Bundesamt
für Sicherheit in der
Informationstechnik

Common Criteria Schutzprofil

für

Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte

Common Criteria

BSI-CC-PP-0037

Version 1.0, 18. April 2008

Anwendungshinweis:

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 nicht-politische Wahlen mit geringem Angriffspotential sicher auszuführen. Zur sicheren Durchführung von Online-Wahlen mit höherem Angriffspotential, wie etwa Betriebsratswahlen oder parlamentarische Wahlen, sind weitere Sicherheitsanforderungen zu formulieren und mit nachweisbaren Maßnahmen durchzusetzen, um die Annahmen über die Anwendungsumgebungen, wie sie hier beschrieben sind, zu erfüllen. Weitergehende Anforderungen zur Erfüllung der Annahmen über die Wahlumgebung mit höherem Angriffsrisiko können nahtlos auf den hier beschriebenen Kern der zentralen Anforderungen aufbauen und diesen ergänzen, keinesfalls ersetzen.

Vorwort

Das vorliegende Schutzprofil „Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte“ wurde vom Bundesamt für Sicherheit in der Informationstechnik der Bundesrepublik Deutschland herausgegeben.

Das Dokument wurde gemäß den Regeln und der Strukturvorgabe der Common Criteria Version 3.1 Revision 2 für Schutzprofile erstellt.

Die CC-Terminologie und der Wortlaut der im Teil 2 der CC in englischer Sprache definierten funktionalen Anforderungen wurden in Abstimmung mit dem BSI ins Deutsche übersetzt. Bezogen auf die Konformität zu Teil 2 der CC gilt im Zweifelsfall die englische Originalfassung.

Anmerkungen und Kommentare zu diesem Schutzprofil richten Sie an:

KONTAKTADRESSE:

Bundesamt für Sicherheit in der Informationstechnik
Postfach 200362
D-53133 Bonn, Deutschland
Tel +49 228 9582-0
Fax +49 228 9582-5400
Email bsi@bsi.bund.de

Variablen

Name	Wert (mit Textmarken versehen)	Kontrollanzeige der Textmarken
Titel	Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte	Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte
Kennzeichen	BSI-CC-PP-0037	BSI-CC-PP-0037
Version	1.0	1.0
Datum	18. April 2008	18. April 2008
Vertraulichkeit	Offen	Offen
Editoren	Melanie Volkamer (ehem. DFKI) und Roland Vogt (DFKI) DFKI: Deutsches Forschungszentrum für Künstliche Intelligenz GmbH	Melanie Volkamer (ehem. DFKI) und Roland Vogt (DFKI) DFKI: Deutsches Forschungszentrum für Künstliche Intelligenz GmbH
Dateiname (-größe)	*Set automatically*	BSI-CC-PP-0037-v10.doc (637952 Byte)

Änderungshistorie

Version	Datum	Beschreibung	Bemerkung
0.x		Verschiedene Entwurfsfassungen	
1.0	18.04.2008	Finale Version für Erstzertifizierung	

Inhaltsverzeichnis

PP Einführung

1 Dieses Schutzprofil definiert einen Basissatz von Sicherheitsanforderungen, den jedes Online-Wahlprodukt zumindest erfüllen muß, um einige Arten von Vereinswahlen, Gremienwahlen, etwa in den Hochschulen, im Bildungs- und Forschungsbereich, und insbesondere nicht-politische Wahlen mit geringem Angriffspotential sicher auszuführen.

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

Anwendungsnotiz 1: *Zur sicheren Durchführung von Online-Wahlen mit höherem Angriffspotential, wie etwa Betriebsratswahlen oder parlamentarische Wahlen, sind weitere Sicherheitsanforderungen zu formulieren und mit nachweisbaren Maßnahmen durchzusetzen, um die Annahmen über die Anwendungsumgebungen, wie sie hier beschrieben sind, zu erfüllen. Weitergehende Anforderungen zur Erfüllung der Annahmen über die Wahlumgebung mit höherem Angriffsrisiko können nahtlos auf den hier beschriebenen Kern der zentralen Anforderungen aufbauen und diesen ergänzen, keinesfalls ersetzen. Damit wird dem ST-Autor die Möglichkeit angeboten, auf der Grundlage dieses Schutzprofils weitere Sicherheitsanforderungen zur Erfüllung komplexerer Wahlprozesse hinzuzunehmen. Die Angemessenheit solcher zusätzlicher Anforderungen muß dann im Einzelfall geprüft werden.*

3 Vom Wahlveranstalter muß geprüft werden, ob die im Abschnitt „Problemdefinition“ beschriebenen Annahmen, Bedrohungen und Sicherheitspolitiken den geltenden Wahlordnungen und der Einsatzumgebung (technisch wie soziologisch) entsprechen (siehe hierzu auch Anhang A). Da sowohl die Wahlordnungen als auch die Einsatzumgebungen sehr unterschiedlich sein können, kann es keine Allround-Lösung, die alle denkbaren Wahlen unterstützt, geben.

4 Beim Einsatz eines Online-Wahlprodukts, das mit diesem Schutzprofil konform ist, ist zu beachten, daß es sich um ein Anwendungsprogramm handelt, das zur Durchsetzung seiner Sicherheitsfunktionen von dem darunterliegenden Betriebssystem und dessen Konfiguration abhängig ist. Die Anforderungen an diese Anwendungsumgebung sind in den Sicherheitszielen für die Umgebung adressiert.

1.1 PP Referenz

5	Titel:	Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte
6	Herausgeber:	Bundesamt für Sicherheit in der Informationstechnik
7	Editoren:	Melanie Volkamer und Roland Vogt
8	Versionsnummer:	1.0
9	Registrierung:	BSI-CC-PP-0037
10	Schlüsselwörter:	remote Voting, eVoting, Online-Wahlen, elektronische Wahlen

1.2 EVG-Übersicht

11 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.

1.2.1 Art des EVG

12 Der betrachtete Evaluationsgegenstand (EVG) 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.

13 Die 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.

Anwendungsnotiz 2: *Dieses Schutzprofil legt einen Basissatz von Anforderungen für die Phase Wahldurchführung inkl. Stimmauszählung fest. Der EVG kann weitere Funktionen für diese oder andere Phasen einer Online-Wahl bereitstellen. Vom ST-Autor ist die Beschreibung des Funktionsumfangs angemessen zu ergänzen.*

14 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.

15 Der EVG ist ein verteiltes Produkt, das aus einem serverseitigen EVG und aus einem clientseitigen EVG besteht (vgl. Abbildung 1). Der serverseitige EVG verwaltet die Wahlberechtigungsliste und die Urne. Am clientseitigen EVG führt der Wähler die Wahlhandlung aus um seine Stimme abzugeben.

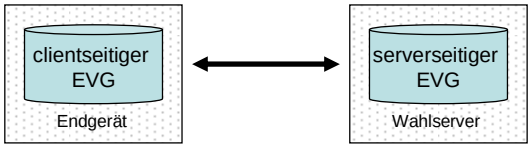


Abbildung 1 Struktur des EVG

Anwendungsnotiz 3: *Die Abgrenzung zwischen dem Funktionsumfang des EVG auf dem Wahlserver und auf dem Endgerät ist vom ST-Autor festzulegen. Die Konformität mit dem Schutzprofil kann mit unterschiedlicher Funktionsverteilung nachgewiesen werden. Dies gilt auch, falls auf dem Endgerät keine spezifische Software auszuführen ist, sondern der Wähler über einen Webbrowser die Wahlhandlung ausführt. In einem solchen Fall sind die vom serverseitigen EVG bereitgestellten und auf das End-*

gerät übertragenen Daten so zu gestalten, daß die korrekte Anzeige des Stimmzettels und die korrekte Übertragung der Eingaben des Wählers gewährleistet sind. Außerdem muß der serverseitige EVG Daten oder Informationen bereitstellen, die dem Wähler die Möglichkeit geben, seine abgegebene Stimme nach der Wahlhandlung auf dem Endgerät zu löschen.

16 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.

Anwendungsnotiz 4: *Die obige Liste enthält nur solche Merkmale, die von jedem EVG, der konform mit diesem Schutzprofil ist, unterstützt werden müssen. Sie kann vom ST-Autor selektiv um folgende oder andere Merkmale erweitert werden:*

- *Die Authentizität der Wahldaten muß vor der Wahldurchführung überprüft werden.*
- *Vom Wahlvorstand genehmigte Veränderungen der Wahlberechtigungsliste[1] während der Wahldurchführung sind zulässig.*
- *Vom Wahlvorstand genehmigte Veränderungen der Stimmberechtigung[2] von Wählern während der Wahldurchführung sind zulässig.*
- *Jeder Wähler muß verifizieren können, ob die von ihm abgegebene Stimme in der Urne gespeichert ist.*
- *Anforderungen an die Gestaltung des Stimmzettels, die sich durch den Einsatz von Technik ergeben*
- *Für sehbehinderte oder blinde Wähler müssen geeignete Schnittstellen und Hilfsmittel bereitgestellt werden.*
- *Entsprechend den Vorgaben des Wahlveranstalters müssen statistische Daten erhoben werden.*

Anwendungsnotiz 5: *Falls der EVG dem Wähler die Verifikation der Speicherung seiner Stimme ermöglicht oder dem Wahlvorstand Funktionen zur Veränderung der Wahlberechtigungsliste oder der Stimmberechtigung einzelner Wähler anbietet, so müssen vom ST-Autor zusätzliche Sicherheitsanforderungen für diese Operationen formuliert werden. Die Anforderungen von solchen zusätzlichen Operationen müssen mit den Anforderungen des Schutzprofils konsistent sein.*

---

[1] Eine Veränderung der Wahlberechtigungsliste kann durch kurzfristigen Eintritt oder Austritt eines Mitglieds notwendig sein.

