERTE OPERATION ANFORDERN]

FIA_USB.1B.2 Die SERVERSEITIGE TSF muß die folgenden Regeln für die initiale Verknüpfung der Benutzersicherheitsattribute mit den Subjekten, die NACH ERFOLGREICHER WIEDERAUTHENTISIERUNG für den WAHLVORSTAND EINE VON DER SFP FÜR ONLINE-WAHLEN KONTROLLIERTE OPERATION ANFORDERN, durchsetzen: **Die Anzahl der Autorisierungen für die angeforderte Operation wird inkrementiert (der Wert wird um die Zahl Eins erhöht)**.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

[VERFEINERUNG FÜR für den Benutzer: NACH ERFOLGREICHER WIEDERAUTHENTISIERUNG für den WAHLVORSTAND]

[VERFEINERUNG FÜR handeln: EINE VON DER SFP FÜR ONLINE-WAHLEN KONTROLLIERTE OPERATION ANFORDERN]

FIA_USB.1B.3 Die SERVERSEITIGE TSF muß die folgenden Regeln bei Änderungen an den Benutzersicherheitsattributen, die mit den für den WAHLVORSTAND handelnden Subjekten verknüpft sind, durchsetzen: **Wenn die Bindung zu einem Mitglied des Wahlvorstands durch *Abmeldung* aufgelöst wird, wird die Anzahl der Autorisierungen für die angeforderte Operation dekrementiert (der Wert wird um die Zahl Eins erniedrigt)**.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

[VERFEINERUNG FÜR Benutzer: WAHLVORSTAND]

FMT_SMR.2 Einschränkungen der Sicherheitsrollen

Ist hierarchisch zu: FMT_SMR.1 Sicherheitsrollen
Abhängigkeiten: FIA_UID.1 Zeitpunkt der Identifikation

FMT_SMR.2.1 Die SERVERSEITIGE TSF muß die Rollen **Wähler, Wahlvorstand und keine weitere identifizierte Rollen** erhalten.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

FMT_SMR.2.2 Die SERVERSEITIGE TSF muß Benutzer mit Rollen verknüpfen können.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

FMT_SMR.2.3 Die SERVERSEITIGE TSF muß sicherstellen, daß die FOLGENDEN Bedingungen erfüllt werden: **Benutzer dürfen nicht gleichzeitig mit den Rollen Wähler und Wahlvorstand verknüpft werden; und keine weiteren Bedingungen**.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

[VERFEINERUNG FÜR die Bedingungen … erfüllt werden: die FOLGENDEN Bedingungen erfüllt werden: …]

FPR_ANO.1 Anonymität

Ist hierarchisch zu: Keinen anderen Komponenten.
Abhängigkeiten: Keine Abhängigkeiten

FPR_ANO.1.1 Die TSF muß sicherstellen, daß **alle Benutzer** nicht in der Lage sind, den mit **einer Stimme** verbundenen tatsächlichen NAMEN DES REGISTRIERTEN WÄHLERS festzustellen.

[VERFEINERUNG FÜR Benutzernamen: NAMEN DES REGISTRIERTEN WÄHLERS]

FPR_UNL.1A Unverkettbarkeit (Netzwerk)

Ist hierarchisch zu: Keinen anderen Komponenten.
Abhängigkeiten: Keine Abhängigkeiten.

FPR_UNL.1A.1 Die TSF muß sicherstellen, daß **alle Benutzer** nicht in der Lage sind festzustellen, ob **die Operationen Einleitung der Stimmabgabe und endgültige Stimmabgabe** *in folgenden Beziehungen* ZUR ABGEGEBENEN STIMME *stehen*: ***die Länge der übertragenen Stimmzettel oder Stimmdatensätze korrespondiert zur Anzahl der ausgewählten Wahlvorschläge, Position der Wahlvorschläge im Stimmzettel oder der Ungültigkeit der Stimme***.

[VERFEINERUNG FÜR *in folgenden Beziehungen stehen*: *in folgenden Beziehungen* ZUR ABGEGEBENEN STIMME *stehen*]

FPR_UNL.1B Unverkettbarkeit (Urne)

Ist hierarchisch zu: Keinen anderen Komponenten.
Abhängigkeiten: Keine Abhängigkeiten.

FPR_UNL.1B.1 Die SERVERSEITIGE TSF muß sicherstellen, daß **der Wahlvorstand** NACH DER FESTSTELLUNG DES WAHLERGEBNISSES nicht in der Lage ist festzustellen, ob **die Speicherung von Stimmdatensätzen in der Urne** *in folgenden Beziehungen stehen: **die Speicherung wurde in einer bestimmten Reihenfolge oder zu einem bestimmten Zeitpunkt ausgeführt***.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

[VERFEINERUNG FÜR nicht in der Lage ist: NACH DER FESTSTELLUNG DES WAHLERGEBNISSES nicht in der Lage ist]

FPT_ITT.1 Einfacher Schutz bei internem TSF-Datenaustausch

Ist hierarchisch zu: Keinen anderen Komponenten.
Abhängigkeiten: Keine Abhängigkeiten.

FPT_ITT.1.1 Die TSF muß die TSF-Daten während der Übertragung zwischen getrennten Teilen des EVG gegen Preisgabe und Modifizierung schützen.

FPT_RCV.1 Manuelle Wiederherstellung

Ist hierarchisch zu: Keinen anderen Komponenten.

Abhängigkeiten: AGD_OPE.1 Benutzerhandbücher für den Betrieb

FPT_RCV.1.1 Nach **einer Unterbrechung der Wahldurchführung durch Absturz / Herunterfahren des serverseitigen EVG oder des Wahlservers oder durch Ausfall der Kommunikation oder der Speichermedien** muß die SERVERSEITIGE TSF in einen Erhaltungsmodus wechseln, der die Fähigkeit bereitstellt, zu einem sicheren Zustand zurückzukehren, D.H.

A FÜR JEDE KONTROLLIERTE OPERATION DER SFP FÜR ONLINE-WAHLEN ERHÄLT DAS ATTRIBUT ANZAHL DER AUTORISIERUNGEN FÜR DIE ANGEFORDERTE OPERATION DEN WERT NULL;

B DAS ATTRIBUT WAHLZEITRAUM BEHÄLT DEN WERT DURCHFÜHRUNG; UND

C VOR DER UNTERBRECHUNG LAUFENDE WAHLHANDLUNGEN WERDEN ABGEBROCHEN. DABEI MUSS DER STIMMABGABEVERMERK DES WÄHLERS UNVERÄNDERT ERHALTEN BLEIBEN UND ZUGETEILTER ZWISCHENSPEICHER FÜR AUSGEFÜLLTE STIMMZETTEL WIEDER FREIGEGEBEN WERDEN.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

[VERFEINERUNG FÜR sicherer Zustand: D.H. a) …; b) …; UND c) …]

FPT_RCV.4 Funktionelle Wiederherstellung

Ist hierarchisch zu: Keinen anderen Komponenten.
Abhängigkeiten: Keine Abhängigkeiten

FPT_RCV.4.1 Die SERVERSEITIGE TSF muß sicherstellen, daß **bei einer Unterbrechung der Wahldurchführung durch Absturz / Herunterfahren des serverseitigen EVG oder des Wahlservers oder durch Ausfall der Kommunikation oder der Speichermedien** die Eigenschaft besitzt, daß die Funktion SPEICHERN DER STIMMDATENSÄTZE IN DER URNE ZUSAMMEN MIT DEM VERMERK DER STIMMABGABE entweder erfolgreich abgeschlossen wird, oder im Fall eines der aufgeführten Fehlerszenarien, diese bis zu DEM ZUSTAND VOR DER AUSFÜHRUNG DER OPERATION ZUR STIMMABGABE wiederherzustellen.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

[VERFEINERUNG FÜR die Funktion: die Funktion SPEICHERN DER STIMMDATENSÄTZE IN DER URNE ZUSAMMEN MIT DEM VERMERK DER STIMMABGABE]

[VERFEINERUNG FÜR einem konsistenten und sicheren Zustand: DEM ZUSTAND VOR DER AUSFÜHRUNG DER OPERATION ZUR STIMMABGABE

FPT_TST.1 TSF Testen

Ist hierarchisch zu: Keinen anderen Komponenten.
Abhängigkeiten: Keine Abhängigkeiten.

FPT_TST.1.1 Die SERVERSEITIGE TSF muß *beim Erstanlauf und auf Anforderung DES WAHLVORSTANDS* eine Testfolge als Nachweis für den korrekten Betrieb der *SERVERSEITIGEN TSF* durchführen.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

[VERFEINERUNG FÜR *eines autorisierten Benutzers*: *DES WAHLVORSTANDS*]

[VERFEINERUNG: *TSF*: *SERVERSEITIGEN TSF*]

FPT_TST.1.2 Die SERVERSEITIGE TSF muß für DEN WAHLVORSTAND die Fähigkeit zur Verifizierung der Integrität von *SERVERSEITIGEN BENUTZER- UND TSF-Daten* bereitstellen.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

[VERFEINERUNG FÜR autorisierte Benutzer: DEN WAHLVORSTAND]

[VERFEINERUNG FÜR *TSF-Daten*: *SERVERSEITIGEN BENUTZER- UND TSF-Daten*]

FPT_TST.1.3 Die SERVERSEITIGE TSF muß für DEN WAHLVORSTAND die Fähigkeit zur Verifizierung der Integrität von ***gespeichertem ausführbarem serverseitigem TSF-Code*** bereitstellen.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

[VERFEINERUNG FÜR autorisierte Benutzer: DEN WAHLVORSTAND]

[…]

FTA_SSL.3 Durch TSF eingeleitete Beendigung

Ist hierarchisch zu: Keinen anderen Komponenten.
Abhängigkeiten: Keine Abhängigkeiten.

FTA_SSL.3.1 Die SERVERSEITIGE TSF muß VOR DER ENDGÜLTIGEN STIMMABGABE eine WAHLHANDLUNG nach **einer konfigurierbaren Frist** beenden. DABEI MUSS DER STIMMABGABEVERMERK DES WÄHLERS UNVERÄNDERT ERHALTEN BLEIBEN UND ZUGETEILTER ZWISCHENSPEICHER FÜR AUSGEFÜLLTE STIMMZETTEL WIEDER FREIGEGEBEN WERDEN.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

[VERFEINERUNG (Erlaubnis der Beendigung): VOR DER ENDGÜLTIGEN STIMMABGABE]

[VERFEINERUNG FÜR interaktive Sitzung: WAHLHANDLUNG]

[VERFEINERUNG (Beenden der Wahlhandlung): DABEI MUSS DER STIMMABGABEVERMERK DES WÄHLERS UNVERÄNDERT ERHALTEN BLEIBEN UND ZUGETEILTER ZWISCHENSPEICHER FÜR AUSGEFÜLLTE STIMMZETTEL WIEDER FREIGEGEBEN WERDEN.]

FTA_SSL.4 Durch Benutzer eingeleitete Beendigung

Ist hierarchisch zu: Keinen anderen Komponenten.
Abhängigkeiten: Keine Abhängigkeiten.

