BSI-PP-0031

Digitales Wahlstift-System

Version 1.0.1

28.02.2007

Freie und Hansestadt Hamburg

INHALTSVERZEICHNIS

Vorwort

Die Behörde für Inneres (BfI) der Freien und Hansestadt Hamburg nimmt neben anderen auch die Funktion des Landeswahlamtes wahr. Als Geschäftsstelle des Landeswahlleiters ist das Landeswahlamt für die Vorbereitung und Durchführung von Wahlen sowie Volksabstimmungen zuständig. Neben der Umsetzung von Rechtsvorschriften in fachliche Vorgaben zur Wahldurchführung unterstützt es die Bezirke bei der Wahlorganisation (http://www.wahlen.hamburg.de).

Durch den Einsatz eines Digitalen Wahlstift-Systems soll gewährleistet werden, dass auch nach Änderung des Wahlrechts für die Bürgerschaft und die Bezirksversammlungen unter Einführung von Kumulieren und Panaschieren die Feststellung des vorläufigen amtlichen Endergebnisses noch in der Wahlnacht erfolgen kann.

Das Deutsche Forschungszentrum für Künstliche Intelligenz (DFKI) hat im Auftrag der Freien und Hansestadt Hamburg und in enger Abstimmung mit dem Landeswahlamt das vorliegende Schutzprofil erstellt (http://www.dfki.de/fuse).

Das Schutzprofil (Protection Profile – PP) enthält die implementierungsunabhängige Darstellung von Sicherheitsanforderungen, die den relevanten Sicherheitszielen für ein Digitales Wahlstift-System entsprechen. Das PP ist wiederverwendbar und definiert die Anforderungen, die als nützlich und als wirksam nachgewiesen sind, um die identifizierten Schutzziele zu erfüllen. Es eignet sich daher zum Gebrauch als Darlegung der Anforderungen an einen Evaluationsgegenstand (EVG). Die Common Criteria (CC) enthalten die Evaluationskriterien, die es einem Evaluator erlauben auszusagen, dass ein EVG die Anforderungen des PP einwandfrei erfüllt.

1 PP-Einführung

Die PP-Einführung enthält Informationen zur Dokumentenverwaltung und allgemeine Informationen, die zum Führen eines PP-Registers benötigt werden.

1.1 PP-Identifikation

Die PP-Identifikation stellt die Kennzeichnungen und beschreibenden Informationen bereit, die benötigt werden, um das Schutzprofil zu identifizieren, katalogisieren, registrieren und auf das Schutzprofil zu verweisen.

Titel	Digitales Wahlstift-System
Version	1.0.1
Datum	28.02.2007
Entwickler	Melanie Volkamer, Roland Vogt Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI) GmbH Prüfstelle für IT-Sicherheit http://www.dfki.de/
Antragsteller	Behörde für Inneres, Freie und Hansestadt Hamburg
Registrierung	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Zertifizierungskennung	BSI-PP-0031
CC-Version	Für die Erstellung des PP wurde CC 2.3 verwendet.
Konformität zu CC (Teil 2 und Teil 3)	Das PP ist konform zu Teil 2 und Teil 3 der CC 2.3.
EAL-Stufe	Das PP verwendet eine Erweiterung von EAL 3 mit den Komponenten ADV_SPM.1 und AVA_MSU.3 (ersetzt AVA_MSU.1).

1.2 PP-Übersicht

Die PP-Übersicht fasst das Schutzprofil verbal zusammen. Sie ist genügend detailliert, so dass ein potentieller Benutzer des PP feststellen kann, ob es für ihn von Interesse ist. Die Übersicht kann auch allein als Zusammenfassung in Katalogen und Registern der Schutzprofile verwendet werden.

1.2.1 Kurzbeschreibung

Das Schutzprofil (Protection Profile – PP) „Digitales Wahlstift-System“ bezieht sich auf die technische Wahlunterstützung im Wahllokal und zielt insbesondere auf politische Wahlen ab. Es umfasst die Mindestanforderungen an die IT-Sicherheit von technischen Systemen zur Wahlunterstützung, die auf der Verwendung eines Digitalen Stiftes beruhen.

Der Einsatz des Digitalen Wahlstift-Systems läuft folgendermaßen ab:

Der Wähler erhält vom Wahlvorstand in seinem Wahllokal außer den mit einer Rasterung bedruckten Stimmzetteln auch einen Digitalen Wahlstift ausgehändigt. Dieser wird einer Dockingstation entnommen, die dafür sorgt, dass der Stift auf seine Funktionsfähigkeit überprüft und freigeschaltet wird. Damit kreuzt der Wähler in der Wahlkabine seine Kandidaten in den dafür vorgesehenen Feldern an. Anschließend gibt er den Stift wieder zurück und wirft die Stimmzettel in die Wahlurne.

Das Besondere an dem verwendeten Stift ist, dass er außer der Schreibmine eine Kamera, oder genauer, ein elektronisches Auge besitzt. Das elektronische Auge erfasst über die kaum sichtbare feine Rasterung des Papiers die genaue Position der Kreuze auf den Stimmzetteln. Die so von dem Digitalen Wahlstift aufgenommenen Daten werden im Beisein des Wählers über eine zweite Dockingstation auf einen Computer übertragen und dort gespeichert. Anschließend werden die im Stift gespeicherten Daten gelöscht und der Stift wird gesperrt, um eine erneute Stimmabgabe zu verhindern.

Falls der Wahlvorstand feststellt, dass der Wähler nicht wahlberechtigt ist, oder falls der Wähler seine Stimmabgabe vor der endgültigen Speicherung in der elektronischen Urne revidieren möchte, müssen die auf dem Stift enthaltenen Stimmen gelöscht und der Stift gesperrt werden. Daran anschließend kann der Stift erst wieder benutzt werden, wenn er erneut aktiviert wird.

Die elektronisch abgegebenen Stimmen werden lokal gespeichert. Die Bewertung der Daten erfolgt direkt im Wahllokal. Das Auszählen der Stimmen von Hand entfällt. Es bleibt zwar grundsätzlich möglich, ist jedoch sehr aufwändig und langwierig. Eine Feststellung des Wahlergebnisses auf Basis der elektronisch abgegebenen Stimmen durch den Wahlvorstand kann bereits kurz nach Schließung der Wahllokale erfolgen; das vorläufige amtliche Endergebnis steht somit frühzeitig fest.

Die Erstellung des Wählerverzeichnisses erfolgt wie bisher. Das Wählerverzeichnis steht am Wahltag in gedruckter Form zur Verfügung. Die Prüfung der Wahlberechtigung und Kennzeichnung der Wähler im Wählerverzeichnis erfolgt manuell durch den Wahlvorstand, also ohne technische Unterstützung. Diese Vorgänge sind daher auch nicht Bestandteil dieses Schutzprofils.

1.2.2 Motivation für das Digitale Wahlstift-System

Die Wähler sollen mit dem Digitalen Wahlstift-System ihre Stimmen abgeben können. Folgende zum Teil allgemeinen, aber auch spezifischen Vorteile sind damit verbunden.

1. Die Stimmabgabe mit dem Digitalen Wahlstift erfolgt in einem den Wählern vertrauten Verfahren und ist daher überschaubar und leicht handhabbar.
2. Die Auszählung elektronischer Stimmen erfolgt schneller und einfacher. Dies gilt insbesondere für Verfahren, die die Möglichkeit zum Kumulieren und Panaschieren anbieten.
3. Typische Fehler bei der manuellen Auszählung, z.B. Übertragungsfehler bei Verwendung von Auszählungslisten, werden vermieden.
4. Es bleibt grundsätzlich möglich, das Wahlergebnis durch manuelle Auszählung der Papierstimmzettel zu überprüfen.
5. Das Digitale Wahlstift-System entspricht dem Trend zur Einführung elektronischer Mittel zur Wahlunterstützung im Besonderen und elektronischer Wahlen im Allgemeinen.
6. Das Digitale Wahlstift-System bietet die Perspektive, komplexe Wahlverfahren ohne zusätzlichen Personalbedarf durchzuführen und damit zumindest langfristig die Kosten zu senken.

1.3 PP-Organisation

Die wesentlichen Bestandteile des Schutzprofils sind die EVG-Beschreibung, die EVG-Sicherheitsumgebung, die Sicherheitsziele, die IT-Sicherheitsanforderungen und die Erklärung.

Die **EVG-Beschreibung** liefert allgemeine Informationen über den EVG, dient als Hilfe zum Verständnis der Sicherheitsanforderungen und liefert Zusammenhänge für die Evaluation des Schutzprofils. Es werden die Art des Produkts und die allgemeinen IT-Leistungsmerkmale des EVG beschrieben. In den Abschnitten EVG-Abgrenzung und Betriebsumgebung des EVG werden die Bestandteile des EVG und seine Einbettung in die Betriebsumgebung beschrieben.