[2] Eine Veränderung der Stimmberechtigung kann notwendig sein, wenn neben der Online-Wahl eine alternative Wahlform, z.B. Briefwahl, zur Verfügung steht und vom Wähler benutzt wird.

Anwendungsnotiz 6: *Falls ein Online-Wahlprodukt die Erfassung von statistischen Daten vorsieht, kann der ST-Autor entsprechende Sicherheitsanforderungen ergänzen. Dabei ist insbesondere sicherzustellen, daß das Wahlgeheimnis gewahrt bleibt.*

1.2.2 Abkürzungen und Glossar

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
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation (=EVG)
TSF	TOE Security Function
TSP	TOE Security Policy

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

18 **Authentisierungsdaten** Daten, gegen die geprüft wird, ob die angebliche Identität des Wählers echt ist. Dies sind beispielsweise der Hashwert der TAN oder der öffentliche Schlüssel des registrierten Wählers. Die Daten können in der Wahlberechtigungsliste oder an anderer Stelle gespeichert sein.

19 **Authentisierungsmerkmal** Merkmal, das jeder registrierte Wähler besitzt, um sich am EVG zu authentisieren. Dies ist beispielsweise eine TAN oder eine Signaturkarte, auf der sein geheimer Schlüssel gespeichert ist.

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

21 **Clientseitiger EVG** Die Software, die die clientseitige Funktionalität zur Wahldurchführung beinhaltet und die damit verbundenen Sicherheitsanforderungen an den EVG durchsetzt. Sie muß auf dem Endgerät installiert sein, damit der Wähler von dort die Wahlhandlung ausführen kann.

22 **Endgerät** Das Gerät, auf dem der clientseitige EVG installiert ist und über das die Verbindung zum Wahlserver hergestellt wird.

23 **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.

24 **Identifikationsdaten**[3] Zum einen ein Merkmal, das jeder registrierte Wähler besitzt, um sich am EVG zu identifizieren. Dies kann z.B. eine Mitgliedsnummer, ein Name, ein Geburtsdatum oder eine Adresse sein. Zum anderen die wählerbezogenen Daten in der Wahlberechtigungsliste, mit denen ein registrierter Wähler eindeutig identifiziert werden kann.

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

26 **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 EVG eine entsprechende Nachricht und der clientseitige EVG informiert dann den Wähler; in der Regel über eine entsprechende Anzeige am Bildschirm.

27 **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.

28 **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. Falls die Funktionen des serverseitigen EVG auf mehrere Wahlserver verteilt werden, müssen die Anforderungen im Zusammenwirken erfüllt werden.

29 **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.

30 **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.

31 **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.

[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

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

33 **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.

34 **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.

35 **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).

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

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

38 **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.

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

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

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

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

- Stimmzetteldaten
- Wahlberechtigungsliste mit Authentisierungsdaten
- Wahlende-Zeitpunkt

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

44 **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

45 **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.

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

47 **Wahlergebnis** Nach der Wahldurchführung festgestelltes Ergebnis der Stimmauszählung.

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

49 **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.

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

51 **Wahlveranstalter** Gruppe von Personen, die die Wahl ausrichtet.

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

53 **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.

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

55 **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.

56 **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.

57 **Zwischenergebnis** Während der Wahldurchführung festgestelltes Ergebnis der Stimmauszählung.

58 **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.

1.2.3 Generelle Sicherheitserwartungen an den EVG

59 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).

Anwendungsnotiz 7: *Bei der Umsetzung des Grundsatzes der geheimen Wahl unterscheidet man bei Online-Wahlen zwei Ansätze: i) Die geheime Wahl wird während der Wahldurchführung sichergestellt. Hier darf nach der Wahl keine Möglichkeit bestehen, den Zusammenhang zwischen Wähler und Stimme herzustellen, auch nicht unter zu Hilfenahme sämtlicher Zusatzdaten, wie bspw. Entschlüsselungskeys. ii) Die geheime Wahl wird während der Stimmauszählung sicher gestellt, in dem kryptographische Verfahren eingesetzt werden, wobei eine Zuordnung zwischen Wähler und verschlüsselter Stimme bekannt ist. Diese Verfahren vertrauen auf eine organisatorische Separation of Duty, d.h. sie nehmen an, daß eine Gruppe von Personen nicht kooperiert. Hier gilt also nicht, daß unter zu Hilfenahme sämtlicher Zusatzdaten, wie bspw. Entschlüsselungskeys das Wahlgeheimnis geschützt bleibt, sondern es ist eine organisatorische Anforderung.*

- 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).

Anwendungsnotiz 8: *Die Gewährleistung des Wahlgeheimnisses erfordert häufig die zeitliche Entkopplung von Authentisierung und Stimmabgabe. Die Authentisierung sollte aber in einem möglichst engen zeitlichen Zusammenhang mit der endgültigen Stimmabgabe stehen um zu verhindern, daß eine begonnene Wahlhandlung von einem unbefugten Wähler erfolgreich beendet wird.*

- 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).

1.2.4 Gebrauch und wesentliche Sicherheitsmerkmale

1.2.4.1 Zustand des EVG vor der Wahldurchführung inkl. Stimmauszählung

60 In der Phase Wahlvorbereitung werden die Wahldaten angelegt, ggf. korrigiert und vom Wahlveranstalter verabschiedet. Jeder registrierte Wähler verfügt über seine Identifikationsdaten und sein Authentisierungsmerkmal. 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.

61 Vor dem Beginn der Wahldurchführung werden die Wahldaten in der genehmigten, d.h. in der vom Wahlveranstalter verabschiedeten Fassung, auf dem Wahlserver für die Verwendung durch den EVG bereitgestellt. Die Installation und Konfiguration des serverseitigen EVG ist vom Wahlveranstalter durchgeführt und erfolgreich abgeschlossen. Der clientseitige EVG ist, falls erforderlich, vom Wahlveranstalter an alle registrierten Wähler ausgeliefert.

Anwendungsnotiz 9: *Abhängig vom Entwurf des EVG kann die Auslieferung des clientseitigen EVG in mehreren Schritten erfolgen. Wenn der Wähler aktiv in die Auslieferung einbezogen ist (z.B. durch Herunterladen), kann sie auch erst unmittelbar vor der Eröffnung der Wahlhandlung abgeschlossen werden. Der ST-Autor soll bei Bedarf die Beschreibung der Auslieferung des clientseitigen EVG anpassen.*

1.2.4.2 Prozessbeschreibung für die Wahldurchführung inkl. Stimmauszählung

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

63 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 dürfen nicht in der Urne gespeichert werden. Falls eine kurzfristige Zwischenspeicherung außerhalb der Urne erforderlich ist, muß das Wahlgeheimnis gewahrt bleiben.

64 Während der Wahldurchführung kann am serverseitigen 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.

65 Zur Beendigung der Wahldurchführung leitet der Wahlvorstand am serverseitigen 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.

66 Nach dem Wahlende kann der Wahlvorstand die Stimmauszählung veranlassen. 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 EVG so gespeichert, daß sie vor nachträglichen Manipulationen, also unbefugten Modifikationen außerhalb der Kontrolle des serverseitigen EVG, geschützt sind.

Anwendungsnotiz 10: *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. Der ST-Autor soll prüfen, ob der EVG zunächst ermitteln soll, wie viele ungültige und gültige Stimmen in der Urne gespeichert sind, bevor die gültigen Stimmen ausgezählt werden. Ggf. sind angemessene Anforderungen zu ergänzen.*

67 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.

68 Der Prozessablauf für die individuelle Wahlhandlung jedes Wählers muß folgenden Prinzipien genügen:

- Spätestens zum Zeitpunkt 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 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.