FTA_SSL.4.1 Die SERVERSEITIGE TSF muß VOR DER ENDGÜLTIGEN STIMMABGABE die durch den WÄHLER eingeleitete Beendigung der eigenen WAHLHANDLUNG DES WÄHLERS erlauben. DABEI MUSS DER STIMMABGABEVERMERK DES WÄHLERS UNVERÄNDERT ERHALTEN BLEIBEN UND ZUGETEILTER ZWISCHENSPEICHER FÜR AUSGEFÜLLTE STIMMZETTEL WIEDER FREIGEGEBEN WERDEN.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

[VERFEINERUNG (Erlaubnis der Beendigung): VOR DER ENDGÜLTIGEN STIMMABGABE]

[VERFEINERUNG FÜR Benutzer: WÄHLER]

[VERFEINERUNG FÜR interaktiven Sitzung des Benutzers: WAHLHANDLUNG DES WÄHLERS]

[VERFEINERUNG (Beenden der Wahlhandlung): DABEI MUSS DER STIMMABGABEVERMERK DES WÄHLERS UNVERÄNDERT ERHALTEN BLEIBEN UND

ZUGETEILTER ZWISCHENSPEICHER FÜR AUSGEFÜLLTE STIMMZETTEL WIEDER FREIGEGEBEN WERDEN.]

FTA_TSE.1 TOE-Sitzungseinrichtung

Ist hierarchisch zu: Keinen anderen Komponenten.
Abhängigkeiten: Keine Abhängigkeiten.

FTA_TSE.1.1 Die SERVERSEITIGE TSF muß basierend auf *dem Attribut Wahlzeitraum* eine ERÖFFNUNG DER WAHLHANDLUNG verweigern, WENN DAS ATTRIBUT WAHLZEITRAUM NICHT DEN WERT DURCHFÜHRUNG BESITZT.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

[VERFEINERUNG FÜR Sitzungseinrichtung: ERÖFFNUNG DER WAHLHANDLUNG]

[VERFEINERUNG FÜR muß in der Lage sein, … zu verweigern: muß … verweigern, WENN DAS ATTRIBUT WAHLZEITRAUM NICHT DEN WERT DURCHFÜHRUNG BESITZT]

FTP_TRP.1A Vertrauenswürdiger Pfad (Wähler)
Ist hierarchisch zu: Keinen anderen Komponenten.
Abhängigkeiten: Keine Abhängigkeiten.

FTP_TRP.1A.1 Die SERVERSEITIGE TSF muß einen Kommunikationspfad zwischen sich und WÄHLERN ALS *entfernten* Benutzern bereitstellen, der logisch von den anderen Kommunikationspfaden getrennt ist und eine gesicherte GEGENSEITIGE IDENTIFIKATION VON WÄHLER UND SERVERSEITIGEM EVG sowie den Schutz der Kommunikationsdaten vor *Modifizierung oder Preisgabe* bereitstellt.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

[VERFEINERUNG FÜR Benutzern: WÄHLERN ALS … Benutzern]

[VERFEINERUNG FÜR Identifikation seiner Endpunkte: GEGENSEITIGE IDENTIFIKATION VON WÄHLER UND SERVERSEITIGEM EVG]

FTP_TRP.1A.2 Die SERVERSEITIGE TSF muß *WÄHLERN ALS entfernten Benutzern* erlauben, eine Kommunikation über den vertrauenswürdigen Pfad einzuleiten.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

[VERFEINERUNG FÜR Benutzern: WÄHLERN ALS … Benutzern]

FTP_TRP.1A.3 Die SERVERSEITIGE TSF muß den Gebrauch des vertrauenswürdigen Pfads für ***die Wahlhandlung*** erfordern.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

FTP_TRP.1B Vertrauenswürdiger Pfad (Wahlvorstand)
Ist hierarchisch zu: Keinen anderen Komponenten.
Abhängigkeiten: Keine Abhängigkeiten.

FTP_TRP.1B.1 Die SERVERSEITIGE TSF muß einen Kommunikationspfad zwischen sich und WAHLVORSTAND ALS *entfernten* Benutzern bereitstellen, der logisch von den anderen Kommunikationspfaden getrennt ist und eine gesicherte GEGENSEITIGE IDENTIFIKATION VON WAHLVORSTAND UND SERVERSEITIGEM WAHLVORSTANDSINTERFACE EVG sowie den Schutz der Kommunikationsdaten vor *Modifizierung oder Preisgabe* bereitstellt.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

[VERFEINERUNG FÜR Benutzern: WAHLVORSTAND ALS … Benutzern]

[VERFEINERUNG FÜR Identifikation seiner Endpunkte: GEGENSEITIGE IDENTIFIKATION VON WAHLVORSTAND UND SERVERSEITIGEM WAHLVORSTANDSINTERFACE EVG]

FTP_TRP.1B.2 Die SERVERSEITIGE TSF muß *DEM WAHLVORSTAND ALS entfernten Benutzern* erlauben, eine Kommunikation über den vertrauenswürdigen Pfad einzuleiten.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

[VERFEINERUNG FÜR Benutzern: WAHLVORSTAND ALS … Benutzern]

FTP_TRP.1B.3 Die SERVERSEITIGE TSF muß den Gebrauch des vertrauenswürdigen Pfads für ***die Ausführung sämtlicher Operationen des Wahlvorstands*** erfordern.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

5.2 Anforderungen an die Vertrauenswürdigkeit des EVG

Die Anforderungen an die Vertrauenswürdigkeit, welche vom EVG erfüllt werden müssen, sind in Tabelle 4 aufgeführt. Sie enthalten die Komponenten der Vertrauenswürdigkeitsstufe EAL2 aus Teil 3 der Common Criteria. Die augmentierten Komponenten aus der Klasse ALC (Kennzeichnung mit **fetter** Schrift) entsprechen den Anforderungen der Vertrauenswürdigkeitsstufe EAL3.

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	**ALC_CMC.3 Authorisation controls**
	ALC_CMS.3 Implementation representation CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing

	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

Tabelle 4: Anforderungen an die Vertrauenswürdigkeit des EVG

5.3 Erklärung der Sicherheitsanforderungen

Die Erklärung der Sicherheitsanforderungen weist nach, daß die Menge der Sicherheitsanforderungen (EVG und Umgebung) geeignet ist, die Sicherheitsziele zu erfüllen, und auf die Sicherheitsziele zurückverfolgbar ist. Das Folgende wird nachgewiesen:

- Die Kombination aus den einzelnen Komponenten der funktionalen und Vertrauenswürdigkeitsanforderungen für den EVG und dessen IT-Umgebung zusammen erfüllt die dargelegten Sicherheitsziele.
- Die Menge der Sicherheitsanforderungen zusammen bildet ein sich gegenseitig unterstützendes und in sich konsistentes Ganzes.
- Die Auswahl der Sicherheitsanforderungen ist gerechtfertigt. Jede der folgenden Entscheidungen ist ausdrücklich gerechtfertigt:
- Wahl von Anforderungen, die nicht im Teil 2 bzw. 3 enthalten sind.
- Wahl von Anforderungen an die Vertrauenswürdigkeit, die keine EAL enthalten; und Nichterfüllung von Abhängigkeiten.

5.3.1 Erklärung der funktionalen Sicherheitsanforderungen an den EVG

Die Rückverfolgung der Sicherheitsanforderungen auf die Sicherheitsziele für den EVG ist in Tabelle 5 dargestellt. Die Eignung zur Abdeckung aller EVG-Sicherheitsziele wird im Folgenden nachgewiesen.

O.StimmberechtigterWähler Die SFP für Wahlhandlungen (Komponenten FDP_IFC.1A und FDP_IFF.1A) stellt sicher, daß nur Wähler mit Stimmberechtigung nach erfolgreicher Identifikation und Authentisierung (Komponenten FIA_UAU.1, FIA_UID.1 und FMT_SMR.2) eine Stimme abgeben können. Bei der Erreichung des Ziels werden diese Komponenten von FIA_USB.1A und FIA_ATD.1 durch Bindung der Sicherheitsattribute an den Wähler; von FTA_SSL.3, FTA_SSL.4 und FTA_TSE.1 durch Beschränkung der Eröffnung und Beendigung der Wahlhandlung; von FDP_IFF.5 durch Beseitigung unerwünschter Informationsflüsse; und von FDP_UCT.1A und FTP_TRP.1A durch Schutz der Vertraulichkeit bei der Kommunikation des Wählers mit dem serverseitigen EVG unterstützt.

O.Beweis Die Komponenten FDP_IFC.1A (Element 1e) und FDP_IFF.5 (Element 1a) stellen sicher, daß der EVG dem Wähler keine Daten zur Verfügung stellt, die der Wähler verwenden könnte, um seine Wahlentscheidung gegenüber Dritten zu beweisen.

O.IntegritätNachricht Die Komponente FDP_UIT.1A stellt in Verbindung mit der Komponente FTP_TRP.1A sicher, daß Identifikationsdaten, Authentisierungsnachrichten, Stimmzettel, Stimmdatensätze, Stimmzetteldaten und Rückmeldungen auf dem Übertragungsweg zwischen Wähler und serverseitigem EVG nicht unbemerkt verändert, gelöscht, hinzugefügt oder wiedereingespielt werden können.

O.IntegritätNachrichtWahlvorstand Die Komponente FDP_UIT.1B stellt in Verbindung mit der Komponente FTP_TRP.1B sicher, dass Identifikationsdaten und Authentisierungsnachrichten des Wahlvorstands sowie das Ergebnis auf dem Übertragungsweg zwischen Wahlvorstand und server-

seitigem EVG nicht unbemerkt verändert, gelöscht, hinzugefügt oder wiedereingespielt werden können.

O.IntegritätNachrichtServerServer Die Komponente FPT_ITT.1 stellt sicher, dass Wählertoken und Serverkommunikationsdaten auf dem Übertragungsweg zwischen zwei serverseitigen EVG Komponenten nicht unbemerkt verändert, gelöscht, hinzugefügt oder wiedereingespielt werden können.

O.AuthentizitätServer Durch die Komponente FTP_TRP.1A wird ein vertrauenswürdiger Pfad zwischen Wähler und serverseitigem EVG aufgebaut, der logisch von anderen Kommunikationspfaden getrennt ist und eine gesicherte gegenseitige Identifikation von Wähler und serverseitigem EVG bereitstellt. Für die Wahlhandlung kann der Wähler am Endgerät eine Kommunikation mit dem serverseitigen EVG über den vertrauenswürdigen Pfad einleiten.

O.AuthentizitätServerWahlvorstand Durch die Komponente FTP_TRP.1B wird ein vertrauenswürdiger Pfad zwischen Wahlvorstand und serverseitigem Wahlvorstandsinterface EVG aufgebaut, der logisch von anderen Kommunikationspfaden getrennt ist und eine gesicherte gegenseitige Identifikation von Wahlvorstand und serverseitigem Wahlvorstandsinterface EVG bereitstellt. Für die Ausführung sämtlicher Operationen kann der Wahlvorstand an seinem Endgerät eine Kommunikation mit dem serverseitigen Wahlvorstandsinterface EVG über den vertrauenswürdigen Pfad einleiten.