Die **EVG-Sicherheitsumgebung** beschreibt Sicherheitsaspekte der Umgebung, in welcher der EVG verwendet wird und die Art und Weise, wie er zu gebrauchen ist. Die EVG-Sicherheitsumgebung beinhaltet Beschreibungen von

a) Annahmen in Bezug auf die Umgebung, in der der EVG eingesetzt wird,

b) Bedrohungen, die vom EVG abgewendet werden sollen, und

c) organisatorischen Sicherheitspolitiken, die vom EVG durchzusetzen sind.

Die **Sicherheitsziele** legen (produktunabhängig) den Zweck des Schutzprofils dar. Dazu gehört, wie der EVG erkannten Bedrohungen begegnet und wie er ausgewiesene organisatorische Sicherheitspolitiken und Annahmen abdeckt. Für jedes Sicherheitsziel ist festgelegt, ob es für den EVG oder die Umgebung gilt.

Das Kapitel **IT-Sicherheitsanforderungen** stellt, in separaten Teilabschnitten, detaillierte Sicherheitsanforderungen für den EVG und seine Umgebung zur Verfügung. Die EVG-Sicherheitsanforderungen sind wie folgt unterteilt:

a) Funktionale Sicherheitsanforderungen an den EVG und

b) Anforderungen an die Vertrauenswürdigkeit des EVG

Die **Erklärung** weist nach, dass das Schutzprofil eine vollständige und zusammengehörige Menge von IT-Sicherheitsanforderungen ist und dass ein konformer EVG die Sicherheitserfordernisse wirksam erfüllen würde. Die Erklärung besteht aus zwei Hauptteilen. Zuerst wird anhand einer Erklärung zu den Sicherheitszielen gezeigt, dass die Sicherheitsziele auf alle in der EVG-Sicherheitsumgebung genannten Aspekte zurückgeführt werden können und dass sie geeignet sind diese abzudecken. Dann wird anhand einer Erklärung zu den Sicherheitsanforderungen gezeigt, dass die Sicherheitsanforderungen (für den EVG wie auch für die Umgebung) auf die Sicherheitsziele zurückgeführt werden können und dass sie geeignet sind, diese Ziele zu erreichen.

2 EVG-Beschreibung

Dieser Teil des PP beschreibt den EVG zur Erleichterung des Verständnisses seiner Sicherheitsanforderungen und geht auf den Produkttyp und die allgemeinen IT-Leistungsmerkmale des EVG ein. Die EVG-Beschreibung ist ein Hilfsmittel zum Verständnis der EVG-Sicherheitsanforderungen.

2.1 Art des Produktes

Der EVG ist ein Wahlgerät, das

- die Stimmabgabe mit Digitalen Wahlstiften,
- die Registrierung der Stimmen in einer zentralen elektronischen Urne im Wahllokal,
- die Bewertung und Auszählung der in der Urne gespeicherten Stimmen,
- die Feststellung und den Ausdruck des Ergebnisses und
- die Protokollierung der in Tabelle 3 aufgelisteten Ereignisse

ermöglicht.

Der EVG besteht somit aus

- den Digitalen Wahlstiften und zugehörigen Dockingstationen (es werden mind. drei Stationen benötigt; s. Abschnitt 2.1.1),
- ihrer Firmware zur Aufzeichnung der Stimmen,
- Dateien/Datenbanken zur Speicherung der Stimmen (elektronische Urne) und
- Software zur Kontrolle der Abläufe der Wahlhandlung, Bewertung, Auszählung und Feststellung.

Ein Digitaler Wahlstift wird in Verbindung mit speziell gerasterten Papierstimmzetteln dazu benutzt, handschriftliche Kennzeichnungen zu erfassen, zu speichern und auf einen Computer zu übertragen. Dazu sind im Digitalen Wahlstift eine Kugelschreibermine, eine Kamera (elektronisches Auge), ein Prozessor, ein Datenspeicher, eine Kommunikationseinheit und eine Batterie integriert. Die Kamera erfasst während des Schreibens das Punktraster auf dem Stimmzettel. Diese Daten werden im Digitalen Wahlstift gespeichert und über die Kommunikationseinheit in einer Dockingstation auf einen Computer übertragen. Die Funktionen des Digitalen Wahlstifts werden von einer darin befindlichen Firmware gesteuert.

Eine Verkabelung im Wahllokal ist erforderlich, um die Stimmen vom Stift in die elektronische Urne zu transportieren, um am Ende das Ergebnis zum Drucker schicken zu können und um die Wahldaten auf einen transportablen Datenspeicher zu übertragen. Es besteht darüber hinaus keine Möglichkeit eine externe Verbindung zum EVG oder seiner IT-Umgebung aufzunehmen (insbesondere keine drahtlose Verbindung).

2.1.1 Ablauf des Wahlvorgangs im Wahllokal

Der grundsätzliche Ablauf des Wahlvorgangs im Wahllokal ist in Abbildung 1 dargestellt. Dieser Prozess entspricht den gewöhnlichen Rahmenbedingungen politischer Wahlen und muss vom EVG technisch unterstützt werden. Durch den Einsatz des digitalen Wahlstifts wird sich am Ablauf im Wahllokal grundsätzlich nichts ändern.

Der Wahlvorgang beginnt für den Wähler mit Betreten des Wahllokals. Ein Wahlhelfer stellt durch Sichtkontrolle der Wahlbenachrichtigungskarte fest, ob sich der Wähler im richtigen Wahllokal befindet. Dann händigt der Wahlhelfer dem Wähler die Stimmzettel und den Digitalen Wahlstift aus. Er entnimmt dazu den Stift einer Dockingstation, die den Stift auf Funktionsfähigkeit überprüft und ihn zur Aufzeichnung der Stimmabgabe aktiviert. Der Wähler geht in die Wahlkabine und trifft seine Wahlentscheidung durch Kennzeichnung des Stimmzettels mit dem Digitalen Wahlstift.

Danach tritt der Wähler an den Tisch des Wahlvorstandes. Ein Wahlhelfer überprüft anhand des Wählerverzeichnisses die Wahlberechtigung des Wählers. Ist der Wähler wahlberechtigt, gibt ein weiterer Wahlhelfer die zweite Dockingstation zur endgültigen Stimmabgabe frei. Der Wähler steckt den Stift in die Dockingstation. Auf dem zum Wähler gewandten Bildschirm wird die Stimmenübertragung für den Wähler visualisiert, so dass er sicher sein kann, dass seine Stimmabgabe erfolgt ist. Die Papierstimmzettel wirft er in eine Wahlurne. Damit ist der Wahlvorgang abgeschlossen.

Anmerkung: Die Papierstimmzettel müssen im Wahllokal in eine Wahlurne geworfen werden, damit sichergestellt ist, dass Wähler ihre Stimmabgabe an Hand der Papierstimmzettel nicht gegenüber Dritten beweisen können. Außerdem können nur so die Papierstimmzettel überprüft oder im Fall eines Totalausfalls des Digitalen Wahlstift-Systems manuell ausgezählt werden.

Falls der Wahlvorstand feststellt, dass der Wähler nicht wahlberechtigt ist oder falls der Wähler seine Kennzeichnung des Stimmzettels vor der endgültigen Speicherung revidieren möchte, steht eine dritte Dockingstation bereit, die die auf dem Stift enthaltene Kennzeichnung löscht und den Stift sperrt. Die Papierstimmzettel müssen in diesen Fällen unter Aufsicht des Wahlvorstands vernichtet werden. Der Stift kann erst wieder benutzt werden, wenn er in der dafür vorgesehenen ersten Dockingstation überprüft und aktiviert wurde.