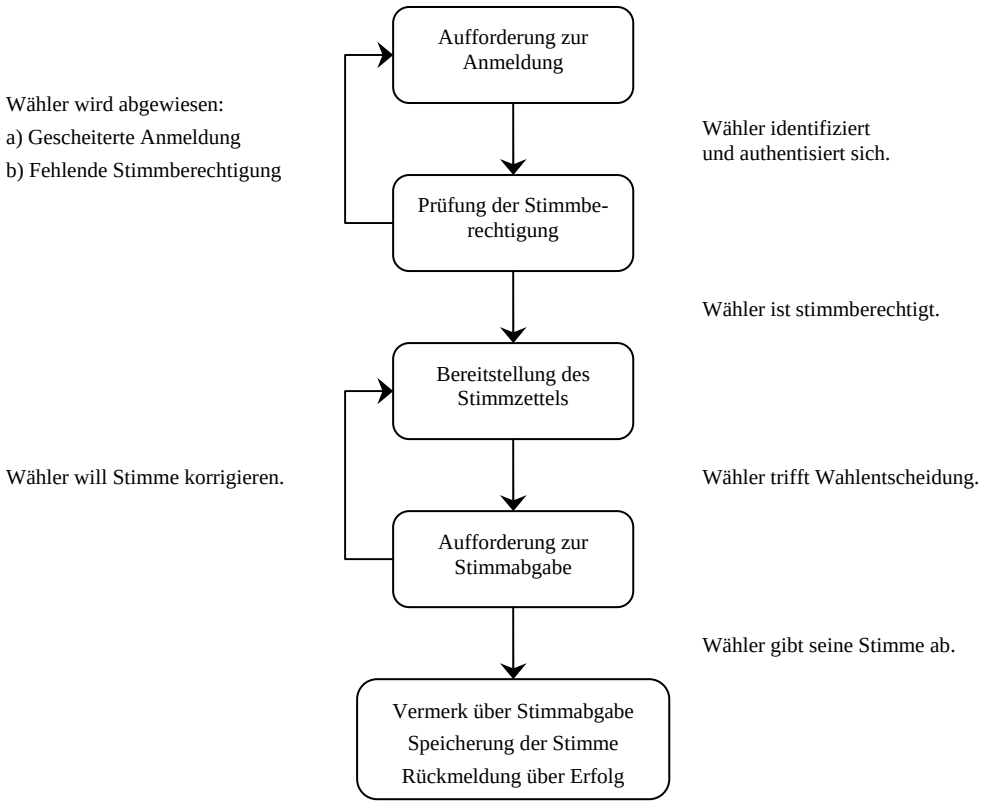
Anwendungsnotiz 11: *Für den Ablauf der Wahlhandlung jedes Wählers lassen sich verschiedene Modelle unterscheiden, von denen nachfolgend zwei Varianten aufgezeigt werden. Der ST-Autor muß diese Beispiele durch die Beschreibung des vom EVG tatsächlich realisierten Ablaufs ersetzen.*

Beispiel für den Ablauf der Wahlhandlung (Variante 1)

69 Die erste Variante wird mit „Anmeldung bei Start der Wahlhandlung“ bezeichnet und ist ohne Berücksichtigung von Fehlern und Unterbrechungen in Abbildung 2 dargestellt. Der Wähler eröffnet die Wahlhandlung am clientseitigen EVG. 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.

70 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 2 Ablauf der Wahlhandlung aus Sicht des Wählers (Variante 1)

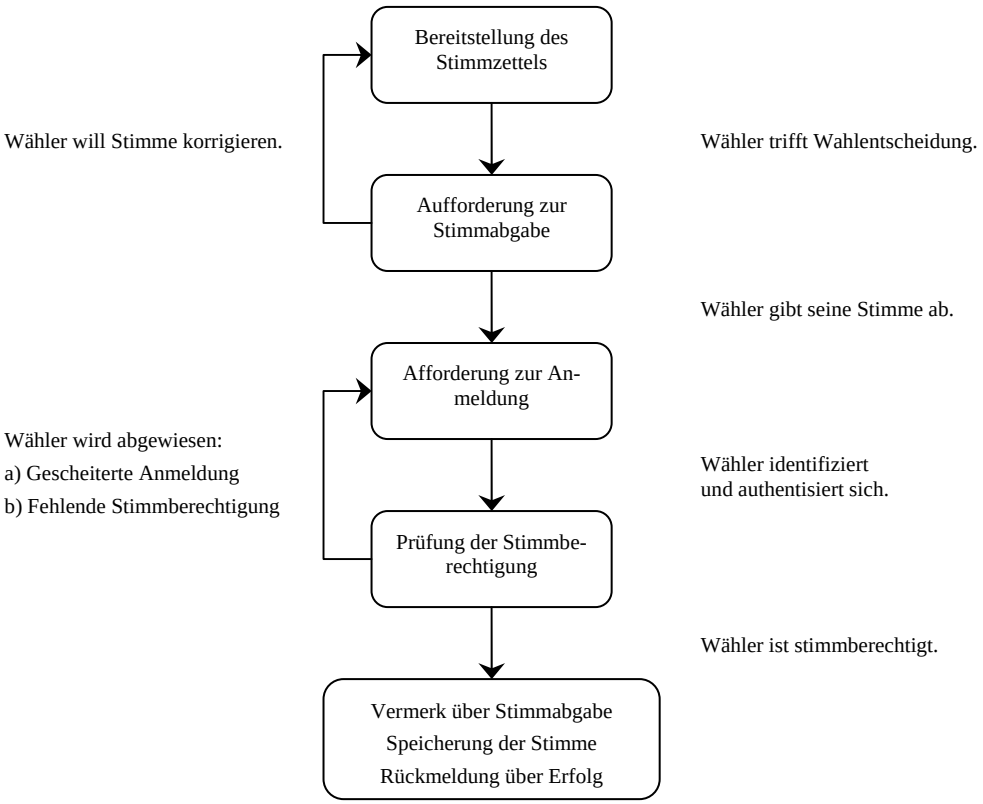


Beispiel für den Ablauf der Wahlhandlung (Variante 2)

71 Die zweite Variante wird mit „Anmeldung bei Stimmabgabe“ bezeichnet und ist ohne Berücksichtigung von Fehlern und Unterbrechungen in Abbildung 3 dargestellt. Der Wähler eröffnet die Wahlhandlung am clientseitigen EVG und erhält den Stimmzettel. Nun kann der Wähler seinen Stimmzettel ausfüllen, beliebig oft ändern und mit der Einleitung der Stimmabgabe seine Wahlentscheidung treffen. Anschließend zeigt der EVG dem Wähler seine Stimme erneut an. Er hat nun die Möglichkeit, die Stimme abzugeben oder die Einleitung der Stimmabgabe zu widerrufen um die Stimme zu korrigieren.

72 Nachdem der Wähler die Stimmabgabe veranlasst hat, identifiziert und authentisiert er sich gegenüber dem serverseitigen EVG. Der serverseitige EVG prüft die Stimmberechtigung des registrierten Wählers. Im nächsten Schritt wird die Stimmabgabe des Wählers mit Stimmberechtigung ausgeführt, alle anderen Wähler werden vom serverseitigen EVG abgewiesen. 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 3 Ablauf der Wahlhandlung aus Sicht des Wählers (Variante 2)



1.2.4.3 Zustand des EVG nach der Wahldurchführung inkl. Stimmauszählung

73 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.

74 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.

75 Die Veröffentlichung der Wahlergebnisse liegt im Verantwortungsbereich der Wahlveranstalter.

1.2.4.4 Bedienung durch den Wähler

76 Neben dem ggf. erforderlichen Starten und Beenden des clientseitigen EVG stehen dem Wähler 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.

Anwendungsnotiz 12: *Es ist zulässig, daß einige der aufgezählten Aktionen nicht vom clientseitigen EVG selbst, sondern vom serverseitigen EVG auf dem Endgerät bereitgestellt werden. Im Extremfall werden alle Aktionen vom serverseitigen EVG bereitgestellt und entsprechende Daten so auf das Endgerät übertragen, daß die korrekte Anzeige des Stimmzettels, die korrekte Eingabe und Übertragung der Stimme und das Löschen der Daten am Endgerät mit Unterstützung der IT-Umgebung möglich ist.*

Anwendungsnotiz 13: *Darüber hinausgehende Funktionen, z.B. der Abruf von Informationen zur Wahl oder zur Bedienung des EVG, werden für eine konkrete Realisierung nicht ausgeschlossen, dürfen aber den hier dargelegten Basisanforderungen nicht widersprechen. Der ST-Autor soll auch die Anwendungsnotizen in Abschnitt 1.2.1 beachten, um in diesem Abschnitt ggf. Ergänzungen vorzunehmen.*

1.2.4.5 Bedienung durch den Wahlvorstand

77 Der Wahlvorstand wird am serverseitigen EVG identifiziert und authentisiert, bevor ihm die Ausführung jeglicher anderer Aktion erlaubt wird.

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

79 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.

80 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.

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

Anwendungsnotiz 14: *Darüber hinausgehende Funktionen, z.B. eine zeitlich befristete Wahlunterbrechung, werden für eine konkrete Realisierung nicht ausgeschlossen, dürfen aber den hier dargelegten Basisanforderungen nicht widersprechen. Der ST-Autor soll auch die Anwendungsnotizen in Abschnitt 1.2.1 beachten, um in diesem Abschnitt ggf. Ergänzungen vorzunehmen.*

1.2.4.6 Störungen, Selbsttests und Wiederanlauf

82 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.

83 Über Störungen der Netzwerkanbindung oder der Speicherung von Daten, die dem serverseitigen EVG gemeldet werden, wird der Wahlvorstand 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.

84 Der EVG muß einen Mechanismus zur Verfügung stellen, 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.

85 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.

86 Die Benutzung des Wiederanlaufmechanismus nach Wahlende ist vom EVG zu verhindern. Eine Rückkehr zur Wahldurchführung ist somit nicht möglich.