O.ArchivierungIntegrität Die Komponenten FDP_IFC.1B und FDP_IFF.1B [Regel5] stellen sicher, daß nach der Stimmauszählung mit Feststellung des Wahlergebnisses vom serverseitigen EVG ein Manipulationsschutz für die Wahldurchführungsdaten, das Wahlergebnis und [..] Protokollaufzeichnungen [..] erzeugt wird. Die Komponente FDP_DAU.1 gewährleistet, daß durch diesen Manipulationsschutz nachträgliche Fälschungen oder betrügerische Manipulationen der geschützten Daten außerhalb der Kontrolle des serverseitigen EVG und außerhalb des Wahlservers feststellbar sind.

O.ArchivierungWahlgeheimnis Die Komponente FPR_ANO.1 stellt sicher, daß nach Wahlende eine Zuordnung zwischen Wähler und seiner Stimme nicht mehr möglich ist. Durch die Verwendung der Komponente FPR_UNL.1B wird darüber hinaus sichergestellt, daß über die Reihenfolge und/oder den Zeitpunkt der Speicherung der Stimme in der Urne keine Zuordnung zwischen Wähler und Stimme möglich ist. Beides wird durch die Komponente FDP_RIP.1A unterstützt, die gewährleistet, daß keine zwischengespeicherten Stimmzettel erhalten bleiben, die das Wahlgeheimnis gefährden könnten.

O.Wahlgeheimnis Durch die Komponente FDP_UCT.1A wird in Verbindung mit der Komponente FTP_TRP.1A sichergestellt, daß Stimmdatensätze und somit die Stimme nicht im Klartext übertragen werden. Damit ist es nicht möglich, dem Wähler seine Stimme im Klartext zuzuordnen. Darüber hinaus stellt die Komponente FPR_UNL.1A sicher, daß auch über die Anzahl der Nachrichten oder die Größe der Stimmnachricht keine Rückschlüsse auf die Anzahl der Kreuze und/oder auf die ungültige Stimme gemacht werden können. Damit stellen beide Komponenten zusammen das Wahlgeheimnis auf dem Übertragungsweg sicher.

O.GeheimNachricht Der EVG stellt die Vertraulichkeit der Wählertoken, Identifikationsdaten und der Authentisierungsnachricht auf dem Übertragungsweg durch die Verwendung der Komponente FDP_UCT.1A in Verbindung mit der Komponente FTP_TRP.1A sicher.

O.GeheimNachrichtWahlvorstand Der EVG stellt die Vertraulichkeit der Identifikationsdaten und Authentisierungsnachrichten des Wahlvorstandes auf dem Übertragungsweg durch die Verwendung der Komponente FDP_UCT.1B in Verbindung mit der Komponente FTP_TRP.1B sicher.

O.GeheimNachrichtServerServer Der EVG stellt die Vertraulichkeit der Wählertoken auf dem Übertragungsweg durch die Verwendung der Komponente FPT_ITT.1 sicher.

O.Abbruch Die Komponente FTA_SSL.4 stellt sicher, daß der Wähler die Möglichkeit hat, seine Wahlhandlung bis zur Stimmabgabe zu beenden, ohne seine Stimmberechtigung zu verlieren.

O.WahlBeenden Die Komponenten FDP_IFC.1B und FDP_IFF.1B [Regel 3] stellt sicher, daß das Beenden der Wahldurchführung nicht versehentlich vor dem geplanten Wahlende-Zeitpunkt erlaubt ist. Die Komponente FDP_IFF.1B [Regel 6] ermöglicht, daß der Wahlvorstand das Beenden der Wahldurchführung explizit bestätigen kann.

O.Wahlende Die Komponente FTA_TSE.1 stellt sicher, daß Wahlhandlungen nur während der Wahldurchführung eröffnet werden können. Die Komponenten FDP_IFC.1A, FDP_IFF.1A und FDP_IFF.5 (Element 1d) gewährleisten, daß nach dem Beenden der Wahldurchführung keine Wahlhandlung eröffnet oder fortgeführt werden kann, denn die Ausführung der kontrollierten Operationen wird in diesem Fall explizit verweigert. Die Zeitspanne für das Beenden der Wahldurchführung bis zur Versiegelung der Urne gewährleistet, daß alle begonnenen Wahlhandlungen vor dem Ende der Wahldurchführung beendet werden können. Schließlich wird durch die Komponenten FPD_IFC.1B und FDP_IFF.1B der Wiederanlauf des EVG nur während der Wahldurchführung ermöglicht.

O.WahlgeheimnisWahlvorstand Die Komponente FPR_ANO.1 stellt das Wahlgeheimnis am Wahlserver während der Wahldurchführung inkl. Stimmauszählung sicher, da der Wahlvorstand keine Zusammenführung der Identität des Wählers mit der abgegebenen Stimme herstellen kann. Dies wird durch die Komponente FDP_RIP.1A unterstützt, die gewährleistet, daß keine zwischengespeicherten Stimmzettel erhalten bleiben, die das Wahlgeheimnis gefährden könnten.

O.IntegritätWahlvorstand Die Komponenten FDP_IFC.1A, FDP_IFF.1A und FDP_UIT.1A stellen in Verbindung mit den Komponenten FDP_IFC.1B, FDP_IFF.1B und FTP_TRP.1A sicher, daß Stimme nur von Wählern abgegeben und Stimmdatensätze nicht durch den Wahlvorstand verändert, gelöscht, hinzugefügt oder wiedereingespielt werden können. Insbesondere wird durch die Komponenten FPD_IFC.1B und FDP_IFF.1B sichergestellt, daß der Wahlvorstand den EVG nach dem Start der Wahldurchführung auch durch einen Wiederanlauf nicht in seinen Anfangszustand zurückversetzen kann.

O.Zwischenergebnis Die Komponenten FDP_IFC.1B und FDP_IFF.1B stellen sicher, daß der Wahlvorstand die Stimmauszählung nicht vor dem Ende der Wahldurchführung starten kann. Die Komponente FDP_UCT.1A in Verbindung mit der Komponente FTP_TRP.1A gewährleistet, daß während der Übertragung keine Stimmen preisgegeben werden und somit die Ermittlung von Zwischenergebnissen nicht möglich ist. Bei der Erreichung des Ziels werden diese Komponenten von FDP_IFF.5 durch Beseitigung unerwünschter Informationsflüsse unterstützt.

O.Übereilungsschutz Durch die Komponenten FDP_IFC.1A und FDP_IFF.1A [Regel 2] wird sichergestellt, daß der Wähler seine Stimmabgabe zunächst einleiten muß, dies aber noch keine Speicherung in der Urne bedeutet, sondern nur die Zwischenspeicherung zur erneuten Anzeige der Stimme verursacht. Der Wähler muß die Stimmabgabe explizit bestätigen (Komponente FDP_IFF.1A [Regel 4]). Damit ist klar, daß nur solche Stimmen in der Urne gespeichert werden, die vom Wähler ausdrücklich kontrolliert und bestätigt wurden.

O.Korrektur Durch die Komponenten FDP_IFC.1A und FDP_IFF.1A [Regel 2] wird sichergestellt, daß der Wähler seine Stimmabgabe zunächst einleiten muß, dies aber noch keine Speicherung in der Urne bedeutet, sondern nur die Zwischenspeicherung zur erneuten Anzeige der Stimme verursacht. Der Wähler hat noch die Möglichkeit, seine Stimme nach der erneuten Anzeige zu kor-

rigieren (Komponente FDP_IFF.1A) oder die Stimmabgabe sogar abzubrechen (Komponente FTA_SSL.4).

O.Rückmeldung Die Komponenten FDP_IFC.1A und FDP_IFF.1A [Regel 5] stellen sicher, daß der registrierte Wähler eine zutreffende Rückmeldung über die Erlaubnis bzw. Verweigerung und den Erfolg bzw. Misserfolg seiner Stimmabgabe erhält. Dem registrierten Wähler wird damit nach erfolgreicher Identifikation und Authentisierung (Komponente FDP_IFF.1A [Regel 1]) die Möglichkeit gegeben, zu prüfen, ob er bereits eine Stimme abgegeben hat. Dies bedeutet, daß ein Wähler mit Stimmberechtigung nach der Stimmabgabe (Komponente FDP_IFF.1A [Regel 4]) eine Meldung über deren Erfolg bzw. Misserfolg erhält. Ein Wähler ohne Stimmberechtigung erhält eine Meldung, daß er sein Stimmrecht bereits ausgeübt hat.

O.Störung Durch die Komponente FPT_TST.1 ist es dem Wahlvorstand beim Erstanlauf und auf Anforderung möglich, eine Testfolge als Nachweis für den korrekten Betrieb durchzuführen. Auf diese Weise ist sichergestellt, daß der Wahlvorstand Störungen am serverseitigen EVG erkennen kann. Hinweise auf solche Störungen werden dem Wahlvorstand durch die Komponente FDP_SDI.2 bereitgestellt. Durch die Komponenten FPT_RCV.1 und FPT_RCV.4 ist es dem Wahlvorstand möglich, nach einem Absturz / Herunterfahren des Systems oder einem Ausfall der Kommunikation oder der Speichermedien einen Wiederanlauf durchzuführen, der die Integrität der Wahldurchführungsdaten gewährleistet und insb. sicherstellt, daß kein Wähler mehr als eine Stimme abgeben kann oder seine Stimmberechtigung verliert ohne eine Stimme abgegeben zu haben.

O.Protokoll Die Komponente FAU_GEN.1 stellt sicher, daß mindestens die in Kapitel 1.3.3.8 aufgelisteten Ereignisse vom serverseitigen EVG protokolliert werden, und die Komponente FAU_SAR.1 gewährleistet, daß der Wahlvorstand die Protokollaufzeichnungen durchsehen kann.

O.OneVoterOneVote Durch die Komponenten FDP_IFC.1A und FDP_IFF.1A wird das Prinzip eingehalten, daß jeder Wähler nur eine Stimme abgeben kann. Das Speichern eines Stimmdatensatzes in der Urne ist untrennbar mit dem Vermerk der Stimmabgabe verbunden (Komponenten FDP_IFF.1A [Regel 4] und FPT_RCV.4). Zusammen mit der Überwachung der Speicherung (Komponente FDP_SDI.2) wird sichergestellt, daß ein registrierter Wähler seine Stimmberechtigung auch bei technischen Fehlern nicht verliert ohne eine Stimme abgegeben zu haben. Auch bei einem Abbruch durch den Wähler (Komponente FPT_SSL.4) oder einem technisch bedingten Abbruch wegen Zeitablauf (Komponente FPT_SSL.3) wird die Erhaltung der Stimmberechtigung sichergestellt. Außerdem stellt der serverseitige EVG sicher, daß bei einem Wiederanlauf der Wahldurchführung (Komponente FPT_RCV.1) kein Wähler seine Stimmberechtigung verliert oder mehr als eine Stimme abgeben kann.