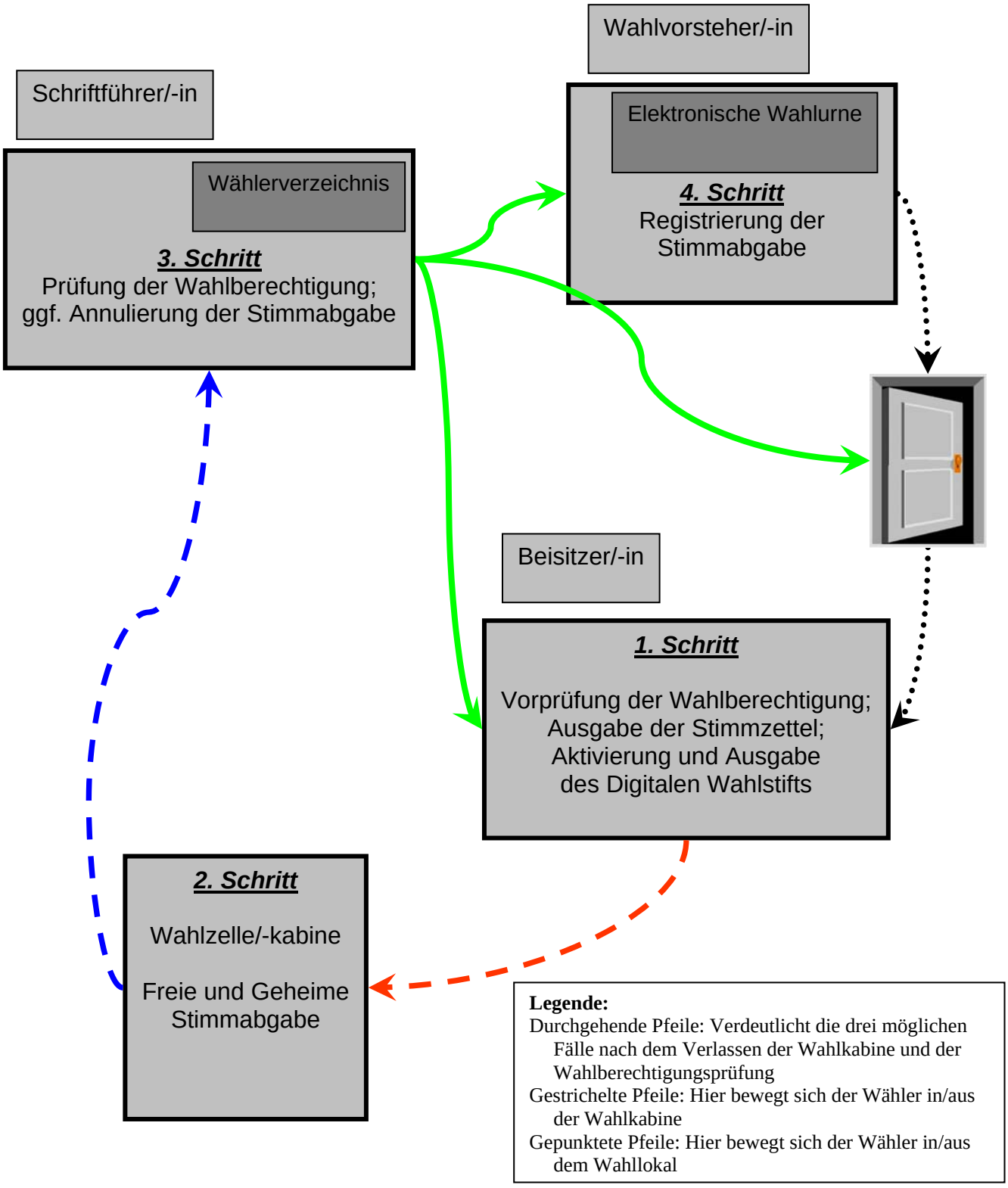

Abbildung 1: Ablaufskizze des Wahlvorgangs im Wahllokal

Die Aufteilung der Funktionen auf drei Dockingstationen wird als notwendig angesehen, um den Wahlablauf gegenüber dem Wahlberechtigten und dem Publikum transparent und glaubwürdig darstellen zu können und ein Fehlverhalten der Wähler und des Wahlvorstandes zu minimieren:

a) Für den einzelnen Wähler muss aus Gründen der Transparenz während seiner Anwesenheit im Wahllokal der Wahlvorgang eingeleitet (Aktivierung) und abgeschlossen werden (Registrierung/Annullierung). Zur Einleitung des Wahlvorgangs wird der Wahlstift initialisiert und für die Aufzeichnung freigeschaltet (Aktivierung). Der Stift ist leer und zur Stimmaufzeichnung bereit. Zum Abschluss der Wahlvorgangs wird der Stift entweder ausgelesen und geleert (Registrierung – die Stimmen werden in der elektronischen Urne gespeichert) oder nur geleert (Annullierung – die Stimmabgabe wird verhindert). Der Stift ist jetzt leer, aber noch nicht wieder zur Stimmaufzeichnung bereit. Diese Vorgänge müssen in zwei getrennten Schritten durchgeführt werden, weil sonst der nächste Wähler bei Aushändigung des Stiftes nicht einschätzen kann, ob dieser geleert worden ist. Nur durch die Trennung von Registrierung und erneuter Aktivierung kann technisch ausgeschlossen werden, dass zwei Wähler ihre Stimmen versehentlich mit einem Entladungsvorgang abgeben. Eine Verteilung dieser beiden Schritte auf verschiedene Dockingstationen ist zu bevorzugen, weil sie sich dann auch nahtlos in die typischen arbeitsorganisatorischen Abläufe im Wahllokal einfügen lassen, denn gewöhnlich ist der Ort der Stimmzettelausgabe räumlich von der Wahlurne getrennt. Die verschiedenen Funktionen sind so bereits durch den Aufstellungsort der Dockingstationen deutlich unterscheidbar.

b) Es muss die Möglichkeit geben, Stimmen vom Stift in die elektronische Urne zu verschieben (registrieren) und Stimmen vom Stift ohne Speicherung zu löschen (annullieren). Die Unterscheidung zwischen beiden Vorgängen erzwingt einen Bedienschritt, weil die Entscheidung vom Wahlvorstand getroffen wird. Dieser Bedienschritt kann sehr wirksam durch die Verwendung von zwei Dockingstationen für die beiden unterschiedlichen Vorgänge kontrolliert werden. Es genügt eine deutliche Kennzeichnung der Stationen, um Wähler und Wahlvorstand die jeweiligen Funktionen zu verdeutlichen. Bei Verwendung einer einzigen Dockingstation wäre neben dem Einsetzen des Stiftes eine zusätzliche Handlung erforderlich, die schwerer zu kontrollieren ist. So ist insbesondere nicht klar, von wem sie ausgeführt werden sollte.

   - Ausführung durch den Wahlvorstand: Wie kann der Wähler nachvollziehen, dass seine Stimmabgabe registriert wird?

   - Ausführung durch den Wähler: Wie kann der Wahlvorstand gewährleisten, dass die Stimmabgabe annulliert wird?

Das Modell „Drei Dockingstationen“ erfüllt folgendes Prinzip: Die Stimmen eines Wählers sind nur während „seines“ Wahlvorgangs auf dem Stift gespeichert, d.h. nur solange dieser Wähler die Kontrolle über den Stift hat. Sonst ist der Stift leer und die Stimmaufzeichnung ist gesperrt.

2.1.2 Abgrenzung des EVG

Weder der Aufdruck der Rasterung auf dem Papierstimmzettel noch der Papierstimmzettel selbst ist Bestandteil des EVG. Der EVG kann mehrere baugleiche Digitale Wahlstifte als Stimmabgabegeräte umfassen. Für den beschriebenen Ablauf des Wahlvorgangs sind mindestens drei Dockingstationen (jeweils eine Station für Aktivierung, Registrierung, Annullierung) erforderlich. Pro Wahllokal gibt es eine elektronische Urne, in der alle Stimmen gespeichert sind.

Komponenten, die außerhalb des Schutzprofils liegen:

Nach der Auszählung der elektronischen Stimmen wird das Ergebnis ausgedruckt. Der Drucker ist nicht Teil des EVG.

Der EVG speichert die Stimmen in der elektronischen Urne und das Ergebnis manipulationssicher ab. Diese Daten werden zeitgleich redundant auf einem transportablen Datenspeicher gespeichert. Das transportable Speichermedium ist nicht Teil des EVG.

Ebenso bleiben die Wahlzentralen, die aus den Ergebnissen der einzelnen Wahllokale das Gesamtergebnis ermitteln, außerhalb der Betrachtung des Schutzprofils.

Die Erhebung von statistischen Daten ist nicht Teil der Sicherheitsfunktionalität des EVG.

Zusammenfassend gehören weder der Drucker, noch das transportable Speichermedium, noch die Software in der Wahlzentrale, noch statistische Daten zum EVG.

Es ergeben sich daraus folgende externe Schnittstellen:

EVG – Drucker (Druckerschnittstelle)

EVG – transportables Speichermedium

EVG – Dockingstationen (Benutzerschnittstelle zur Steuerung der Wahlvorgänge)

EVG – Bildschirm/Tastatur (Benutzerschnittstelle)

ANWENDUNGSBEMERKUNG

Der EVG wird vor der Wahl in benötigter Stückzahl durch Integration der Wahlvorschläge für die Wahl konfiguriert. Dieser Arbeitsschritt erfolgt durch den Administrator (in der Regel ein vertrauenswürdiger Dienstleister). Der Wahlvorstand nimmt also einen fertig konfigurierten EVG in Betrieb.