1.2.4.7 Protokollierung

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

- 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 des serverseitigen EVG beeinträchtigen

Anwendungsnotiz 15: *Die Liste der Ereignisse kann vom ST-Autor ergänzt werden. Insbesondere soll geprüft werden, ob das Eröffnen und das Beenden einer Wahlhandlung oder bestimmte Ereignisse während der Ausführung einer Wahlhandlung, z.B. die Änderung von Sicherheitsattributen, protokolliert werden sollen. Dabei muß sichergestellt sein, daß die aufgezeichneten Daten den Sicherheitszielen nicht widersprechen und insbesondere das Wahlgeheimnis nicht verletzen.*

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

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

1.2.5 Benötigte nicht-EVG Hardware/Firmware/Software

90 Der clientseitige EVG wird auf dem Endgerät des Wählers betrieben, über das der Wähler mit dem Wahlserver bzw. dem serverseitigen EVG kommuniziert. Zur IT-Umgebung des clientseitigen EVG zählen die Teile des Endgerätes, die zur Verwendung des EVG notwendig sind, also z.B. die Hardware, Betriebs- und Applikationssoftware und das lokale Netzwerk in einer PC-Umgebung.

91 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.

Anwendungsnotiz 16: *Das Schutzprofil schreibt keine bestimmten Endgeräte vor. Der Wähler soll die Wahlhandlung an jedem Endgerät, das die Anforderungen an die clientseitige IT-Einsatzumgebung erfüllt, ausführen können. Eine einheitliche Darstellung der Stimmzettel auf allen Endgeräten und damit bei allen Wählern wird nicht gefordert, da dies bei der Vielzahl der möglichen Endgeräte nicht gewährleistet werden kann. Der ST-Autor muß eine Liste der Endgeräte angeben, von denen aus der Wähler die Wahlhandlung ausführen kann. Falls das Authentisierungsmerkmal des Wählers an spezifische Hardware, Firmware oder Software, z.B. eine SmartCard, gebunden ist, muß der ST-Autor diese Teile der IT-Umgebung ebenfalls angeben.*

92 Der serverseitige EVG wird auf dem Wahlserver betrieben. Zur IT-Umgebung des serverseitigen EVG zählen die Teile des Wahlservers, die zur Verwendung des EVG notwendig sind, also z.B. die Hardware, das Betriebssystem und das lokale Netzwerk in einer Rechenzentrumsumgebung.

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

Anwendungsnotiz 17: *Eine präzisere Beschreibung der benötigten nicht-EVG Hardware/Firmware/Software ist in vorliegendem Schutzprofil wegen der Vielzahl möglicher Wahlprotokolle und der zugehörigen Funktionsverteilung im EVG nicht möglich. Dieser Abschnitt muß vom ST-Autor konkretisiert werden.*

2 Postulate zur Übereinstimmung

94 Dieses PP postuliert Übereinstimmung mit CC Version 3.1 Revision 2

95 Dieses PP ist CC **Part 2 conformant**.
Der Wortlaut der im Teil 2 der CC in englischer Sprache definierten funktionalen Anforderungen wurden in Abstimmung mit dem BSI ins Deutsche übersetzt. Bezogen auf die Konformität zu Teil 2 der CC gilt im Zweifelsfall die englische Originalfassung.

96 Dieses PP ist CC **Part 3 conformant**.

97 Dieses PP ist **EAL 2 augmented** with components

- ALC_CMC.3 (substituting ALC_CMC.2)
- ALC_CMS.3 (substituting ALC_CMS.2)
- ALC_DVS.1
- ALC_LCD.1

98 Dieses PP verlangt **strict conformance**.

Anwendungsnotiz 18: *Falls das Schutzprofil für ein Online-Wahlsystem angewendet werden soll, welches die Mehrfachstimmabgabe unterstützt, so sind entsprechende Änderungen notwendig, damit der Wähler die Möglichkeit hat, mehrfach zu wählen (beispielsweise die Bedrohung: T.Mehrfach). Es muß aber weiterhin sichergestellt werden, daß nur eine (beispielsweise die letzte) Stimme gezählt wird. Daher sollte man unterscheiden zwischen der Stimmabgabe, die pro Wähler mehrfach durchgeführt werden kann, und der Stimmauszählung, in die pro Wähler genau eine abgegebene Stimme einfließen darf. Solche Wahlverfahren bieten bestimmte Vorteile im Hinblick auf Erpressung und Bestechung des Wählers. Selbst wenn der Angreifer für den Wähler die Stimme abgibt (Impersonation), kann der Wähler dennoch seine Stimme abgeben und werten lassen.*

3 Definition des Sicherheitsproblems

99 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.

100 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.

101 *Zu schützende Werte*

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

102 *Subjekte*

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

- Registrierter Wähler
- Wahlvorstand

104 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

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

3.1.1 Definitionen – Methode, Gelegenheit, Fachkenntnis

106 *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.

107 *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.

108 *Fachkenntnis und Verfügbare Betriebsmittel des Angreifers*

109 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.

110 B) Registrierter Wähler

- Fachkenntnis: Laie
- Verfügbare Betriebsmittel: Endgerät mit clientseitigem EVG

111 C) Unbefugter Wähler

- Fachkenntnis: Laie
- Verfügbare Betriebsmittel: Endgerät mit clientseitigem EVG und Betriebsmittel, die leicht zu beschaffen sind.

112 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 und ggf. Zusatzdaten wie beispielsweise Entschlüsselungskeys (vgl. Anwendungsnotiz 7).

3.1.2 Definition von Bedrohungen

113 **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, Authentisierungsmerkmal, Authentisierungsnachricht, Ergebnis.

114 **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.

115 **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.

- Angriffsmethode: direkt
- Gelegenheiten: aktiv
- Ausgenutzte Schwachstelle: Netzwerk
- Angegriffener Wert: Ergebnis und (a) Stimmdatensatz; (b) Stimmdatensatz, Identifikationsdaten, Authentisierungsnachricht; (c) Stimmzetteldaten; (d) Rückmeldung.

116 **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 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.
- Angriffsmethode: direkt
- Gelegenheiten: passiv
- Ausgenutzte Schwachstelle: Kommunikationsnetz
- Angegriffener Wert: (a) Identifikationsdaten, Stimmdatensatz, Stimme; (b) Stimmdatensatz, Stimme, Ergebnis.

117 **T.AuthentizitätServer** Ein Netzwerkangreifer leitet den Wähler auf einen gefälschten Wahlserver um. Der Wähler 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

118 **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

119 **T.ArchivierungWahlgeheimnis** Eine Person, die nach der Phase „Wahldurchführung inkl. der Stimmauszählung“ Zugriff auf die im EVG gespeicherten Daten hat und ggf. Zusatzdaten wie beispielsweise Entschlüsselungskeys kennt (vgl. Anwendungsnotiz 7), 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

120 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.

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

122 **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.

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

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

125 **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.

126 **P.Zwischenergebnis** Es muß sichergestellt werden, daß der Wahlvorstand keine Zwischenergebnisse berechnen kann.

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

128 **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.

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

130 **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.

131 **P.Protokoll** Vom serverseitigen EVG müssen mindestens für die in Kapitel 1.2.4.7 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.

132 **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 clientseitigen EVG, die IT-Umgebung des EVG sowie durch das Netzwerk verursacht werden, und bei jedem Wiederanlauf der Wahldurchführung gegeben sein.

133 **P.AuthWahlvorstand** Der EVG muß den Wahlvorstand vor jeder anderen Akion 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.

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

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

3.3 Annahmen

136 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.

137 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

138 **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.

139 **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.

140 **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.

141 **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 und Authentisierungsmerkmalen 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

142 **A.Endgerät** Der Wähler nimmt seine Verantwortung zur Sicherung des Endgerätes wahr. Es wird angenommen, daß der clientseitige EVG, falls erforderlich, vom Wähler so installiert bzw. 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.

143 **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.

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

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

Anwendungsnotiz 19: *Falls der EVG einen Zugriff aus der Ferne zulässt, muß der Hersteller nachweisen, daß die dadurch entstehenden Bedrohungen durch zusätzliche Sicherheitsfunktionen abgewehrt werden.*

146 **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.

147 **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.

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

149 **A.AuthentizitätServer** Der Wähler überprüft, ob er mit dem richtigen serverseitigen EVG kommuniziert.

150 **A.ArchivierungWahlgeheimnis** Für alle Zusatzdaten, wie beispielsweise Entschlüsselungskeys, die nach Fertigstellung der Stimmauszählung eine Zuordnung zwischen dem Wähler und seiner Stimme möglich machen würden (vgl. Anwendungsnotiz 7), wird die vom Online-Wahlverfahren vorgegebene Lebenszyklus- und Zugriffskontrolle vom Wahlvorstand mit geeigneten technischen und organisatorischen Maßnahmen wirksam umgesetzt.

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

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

4 Sicherheitsziele

153 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

154 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.

155 **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.

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

157 **O.IntegritätNachricht** Der EVG verwendet einen geschützten Kommunikationspfad um sicherstellen, 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.

158 **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.

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

160 **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 clientseitigen EVG eine Kommunikation mit dem serverseitigen EVG über den vertrauenswürdigen Pfad einleiten.

161 **O.ArchivierungIntegrität** Der serverseitige EVG stellt sicher, daß nach der Stimmauszählung mit Feststellung des Wahlergebnisses für die Wahldurchführungsdaten, für das Wahlergebnis und, bei Bedarf, für die Protokollaufzeichnungen oder für weitere Daten ein Manipulationsschutz erzeugt wird, der außerhalb der Kontrolle des EVG und außerhalb des Wahlservers wirksam ist. Nachträgliche Fälschungen oder betrügerische Manipulationen sind feststellbar.