O.AuthWahlvorstand Durch die Komponenten FIA_UAU.2, FIA_UID.2 und FMT_SMR.2 ist sichergestellt, daß der Wahlvorstand vor jeder anderen Aktion identifiziert und authentisiert wird. Die Komponenten FDP_IFC.1B und FDP_IFF.1B [Regel 7] gewährleisten eine Separation of Duty unter den Mitgliedern des Wahlvorstands für die Autorisierung der Operationen zum Starten, Wiederanlaufen und Beenden der Wahldurchführung sowie zum Starten der Stimmauszählung mit Feststellung des Wahlergebnisses. Die Autorisierung für diese kontrollierten Operationen erfolgt durch Wiederauthentisierung des Wahlvorstands (Komponente FIA_UAU.6) zusammen mit der Bindung der Anzahl der Autorisierungen an die Mitglieder des authentisierten Wahlvorstands (Komponenten FIA_ATD.1 und FIA_USB.1B).

O.StartStimmauszählung Die Komponenten FDP_IFC.1B und FDP_IFF.1B [Regel 4] ermöglicht das Starten der Stimmauszählung erst nach dem Beenden der Wahldurchführung (Komponente FDP_IFF.1B [Regel 3]).

O.Stimmauszählung Die Komponenten FDP_IFC.1B, FDP_IFF.1B [Regel 1] und FDP_RIP.1B stellen sicher, daß beim Start der Wahldurchführung keine Stimmdatensätze in der Urne gespei-

chert sind. Die Komponenten FDP_IFC.1B und FDP_IFF.1B [Regel 4] stellen sicher, daß in die Stimmauszählung mit Feststellung des Wahlergebnisses alle Stimmen, die nach Wahlende in der Urne gespeichert sind, eingehen.

	O.StimmberechtigterWähler	O.Beweis	O.IntegritätNachricht	O.AuthentizitätServer	O.ArchivierungIntegrität	O.ArchivierungWahlgeheimnis	O.Wahlgeheimnis	O.GeheimNachricht	O.Abbruch	O.WahlBeenden	O.Wahlende	O.WahlgeheimnisWahlvorstand	O.IntegritätWahlvorstand	O.Zwischenergebnis	O.Übereilungsschutz	O.Rückmeldung	O.Störung	O.Protokoll	O.OneVoterOneVote	O.Korrektur	O.AuthWahlvorstand	O.StartStimmauszählung	O.Stimmauszählung	O.Integrit-tNachrichtWahlvorstand	O.IntegritätNachrichtServerServer	O.AuthentizitätServerWahlvorstand	O.GeheimNachrichtWahlvorstand	O.GeheimNachrichtServerServer
FAU_GEN.1																		x										
FAU_SAR.1																		x										
FDP_DAU.1					x																							
FDP_IFC.1A	x	x									x		x		x	x			x	x								
FDP_IFF.1A	x										x		x		x	x			x	x								
FDP_IFC.1B					x					x	x		x	x							x	x	x					
FDP_IFF.1B					x					x	x		x	x							x	x	x					
FDP_IFF.5	x	x									x			x														
FDP_SDI.2																	x		x									
FDP_RIP.1A						x						x																
FDP_RIP.1B																							x					
FDP_UCT.1A	x						x	x						x														
FDP_UIT.1A			x										x															
FIA_ATD.1	x																				x							
FIA_UAU.1	x																											
FIA_UAU.2																					x							
FIA_UAU.6																					x							
FIA_UID.1	x																											
FIA_UID.2																					x							
FIA_USB.1A	x																											
FIA_USB.1B																					x							
FMT_SMR.2	x																				x							
FPR_ANO.1						x						x																
FPR_UNL.1A							x																					
FPR_UNL.1B						x																						
FPT_ITT.1																								x				x
FPT_RCV.1																	x		x									
FPT_RCV.4																	x		x									
FPT_TST.1																	x											
FTA_SSL.3	x																		x									
FTA_SSL.4	x								x										x	x								
FTA_TSE.1	x										x																	
FTP_TRP.1A	x		x	x			x	x					x	x														
FDP_UCT.1B																											x	
FDP_UIT.1B																								x				
FTP_TRP.1B																								x		x	x	

Tabelle 5: Abdeckung der Sicherheitsziele an den EVG

5.3.2 Gegenseitige Unterstützung der funktionalen Sicherheitsanforderungen an den EVG

Dieser Abschnitt beschreibt die gegenseitige Unterstützung und die interne Konsistenz der für diese Sicherheitsvorgaben ausgewählten Komponenten. Diese Eigenschaften werden sowohl für funktionale Komponenten als auch für Komponenten der Vertrauenswürdigkeit gezeigt.

Die funktionalen Komponenten wurden aus den vordefinierten CC Komponenten ausgewählt. Die Verwendung der Verfeinerungsoperationen erfüllen die CC Richtlinien.
Mehrfache Iteration von identischen oder hierarchischen Komponenten wurde verwendet um die geforderte Funktionalität an einen EVG, der mit dem Schutzprofil konform ist, im notwendigen Umfang zu verdeutlichen.
Alle Zuweisungs-, Auswahl- und Verfeinerungsoperationen innerhalb der ausgewählten Komponenten wurden unter Verwendung einer konsistenten Wahl- und Sicherheitsterminologie ausgeführt. Dies hilft die Mehrdeutigkeit durch andere Interpretationen der verwendeten Komponenten zu verhindern.

5.3.3 Rechtfertigung der Abhängigkeiten der funktionalen Sicherheitsanforderungen

Tabelle 6 zeigt die Auflösung der Abhängigkeiten der funktionalen Sicherheitsanforderungen. Aufgelöste Abhängigkeiten sind mit „Done“ gekennzeichnet. Falls es mehrere Möglichkeiten gibt, die Abhängigkeit aufzulösen, so ist angegeben, welche Variante gewählt wurde. Falls eine Abhängigkeit nicht aufgelöst wurde, ist dies in der Tabelle erklärt.

SFR	Abhängigkeiten	Auflösung
FAU_GEN.1	FPT_STM.1	kommt aus der IT-Umgebung (OE.Systemzeit)
FAU_SAR.1	FAU_GEN.1	Done
FDP_DAU.1	keine	
FDP_IFC.1	FDP_IFF.1	Done (jeweils für die Iterationen A und B)
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	Done (jeweils für die Iterationen A und B) Die Sicherheitsattribute werden innerhalb der Informationsflusskontrollpolitiken für die Steuerung verwendet. Eine Vorgabe für Standardwerte der Attribute ist nicht sinnvoll.
FDP_IFF.5	keine	
FDP_RIP.1	keine	(jeweils für die Iterationen A und B)
FDP_SDI.2	keine	
FDP_UCT.1A	FTP_ITC.1 oder FTP_TRP.1 FDP_ACC.1 oder FDP_IFC.1	FTP_TRP.1A FDP_IFC.1A
FDP_UCT.1B	FTP_ITC.1 oder FTP_TRP.1 FDP_ACC.1 oder FDP_IFC.1	FTP_TRP.1B FDP_IFC.1B
FDP_UIT.1A	FDP_ACC.1 oder FDP_IFC.1 FTP_ITC.1 oder FTP_TRP.1	FDP_IFC.1A FTP_TRP.1A
FDP_UIT.1B	FDP_ACC.1 oder FDP_IFC.1 FTP_ITC.1 oder FTP_TRP.1	FDP_IFC.1B FTP_TRP.1B
FIA_USB.1A	FIA_ATD.1	Done
FIA_USB.1B	FIA_ATD.1	Done
FIA_ATD.1	keine	
FIA_UAU.1	FIA_UID.1	Done
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UAU.6	keine	
FIA_UID.1	keine	

SFR	Abhängigkeiten	Auflösung
FIA_UID.2	keine	
FMT_SMR.2	FIA_UID.1	FIA_UID.1 (Wähler) bzw. FIA_UID.2 (Wahlvorstand)
FPR_ANO.1	keine	
FPR_UNL.1	keine	(jeweils für die Iterationen A und B)
FPT_ITT.1	keine	
FPT_RCV.1	AGD_OPE.1	Done
FPT_RCV.4	keine	
FPT_TST.1	keine	
FTA_SSL.3	keine	
FTA_SSL.4	keine	
FTA_TSE.1	keine	
FTP_TRP.1A	Keine	
FTP_TRP.1B	Keine	

Tabelle 6: Abhängigkeiten zwischen SFR für den EVG

5.3.4 Erklärung der Anforderungen an die Vertrauenswürdigkeit des EVG

Die ausgewählten Anforderungen an die Vertrauenswürdigkeit enthalten mit EAL 2 eine in Teil 3 der CC beschriebene Vertrauenswürdigkeitsstufe.
Es wird ein EVG für Online-Wahlen betrachtet, der definierte zentrale Anforderungen erfüllen muß. Die Erfüllung der in diesem Schutzprofil festgelegten Anforderungen reicht aus, um einige Arten von Vereinswahlen, Gremienwahlen, etwa in den Hochschulen, im Bildungs- und Forschungsbereich, und insbesondere auch nicht-politische Wahlen mit geringem Angriffspotential sicher auszuführen. Es besteht eine hohe Abhängigkeit zur definierten Einsatzumgebung, die als vertrauenswürdig angenommen wird. Vor diesem Hintergrund ist die gewählte Vertrauenswürdigkeitsstufe EAL 2 als angemessen zu betrachten.
Die gewählte Augmentierung mit den zur Vertrauenswürdigkeitsstufe EAL 3 gehörenden Komponenten der Klasse ALC gewährleistet einen gegenüber EAL 2 verbesserten Schutz der Darstellung der Implementierung vor unkontrollierter Manipulation. Dies ermöglicht bei Bedarf die unabhängige Untersuchung und Bewertung der Implementierung des EVG durch bestallte und ggf. öffentlich kontrollierte Experten.

6 EVG Übersichtsspezifikation

Nachfolgend ist dargelegt, wie der EVG die funktionalen Anforderungen aus Abs. 5.1 erfüllt.

FAU_GEN.1

Der EVG protokolliert pro Teilsystem die in FAU_GEN.1 aufgeführten Ereignisse in einer jeweils separaten Logdatei: Das Starten der Protokollfunktion erfolgt mit dem Starten des Wahlvorstandsinterface EVG. Das Starten der Protokollierung wird ebenfalls protokolliert. Das Ereignis „Beenden der Protokollierungsfunktionen“ tritt nicht ein, weil die Protokollierung dauerhaft aktiv ist.

Der EVG protokolliert folgende Ereignisse:

- Erfolgreiche Identifikation und Authentisierung des Wahlvorstands
- Starten und Wiederanlaufen und Beenden der Wahldurchführung
- Starten der Stimmauszählung mit Feststellung des Wahlergebnisses
- Durchführung und Resultate jedes Selbsttests
- Festgestellte Störungen bei der Verwendung unterstützender Mechanismen der IT-Umgebung, die die Betriebsfähigkeit der serverseitigen EVG beeinträchtigen

Für diese Ereignisse werden

- Datum und Uhrzeit,
- Art des Ereignisses (siehe oben) sowie
- das Ergebnis (Erfolg ggf. inkl. Ergebnis oder Misserfolg inkl. Fehlermeldung)

protokolliert.