Falls Stimmen nicht eindeutig als gültige oder ungültige Stimmen erkannt werden, zeigt der EVG diese dem Wahlvorstand nach dem Schluss der Wahlhandlung an und erfasst dessen Entscheidung über die Gültigkeit oder Ungültigkeit. Diese Stimmen gehen entsprechend der Entscheidung des Wahlvorstandes in das Ergebnis ein.

Falls der EVG zusätzlich die Möglichkeit bietet, Daten für die repräsentative Wahlstatistik zu erheben, dann müssen diese die Sicherheitsanforderungen auch erfüllen. Insbesondere muss die Anonymisierung der Stimmen/Wählerdaten gemäß der rechtlichen Vorgabe gewährleistet werden.

Die Bereinigung (Löschen aller Daten) und Deinstallation des EVG soll nach dem Ende der Wahl durch den Administrator (Dienstleister) erfolgen. Sie darf auch nur durch ihn erfolgen, d.h. die auf den Administrator beschränkte Berechtigung wird technisch durch die Zugangs- und Zugriffskontrolle in der IT-Umgebung durchgesetzt. Dem Wahlvorstand stehen keine technischen Möglichkeiten zur Deinstallation zur Verfügung, und er kann damit auch versehentlich keine Daten löschen.

2.2 Generelle Sicherheitserwartungen an den EVG

Die generellen Sicherheitserwartungen werden von den allgemeinen Grundsätzen einer freien, gleichen, geheimen, allgemeinen und unmittelbaren Wahl abgeleitet. Zusammenfassen lassen sich die Sicherheitserwartungen wie folgt:

1. Zu keinem Zeitpunkt darf eine Zusammenführung von Wähler und abgegebener Stimme hergestellt werden können. Eine Zuordnung darf auch nicht über die Zeit oder die Reihenfolge der Stimmabgaben ableitbar sein. Darüber hinaus darf das Digitale Wahlstift-System dem Wähler nicht die Möglichkeit geben, seine Stimme gegenüber anderen zu beweisen *(Anonymität und Quittungsfreiheit: Grundsatz der geheimen und freien Wahl).*
2. Jeder Wähler darf seine Stimmen nur einmal abgeben, und die Stimmen dürfen auch nur einmal gespeichert werden. Umgekehrt muss der Wähler aber auch die Möglichkeit haben, seine Stimmen einmal abzugeben *(Grundsatz der allgemeinen und gleichen Wahl).*
3. Es darf an keiner Stelle – weder bei der Stimmabgabe noch bei der Speicherung – möglich sein, Stimmen zu verändern oder zu löschen. Das unberechtigte Hinzufügen von Stimmen in die Urne muss ausgeschlossen werden *(Integrität: Grundsatz der allgemeinen und gleichen Wahl).*
4. Die Berechnung von Zwischenergebnissen vor dem Schluss der Wahlhandlung muss ausgeschlossen werden *(Grundsatz der geheimen und gleichen Wahl).*
5. Das Ergebnis muss korrekt ermittelt werden, insbesondere müssen alle abgegebenen gültigen Stimmen auch gezählt werden (*Korrektheit: Grundsatz der allgemeinen und gleichen Wahl).*
6. Der EVG muss eine Wiederanlauffunktion definieren, falls es zu einer technischen Betriebsstörung oder -unterbrechung kommt. Dabei muss auch der Gefahr des Verlusts oder der Veränderung bereits gespeicherter Stimmen geeignet begegnet werden. *(Robustheit: Grundsatz der allgemeinen und gleichen Wahl).*

Es wird angenommen, dass der Wahlvorstand vertrauenswürdig ist und den EVG nicht absichtlich manipuliert. Generell wird angenommen, dass nur in der Wahlkabine ein Manipulationsversuch am EVG stattfinden kann, da hier die Wähler unbeobachtet sind. Eine weitere Angriffsgelegenheit bietet der Transport der Daten nach Wahlende vom EVG zur Wahlzentrale.

2.3 Allgemeine IT-Leistungsmerkmale

Wahlvorgang Um den gewöhnlichen Ablauf des Wahlvorgangs abbilden zu können, muss der EVG für jeden Digitalen Wahlstift folgende Funktionen zur Verfügung stellen:

- Aktivierung der Stimmabgabe (Freigabe für die Aufzeichnung von Stimmen)
- Annullierung der Stimmabgabe (bei Irrtum durch den Wähler oder nicht vorhandener Wahlberechtigung und Löschen der Daten auf dem Stift)
- Registrierung der Stimmabgabe (endgültige Speicherung der Stimmen in der zentralen elektronischen Urne und Löschen der Daten auf dem Stift)

Für jeden Digitalen Wahlstift sind damit die Übergänge zwischen den in Tabelle 1 beschriebenen Betriebszuständen definiert.

Name	Beschreibung
Neutral	Stift ist leer; keine Aufzeichnung möglich
Aktiv	Stift zeichnet die Stimmabgabe auf und speichert die Daten

Tabelle 1: Betriebszustände eines Digitalen Wahlstifts

Aktivierung der Stimmabgabe Wenn eine Stimme im EVG endgültig gespeichert wurde, ist durch eine Funktionsprüfung sicherzustellen, dass der EVG für den nächsten Wähler aktiviert werden kann. Die vorherige Stimme darf dem nächsten Wähler nicht zugänglich sein. Es muss erkennbar sein, dass der Digitale Wahlstift aktiviert ist.

Annullierung der Stimmabgabe Falls der Wahlvorstand feststellt, dass der Wähler nicht wahlberechtigt ist, oder falls der Wähler seine Stimmabgabe vor der endgültigen Speicherung in der elektronischen Urne revidieren möchte, muss die auf dem Stift enthaltene Stimmabgabe gelöscht und der Stift gesperrt werden. Daran anschließend kann der Stift erst wieder benutzt werden, wenn er erneut aktiviert wird.

Registrierung der Stimmabgabe Es muss für den Wähler erkennbar sein, dass der Wahlvorgang abgeschlossen ist, die Stimme registriert und der Stift anschließend geleert wurde. Die endgültige Stimmabgabe darf nur einmal erfolgen.

Bei technischen Störungen während der Registrierung der Stimmabgabe können Zweifel über die endgültige Speicherung nicht ausgeschlossen werden. Eine erneute Registrierung kann aber zu einer doppelten Speicherung führen. Diese Gefahr kann vermindert werden, weil die im Digitalen Wahlstift aufgezeichneten Stimmen mit hoher Wahrscheinlichkeit eindeutig sind. Der EVG kann somit Duplikate erkennen und soll ihre erneute Speicherung verhindern.

Digitaler Wahlstift in der Wahlkabine Der Digitale Wahlstift muss besonders vor Manipulationen seiner Hardware oder Firmware in der Wahlkabine geschützt sein. Austausch oder Manipulation der Hardware sollen leicht erkennbar sein. Austauch oder Manipulation der Firmware soll vom EVG automatisch widerstanden werden.

Elektronische Wahlurne Es gibt eine zentrale elektronische Wahlurne pro Wahllokal, in der jede Stimme unmittelbar nach der Abgabe gespeichert wird. Die unberechtigte Speicherung von Stimmen wird vom Wahlvorstand verhindert. Stimmen können ausschließlich während der Wahlhandlung in der Urne gespeichert werden. Eine andere Operation ist während der Wahlhandlung mit der Urne nicht möglich. Insbesondere können keine Stimmdatensätze angezeigt, verändert oder gelöscht und keine Zwischenergebnisse berechnet werden. Nach Schluss der Wahlhandlung liegen alle abgegebenen Stimmen des Wahllokals in der zentralen elektronischen Wahlurne vor. Hieraus wird dann das Ergebnis berechnet.

Bedienung durch den Wahlvorstand Die Bedienungsmöglichkeit des EVG durch den Wahlvorstand ist auf die folgenden Aktionen beschränkt, womit die Übergänge zwischen den in Tabelle 2 beschriebenen Betriebszuständen einer elektronischen Urne definiert sind:

- Beginn der Wahlhandlung (Stimmabgabe möglich)
- Kontrolle des Wahlvorgangs (Aktivierung, Annullierung, Registrierung)
- Schluss der Wahlhandlung (keine Stimmabgabe mehr möglich)
- Entscheidung über unklare Stimmen
- Ergebnisermittlung
- Ergebnisfeststellung

Zusätzlich kann der Wahlvorstand nach einer technischen Störung oder Unterbrechung den geschützten Wiederanlauf auslösen. Darüber hinausgehende notwendige administrative Handlungen werden für eine konkrete Realisierung des EVG nicht ausgeschlossen, müssen aber den Erhalt der Stimmzettel und des Urneninhaltes garantieren.