Anwendungsnotiz 20: *Der ST-Autor soll festlegen, ob Bedarf an einem Manipulationsschutz für Protokollaufzeichnungen oder für weitere Daten besteht und das Sicherheitsziel geeignet verfeinern.*

162 **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.

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

164 **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.

165 **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.

166 **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.

167 **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.

168 **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.

169 **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.

170 **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.

171 **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.

172 **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 EVG dem Wahlvorstand die Ausführung eines Wiederanlaufs der Wahldurchführung. Dabei gewährleistet der EVG die Integrität der Wahldurchführungsdaten.

173 **O.Protokoll** Der serverseitige EVG erzeugt mindestens für die in Kapitel 1.2.4.7 aufgelisteten Ereignisse inkl. der Zeitpunkte des Auftretens der Ereignisse Protokollaufzeichnungen. Der serverseitige EVG ermöglicht dem Wahlvorstand die Durchsicht der Protokollaufzeichnungen.

174 **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.

175 **O.AuthWahlvorstand** Der EVG muß den Wahlvorstand vor jeder anderen Akion 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.

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

177 **O.Stimmauszählung** Der EVG stellt sicher, daß zu Beginn der Wahldurchfürhung die Urne keine Stimmdatensätze enthält und daß alle Stimmdatensätze, die nach Wahlende in der Urne gespeichert sind, ausgezählt (ggf. zuvor auch entschlüsselt) werden und in die Stimmauszählung mit Feststellung des Wahlergebnisses eingehen.

4.2 Sicherheitsziele für die Einsatzumgebung

178 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.

179 **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.

180 **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.

181 **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.

182 **OE.AuthDaten** Nur registrierte Wähler sind im Besitz der zur Teilnahme an der Wahl benötigten Daten, insb. Identifikationsdaten und Authentisierungsmerkmal. 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.

183 **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 clientseitige EVG wird, falls erforderlich, von dem Wähler so installiert bzw. 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.

Anwendungsnotiz 21: *Der ST-Autor soll unter Berücksichtigung der benötigten nicht-EVG Hardware/Firmware/Software konkretisieren, welche Maßnahmen der Wähler an seinem Endgerät treffen muß, um die Vertrauenswürdigkeit des Endgeräts zu gewährleisten. 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.*

184 **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.

Anwendungsnotiz 22: *Der ST-Autor soll unter Berücksichtigung der benötigten nicht-EVG Hardware/Firmware/Software konkretisieren, welche Maßnahmen (z.B. die Verwendung sicherer Betriebssysteme/Firewalls oder die Separierung des serverseitigen EVG von anderer Software auf dem Wahlserver) der Wahlvorstand am Wahlserver treffen muß, um die Vertrauenswürdigkeit des Wahlservers zu gewährleisten.*

185 **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.

Anwendungsnotiz 23: *Der ST-Autor soll unter Berücksichtigung der benötigten nicht-EVG Hardware/Firmware/Software konkretisieren, welchen Arten von Störungen und Ausfällen begegnet werden soll und unter welchen Bedingungen die Verfügbarkeit als angemessen bezeichnet werden kann. Die vom Wahlveranstalter zu bestimmenden Notfallszenarios können z.B. die Verschiebung des geplanten Wahlende-Zeitpunktes oder den Rückfall zur reinen Papierwahl enthalten.*

186 **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.

187 **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.

188 **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.

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

190 **OE.AuthentizitätServer** Der Wähler überprüft, ob er mit dem richtigen serverseitigen EVG kommuniziert.

Anwendungsnotiz 24: *Der ST-Autor soll unter Berücksichtigung der benötigten nicht-EVG Hardware/Firmware/Software konkretisieren, wie der Wähler überprüfen kann, ob er mit dem richtigen serverseitigen EVG verbunden ist.*

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

192 **OE.ArchivierungWahlgeheimnis** Für alle Zusatzdaten, wie beispielsweise Entschlüsselungskeys, die nach Fertigstellung der Stimmauszählung eine Zuordnung zwischen dem Wähler und seiner Stimme möglich machen würden (vgl. Anwendungsnotiz 7), wird die vom Online-Wahlverfahren vorgegebene Lebenszyklus- und Zugriffskontrolle vom Wahlvorstand mit geeigneten technischen und organisatorischen Maßnahmen wirksam umgesetzt.

Anwendungsnotiz 25: *Der ST-Autor soll unter Berücksichtigung der benötigten nicht-EVG Hardware/Firmware/Software und den Vorgaben des Online-Wahlverfahrens konkretisieren, welche technischen und organisatorischen Maßnahmen für die wirksame Umsetzung der Lebenszyklus- und Zugriffskontrolle geeignet sind.*

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

194 **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.

Anwendungsnotiz 26: *Der ST-Autor soll unter Berücksichtigung der benötigten nicht-EVG Hardware/Firmware/Software und den Vorgaben des Online-Wahlverfahrens konkretisieren, welche technischen und organisatorischen Maßnahmen für die wirksame Umsetzung der Bereinigung geeignet sind. Der ST-Autor soll prüfen, welchen Beitrag der EVG zur Bereinigung leisten kann, und ggf. angemessene Sicherheitsziele für den EVG und funktionale EVG-Sicherheitsanforderungen ergänzen.*

4.3 Erklärung der Sicherheitsziele

195 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.

196 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.

197 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.

4.3.1 Abwehr der Bedrohungen durch den EVG

198 **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

199 **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) und
- OE.Zwischenspeicherung (da hierdurch keine verwertbaren Daten auf dem Endgerät verbleiben).

200 **T.IntegritätNachricht** Die Bedrohung wird durch das Ziel O.IntegritätNachricht abgewehrt. Das Ziel O.AuthentizitätServer gewährleistet die authentische Verbindung zum Wahlserver. Hierbei werden die EVG-Sicherheitsziele durch die folgenden Ziele der IT-Umgebung unterstützt:

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

201 **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 das Ziel O.GeheimNachricht abgewehrt, wodurch sichergestellt wird, daß ein Netzwerkangreifer weder Authentisierungsnachrichten noch Identifikationsdaten im Klartext erhält. Das Ziel O.Zwischenergebnis gewährleistet, daß keine Zwischenergebnisse ermittelt werden können, weil die Stimme während der Übertragung nicht preisgegeben wird. Das Ziel O.AuthentizitätServer gewährleistet die authentische Verbindung zum Wahlserver. Hierbei werden die EVG-Sicherheitsziele durch die folgenden Ziele der IT-Umgebung unterstützt:

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

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

- OE.AuthentizitätServer (da der Wähler 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).

203 **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).

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

- OE.ArchivierungWahlgeheimnis (da hierdurch dem Angreifer keine Zusatzdaten zur Verfügung stehen, die das Wahlgeheimnis gefährden könnten),
- 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).

Tabelle 2 Abwehr der Bedrohungen

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

4.3.2 Durchsetzung der organisatorischen Sicherheitspolitiken durch den EVG

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

206 **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).

207 **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),
- OE.Wahlserver (da hierdurch keine Schadsoftware auf dem Wahlserver ist, die den gesamten EVG verändert oder austauscht) und

208 **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).

209 **P.IntegritätWahlvorstand** Die Politik wird von dem Ziel O.Integrität-Wahlvorstand 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)

210 **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)

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

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

213 **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).

214 **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).

215 **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).

216 **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).

217 **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).

218 **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).

219 **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).

Tabelle 3 Durchsetzung der organisatorischen Sicherheitspolitiken

	P.Abbruch	P.WahlBeenden	P.Wahlende	P.Wahlgeheimnis Wahlvorstand	P.IntegritätWahlvorstand	P.Zwischenergebnis	P.Übereilungsschutz	P.Korrektur	P.Rückmeldung	P.Störung	P.Protokoll	P.OneVoterOneVote	P.AuthWahlvorstand	P.StartStimmauszählung	P.Stimmauszählung
O.StimmberechtigterWähler															
O.Beweis															
O.IntegritätNachricht															
O.Wahlgeheimnis															
O.GeheimNachricht															
O.AuthentizitätServer															
O.ArchivierungIntegrität															
O.ArchivierungWahlgeheimnis															
O.Abbruch	**X**														
O.WahlBeenden		**X**													

	P.Abbruch	P.WahlBeenden	P.Wahlende	P.Wahlgeheimnis Wahlvorstand	P.IntegritätWahlvorstand	P.Zwischenergebnis	P.Übereilungsschutz	P.Korrektur	P.Rückmeldung	P.Störung	P.Protokoll	P.OneVoterOneVote	P.AuthWahlvorstand	P.StartStimmauszählung	P.Stimmauszählung
O.Wahlende			X												
O.WahlgeheimnisWahlvorstand				X											
O.IntegritätWahlvorstand					X										
O.Zwischenergebnis						X									
O.Übereilungsschutz							X								
O.Korrektur								X							
O.Rückmeldung									X						
O.Störung										X					
O.Protokoll											X				
O.OneVoterOneVote												X			
O.AuthWahlvorstand													X		
O.StartStimmauszählung														X	X
O.Stimmauszählung															X
OE.Wahlvorbereitung		X													
OE.Beobachten															
OE.Wahlvorstand		X		X	X	X					X	X	X	X	X
OE.AuthDaten															
OE.Endgerät									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	X
OE.Speicherung															
OE.Systemzeit		X									X				
OE.Protokollschutz											X				
OE.AuthentizitätServer															
OE.ArchivierungIntegrität															
OE.ArchivierungWahlgeheimnis															
OE.GeschützteKommunikation															
OE.Zwischenspeicherung															

4.3.3 Abdeckung der Annahmen

220 Die Abdeckung der Annahmen ist durch deren erneute Darlegung als Sicherheitsziele für die Einsatzumgebung offensichtlich (vgl. Tabelle 4). 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.