Die Protokollierung erfolgt auf jedem der vier Komponenten des serverseitigen EVG, so dass damit angegeben wird, auf welcher Komponente sich ein Ereignis ergeben hat. Dabei wird die Identität des Wählers nicht protokolliert. Im Wahlvorstandsinterface können diese Protokolldateien vom Wahlvorstand in verständlicher und lesbarer Form eingesehen werden.

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 ein Manipulationsschutz erzeugt, vgl. Ausführungen in Abs. 1.4.9.

Wie im Glossar erläutert, wird die Archivprüfsumme wie folgt realisiert: „Archivprüfsumme: Eine Prüfsumme, die unmittelbar nach Erstellung des Wahlarchivs, welches die Protokolldateien der EVGs, ein Abbild der Datenbank sowie das Wahlergebnis enthält, im Anschluss an das Wahlende über dieses Wahlarchiv gebildet wird, um anschließende Manipulation des Archivs zu verhindern.“

Die Archivprüfsumme wird auf dem Wahlvorstandsinterface-Server abgelegt und kann dort vom Wahlvorstand entnommen werden, so dass der Wahlvorstand „mit der Fähigkeit zur Verifizierung“ feststellen kann, ob der Inhalt nachträglich verändert wurde.

FDP_IFC.1A

Diese funktionale Anforderung wird durch den in Abs. 1.4 beschriebenen Ablauf zur Wahlhandlung realisiert: Die TSF realisieren die Wahlhandlung so, dass die funktionalen Anforderungen umgesetzt werden. Insb. wird durch den Ablauf sichergestellt,

- dass die kontrollierten Operationen nur während der Wahldurchführung ausgeführt werden können,
- dass nur während der Wahldurchführung Stimmdatensätze in der Urne gespeichert werden können,
- dass nur registrierte Wähler eine Stimme abgeben können,
- dass jeder Wähler nur einmal eine Stimme abgeben kann,
- dass kein Informationsfluss dem Wähler Informationen zur Verfügung stellen kann, die ihm die Möglichkeit geben würden, seine Wahlentscheidung gegenüber anderen zu beweisen
- dass kein Informationsfluss zwischen dem Wähler und dem Inhalt der Urne dazu führen kann, dass gespeicherte Stimmdatensätze verändert oder gelöscht werden,
- dass kein Informationsfluss zwischen dem Wähler und dem Inhalt der Urne dazu führen kann, dass direkt, d.h. durch Stimmauszählung, oder indirekt, d.h. durch Preisgabe des Inhalts gespeicherter Stimmdatensätze, Zwischenergebnisse ermittelt werden können.

FDP_IFF.1A

Diese funktionale Anforderung wird durch den in Abs. 1.4 beschriebenen Ablauf zur Wahlhandlung realisiert. Dabei werden die Attribute wie folgt realisiert:

Stimmberechtigungsattribut wird vom EVG implizit realisiert:

- „unbekannt“ vor der Prüfung, ob ein Wähler bereits gewählt hat
- „mit“ nach Prüfung und Feststellung, dass ein Wähler noch nicht gewählt hat,
- „ohne“ nach Prüfung und Feststellung, dass ein Wähler bereits gewählt hat.

Das Wahlhandlungsattribut wird vom EVG dadurch dargestellt,

- dass der Wert „nach“ erreicht wird, sobald eine Stimme im System hinterlegt, aber noch nicht in der Urne gespeichert ist.
- Ansonsten liegt der Wert „vor“ vor.

Der Wahlzeitraum wird intern darüber dargestellt, ob die Systeme gestartet oder bereits gestoppt sind:

- „Vorbereitung“ für noch nicht gestartete / freigeschaltete und noch nicht gestoppte Systeme,
- „Durchführung“ für bereits gestartete und noch nicht gestoppte Systeme,
- „Auszählung“ für gestartete und bereits wieder gestoppte Systeme.

Die Regeln dieser SFR werden dabei durch die TSF wie folgt umgesetzt:

Regel 1: Der Wähler muss sich mit PIN/TAN anmelden. Nur wenn diese Identifikation und Authentisierung erfolgreich verlief, wechselt der Wert von „unbekannt“ auf „mit“ bzw. „ohne“ – je nachdem, ob das Stimmabgabevermerk den Wähler dahingehend kennzeichnet, dass dieser bereits gewählt hat. .

Regel 2: Das Wahlhandlungsattribut ist zunächst auf zunächst auf „vor“ gesetzt und wechselt auf den Wert „nach“ nach Einleitung der Stimmabgabe, aber noch vor der verbindlichen Bestätigung der Stimmabgabe.

Regel 3: Der Wähler kann im beschriebenen Ablauf seine Stimmabgabe widerrufen; das Wahlhandlungsattribut wird in diesem Fall auf den Wert „vor“ gesetzt.

Regel 4: Eine verbindliche Stimmabgabe ist möglich, wenn das Stimmberechtigungsattribut den Wert „mit“ enthält (der Wähler als angemeldet ist und noch nicht gewählt hat) und das Wahlhandlungsattribut den Wert „nach“ besitzt (d.h. seine Stimme im System hinterlegt, aber noch nicht gespeichert ist). Dabei wird durch den beschriebenen Ablauf in einer untrennbaren Aktion die Stimme in der Urne gespeichert (das Stimmberechtigungsattribut also auf den Wert „ohne“ gesetzt), sonst verbleibt es auf dem Wert „mit“.

Regel 5: Der Wähler erhält entsprechende Rückmeldungen angezeigt.

Insbesondere werden die genannten Aktionen zur Identifikation/Authentisierung, Einleitung und Widerruf der Stimmabgabe sowie endgültige Stimmabgabe verweigert, wenn das System noch nicht gestartet oder nach Start wieder gestoppt ist, da hierzu die Schlüssel der Teilsysteme zur sicheren Kommunikation benötigt werden, welche vor dem Start sowie nach dem Stopp den Systemen noch nicht bzw. nicht mehr zur Verfügung stehen.

FDP_IFC.1B

Diese funktionale Anforderung wird durch den in Abs. 1.4 beschriebenen Ablauf bzgl. der Aktivitäten des Wahlvorstands realisiert – insb. durch Separation of Duty

Durch den implementierten Ablauf ist sichergestellt,

- dass kein Informationsfluss zwischen dem Wahlvorstand und dem Inhalt der Urne dazu führen kann, dass Stimmdatensätze gespeichert oder gespeicherte Stimmdatensätze verändert oder gelöscht werden,
- dass kein Informationsfluss zwischen dem Wahlvorstand und dem Inhalt der Urne dazu führen kann, dass direkt, d.h. durch Stimmauszählung, oder indirekt, d.h. durch Preisgabe des Inhalts gespeicherter Stimmdatensätze, Zwischenergebnisse ermittelt werden

Auf den Inhalt der Urne wird ausschließlich lesend zugegriffen und es werden dem Wahlvorstand ausschließlich die Anzahl der bereits eingegangenen Stimmen sowie die Übereinstimmung bzw. Nichtübereinstimmung der Prüfsummenkette von Wählerverzeichnis und Urne als Information angezeigt.

Die TSF berücksichtigen bei der Auszählung,

- dass für die Stimmauszählung alle abgegebenen Stimmen, d.h. alle in der Urne gespeicherten Stimmdatensätze berücksichtigt werden.

Die TSF berücksichtigen nach der Auszählung,

- dass nach der Stimmenauszählung mit Feststellung des Wahlergebnisses für die Wahldurchführungsdaten, das Wahlergebnis und die Protokollaufzeichnungen ein Manipulationsschutz als Gültigkeitsgarantie erzeugt wird.

FDP_IFF.1B

Diese funktionale Anforderung wird durch den in Abs. 1.4 beschriebenen Ablauf bzgl. der Aktivitäten des Wahlvorstands realisiert.

Die Sicherheitsattribute werden dabei wie folgt realisiert: Der Wahlzeitraum wird intern darüber dargestellt, ob die Systeme gestartet oder bereits gestoppt sind:

- „Vorbereitung“ für noch nicht gestartete Systeme und noch nicht gestoppte Systeme,
- „Durchführung“ für bereits gestartete Systeme und noch nicht gestoppte Systeme,
- „Auszählung“ für gestartete Systeme und bereits gestoppte Systeme.

Die Anzahl der Autorisierungen für die angeforderte Operation wird durch einen Zähler realisiert.

Insb. die in dieser SFR genannten Regeln werden umgesetzt, wobei dazu der Status der Systeme bzgl. Starten und Stoppen berücksichtigt wird, vgl. zusätzlich Ausführungen zur Realisierung von FDP_DAU.1. FDP_IFF.1B.5 wird dabei insb. durch die Separation of Duty umgesetzt. Ein Wiederanlauf ist für bereits gestartete, aber noch nicht gestoppte Systeme – also Wahlzeitraum mit Attribut „Durchführung“ möglich.

In der Konfiguration kann der Wahlendezeitpunkt hinterlegt werden. Wird die Aktion Wahlstopp zeitlich vor dem konfigurierten Wahlendezeitpunkt ausgelöst, erscheint ein Warnhinweis. Dennoch ist durch ein explizites Bestätigen des Wahlvorstandes ein Wahlstopp möglich.

FDP_IFF.5

Diese funktionale Anforderung wird durch den in Abs. 1.4 beschriebenen Ablauf zur Wahlhandlung und bzgl. der Aktivitäten des Wahlvorstands realisiert. Die TSF realisieren dabei insb.

- dass dem Wähler keine Quittung oder andere Daten zur Verfügung gestellt werden, mit deren Hilfe der Wähler seine Wahlentscheidung beweisen könnte (Insbesondere enthält die Rückmeldung über die erfolgreiche Stimmabgabe keinen solchen Beweis),
- dass kein Informationsfluss zwischen dem Wahlvorstand und dem Inhalt der Urne dazu führen kann, dass Stimmdatensätze gespeichert werden; Auf den Inhalt der Urne wird vom Wahlvorstandsinterface ausschließlich lesend zugegriffen und es werden dem Wahlvorstand ausschließlich die Anzahl der bereits eingegangenen Stimmen sowie die Übereinstimmung bzw. Nichtübereinstimmung der Prüfsummenkette von Wählerverzeichnis und Urne als Information angezeigt.
- dass kein Informationsfluss zwischen dem Wähler oder dem Wahlvorstand und dem Inhalt der Urne dazu führen kann, dass gespeicherte Stimmdatensätze verändert oder gelöscht werden; siehe Erläuterung im vorherigen Punkt; Es besteht für den Wähler keinerlei Möglichkeit manipulativ auf den Inhalt der Urne zu wirken außer der Veränderung bzw. Abgabe seiner eigenen Stimme.
- dass kein Informationsfluss zwischen dem Wähler oder dem Wahlvorstand und dem Inhalt der Urne dazu führen kann, dass direkt, d.h. durch Stimmauszählung, oder indirekt, d.h. durch Preisgabe des Inhalts gespeicherter Stimmdatensätze, Zwischenergebnisse ermittelt werden. Siehe Erläuterung in den vorherigen Punkten.