Name	Beschreibung
Start	Urne ist leer (Anfangszustand)
Abgabe	Endgültige Abgabe von Stimmen (Registrierung, Speicherung in der Urne und Löschen auf dem Stift) ist möglich
Bewertung	Wahlhandlung ist geschlossen (es ist keine Stimmabgabe mehr möglich); Wahlvorstand entscheidet über unklare Stimmen
Auszählung	Ermittlung des Ergebnisses
Ende	Feststellung/Erfassung/Ausdruck des Ergebnisses

Tabelle 2: Betriebszustände einer elektronischen Urne

Schluss der Wahlhandlung Der Wahlvorstand legt das Ende der Wahlhandlung fest, das nicht umkehrbar ist. Falls der Wahlvorstand die Wahlhandlung vorzeitig schließen möchte, erhält er eine Warnmeldung vom EVG. Mit dem Schluss der Wahlhandlung muss die Speicherung weiterer elektronischer Stimmen in der elektronischen Wahlurne verhindert werden.

Eindeutigkeit der Stimmabgabe Der EVG muss die aufgezeichneten Stimmen automatisch bewerten. Es muss eine Funktion angeboten werden, mit deren Hilfe der Wahlvorstand die Stimmen bewerten kann, die nicht eindeutig gültig oder ungültig sind. Die Bewertung und Beschlussfassung über unklare Stimmen sowie die Ergebnisermittlung dürfen erst nach dem Schluss der Wahlhandlung erfolgen. Der EVG muss dem Wahlvorstand eine Entscheidungshilfe anbieten, um Stimmen effizient bewerten zu können. Dabei soll es aber eine Kontrollfrage geben, um übereilte Handlungen des Wahlvorstands zu vermeiden. Der EVG speichert sowohl die aufgezeichneten Stimmen als auch die Entscheidung des Wahlvorstandes, wie die Stimmen zu bewerten sind. Falls eine korrigierte Bewertung bei den bereits vom EVG ausgewerteten Stimmen erforderlich ist, haben diese Korrekturen Vorrang vor dem Ergebnis der automatischen Bewertung.

Manipulationssichere Speicherung nach Wahlende Der EVG bietet die Möglichkeit, die Authentizität und Integrität der Wahldaten nach Wahlende zu schützen. Die Wahldaten umfassen:

- Stammdaten/Konfiguration (Bezeichnung des Wahlbezirks, Stimmzetteldaten, etc.)
- Aufgezeichnete Stimmdatensätze
- Bewertete Stimmdatensätze
- Anzahl der insgesamt abgegebenen Stimmzettel
- Summarisches Ergebnis der Auszählung
- Protokolle

Die mit einem Authentizitäts- und Integritätsprüfmerkmal versehenen Wahldaten sollen nach Wahlende auf einem transportablen Speichermedium gespeichert sein. Der EVG muss hierzu die Funktionalität bereitstellen; das Speichermedium selbst sowie sein Transport zur Wahlzentrale werden nicht im Schutzprofil betrachtet.

Drucken des Ergebnisses Der EVG bietet die Möglichkeit, das Ergebnis zu drucken. Der Drucker liegt außerhalb des Schutzprofils.

Protokollierung Mindestens die in Tabelle 3 aufgelisteten Ereignisse sollen protokolliert werden.

Ereignis
Starten und Beenden des EVG
Störungen eines Digitalen Wahlstifts oder anderer Teile des EVG
Wiederanlauf nach Störungen/Unterbrechungen
Entscheidungen des Wahlvorstands über unklare Stimmen

Tabelle 3: Protokollierbare Ereignisse

Störungen und Fehler Der EVG soll Fehlfunktionen von Digitalen Wahlstiften, Lesefehler beim Entladen von Digitalen Wahlstiften, Integritätsfehler ausgelesener Stimmen, Schreibfehler beim Speichern von Stimmdatensätzen und andere Störungen und Fehler bei der Ausführung von Sicherheitfunktionen des EVG oder der IT-Umgebung erkennen. Der EVG muss dem Wähler und dem Wahlvorstand solche Störungen und Fehler anzeigen und verhindern, dass sie zu Veränderungen/Verlust von Stimmen oder anderen Auswirkungen auf das Wahlergebnis führen.

Speicherung Durch Medienfehler oder andere technische Ursachen können gespeicherte Daten vorlorengehen. Die Verhinderung eines solchen Verlusts wird nicht als Teil des EVG betrachtet. Der EVG reagiert aber auf festgestellte Medienfehler im Rahmen des geschützten Wiederanlaufs so, dass ein sicherer Zustand aufrechterhalten wird.

Bildschirmausgaben Alle Ausgaben des EVG auf dem Bildschirm müssen für den Wähler und den Wahlvorstand erkennbar und verständlich sein. Die Visualisierung der Datenübertragung vom Stift in die elektronische Urne muss für den Wähler erkennbar und verständlich sein. Alle Eingabeaufforderungen, Störungesmeldungen und Anzeigen der unklaren Stimmabgabe müssen für den Wahlvorstand erkennbar und verständlich sein.

3 EVG-Sicherheitsumgebung

Um festzustellen, ob die im Schutzprofil enthaltenen IT-Sicherheitsanforderungen ausreichend sind, ist es wichtig, dass das zu lösende Sicherheitsproblem klar verstanden wird. Dieser Abschnitt des Schutzprofils enthält die Definition des Sicherheitsproblems.

Die Darlegung der EVG-Sicherheitsumgebung beschreibt die Sicherheitsaspekte der Umgebung, in der der EVG eingesetzt werden soll und die erwartete Art des Gebrauchs. Sie umfasst all die Gesetze, organisatorischen Sicherheitspolitiken, Gewohnheiten, das Wissen und die Fachkenntnisse, die als relevant gelten. Sie definiert daher den Zusammenhang, in dem der EVG gebraucht werden soll. Zur Sicherheitsumgebung gehören insbesondere die Bedrohungen der Sicherheit, die in der Umgebung vorhanden sind bzw. von deren Vorhandensein ausgegangen wird.

Bei der Feststellung der Sicherheitsumgebung wurde Folgendes berücksichtigt:

a) die materielle Umgebung des EVG, die alle für die Sicherheit relevanten Aspekte der EVG-Einsatzumgebung angibt, einschließlich bekannter materieller und personeller Sicherheitsvorkehrungen;

b) die Werte, die Schutz durch die Bestandteile des EVG benötigen, für die die Sicherheitsanforderungen oder -politiken gelten werden;

c) der Zweck des EVG einschließlich Angaben zum Produkttyp und zum vorgesehenen Gebrauch.

Werte

Die folgenden Werte benötigen Schutz durch Bestandteile des EVG.

Stimmen Die Stimmen repräsentieren den Wählerwillen und umfassen den Inhalt der aufgezeichneten Kennzeichnung der Stimmzettel.

Stimmdatensätze Ein Stimmdatensatz umfasst die bei der Kennzeichnung eines Stimmzettels aufgezeichneten Stimmen. Die Aufzeichnungen eines Wahlvorgangs werden entsprechend den zugehörigen Stimmzetteln verschiedenen Stimmdatensätzen zugeordnet, die auf der Grundlage ihres Typs (Attribut ‚Typ von Stimmdatensätzen’) getrennt weiterverarbeitet werden. Jeder aufgezeichnete Stimmdatensatz entspricht dem Inhalt des zugehörigen Stimmzettels. Durch Entscheidung über die Erkennbarkeit des Wählerwillens entstehen bewertete Stimmdatensätze.

Wahldaten Die Wahldaten umfassen folgende Bestandteile:

- Stammdaten/Konfiguration (Bezeichnung des Wahlbezirks, Stimmzetteldaten, etc.)
- Aufgezeichnete Stimmdatensätze
- Bewertete Stimmdatensätze
- Anzahl der insgesamt abgegebenen Stimmzettel
- Summarisches Ergebnis der Auszählung
- Protokolle

ANWENDUNGSBEMERKUNG: Der Autor der Sicherheitsvorgaben kann den Umfang der Wahldaten ergänzen (z.B. mit Daten für die repräsentative Wahlstatistik). Für solche zusätzlichen Daten müssen die Gefährdungen der EVG-Sicherheitsumgebung überprüft werden. Insbesondere muss die Anonymität der Wähler gewährleistet bleiben.

Benutzer

Als Benutzer wird grundsätzlich jede aktive Einheit (Person oder externe IT-Einheit) außerhalb des EVG verstanden, die mit dem EVG interagiert. Für das vorliegende Schutzprofil werden folgende Benutzer unterschieden.