Tabelle 4 Abdeckung der Annahmen

	A.Wahlvorbereitung	A.Verfügbarkeit	A.Beobachten	A.ServerRaum	A.Endgerät	A.Wahlserver	A.Speicherung	A.Wahlvorstand	A.AuthDaten	A.Systemzeit	A.Protokollschutz	A.AuthentizitätServer	A.ArchivierungIntegrität	A.ArchivierungWahlgeheimni	A.GeschützteKommunikation	A.Zwischenspeicherung
OE.Wahlvorbereitung	X															
OE.Verfügbarkeit		X														
OE.Beobachten			X													
OE.ServerRaum				X												
OE.Endgerät					X											
OE.Wahlserver						X										
OE.Speicherung							X									
OE.Wahlvorstand								X								
OE.AuthDaten									X							
OE.Systemzeit										X						
OE.Protokollschutz											X					
OE.AuthentizitätServer												X				
OE.ArchivierungIntegrität													X			
OE.ArchivierungWahlgeheimnis														X		
OE.GeschützteKommunikation															X	
OE.Zwischenspeicherung																X

5 IT-Sicherheitsanforderungen

221 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.

222 Vorbemerkung:

- **Zuweisungs**-Operationen sind **fett** gedruckt.
- *Auswahl*-Operationen sind *kursiv* gedruckt.
- VERFEINERUNGEN sind in GROßBUCHSTABEN gedruckt.
- Werte von Sicherheitsattributen sind unterstrichen dargestellt.
- Für nicht ausgeführte Operationen wird der Originaltext aus den CC übernommen.

5.1 Funktionale EVG-Sicherheitsanforderungen

223 Die Darlegung der funktionalen EVG-Sicherheitsanforderungen definiert die funktionalen Anforderungen an den EVG in Form funktionaler Komponenten aus Teil 2 der CC.

Anwendungsnotiz 27: *Wenn Anforderungen unspezifisch an die TSF gestellt werden, soll der ST Autor entscheiden, welche Anteile vom clientseitigen bzw. serverseitigen EVG erfüllt werden.*

224 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.

225 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.

226 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 clientseitigen oder serverseitigen 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.

227 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
- Wahlergebnis
- Zwischenergebnis

228 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.

229 **FAU_GEN.1 Generierung der Protokolldaten**

230 Ist hierarchisch zu: Keinen anderen Komponenten.

231 Abhängigkeiten: FPT_STM.1 Verlässliche Zeitstempel

232 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 [eindeutige Auswahl: *Minimal, Einfach, Detailliert, nicht angegeben*]; und
c) die Ereignisse aus Kapitel 1.2.4.7 sowie [Zuweisung: *weitere speziell festgelegte protokollierbare Ereignisse*].

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

233 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 [Zuweisung: *sonstige protokollierungsrelevante Information*].

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

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

234 **FAU_SAR.1 Durchsicht der Protokollierung**

235 Ist hierarchisch zu: Keinen anderen Komponenten.

236 Abhängigkeiten: FAU_GEN.1 Generierung der Protokolldaten

237 FAU_SAR.1.1 Die SERVERSEITIGE TSF muß für **den Wahlvorstand** die Fähigkeit bereitstellen, die **in Kapitel 1.2.4.7 genannten Protokoll-**

informationen und [Zuweisung: *Liste weiterer Protokoll-informationen*] aus den Protokollaufzeichnungen zu lesen.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

238 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]

239 **FDP_DAU.1 Einfache Datenauthentisierung**

240 Ist hierarchisch zu: Keinen anderen Komponenten.

241 Abhängigkeiten: Keine Abhängigkeiten.

242 FDP_DAU.1.1 Die SERVERSEITIGE TSF muß die Fähigkeit zur Generierung von Nachweisen als Gültigkeitsgarantie von **Wahldurchführungsdaten, Wahlergebnis und [Auswahl: *Protokollaufzeichnungen*, [Zuweisung: *weitere Daten*]]** bereitstellen.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

243 FDP_DAU.1.2 Die SERVERSEITIGE TSF muß [Zuweisung: *Liste der Subjekte*] 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,]

244 **FDP_IFC.1A Teilweise Informationsflusskontrolle (Wahlhandlung)**

245 Ist hierarchisch zu: Keinen anderen Komponenten.

246 Abhängigkeiten: FDP_IFF.1 Einfache Sicherheitsattribute

247 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.

248 **FDP_IFF.1A.1 Einfache Sicherheitsattribute (Wahlhandlung)**

249 Ist hierarchisch zu: Keinen anderen Komponenten.

250 Abhängigkeiten: FDP_IFC.1 Teilweise Informationsflusskontrolle

FMT_MSA.3 Initialisierung statischer Attribute

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

- **Stimmberechtigungsattribut**
- **Wahlhandlungsattribut**
- **Wahlzeitraum**

252 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.**

253 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.**

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

255 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 end-**

gültige Stimmabgabe [Regel 4] ist explizit zu verweigern, wenn das Attribut Wahlzeitraum nicht den Wert Durchführung besitzt.

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

257 Ist hierarchisch zu: Keinen anderen Komponenten.

258 Abhängigkeiten: FDP_IFF.1 Einfache Sicherheitsattribute

259 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 STIMMAUSZÄHUNG MIT FESTELLUNG DES WAHLERGEBNISSES MUß FÜR DIE WAHLDURCHFÜHRUNGSDATEN, DAS WAHLERGEBNIS UND [AUSWAHL: DIE *PROTOKOLLAUFZEICHNUNGEN*, [ZUWEISUNG: *WEITERE DATEN*]] EIN MANI-

PULATIONSSCHUTZ ALS GÜLTIGKEITSGARANTIE ERZEUGT WERDEN.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

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

261 Ist hierarchisch zu: Keinen anderen Komponenten.

262 Abhängigkeiten: FDP_IFC.1 Teilweise Informationsflusskontrolle

FMT_MSA.3 Initialisierung statischer Attribute

263 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]

264 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]

265 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 [Auswahl: *Protokollaufzeichnungen*, [Zuweisung: *weitere Daten*]] erzeugt.**

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

266 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]

267 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]

268 **FDP_IFF.5 Keine unerwünschten Informationsflüsse**

269 Ist hierarchisch zu: FDP_IFF.4 Teilweise Beseitigung der unerwünschten Informationsflüsse

270 Abhängigkeiten: FDP_IFC.1 Teilweise Informationsflußkontrolle

271 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 ANDAUEREN, DAß ALLE BEGONNENEN WAHLHANDLUNGEN BEENDET WERDEN KÖNNEN.

[VERFEINERUNG FÜR keine unerwünschten Informationsflüsse: a) …; b) …; und c) ….]

272 **FDP_SDI.2 Überwachung der Integrität der gespeicherten Daten und Reaktionen**

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

274 Abhängigkeiten: Keine Abhängigkeiten.

275 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]

276 FDP_SDI.2.2 Bei Erkennen eines Datenintegritätsfehlers muß die SERVERSEITIGE TSF **den Wahlvorstand informieren und [Zuweisung: weitere Aktionen auszuführen].**

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

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

278 Ist hierarchisch zu: Keinen anderen Komponenten.

279 Abhängigkeiten: Keine Abhängigkeiten

280 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]

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

282 Ist hierarchisch zu: Keinen anderen Komponenten.

283 Abhängigkeiten: Keine Abhängigkeiten

284 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]

285 **FDP_UCT.1 Einfache Vertraulichkeit des Datenaustausches**

286 Ist hierarchisch zu: Keinen anderen Komponenten.

287 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]

288 FDP_UCT.1.1 Die TSF muß die **SFP für Wahlhandlungen** durchsetzen, um in der Lage zu sein, IDENTIFIKATIONSDATEN, AUTHENTISIERUNGSNACHRICHTEN, STIMMZETTEL UND STIMMDATENSÄTZE vor nichtautorisierter Preisgabe geschützt zu *übertragen und empfangen*.

[VERFEINERUNG FÜR Benutzerdaten: IDENTIFIKATIONSDATEN, AUTHENTISIERUNGSNACHRICHTEN, STIMMZETTEL UND STIMMDATENSÄTZE]

289 **FDP_UIT.1 Einfache Integrität des Datenaustausches**

290 Ist hierarchisch zu: Keinen anderen Komponenten.

291 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]

292 FDP_UIT.1.1 Die TSF muß die **SFP für Wahlhandlungen** durchsetzen, um in der Lage zu sein, IDENTIFIKATIONSDATEN, AUTHENTISIERUNGSNACHRICHTEN, STIMMZETTEL, STIMMDATENSÄTZE, STIMMZETTELDATEN UND RÜCKMELDUNGEN vor *Modifizieren, Löschen, Einfügen und Wiedereinspielen* geschützt zu *übertragen und zu empfangen*.