Darüber hinaus wird realisiert,

- dass die Eröffnung einer Wahlhandlung durch den Wähler darf bereits während der Ausführung der Operation zum Beenden der Wahldurchführung nicht mehr möglich sein.
- Dabei wird durch die Reihenfolge und den Zeitabstand der Deaktivierung der Systeme sichergestellt, dass ein Abschluss der Wahlhandlung für bereits angemeldete Wähler noch möglich ist. Der Zeitabstand ist eine durch den Wahlvorstand vorgegebene Zeit.

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 end-

gültigen 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 FDP_UIT.1B

Der EVG stellt sicher, dass eine Kommunikation nur mittels https mit TLS-Zertifikaten 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.

Die Anzahl der Autorisierungen für die angeforderte Operation wird durch einen Zähler realisiert, der bei Null beginnt.

FIA_UAU.1 und FIA_UAU.2 sowie FIA_UID.1 und FIA_UID.2

Diese funktionale Anforderung wird durch den in Abs. 1.4 beschriebenen 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 in Abs. 1.4 beschriebenen Ablauf zur Wahlhandlung realisiert, insofern als dass bei Eröffnung der Wahlhandlung das Stimmberechtigungsattribut den Wert „unbekannt“ und das Wahlhandlungsattribut den Wert „vor“ erhält, vgl. auch. Ausführungen in FDP_IFF.1A.

FIA_USB.1A.3 wird durch den in Abs. 1.4 beschriebenen Ablauf zur Wahlhandlung implizit realisiert, da eine Änderung der Attribute nicht vorgesehen ist.

FIA_USB.1B

Diese funktionale Anforderung wird durch den in Abs. 1.4 beschriebenen 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, vgl. dazu Ausführungen in Abs. 1.4.

Die Rollen Wähler und Wahlvorstand sind von den Funktionen her strikt getrennt, so dass es keine Verknüpfung gibt. Theoretisch könnte ein Benutzer als Wahlvorstand mit Benutzername/Passwort angemeldet sein und trotzdem als Wähler eine Wahlhandlung – identi-

fiziert und authentisiert mit PIN/TAN – durchführen. Gleichwohl ist zu beachten, dass die Trennung per se durch die getrennten Systeme gegeben ist.

FPR_ANO.1

Diese funktionale Anforderung wird durch den in Abs. 1.4 beschriebenen 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. Eine Verknüpfung zwischen Wähler und Stimme wird ausschließlich während der Wahlhandlung über ein temporäres, verschlüsseltes Wählertoken hergestellt, dieses liegt auf beiden Systemen mit dem jeweiligen öffentlichen Schlüssel des System verschlüsselt in der Datenbank. Damit wird eine Zuordnung zwischen Wähler und nicht ausgefülltem Stimmzettel während des Wahlvorgangs erschwert.

Es werden Standardverfahren (SHA256, RSA, Java-SecureRandom) zur Verschlüsselung verwendet. Sollten sich die eingesetzten Verfahren nicht als robust über den Geheimhaltungszeitraum hinaus erweisen, so ist eine Anonymität der Stimmen jedoch weiterhin gewährleistet: ein nachträglicher Abgleich zwischen Wahlberechtigungsliste (Wählerverzeichnis) und Urne ist nicht möglich, da das Wählertoken, dass eine Stimme einem Wähler zuordnet, nur während der Wahlhandlung existiert. Auch bei der Auszählung und Herausgabe des Wählerverzeichnisses und der Auszählung nach Wahlende kann die Anonymität nicht aufgehoben werden, da eine nachträgliche Zuordnung aufgrund des nicht mehr existenten Wählertokens nicht mehr möglich ist. In der Urne besteht keine Beziehung mehr zur Identität des Wählers. Ein Abgleich beider Datenbanken auch zum Zeitpunkt der Wahlhandlung eines Wählers gibt über das Wählertoken die Anonymität aufgrund der Verschlüsselung des Wählertokens nicht preis.

Dass frühere Informationen nicht mehr verfügbar sind, ist aufgrund der Wahlrechtsgrundsätze bei der Realisierung des EVG umfangreich beachtet worden. Dazu ist aufgrund des Designs der verteilten Komponenten und des Protokolls zwischen den Komponenten sichergestellt, dass kein Bezug zwischen Wähler und abgegebener Stimme möglich ist. Wählertoken, die einen Wähler und eine Stimme temporär verknüpfen, werden nach der Stimmabgabe durch Überschreiben mit einem Zufallswert aktiv gelöscht.

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. Dies ist auch dann der Fall, wenn die Stimme ungültig abgegeben wird. Die verwendete Datenstruktur hat eine nur in Intervallen variable Größe, wodurch sichergestellt wird, dass eine Zuordnung der Länge der übertragenen Datensätze zum Inhalt der abgegebenen Stimme nicht möglich ist.

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. Darüber hinaus werden die Wählertoken mit Zufallswerten überschrieben und in 30-Blöcken zusammengefasst; die Reihenfolge innerhalb der 30-Blöcke wird nach den Zufallswerten geordnet, so dass die Reihenfolge zufällig ist. Nach der Feststellung des Wahlergebnisses liegen die Stimmen in der Datenbank der Urne nach einem zufälligen Key sortiert vor.

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 der Erhaltungsmodus wie folgt realisiert:

- Der gespeicherte Zähler für die Anzahl der Autorisierungen wird auf 0 zurückgesetzt.
- Der Zustand des Systems verbleibt auf bereits gestartet, aber noch nicht gestoppt.
- Durch die Realisierung der Wahlhandlung als atomare Aktion wird über die gespeicherten Informationen sichergestellt, dass der Status des Wählers erhalten bleibt.

FPT_TST.1

Beim Wahlstart laufen die Selbsttests automatisch ab. Das Ergebnis der Selbsttests ist im Wahlvorstandsinterface einsehbar.

Die Selbsttests nutzen die Blockprüfsummen für die Datenintegritätsprüfungen, vgl. Ausführungen in Abs. 1.4.8.

Über die vom EVG erzwungene TLS-gesicherte Verbindung kann der Wahlvorstand überprüfen, ob er mit dem richtigen EVG kommuniziert.

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. Der Stimmabgabevermerk des Wählers ist hiervon unberührt und bleibt unverändert erhalten und zugeteilter Zwischenspeicher wird automatisch freigegeben. Die atomare Transaktion bei der Abgabe der Stimme garantiert zudem, dass die Erhaltung des Stimmabgabevermerks auch für den Fall eines Abbruchs im Prozess der endgültigen Stimmabgabe sichergestellt ist.

FTA_SSL.4

Diese funktionale Anforderung wird durch den in Abs. 1.4 beschriebenen 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.

Der Stimmabgabevermerk bleibt hierbei unverändert, und der Zwischenspeicher wird gelöscht.

FTA_TSE.1.

Diese funktionale Anforderung wird durch den in Abs. 1.4 beschriebenen 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.

Anhang A Verantwortung der Wahlveranstalter

a. Alternative Wahlform

Der Wahlveranstalter soll eine alternative Wahlform anbieten, solange die Online-Wahl nicht universell zugänglich ist. Wenn parallel zur Online-Wahl auch herkömmliche Wahlformen (Wahl im Wahllokal und/oder Briefwahl) angeboten werden, liegt es in der Verantwortung des Wahlveranstalters sicher zu stellen, dass Wähler nicht über unterschiedliche Wahlformen eine Stimme abgeben können. Dies kann beispielsweise dadurch geschehen, daß die Online-Wahldurchführung vor der Öffnung des Wahllokals liegt.

b. Festlegung der Fristen

Es liegt in der Verantwortung des Wahlveranstalters, eindeutige Zeitpläne für alle drei Wahlphasen vorzugeben. Der Wahlveranstalter ist insbesondere für die Festlegung des Wahlende-Zeitpunktes der Phase Wahldurchführung verantwortlich. Dabei sollen die Fristen rechtzeitig vor dem Start der Wahldurchführung öffentlich bekannt gegeben werden.
Die Anmeldung eines Wählers am EVG darf nach dem Ende der Wahldurchführung nicht mehr möglich sein. Die Annahme von Stimmen zur Speicherung sollte erst später abgeschaltet werden, damit Wähler, die sich kurz vor Ende der Wahldurchführung noch angemeldet haben, ihre Stimmabgabe noch beenden können. Die Zeitspanne für das Beenden der Wahldurchführung bis zur Versiegelung der Urne muss angemessen definiert werden, damit alle begonnenen Wahlhandlungen beendet werden können. Die benötigte Genauigkeit der Systemzeit wird vom Wahlveranstalter festgelegt.

c. Zugriffsrechte

Bei der Bestimmung des Wahlvorstandes ist vom Wahlveranstalter zu beachten, dass Personen nicht alleine Zugang und Zugriff zum serverseitigen EVG gewährleistet wird, sondern Personen unterschiedlicher Interessengemeinschaften[1] sich gegenseitig kontrollieren. [...][2]
Der Wahlveranstalter soll dafür sorgen, dass über sämtliche Zugriffe auf den serverseitigen EVG oder den Wahlserver sowie der daran beteiligten Personen, Buch geführt wird.
Dem Wahlveranstalter wird empfohlen, Daten nur während der Phase Wahlvorbereitung zu verändern und während der Wahldurchführung keine Änderungen an der Wahlberechtigungsliste und dem Stimmzettel zuzulassen.
Bevor die Stimmen ausgezählt werden, soll der Wahlveranstalter die Anzahl der abgegebenen Stimmen ermitteln. Falls die Anzahl so gering ist, daß das Wahlgeheimnis gefährdet ist, entscheidet der Wahlveranstalter, ob eine Auszählung vorgenommen werden darf.

d. Wahlbeobachtung

Die Wahlveranstalter sollten definieren, inwieweit Beobachter die Handlungen des Wahlvorstandes (wie Initialisierung, Starten und Beenden der Wahldurchführung sowie Ergebnisberechnung) beobachten und kommentieren können.
Im vorliegenden Schutzprofil ist eine Wahlbeobachtung speziell für die Online-Wahl während der Wahldurchführung inkl. der Stimmauszählung nicht vorgesehen. Dennoch wird empfohlen, Wahlbeob-

1 Die Formulierung „Personen aus unterschiedlichen Interessensgemeinschaften“ stammt aus dem traditionellen Wahlumfeld. Hier kontrollieren sich auch immer mindestens zwei Personen unterschiedlicher Parteiangehörigkeit und damit Interessensgruppen, beispielsweise im Wahllokal oder bei der Separierung und der Auszählung der Briefwahlstimmen.