Wähler	führt den Wahlvorgang aus (berechtigt oder unberechtigt)
Wahlvorstand	zuständig für den ordnungsgemäßen Betrieb des EVG
Administrator	zuständig für die ordnungsgemäße Installation und Konfiguration des EVG (in der Regel werden die Administrationsaufgaben von einem vertrauenswürdigen Dienstleister durchgeführt)

3.1 Annahmen

Die Beschreibung der Annahmen gibt die Sicherheitsaspekte der Umgebung an, in der der EVG eingesetzt werden soll. Dazu gehören:

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

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

3.1.1 Annahmen über den beabsichtigten Gebrauch

A.Beobachtung Zur Aufzeichnung der Stimmen wird der Digitale Wahlstift ausschließlich in einer Wahlkabine benutzt, so dass der Wähler seine Stimmen unbeobachtet und unbeeinflusst abgeben kann.

A.Berechtigung Die Registrierung und Speicherung von Stimmdatensätzen wird nur dann vom Wahlvorstand zugelassen, wenn der Wähler auch wahlberechtigt ist.

A.Identifikation Der Wähler wird vom Wahlvorstand eindeutig identifiziert.

A.Notfallvorsorge Für technische Ausfälle der Geräte oder der Stromversorgung während der Wahlhandlung ist ein alternatives Verfahren im Rahmen von technischen und/oder organisatorischen Maßnahmen vorhanden.

A.Stimmzettel Dem Wähler ausgehändigte Papierstimmzettel werden zur Beendigung des Wahlvorgangs nach erfolgreicher Speicherung der elektronischen Stimmen in die Wahlurne geworfen und sonst vernichtet. Die Papierstimmzettel dienen als (zusätzlicher) redundanter Speicher und können ggf. manuell ausgezählt werden.

3.1.2 Annahmen über die Umgebung

A.Administrator Der Administrator installiert und konfiguriert den EVG vor Beginn der Wahl. Er sorgt für die Vergabe der Zugangs- und Zugriffsberechtigungen in der IT-Umgebung und beschränkt diese auf den Wahlvorstand bzw. die an ihn gebundenen Subjekte in der IT-Umgebung. Schließlich werden vom Administrator zu einem vom Wahlveranstalter vorgegebenen Zeitpunkt nach dem Ende der Wahl die Wahldaten gelöscht und der EVG deinstalliert.

A.Konfiguration Die für die Bewertung benötigten Stimmzetteldaten werden vor Beginn der Wahl vom Administrator ordnungsgemäß, vollständig und korrekt auf dem EVG installiert.

A.Personal Adminstrator und Wahlvorstand handeln nicht sorglos, nachlässig oder feindselig. Sie beachten und befolgen die von der Benutzer- und Systemverwalterdokumentation zur Verfügung gestellten Anweisungen.

A.Protokollschutz Die IT-Umgebung muss die vom EVG erzeugten Protokolldaten vor unberechtigtem Löschen und vor unberechtigter Modifikation schützen.

A.Schadsoftware Der Administrator sorgt dafür, dass die IT-Umgebung keine Schadsoftware (Viren etc.) enthält, die den EVG beeinflusst. Hierzu überprüft er die IT-Umgebung vor der Installation des EVG mit geeigneten Werkzeugen (Antivirensoftware etc.).

A.Speicherung Der Administrator sorgt auf der Grundlage sorgfältiger Abschätzungen vor Beginn der Wahl dafür, dass genügend freie Kapazität für die Speicherung der Wahldaten (inkl. der Protokolldaten) in der IT-Umgebung zur Verfügung steht.

A.Systemzeit Die IT-Umgebung stellt dem EVG verlässliche Zeitstempel auf Basis der Systemzeit zur Verfügung.

A.Verbindung Alle Verbindungen zwischen den Geräten in der IT-Umgebung des EVG sind drahtgebunden und befinden sich innerhalb des Wahllokals. Dies wird vom Wahlvorstand bei der Inbetriebnahme des EVG kontrolliert. Es existieren nur vier Schnittstellen zum EVG: zum Drucker, zur Speicherung auf dem transportablen Datenspeicher, über die Dockingstationen und zu Bildschirm/Tastatur. D.h. der Administrator konfiguriert die IT-Umgebung so, dass keine weitere Möglichkeit besteht, eine externe Verbindung zum EVG oder seiner IT-Umgebung aufzunehmen (insbesondere kann keine drahtlose Verbindung hergestellt werden).

A.Wahlvorstand Der Wahlvorstand überwacht den organisatorischen Ablauf im Wahllokal und die Betriebszustände aller Bestandteile des EVG. Er sorgt für den ordnungsgemäßen Anlauf zu Beginn der Wahl bzw. den ordnungsgemäßen Wiederanlauf nach Betriebsstörungen. Während des Betriebs sorgt er dafür, dass kein Administrator Zugang zum EVG oder seiner IT-Umgebung erhält. Er verhindert Manipulationen an der IT-Umgebung und entdeckt vom EVG angezeigte Manipulationen am Digitalen Wahlstift. Er verhindert die vorzeitige Schließung der Wahlhandlung, entscheidet zutreffend über die Gültigkeit der zu bewertenden Stimmdatensätze und stellt am Ende der Wahl das Ergebnis fest.

A.Zugang Durch Identifikation und Authentisierung der Benutzer in der IT-Umgebung (Betriebssystem) wird der Zugang zum EVG auf den Wahlvorstand und den Administrator beschränkt.

A.Zugriff Der Zugriff auf Objekte (bspw. Dateien) in der IT-Umgebung, die im Zusammenhang mit dem EVG oder von ihm erzeugten und gespeicherten Daten stehen, wird von der IT-Umgebung auf Subjekte (bspw. Prozesse) beschränkt, die an den Wahlvorstand oder den Administrator gebunden sind. Der Administrator konfiguriert die IT-Umgebung entsprechend.

A.Zutritt Der Zutritt zum Wahllokal und damit zur IT-Umgebung des EVG wird während der Wahl ständig vom Wahlvorstand kontrolliert.

3.2 Bedrohungen

Eine Aussage zu Bedrohungen der Sicherheit der Werte gibt all die Bedrohungen an, die bei der Sicherheitsanalyse 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 Angriffsmethoden, Gelegenheiten und ausgenutzte Schwachstellen angesprochen werden.

T.Anonymität Ein Angreifer erhält Zugriff auf gespeicherte Daten, die eine Zuordnung von Wähler und Stimmen ermöglicht. Es gibt zahlreiche Gefährdungen der Anonymität. Dazu gehört die Speicherung von zusätzlichen Daten (bspw. in den Protokollen oder für die Wahlstatistik), die die Aufdeckung des Wahlgeheimnisses ermöglichen. Der Angriff kann während oder nach dem Ende der Wahl ausgeführt werden.

Urheber: Person, die angezeigte Daten im Wahllokal mitliest oder nach Wahlende Zugriff auf die vom EVG gespeicherten Daten erhält, über Mittel verfügt, mit Hilfe dieser Daten eine Zuordnung zwischen abgegebenen Stimmen und Wählern herstellen, und die das Wahlgeheimnis brechen will.

Wert: Wahldaten, Stimme in der Urne

Analyse: Diese Bedrohung fokussiert auf Daten, die explizit vom EVG erfasst werden und die geeignet sind, das Wahlgeheimnis zu gefährden.

T.Beweis Ein Angreifer liest Daten aus dem Digitalen Wahlstift, die während der Aufzeichnung oder Registrierung der Stimmen entstehen und als Beweis für die Stimmabgabe geeignet sind. Der Angriff kann während oder nach Ende des Wahlvorgangs ausgeführt werden.

Urheber: Person, die über Mittel verfügt, Daten vom Digitalen Wahlstift auszulesen, und die damit einen Beweis für die abgegebenen Stimmen erhalten will. Der Angreifer kann der Wähler selbst oder eine andere Person sein.

Wert: Stimme auf dem Wahlstift

Analyse: Diese Bedrohung ist auf Daten beschränkt, die im Digitalen Wahlstift enthalten und geeignet sind, mit einem Beweis der Stimmabgabe das Wahlgeheimnis zu gefährden. Alle anderen Aspekte der Gefährdung des Wahlgeheimnisses sind in den Bedrohungen T.Anonymität und T.Verkettung enthalten.

T.Betriebsstörung Ein Angreifer stört den organisatorischen oder technischen Ablauf im Wahllokal und provoziert dadurch Bedien- oder Funktionsfehler bei der Speicherung oder Bewertung der Stimmdatensätze. Dazu gehört auch, dass der Angreifer spontan auftretende technische Störungen ausnutzt.

Urheber: Person, die den Wahlvorstand behindert oder die IT-Umgebung sabotiert und die das Wahlergebnis manipulieren will.