[VERFEINERUNG FÜR Benutzerdaten: IDENTIFIKATIONSDATEN, AUTHENTISIERUNGSNACHRICHTEN, STIMMZETTEL, STIMMDATENSÄTZE, STIMMZETTELDATEN UND RÜCKMELDUNGEN]

293 FDP_UIT.1.2 Die TSF muß in der Lage sein, beim Empfang der IDENTIFIKATIONSDATEN, AUTHENTISIERUNGSNACHRICHTEN, STIMMZETTEL, STIMMDATENSÄTZE, STIMMZETTELDATEN UND RÜCKMELDUNGEN festzustellen, ob ein *Modifizieren, Löschen, Einfügen oder Wiedereinspielen* stattgefunden hat.

[VERFEINERUNG FÜR Benutzerdaten: IDENTIFIKATIONSDATEN, AUTHENTISIERUNGSNACHRICHTEN, STIMMZETTEL, STIMMDATENSÄTZE, STIMMZETTELDATEN UND RÜCKMELDUNGEN]

294 **FIA_ATD.1 Definition der Benutzerattribute**

295 Ist hierarchisch zu: Keinen anderen Komponenten.

296 Abhängigkeiten: Keine Abhängigkeiten

297 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 Wahl-

vorstand verknüpft. Vor der ersten Anforderung der kontrollierten Operation besitzt es den Wert Null.

298 **FIA_UAU.1 Zeitpunkt der Authentisierung (für Wähler)**

299 Ist hierarchisch zu: keiner anderen Komponenten.

300 Abhängigkeiten: FIA_UID.1 Zeitpunkt der Identifikation

301 FIA_UAU.1.1 Die SERVERSEITIGE TSF muß die Ausführung der **Eröffnung der Wahlhandlung und [Zuweisung: Liste weiterer von den TSF vermittelten Aktionen]** für den WÄHLER erlauben, bevor dieser authentisiert wird.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

[VERFEINERUNG FÜR Benutzer: WÄHLER]

Anwendungsnotiz 28: *Die Zuweisung hängt von der gewählten Realisierung für die Authentisierung ab (vgl. Abschnitt Anwendungsnotiz 9:). Anmeldung bei Eröffnung der Wahlhandlung: In diesem Fall ist die Liste der weiteren Aktionen leer. Anmeldung bei Stimmabgabe: In diesem Fall besteht die Liste der Aktionen aus den Operationen Einleitung der Stimmabgabe und Widerruf der Stimmabgabe (vgl. SFP für Wahlhandlungen).*

302 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]

303 **FIA_UAU.2 Benutzerauthentisierung vor jeglicher Aktion (für Wahlvorstand)**

304 Ist hierarchisch zu: FIA_UAU.1

305 Abhängigkeiten: FIA_UID.1 Zeitpunkt der Identifikation

306 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]

Anwendungsnotiz 29: *Wenn mit der erfolgreichen Authentisierung die Eröffnung einer interaktiven Sitzung für das Mitglied des Wahlvorstands verbunden ist, dann soll der ST-Autor prüfen, ob die Ergänzung der Sicherheitsanforderungen mit Komponenten der Klasse FTA angemessen ist.*

307 **FIA_UAU.6 Wiederauthentisierung (für Wahlvorstand)**

308 Ist hierarchisch zu: Keinen anderen Komponenten.

309 Abhängigkeiten: Keine Abhängigkeiten

310 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 …]

311 **FIA_UID.1 Zeitpunkt der Identifikation (für Wähler)**

312 Ist hierarchisch zu: Keinen anderen Komponenten.

313 Abhängigkeiten: Keine Abhängigkeiten

314 FIA_UID.1.1 Die SERVERSEITIGE TSF muß die Ausführung der **Eröffnung der Wahlhandlung und [Zuweisung: Liste weiterer von den TSF vermittelten Aktionen]** für den WÄHLER erlauben, bevor dieser identifiziert wird.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

[VERFEINERUNG FÜR Benutzer: WÄHLER]

Anwendungsnotiz 30: *Die Zuweisung hängt von der gewählten Realisierung für die Authentisierung ab (vgl. Abschnitt Anwendungsnotiz 9:). Anmeldung bei Eröffnung der Wahlhandlung: In diesem Fall ist die Liste der weiteren Aktionen leer. Anmeldung bei Stimmabgabe: In diesem Fall besteht die Liste der Aktionen aus den Operationen Einleitung der Stimmabgabe und Widerruf der Stimmabgabe (vgl. SFP für Wahlhandlungen).*

315 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]

316 **FIA_UID.2 Benutzeridentifikation vor jeglicher Aktion (für Wahlvorstand)**

317 Ist hierarchisch zu: FIA_UID.1

318 Abhängigkeiten: Keine Abhängigkeiten

319 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]

Anwendungsnotiz 31: *Wenn mit der erfolgreichen Identifikation die Eröffnung einer interaktiven Sitzung für das Mitglied des Wahlvorstands verbunden ist, dann soll der ST-Autor prüfen, ob die Ergänzung der Sicherheitsanforderungen mit Komponenten der Klasse FTA angemessen ist.*

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

321 Ist hierarchisch zu: Keinen anderen Komponenten.

322 Abhängigkeiten: FIA_ATD.1 Definition der Benutzerattribute

323 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]

324 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]

325 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]

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

327 Ist hierarchisch zu: Keinen anderen Komponenten.

328 Abhängigkeiten: FIA_ATD.1 Definition der Benutzerattribute

329 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]

330 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]

331 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 [Auswahl: *den Wahlvorstand, den Ablauf der Gültigkeit nach* [Zuweisung: *Zeitintervall für die Gültigkeit der Bindung*], [Zuweisung: *andere Bedingungen*]] 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]

332 **FMT_SMR.2 Einschränkungen der Sicherheitsrollen**

333 Ist hierarchisch zu: FMT_SMR.1 Sicherheitsrollen

334 Abhängigkeiten: FIA_UID.1 Zeitpunkt der Identifikation

335 FMT_SMR.2.1 Die SERVERSEITIGE TSF muß die Rollen **Wähler, Wahlvorstand und [Zuweisung: *weitere identifizierte Rollen*]** erhalten

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

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

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

337 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**
- **[Zuweisung: *weitere Bedingungen für die verschiedenen Rollen*]**

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

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

338 **FPR_ANO.1 Anonymität**

339 Ist hierarchisch zu: Keinen anderen Komponenten.

340 Abhängigkeiten: Keine Abhängigkeiten

341 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]

342 **FPR_UNL.1A Unverkettbarkeit (Netzwerk)**

343 Ist hierarchisch zu: Keinen anderen Komponenten.

344 Abhängigkeiten: Keine Abhängigkeiten.

345 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*]

346 **FPR_UNL.1B Unverkettbarkeit (Urne)**

347 Ist hierarchisch zu: Keinen anderen Komponenten.

348 Abhängigkeiten: Keine Abhängigkeiten.

349 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]

350 **FPT_RCV.1 Manuelle Wiederherstellung**

351 Ist hierarchisch zu: Keinen anderen Komponenten.

352 Abhängigkeiten: AGD_OPE.1 Benutzerhandbücher für den Betrieb

353 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 AUTORISIERUNGN 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) ….]

354 **FPT_RCV.4 Funktionelle Wiederherstellung**

355 Ist hierarchisch zu: Keinen anderen Komponenten.

356 Abhängigkeiten: Keine Abhängigkeiten

357 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]

358 **FPT_TST.1 TSF Testen**

359 Ist hierarchisch zu: Keinen anderen Komponenten.

360 Abhängigkeiten: Keine Abhängigkeiten.

361 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*]

362 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*]

363 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]

[VERFEINERUNG TSF-Code: SERVERSEITIGEM TSF-Code]

Anwendungsnotiz 32: *Der ST-Autor soll prüfen, ob die TSF das korrekte Wirken der Sicherheitsannahmen auf dem Wahlserver kontrollieren kann und ggf. die Komponente FPT_TEE.1 ergänzen.*

364 **FTA_SSL.3 Durch TSF eingeleitete Beendigung**

365 Ist hierarchisch zu: Keinen anderen Komponenten.

366 Abhängigkeiten: Keine Abhängigkeiten.

367 FTA_SSL.3.1 Die SERVERSEITIGE TSF muß VOR DER ENDGÜLTIGEN STIMMABGABE eine WAHLHANDLUNG nach [Zuweisung: *Zeitintervall der Benutzerinaktivität*] 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.]

368 **FTA_SSL.4 Durch Benutzer eingeleitete Beendigung**

369 Ist hierarchisch zu: Keinen anderen Komponenten.

370 Abhängigkeiten: Keine Abhängigkeiten.

371 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.]