2 Entfernt, da der EVG die Separation of Duty durchsetzt

achter unabhängig vom Wahlvorstand zu definieren und den entsprechenden Personen nach der Wahldurchführung und der Stimmauszählung Zugriff zu den Protokolldateien zu geben.

e. Identifikation und Authentisierung

Der Wahlveranstalter entscheidet, welches Wähleridentifikationsmerkmal verwendet und wie Technik zur Authentisierung der Wähler auf sichere Weise eingesetzt wird. Hier können beispielsweise Transaktionsnummern (TAN), wählerbezogene Credentials (im Unterschied zu der üblichen Auffassung von TANs kann man die Credentials ggf. für mehrere Wahlen verwenden) oder digitale Zertifikate zum Einsatz kommen. Die eingesetzten Authentisierungsmerkmale sollten dem Wahlwert entsprechend sicher festgelegt werden und dem anerkannten Stand der Technik entsprechen.
Falls Identifikationsdaten oder Authentisierungsmerkmale an die Wähler verteilt werden müssen, so liegt es in der Verantwortung des Wahlveranstalters diese rechtzeitig bereit zu stellen. Die Verteilung muß dabei authentisch und integer sowie ggf. auch vertraulich erfolgen.
Es liegt in der Verantwortlichkeit des Wahlveranstalters die Wähler zu informieren, wie sie mit ihren Identifikations- und Authentisierungsmerkmalen umgehen sollen.
Es liegt in der Verantwortung des Wahlveranstalters, dass der Wähler die in der Wahlberechtigungsliste enthaltenen Einträge überprüfen und ggf. Berichtigung verlangen kann.

f. Wählervertrauen

Der Wahlveranstalter soll Schritte unternehmen, um sicherzustellen, dass die Wähler das verwendete Online-Wahlsystem verstehen und darin Vertrauen haben. Daher sollten Informationen über die Funktionsweise des Systems öffentlich zugänglich gemacht werden. Es wird daher empfohlen, die Wähler in klaren und einfachen Worten über die Art und Weise der elektronischen Stimmabgabe zu informieren.
In diesem Zusammenhang hat der Wahlveranstalter zu entscheiden, ob das Wahlsystem oder eine identische Kopie außerhalb der eigentlichen Wahl für interessierte Personen zum Kennen lernen und Testen zur Verfügung steht.
Der Wahlveranstalter soll darauf hinweisen, daß es sich bei der elektronischen Stimmabgabe um eine echte Stimmabgabe bei der Wahl und nicht um einen Test handelt.
Der Wahlveranstalter ist dafür verantwortlich, dem Wähler angemessene Hinweise für die unbeobachtete Stimmabgabe zu geben.
Der Wahlveranstalter teilt den Wählern mit, wie sie sich verhalten sollen, wenn sie keine Rückmeldung über die Speicherung ihrer Stimme erhalten oder andere unklare Zustände erreichen.
Der Wahlveranstalter soll die Online-Wahl so gestalten, daß die Registrierung zur Teilnahme kein Hindernis für den Wähler darstellt.
Vor dem Einsatz des Online-Wahlsystems wird eine Veröffentlichung der Darstellung der Implementierung zumindest einer Fachöffentlichkeit empfohlen.

g. Verfügbarkeit

In der Verantwortung des Wahlveranstalters liegt die Wahl des Kommunikationsnetzes. Eine hohe Verfügbarkeit des ausgewählten Netzwerkes sollte sich in einer dem Online-Wahlverfahren vergleichbaren Praxis bestätigt haben. Die erforderliche Qualität des Netzes hängt auch von der definierten Dauer für die Wahldurchführung ab.
Die erforderliche Servicequalität des Netzwerks und des Wahlservers hängt vom vorgegebenen Zeitraum für die Wahldurchführung ab. Der Wahlveranstalter sorgt dafür, daß die Verfügbarkeit des Wahlservers und seiner Netzwerkanbindung bei Störungen und Ausfällen mit angemessenem Service Level wiederhergestellt wird.
Der Wahlveranstalter legt fest, wie der Wahlvorstand das Netzwerk und den Wahlserver überwacht und Störungen oder Ausfälle feststellt, und mit welchen Maßnahmen der Wahlvorstand den Störungen oder Ausfällen begegnen soll. Für Probleme mit der Robustheit, Servicequalität und Verfügbarkeit des

Netzwerks oder des Wahlservers, die nicht in angemessener Zeit behoben werden können, definiert der Wahlveranstalter geeignete Notfallszenarien. Zu den Notfallszenarien kann beispielsweise ein Rollback zur reinen Papierwahl gehören.
Der Wahlveranstalter soll dafür sorgen, daß er vom Wahlvorstand über sämtliche Störungen und Ausfälle informiert wird.

h. Stimmzettel

Der Wahlveranstalter legt die Darstellung des Stimmzettels sowie die Abbildungsmöglichkeit der (absichtlich) ungültigen Stimmabgabe auf den Endgeräten fest. Dabei ist darauf zu achten, daß die Wahlrechtsgrundsätze (insbesondere die Forderung nach einer gleichen Wahl) eingehalten werden und beispielsweise keine Wahlvorschläge durch die Anordnung auf dem elektronischen Stimmzettel benachteiligt werden („Chancengleichheit“).
Es liegt in der Verantwortung der Wahlveranstalter zu entscheiden, ob der Wähler darauf hingewiesen wird, daß er dabei ist, eine ungültige Stimme abzugeben.
Es liegt in der Verantwortung der Wahlveranstalter zu entscheiden, inwieweit das Online-Wahlsystem behinderte Menschen bei ihrer Stimmabgabe unterstützen können soll.

i. Sonstiges

Es sollten Handlungsszenarios existieren für den Fall, daß eine Inkonsistenz bei der Einspeicherung der Stimmen erkannt wird und für den Fall, daß eine Differenz zwischen der Anzahl der Stimmen in der Urne und der Anzahl der Wähler, die laut Wahlberechtigungsliste ihre Stimme abgegeben haben, besteht.
Es liegt in der Verantwortung des Wahlveranstalters, ob öffentliche Wahlkioske als geschützte Endgeräte eingesetzt werden, um Wählern, die kein eigenes Endgerät besitzen oder die der Sicherheit ihres eigenen Endgeräts misstrauen, die Online-Wahl zu ermöglichen.
Die Art und Weise der Archivierung sowie deren Dauer wird vom Wahlveranstalter festgelegt. Die Bereinigung (Deinstallation, Löschen von Daten) des serverseitigen EVG liegt in der Verantwortung des Wahlveranstalters.
Die Veröffentlichung der Wahlergebnisse liegt im Verantwortungsbereich der Wahlveranstalter.

Anhang B Literatur

[1]Council of Europe (2004): Legal, operational and technical standards for e-voting. Recommundation Rec(2004)11 and explanatory memorandum, Council of Europe, Strassbourg, S. 87.

[2]Gesellschaft für Informatik (GI, 2005): GI-Anforderungen an Internetbasierte Vereinswahlen („GI requirements for Internet based elections in non-governmental organisations“). 4. August 2005. www.gi-ev.de/fileadmin/redaktion/Wahlen/GI-Anforderungen_Vereinswahlen.pdf [9.2.2006]

[3]V. Hartmann, N. Meißner, D. Richter (2004): Online Voting Systems for Non-parliamentary Elections: Catalogue of Requirements, Berlin: PTB Bericht 8.5-2004-1, 54

[4]Melanie Volkamer: Diplomarbeit “Elektronisches Wahlsystem – SecVote: Entwicklung und prototypische Realisierung eines Wahlprotokolls für die Durchführung von Personalratswahlen”

[5]Melanie Volkamer, Robert Krimmer: Overview Online-Wahlen, in D*A*CH Sicherheit

[6]Melanie Volkamer, Robert Krimmer: Die Online-Wahl auf dem Weg zum Durchbruch, in Informatikspektrum April 2006

[7]Melanie Volkamer, Roland Vogt: Common Criteria Schutzprofil für Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte, Version 1.0, 18.04.2008

Anhang C Glossar und Abkürzungen

Tabelle 1 Abkürzungen

Begriff	Definition
CC	Common Criteria for Information Technology Security Evaluation (Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik)
EAL	Evaluation Assurance Level
EVG	Evaluationsgegenstand (=TOE)
IT	Information Technology
JAR	Java-Archiv
PP	Protection Profile / Schutzprofil
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
ST	Security Target / Sicherheitsvorgaben
TOE	Target of Evaluation (=EVG)
TSF	TOE Security Function
TSP	TOE Security Policy
WAR	Web-Archiv

Abgegebene Stimme Eine Stimme gilt als abgegeben, wenn sie in der Urne fehlerfrei und unumkehrbar gespeichert ist.

Archivprüfsumme Eine Prüfsumme, die unmittelbar nach Erstellung des Wahlarchivs, welches die Protokolldateien der EVGs, ein Abbild der Datenbank sowie das Wahlergebnis enthält, im Anschluss an das Wahlende über dieses Wahlarchiv gebildet wird, um anschließende Manipulation des Archivs zu verhindern.

Authentisierungsdaten Daten, gegen die geprüft wird, ob die angebliche Identität des Wählers/Wahlvorstandes echt ist. Dies erfolgt mittels einer Einweg-Hash-Funktion entweder von der TAN zu der PIN des registrierten Wählers oder von dem Passwort zu dem Benutzername des Wahlvorstandes. Die Daten können in der Wahlberechtigungsliste oder an anderer Stelle gespeichert sein.

Authentisierungsmerkmal Merkmal, das jeder registrierte Wähler/Wahlvorstand besitzt, um sich am EVG zu authentisieren. Dies ist die PIN/TAN Kombination für Wähler bzw. Benutzername /Passwort für den Wahlvorstand.

Authentisierungsnachricht Bei der Authentisierung wird zwischen dem Authentisierungsmerkmal, den Authentisierungsdaten und der Authentisierungsnachricht, die der Wähler/Wahlvorstand an den serverseitigen EVG schickt, unterschieden. Dies ist beispielsweise eine signierte Nachricht, deren Inhalt damit weder dem Authentisierungsmerkmal noch den Authentisierungsdaten entspricht.

Blockprüfsumme Eine Prüfsumme, die über einen Block von Stimmen in der Urne gebildet wird. Diese Prüfsumme wird stets (iterativ) neu berechnet, sobald sich eine festdefinierte Anzahl weiterer Stimmen in der Urne befindet und bezieht dabei die zuvor auf dieselbe Weise berechnete Prüfsumme über die bisherigen Stimmenblöcke ein.

Clientseitiger Browser Der Webbrowser, der zur Anzeige der Wahlhandlung auf dem Endgerät installiert ist.

Endgerät Das Gerät, auf dem der Webbrowser installiert ist und über das die Verbindung zum Wahlserver hergestellt wird.

Ergebnis Die Ausgabe der Stimmauszählung ist das Ergebnis der Online-Wahl. Die Feststellung des Ergebnisses umfasst die Anzahl der ungültigen Stimmen, die Anzahl der gültigen Stimmen und die summarische Verteilung der gültigen Stimmen auf die einzelnen Wahlvorschläge. Der Zeitpunkt der Stimmauszählung bestimmt die Unterscheidung von Wahlergebnis und Zwischenergebnis.