Wert: Stimmdatensätze

Analyse: Diese Bedrohung ist auf Stimmdatensätze beschränkt, weil alle anderen Bestandteile der Wahldaten entweder nicht veränderlich sind (Stammdaten/Konfiguration) oder automatisch berechnet werden (Anzahl der insgesamt abgegebenen Stimmzettel, Summarisches Ergebnis der Auszählung, Protokolle).

T.ManipulationStift Ein Angreifer manipuliert einen Wahlstift oder er tauscht ihn mit einem gefälschten Wahlstift aus, so dass die Stimmen vor der Registrierung verändert oder sie dem Angreifer zur Kenntnis gebracht werden. Es gibt zahlreiche Methoden der Manipulation oder Verfälschung, zu denen die Aktivierung einer drahtlosen Verbindung, die Verhinderung der Aufzeichnung durch Störung des elektronischen Auges und die Änderung der Funktion durch Modifikation der Firmware gehören. Der Angriff kann in der Wahlkabine oder außerhalb des Wahllokals (mit späterem Austausch von Stiften in der Wahlkabine) ausgeführt werden.

Urheber: Person mit technischen Kenntnissen über die Funktionsweise des Digitalen Wahlstifts und/oder seiner Firmware, die über Mittel verfügt, den Stift zu präparieren bzw. zu manipulieren, und die das Wahlergebnis manipulieren oder das Wahlgeheimnis brechen will.

Wert: Stimmen

Analyse: Diese Bedrohung fokussiert auf den Digitalen Wahlstift als den einzigen Bestandteil des EVG, der nicht unter ständiger Aufsicht des Wahlvorstands steht und der daher in besonderem Maße Gefährdungen der Manipulation ausgesetzt ist.

T.ManipulationErgebnis Nach dem Ende der Wahl fälscht ein Angreifer die Wahldaten durch Austausch oder Veränderung. Dazu gehört auch der Austausch mit echten Wahldaten eines anderen Wahllokals. Der Angriff kann vor, während oder nach der Übertragung der Wahldaten zur Wahlzentrale ausgeführt werden.

Urheber: Person, die Zugriff auf die Wahldaten erhält, über Mittel verfügt, sie zu verändern oder auszutauschen, und die das Wahlergebnis manipulieren will.

Wert: Wahldaten

Analyse: Diese Bedrohung fokussiert auf die Verletzung der Integrität und Authentizität nach dem Ende der Wahl, wenn der EVG den Schutz der Wahldaten nicht mehr aktiv gewährleisten kann. Während der Wahl sind die Wahldaten unter Kontrolle des EVG und seiner IT-Umgebung.

T.Verkettbarkeit Ein Angreifer ermittelt die Zeit und/oder die Reihenfolge der Speicherung der Stimmdatensätze in der elektronischen Urne und erhält damit eine Zuordnung von Wähler und Stimmen. Mit Hilfe dieser Daten kann der Angreifer eine Zuordnung zwischen abgegebenen Stimmen und Wählern herstellen, sofern er die Identität der Wähler sowie die Zeit und/oder die Reihenfolge ihrer Stimmabgabe im Wahllokal protokolliert hat. Der Angriff kann während oder nach dem Ende der Wahl ausgeführt werden.

Urheber: Person, die Zugriff auf die vom EVG gespeicherten Daten erhält, über Mittel verfügt, die Zeit und/oder die Reihenfolge der Speicherung der Stimmdatensätze zu ermitteln, und das Wahlgeheimnis brechen will.

Wert: Stimmdatensätze

Analyse: Diese Bedrohung fokussiert auf Daten, die nicht explizit vom EVG erfasst werden und die dennoch geeignet sind, das Wahlgeheimnis zu gefährden.

T.Wahlvorgang Ein Angreifer bringt für den Wähler unbemerkt Daten in den Digitalen Wahlstift ein, die als Bestandteil der Stimmen abgegeben werden. Der Angriff kann vor Beginn oder während des Wahlvorgangs ausgeführt werden.

Urheber: Person, die über Mittel verfügt, Daten in den Digitalen Wahlstift einzubringen (über das elektronische Auge oder andere Schnittstellen) und die damit Stimmen unberechtigt abgeben oder Stimmen des Wählers löschen oder ungültig machen will.

Wert: Stimmen

Analyse: Diese Bedrohung ist auf Daten beschränkt, die in den Digitalen Wahlstift eingebracht werden und geeignet sind, das Wahlergebnis zu verfälschen. Alle anderen Aspekte der Manipulation des Wahlergebnisses sind entweder in den Bedrohungen T.ManipulationStift und T.ManipulationErgebnis enthalten oder sind durch die vorgesehene Einsatzumgebung abgedeckt.

3.3 Organisatorische Sicherheitspolitiken

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

P.Ergebnisermittlung Die Gültigkeit der in der Urne gespeicherten Stimmdatensätze muss bewertet werden. Bei unklaren Stimmen entscheidet der Wahlvorstand über die Gültigkeit. Die Anzahl der gültigen und der ungültigen Stimmdatensätze muss ermittelt werden. Für alle gültigen Stimmdatensätze muss durch Auszählung das summarische Ergebnis ermittelt werden.

P.Ergebnisfeststellung Das festgestellte Ergebnis muss ausgedruckt werden.

P.Protokollierung Die in Tabelle 3 aufgelisteten Ereignisse müssen protokolliert werden.

P.Wahlhandlung Die Anzeige, Bewertung und die Auszählung von Stimmdatensätzen darf erst nach dem Schluss der Wahlhandlung erfolgen. Der Schluss der Wahlhandlung darf nicht rückgängig gemacht werden. Um eine unbeabsichtigte vorzeitige Schließung zu verhindern, muss der Schluss der Wahlhandlung vom Wahlvorstand explizit bestätigt werden.

4 Sicherheitsziele

Sicherheitsziele werden ermittelt, um alle Sicherheitsbedenken zu berücksichtigen und um zu erklären, welche Sicherheitsaspekte direkt den EVG und welche seine Umgebung betreffen. Eine solche Kategorisierung basiert auf einem Verfahren, bei dem technisches Verständnis, Sicherheitspolitik, wirtschaftliche Faktoren und Entscheidungen zur Inkaufnahme von Risiken eine Rolle spielen.

In diesem Abschnitt sind die Sicherheitsziele für den EVG und dessen Umgebung definiert. Die Sicherheitsziele gehen auf alle identifizierten Sicherheitsumgebungsaspekte ein. Sie spiegeln die dargelegte Absicht wider und sind geeignet, allen identifizierten Bedrohungen entgegenzuwirken, alle organisatorischen Sicherheitspolitiken durchzusetzen und alle Annahmen abzudecken.

4.1 Sicherheitsziele für den EVG

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

OT.Anonymität Der EVG speichert keine Daten, mit deren Hilfe eine Zuordnung zwischen dem Wähler und seinen abgegebenen Stimmen hergestellt werden kann.

OT.Aufzeichnung Der EVG muss gewährleisten, dass nur die während des Wahlvorgangs in den Digitalen Wahlstift eingebrachten Stimmen abgegeben werden können. Das Einbringen von Stimmen in den Digitalen Wahlstift darf nur über das elektronische Auge erfolgen.

OT.Auszählung Der EVG darf die gespeicherten Stimmdatensätze erst nach Abschluss der Bewertungsphase auszählen. Für alle gültigen Stimmdatensätze ermittelt der EVG durch Auszählung das summarische Ergebnis. Der EVG ermittelt die Anzahl der gültigen und der ungültigen Stimmdatensätze.

OT.Bewertung Der EVG darf die gespeicherten Stimmdatensätze erst nach Schluss der Wahlhandlung bewerten. Bei unklaren Stimmen muss der EVG die Entscheidung des Wahlvorstandes für die Bewertung verwenden.

OT.Ergebnisfeststellung Zur Feststellung des Ergebnisses schützt der EVG die Wahldaten vor unbemerkter Manipulation und kennzeichnet sie mit einem eindeutigen Nachweis ihres Ursprungs (zugehöriges Wahllokal). Der EVG veranlasst den Ausdruck des festgestellten Ergebnisses.

OT.Protokollierung Der EVG protokolliert die in Tabelle 3 aufgelisteten Ereignisse.

OT.Quittungsfreiheit Der EVG darf keine Daten zur Verfügung stellen, mit denen der Wähler seine Stimmabgabe beweisen kann. Dies bedeutet insbesondere, dass die Stimmdatensätze nach dem Speichern in der Urne vom Wahlstift gelöscht werden müssen.