372 **FTA_TSE.1 TOE-Sitzungseinrichtung**

373 Ist hierarchisch zu: Keinen anderen Komponenten.

374 Abhängigkeiten: Keine Abhängigkeiten.

375 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]

376 **FTP_TRP.1 Vertrauenswürdiger Pfad**

377 Ist hierarchisch zu: Keinen anderen Komponenten.

378 Abhängigkeiten: Keine Abhängigkeiten.

379 FTP_TRP.1.1 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 GEEGENSEITIGE 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: GEEGENSEITIGE IDENTIFIKATION VON WÄHLER UND SERVERSEITIGEM EVG]

380 FTP_TRP.1.2 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]

381 FTP_TRP.1.3 Die SERVERSEITIGE TSF muß den Gebrauch des vertrauenswürdigen Pfads für ***die Wahlhandlung*** erfordern.

[VERFEINERUNG FÜR TSF: SERVERSEITIGE TSF]

5.2 Anforderungen an die Vertrauenswürdigkeit des EVG

382 Die Anforderungen an die Vertrauenswürdigkeit, welche vom EVG erfüllt werden müssen, sind in Tabelle 5 aufgeführt. Sie enthalten die Komponenten der Vertrauenswürdigkeitsstufe EAL2 aus Teil3 der Common Criteria. Die augmentierten Komponenten aus der Klasse ALC (Kennzeichnung mit fetter Schrift) entsprechen den Anforderungen der Vertrauenswürdigkeitsstufe EAL3.

Tabelle 5 Anforderungen an die Vertrauenswürdigkeit des EVG

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

5.3 Erklärung der Sicherheitsanforderungen

383 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

384 Die Rückverfolgung der Sicherheitsanforderungen auf die Sicherheitsziele für den EVG ist in Tabelle 6 dargestellt. Die Eignung zur Abdeckung aller EVG-Sicherheitsziele wird im Folgenden nachgewiesen.

385 **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.1 und FTP_TRP.1 durch Schutz der Vertraulichkeit bei der Kommunikation des Wählers mit dem serverseitigen EVG unterstützt.

386 **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.

387 **O.IntegritätNachricht** Die Komponente FDP_UIT.1 stellt in Verbindung mit der Komponente FTP_TRP.1 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.

388 **O.AuthentizitätServer** Durch die Komponente FTP_TRP.1 wird ein vertrauenswürdiger Pfad zwischen Wähler und serverseitigem EVG aufgebaut, der logisch von anderen Kommunikationspfaden getrennt ist und eine gesicherte gegenseitige Identifi-

kation von Wähler und serverseitigem EVG bereitstellt. Für die Wahlhandlung kann Der Wähler kann am clientseitigen EVG eine Kommunikation mit dem serverseitigen EVG über den vertrauenswürdigen Pfad einleiten.

389 **O.ArchivierungIntegrität** Die Komponenten FDP_IFC.1B und FDP_IFF.1B [Regel 5] stellen sicher, daß nach der Stimmauszählung mit Feststellung des Wahlergebnisses vom serverseitigen EVG ein Manipulationsschutz für die Wahldurchführungsdaten, das Wahlergebnis und, bei Bedarf, Protokollaufzeichnungen oder weitere Daten 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.

390 **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.

391 **O.Wahlgeheimnis** Durch die Komponente FDP_UCT.1 wird in Verbindung mit der Komponente FTP_TRP.1 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.

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

393 **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.

394 **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.

395 **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.

396 **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.

397 **O.IntegritätWahlvorstand** Die Komponenten FDP_IFC.1A, FDP_IFF.1A und FDP_UIT.1 stellen in Verbindung mit den Komponenten FDP_IFC.1B, FDP_IFF.1B und FTP_TRP.1 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.

398 **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.1 in Verbindung mit der Komponente FTP_TRP.1 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.

399 **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.

400 **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 korrigieren (Komponente FDP_IFF.1A [Regel 3]) oder die Stimmabgabe sogar abzubrechen (Komponente FTA_SSL.4).

401 **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.

402 **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.

403 **O.Protokoll** Die Komponente FAU_GEN.1 stellt sicher, daß mindestens die in Kapitel 1.2.4.7 aufgelisteten Ereignisse vom serverseitigen EVG protokolliert werden, und die Komponente FAU_SAR.1 gewährleistet, daß der Wahlvorstand die Protokollaufzeichnungen durchsehen kann.

404 **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.

405 **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).

406 **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]).

407 **O.Stimmauszählung** Die Komponenten FDP_IFC.1B, FDP_IFF.1B [Regel 1] und FDP_RIP.1B stellen sicher, daß beim Start der Wahldurchführung keine Stimm-

datensätze in der Urne gespeichert 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.

Tabelle 6 Abdeckung der Sicherheitsziele an den EVG

	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
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.1	X						X	X						X									
FDP_UIT.1			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_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.1	X		X	X			X	X					X	X									

5.3.2 Gegenseitige Unterstützung der funktionalen Sicherheitsanforderungen an den EVG

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

409 Die funktionalen Komponenten wurden aus den vordefinierten CC Komponenten ausgewählt. Die Verwendung der Verfeinerungsoperationen erfüllen die CC Richtlinien.

410 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.

411 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

412 Tabelle 7 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.

Tabelle 7 Abhängigkeiten zwischen SFR für den EVG

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.1	FTP_ITC oder FTP_TRP.1 FDP_ACC.1 oder FDP_IFC.1	FTP_TRP.1 FDP_IFC.1A
FDP_UIT.1	FDP_ACC.1 oder FDP_IFC.1 FTP_ITC.1 oder FTP_TRP.1	FDP_IFC.1A FTP_TRP.1
FIA_USB.1A	FIA_ATD.1	Done
FIA_USB.1B	FIA_ATD.1	Done

SFR	Abhängigkeiten	Auflösung
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	
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_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.1	Keine	

5.3.4 Erklärung der Anforderungen an die Vertrauenswürdigkeit des EVG

413 Die ausgewählten Anforderungen an die Vertrauenswürdigkeit enthalten mit EAL 2 eine in Teil 3 der CC beschriebene Vertrauenswürdigkeitsstufe.

414 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.

415 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.

Anhang A. Verantwortung der Wahlveranstalter

a. Alternative Wahlform

416 Der Wahlveranstalter soll eine alternative Wahlform anbieten, solange die Online-Wahl nicht universell zugänglich ist.

417 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

418 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.

419 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

420 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 Interessensgemeinschaften[4] sich gegenseitig kontrollieren (damit sichergestellt wird, daß auf den EVG nur zwecks Wahlstart, -wiederanlauf und -ende sowie Ergebnisberechnung zugegriffen wird).

421 Der Wahlveranstalter soll dafür sorgen, daß über sämtliche Zugriffe auf den serverseitigen EVG oder den Wahlserver sowie der daran beteiligten Personen, Buch geführt wird.

[4] 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.

422 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.

423 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

424 Die Wahlveranstalter sollten definieren, inwieweit Beobachter die Handlungen des Wahlvorstandes (wie Initialisierung, Starten und Beenden der Wahldurchführung sowie Ergebnisberechnung) beobachten und kommentieren können.

425 Im vorliegenden Schutzprofil ist eine Wahlbeobachtung speziell für die Online-Wahl während der Wahldurchführung inkl. der Stimmauszählung nicht vorgesehen. Dennoch wird empfohlen, Wahlbeobachter 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

426 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 eingesetzte Authentisierungsmerkmale sollten dem Wahlwert entsprechend sicher festgelegt werden und dem anerkannten Stand der Technik entsprechen.

427 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.

428 Es liegt in der Verantwortlichkeit des Wahlveranstalters die Wähler zu informieren, wie sie mit ihren Identifikations- und Authentisierungsmerkmalen umgehen sollen.

429 Es liegt in der Verantwortung des Wahlveranstalters, daß der Wähler die in der Wahlberechtigungsliste enthaltenen Einträge überprüfen und ggf. Berichtigung verlangen kann.

f. Wählervertrauen

430 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 ge-

macht werden. Es wird daher empfohlen, die Wähler in klaren und einfachen Worten über die Art und Weise der elektronischen Stimmabgabe zu informieren.

431 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.

432 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.

433 Der Wahlveranstalter ist dafür verantwortlich, dem Wähler angemessene Hinweise für die unbeobachtete Stimmabgabe zu geben.

434 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.

435 Der Wahlveranstalter soll die Online-Wahl so gestalten, daß die Registrierung zur Teilnahme kein Hindernis für den Wähler darstellt.

436 Vor dem Einsatz des Online-Wahlsystems wird eine Veröffentlichung der Darstellung der Implementierung zumindest einer Fachöffentlichkeit empfohlen.

g. Verfügbarkeit

437 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.

438 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.

439 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 Notfallszenarios. Zu den Notfallszenarios kann beispielsweise ein Rollback zur reinen Papierwahl gehören.

440 Der Wahlveranstalter soll dafür sorgen, daß er vom Wahlvorstand über sämtliche Störungen und Ausfälle informiert wird.

h. Stimmzettel

441 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“).

442 Es liegt in der Verantwortung der Wahlveranstalter zu entscheiden, ob der Wähler darauf hingewiesen wird, daß er dabei ist, eine ungültige Stimme abzugeben.

443 Es liegt in der Verantwortung der Wahlveranstalter zu entscheiden, inwieweit das Online-Wahlsystem behinderte Menschen bei ihrer Stimmabgabe unterstützen können soll.

i. Sonstiges

444 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.

445 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.

446 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.

447 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