EVG-Prüfsumme Eine Prüfsumme, die über das Web-Archiv eines EVG erstellt wird. Ein Vergleich einer vor der Wahl erzeugten Prüfsumme eines EVG mit einer nach der Wahl erzeugten Prüfsumme desselben EVG ermöglicht es, nachträgliche Manipulationen an dem EVG festzustellen.

Fingerprint Merkmal zur Feststellung der Authentizität des Wahlservers bzw. die Komponenten der serverseitigen EVGs, dass auf TLS Zertifikaten beruht.

Identifikationsdaten[3] Ein Merkmal, das jeder registrierte Wähler/Wahlvorstand besitzt, um sich am EVG zu identifizieren, […] sowie die wählerbezogenen Daten in der Wahlberechtigungsliste, mit denen ein registrierter Wähler eindeutig identifiziert werden kann. Dies ist die PIN.

Prüfsumme siehe EVG-Prüfsumme, Archivprüfsumme, Blockprüfsumme.

Registrierter Wähler Wähler, der in der Wahlberechtigungsliste aufgeführt ist. Registrierte Wähler werden unterschieden in Wähler mit Stimmberechtigung und Wähler ohne Stimmberechtigung.

Rückmeldung Der registrierte Wähler erhält eine zutreffende Rückmeldung über die Erlaubnis bzw. Verweigerung und den Erfolg bzw. Misserfolg seiner Stimmabgabe. Der serverseitige EVG schickt dazu dem clientseitigen Browser eine entsprechende Nachricht und der clientseitige Browser informiert dann den Wähler; in der Regel über eine entsprechende Anzeige am Bildschirm.

Separation of Duty Keine einzelne als Wahlvorstand handelnde Person hat das Recht zur Ausführung von Operationen zum Starten, Wiederanlaufen und Beenden der Wahldurchführung und zum Starten der Stimmauszählung mit Feststellung des Wahlergebnisses.

Serverkommunikationsdaten Begriff zur Gruppierung aller Steuerungsinformationen, die zwischen dem Wählerverzeichnis, Urne, Validator und Wahlvorstandsinterface ausgetauscht werden. Als Steuerungsinformationen werden in diesem Zusammenhang Informationen verstanden, die der Benutzerführung durch die Wahlhandlung dienen, wie die Nummer des anzuzeigenden Stimmzettels oder die Bezeichnung der ausgeführten Aktion.

Serverseitiger EVG Software, welche auf dem Wahlserver installiert ist, die serverseitige Funktionalität zur Wahldurchführung inkl. der Stimmauszählung beinhaltet und die damit verbundenen Sicherheitsanforderungen an den EVG durchsetzt. POLYAS CORE unterteilt den serverseitigen EVG in Wählerverzeichnis, Validator, Urne und Wahlvorstandsinterface.

Stimmabgabe Die Zustimmung des Wählers zur endgültigen, unwiderruflichen Speicherung seiner Stimme in der Urne. Die Stimmabgabe ist erfolgreich, wenn die Stimme fehlerfrei in der Urne gespeichert wird.

---

3 Bei der Identifikation wird, anders als bei der Authentisierung, nicht zwischen einem Merkmal beim Wähler und Daten in der Wahlberechtigungsliste unterschieden. Beides ist zu einem Begriff zusammengefasst

Stimmabgabevermerk Die dauerhafte Markierung eines registrierten Wählers über dessen erfolgreiche Stimmabgabe. Der Vermerk ist untrennbar mit der Speicherung eines Stimmdatensatzes in der Urne verbunden. Er kann in der Wahlberechtigungsliste oder an anderer Stelle gespeichert werden.

Stimmauszählung Durch Auszählung aller in der Urne gespeicherten Stimmen werden die Anzahl der ungültigen und die Anzahl der gültigen Stimmen ermittelt. Durch Auszählung aller gültigen Stimmen wird die summarische Stimmverteilung für die einzelnen Wahlvorschläge ermittelt.

Stimmdatensatz Für die Speicherung in der Urne aufbereitete, also z.B. verschlüsselte Darstellung einer Stimme.

Stimme (Semantik) Inhalt eines ausgefüllten Stimmzettels, der einen Wählerwillen, d.h. die Wahlentscheidung eines Wählers zum Ausdruck bringt. In der Urne gespeicherte Stimmdatensätze enthalten entweder gültige oder ungültige Stimmen. Nach welchen Bedingungen eine Stimme gültig ist, hängt von der Wahlordnung ab. Beispiele für ungültige Stimmen sind, dass der Wähler keine oder zu viele Wahlvorschläge ausgewählt hat.

Stimmzettel (Syntax) Angezeigtes Formular (entspricht einem Papierstimmzettel). Dieses kann leer oder ausgefüllt sein. Es kann auch die Möglichkeit bieten, willentlich ungültig zu wählen. Von der Einleitung der Stimmabgabe bis zur Speicherung in der Urne wird der ausgefüllte Stimmzettel im Zwischenspeicher verwahrt.

Stimmzetteldaten umfassen

- die Liste der Wahlvorschläge sowie
- weitere Informationen, die der EVG benötigt, um den Stimmzettel darstellen zu können (z.B.: Angaben, die auf dem Stimmzettel angezeigt werden sollen und Informationen über Gestalt des Stimmzettels).

Unbefugter Wähler Wähler, der nicht in der Wahlberechtigungsliste aufgeführt ist, sich aber als registrierter Wähler ausgibt / tarnt und versucht eine / mehrere Stimmen abzugeben.

Urne Bestandteil des Wahlservers, in dem alle Stimmdatensätze elektronisch gespeichert werden.

Validator Bestandteil des Wahlservers zur Umsetzung der Separation of Duty auf Architekturebene. Dient der zusätzliche Validierung der Wählerauthentisierung und Generierung der Wählertoken.

Wähler Person, die am Endgerät den EVG benutzt, d.h. eine Wahlhandlung oder Teile davon ausführt. Wähler werden unterschieden in registrierte Wähler und unbefugte Wähler. Wenn der Begriff ohne Qualifizierung verwendet wird, ist die Identität des Wählers unbekannt oder unbedeutend.

Wähler mit Stimmberechtigung Registrierter Wähler, der noch keine Stimme abgegeben hat.

Wähler ohne Stimmberechtigung Registrierter Wähler, der bereits eine Stimme abgegeben hat.

Wählertoken Temporärer Datensatz um einen Wähler und eine Stimme zu verknüpfen. Das Wählertoken wird nach Ende der Wahl gelöscht, um das Wahlgeheimnis zu gewährleisten.

Wählerverzeichnis Bestandteil des Wahlservers zur Authentisierung der Wähler.

Wahlberechtigungsliste Verzeichnis aller Personen, die zur Teilnahme an der Online-Wahl berechtigt sind, d.h. aller registrierten Wähler.

Wahldaten Daten, die im Rahmen der Wahlvorbereitung authentisch bereitgestellt werden:

- Stimmzetteldaten

- Wahlberechtigungsliste mit Authentisierungsdaten
- Wahlende-Zeitpunkt

Wahldurchführung In dieser Phase kann der Wähler seine individuelle Wahlhandlung durchführen. Der Wahlvorstand startet und beendet die Wahldurchführung.

Wahldurchführungsdaten Daten, die nach der der Wahldurchführung inkl. Stimmauszählung manipulationssicher gespeichert werden:

- Stimmzetteldaten
- Wahlberechtigungsliste sowie alle damit verbundenen Daten einschließlich Daten, die im Laufe der Wahldurchführung entstehen
- Stimmabgabevermerke
- Inhalt der Urne

Wahlende Das Wahlende ist erreicht, wenn der Wahlvorstand die Wahldurchführung am serverseitigen EVG beendet. Anschließend kann kein Wähler mehr am serverseitigen EVG eine Wahlhandlung eröffnen und es wird keine Stimme mehr in der Urne gespeichert.

Wahlende-Zeitpunkt Während der Wahlvorbereitung wird der geplante Zeitpunkt für das Ende der Wahldurchführung definiert. Dieser wird als Wahlende-Zeitpunkt bezeichnet.

Wahlergebnis Nach der Wahldurchführung festgestelltes Ergebnis der Stimmauszählung.

Wahlgeheimnis Bei einer geheimen Wahl bedeutet das Wahlgeheimnis, dass die Wahlentscheidung des Wählers nicht beobachtet und auch nicht nachträglich rekonstruiert werden kann.

Wahlhandlung Umfasst alle Phasen, die ein Wähler durchläuft: Identifikation /Authentisierung mit Stimmberechtigungsprüfung, Stimmzettel ausfüllen / korrigieren und Stimmabgabe einleiten, Anzeige der Stimme, Widerruf oder endgültige Abgabe der Stimme, Rückmeldung an den Wähler.

Wahlserver Server, auf dem der serverseitige EVG installiert ist und über den die Verbindung zum Endgerät hergestellt wird.

Wahlurne Synonym für Urne

Wahlveranstalter Gruppe von Personen, die die Wahl ausrichtet.

Wahlvorschläge Kandidaten, Parteien oder Wählervereinigungen, die auf dem Stimmzettel zur Auswahl stehen.

Wahlvorstand Hierzu gehören sowohl die Personen, die die organisatorische Verantwortung für die Online-Wahl haben und sie leiten, sowie auch alle „Erfüllungsgehilfen“ (z.B. Mitarbeiter eines mit der Abwicklung beauftragten Wahldienstleisters), die im Auftrag und unter Kontrolle leitender Personen des Wahlvorstandes die Administration des Wahlservers durchführen, die Wahldurchführung starten, einen Wiederanlauf veranlassen, die Wahldurchführung beenden sowie die Stimmauszählung mit Feststellung des Wahlergebnisses starten.

Wahlvorstandsinterface Bestandteil des EVG, der dem Wahlvorstand einen entfernten Zugriff zu Steuerung von Wahlhandlungen ermöglicht.

Zugang (zum Wahlserver) Mit Zugang wird die Benutzung des Wahlservers bezeichnet. Zugangsberechtigungen erlauben somit bestimmten Personen, den Wahlserver zu benutzen.

Zugriff (auf die vom EVG kontrollierten Informationen und Daten) Mit Zugriff wird die vom EVG kontrollierte Benutzung von Informationen und Daten bezeichnet. Über Zugriffsberechtigungen wird geregelt, welchen Personen als Wähler oder Wahlvorstand erlaubt wird, Informationen und Daten zu benutzen oder kontrollierte Operationen auszuführen.

Zutritt (zu den Räumen mit den Komponenten des Wahlservers) Mit Zutritt wird das Betreten der Räume, in denen sich die Komponenten des Wahlservers befinden, bezeichnet. Zutrittsberechtigungen erlauben somit bestimmten Personen, diese Räume zu betreten.

Zwischenergebnis Während der Wahldurchführung festgestelltes Ergebnis der Stimmauszählung.

Zwischenspeicher Speicherung der noch nicht endgültig abgegebenen Stimme mit Änderungsmöglichkeit, z.B. auf dem Endgerät oder vorgelagert zur Urne. Eine technisch bedingte Zwischenspeicherung bei der Übertragung gehört nicht dazu.