OT.Robustheit Der EVG soll Fehlfunktionen von Digitalen Wahlstiften, Lesefehler beim Entladen von Digitalen Wahlstiften, Integritätsfehler ausgelesener Stimmen, Schreibfehler beim Speichern von Stimmdatensätzen und andere Störungen und Fehler bei der Ausführung von Sicherheitfunktionen des EVG oder der IT-Umgebung erkennen. Der EVG muss verhindern, dass solche Störungen und Fehler zu Veränderungen/Verlust von Stimmen oder anderen Auswirkungen auf das Wahlergebnis führen.

Falls bei Betriebsstörungen oder -unterbrechungen ein Wiederanlauf technisch möglich ist, gewährleistet der EVG die Rückkehr in einen konsistenten und sicheren Betriebszustand. Dazu gehört nach Störungen während der Registrierung, dass unvollständig gespeicherte Stimmdatensätze aus der Urne entfernt werden. Der EVG verhindert, dass Stimmdatensätze doppelt gespeichert werden (Ausnahme: leerer Stimmdatensatz).

OT.Unverkettbarkeit Für die Speicherung der Stimmdatensätze in der Urne verwendet der EVG einen Mechanismus, der gewährleistet, dass weder die Zeit noch die Reihenfolge der Speicherung rekonstruierbar sind. Werden bei einem Wahlvorgang mehrere Stimmdatensätze gleichzeitig gespeichert, wendet der EVG diesen Mechanismus für jeden einzelnen Stimmdatensatz an.

OT.Verifikation Der EVG muss gewährleisten, dass materielle Manipulationen an der Hardware des Digitalen Wahlstiftes und/oder der Austausch des Digitalen Wahlstifts für Wähler und Wahlvorstand erkennbar sind. Weiterhin muss der Zustand des EVG zu jedem Zeitpunkt im Wahllokal eindeutig feststellbar sein. Dazu muss der EVG insbesondere Manipulationsversuche an der Firmware des Digitalen Wahlstifts entdecken. Wähler und Wahlvorstand erhalten angemessene Hinweise bei Störungen des technischen Betriebs und bei entdeckten Manipulationsversuchen von Wahlstiften. Bei jedem Wahlvorgang ist für Wähler und Wahlvorstand eindeutig erkennbar, ob die Stimmen gelöscht (Annullierung) oder in der Urne gespeichert (Registrierung) wurden.

OT.Wahlhandlung Der EVG muss den Dienst der Stimmabgabe auf den Zeitraum der Wahlhandlung beschränken. Der Schluss der Wahlhandlung ist nicht umkehrbar. Der Versuch, die Wahlhandlung zu schließen, erfordert eine explizite Bestätigung durch den Wahlvorstand.

OT.Wahlvorgang Der EVG muss zu Beginn jedes Wahlvorgangs nach erfolgreicher Funktionsprüfung den Digitalen Wahlstifts zurücksetzen und für die Aufzeichnung von Stimmen freigeben (Aktivierung). Der EVG muss zum Ende des Wahlvorgangs die aufgezeichneten Stimmen vom Digitalen Wahlstift löschen und den Stift für die Aufzeichnung von Stimmen sperren (Registrierung bzw. Annullierung).

4.2 Sicherheitsziele für die Umgebung

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

OE.Beobachtung Zur Aufzeichnung der Stimmen wird der Digitale Wahlstift ausschließlich in einer Wahlkabine benutzt, so dass der Wähler seine Stimmen unbeobachtet und unbeeinflusst abgeben kann.

OE.Berechtigung Die Registrierung und Speicherung von Stimmdatensätzen wird nur dann vom Wahlvorstand zugelassen, wenn der Wähler auch wahlberechtigt ist.

OE.Identifikation Der Wähler wird vom Wahlvorstand eindeutig identifiziert.

OE.Notfallvorsorge Für technische Ausfälle der Geräte oder der Stromversorgung während der Wahlhandlung ist ein alternatives Verfahren im Rahmen von technischen und/oder organisatorischen Maßnahmen vorhanden.

OE.Stimmzettel Dem Wähler ausgehändigte Papierstimmzettel werden zur Beendigung des Wahlvorgangs nach erfolgreicher Speicherung der elektronischen Stimmen in die Wahlurne geworfen und sonst vernichtet. Die Papierstimmzettel dienen als (zusätzlicher) redundanter Speicher und können ggf. manuell ausgezählt werden.

OE.Administrator Der Administrator installiert und konfiguriert den EVG vor Beginn der Wahl. Er sorgt für die Vergabe der Zugangs- und Zugriffsberechtigungen in der IT-Umgebung und beschränkt diese auf den Wahlvorstand bzw. die an ihn gebundenen Subjekte in der IT-Umgebung. Schließlich werden vom Administrator zu einem vom Wahlveranstalter vorgegebenen Zeitpunkt nach dem Ende der Wahl die Wahldaten gelöscht und der EVG deinstalliert.

OE.Konfiguration Die für die Bewertung benötigten Stimmzetteldaten werden vor Beginn der Wahl vom Administrator ordnungsgemäß, vollständig und korrekt auf dem EVG installiert.

OE.Personal Adminstrator und Wahlvorstand handeln nicht sorglos, nachlässig oder feindselig. Sie beachten und befolgen die von der Benutzer- und Systemverwalterdokumentation zur Verfügung gestellten Anweisungen.

OE.Protokollschutz Die IT-Umgebung muss die vom EVG erzeugten Protokolldaten vor unberechtigtem Löschen und vor unberechtigter Modifikation schützen.

OE.Schadsoftware Der Administrator sorgt dafür, dass die IT-Umgebung keine Schadsoftware (Viren etc.) enthält, die den EVG beeinflusst. Hierzu überprüft er die IT-Umgebung vor der Installation des EVG mit geeigneten Werkzeugen (Antivirensoftware etc.).

OE.Speicherung Der Administrator sorgt auf der Grundlage sorgfältiger Abschätzungen vor Beginn der Wahl dafür, dass genügend freie Kapazität für die Speicherung der Wahldaten (inkl. der Protokolldaten) in der IT-Umgebung zur Verfügung steht.

OE.Systemzeit Die IT-Umgebung stellt dem EVG verlässliche Zeitstempel auf Basis der Systemzeit zur Verfügung.

OE.Verbindung Alle Verbindungen zwischen den Geräten in der IT-Umgebung des EVG sind drahtgebunden und befinden sich innerhalb des Wahllokals. Dies wird vom Wahlvorstand bei der Inbetriebnahme des EVG kontrolliert. Es existieren nur vier Schnittstellen zum EVG: zum Drucker, zur Speicherung auf dem transportablen Datenspeicher, über die Dockingstationen und zu Bildschirm/Tastatur. D.h. der Administrator konfiguriert die IT-Umgebung so, dass keine weitere Möglichkeit besteht, eine externe Verbindung zum EVG oder seiner IT-Umgebung aufzunehmen (insbesondere kann keine drahtlose Verbindung hergestellt werden).

OE.Wahlvorstand Der Wahlvorstand überwacht den organisatorischen Ablauf im Wahllokal und die Betriebszustände aller Bestandteile des EVG. Er sorgt für den ordnungsgemäßen Anlauf zu Beginn der Wahl bzw. den ordnungsgemäßen Wiederanlauf nach Betriebsstörungen. Während des Betriebs sorgt er dafür, dass kein Administrator Zugang zum EVG oder seiner IT-Umgebung erhält. Er verhindert Manipulationen an der IT-Umgebung und entdeckt vom EVG angezeigte Manipulationen am Digitalen Wahlstift. Er verhindert die vorzeitige Schließung der Wahlhandlung, entscheidet zutreffend über die Gültigkeit der zu bewertenden Stimmdatensätze und stellt am Ende der Wahl das Ergebnis fest.

OE.Zugang Durch Identifikation und Authentisierung der Benutzer in der IT-Umgebung (Betriebssystem) wird der Zugang zum EVG auf den Wahlvorstand und den Administrator beschränkt.

OE.Zugriff Der Zugriff auf Objekte (bspw. Dateien) in der IT-Umgebung, die im Zusammenhang mit dem EVG oder von ihm erzeugten und gespeicherten Daten stehen, wird von der IT-Umgebung auf Subjekte (bspw. Prozesse) beschränkt, die an den Wahlvorstand oder den Administrator gebunden sind. Der Administrator konfiguriert die IT-Umgebung entsprechend.

OE.Zutritt Der Zutritt zum Wahllokal und damit zur IT-Umgebung des EVG wird während der Wahl ständig vom Wahlvorstand kontrolliert.

5 IT-Sicherheitsanforderungen

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

ANWENDUNGSBEMERKUNG: Die funktionalen Anforderungskomponenten in den Abschnitten 5.1.1 und 5.2 enthalten Hinweise aus Teil 2 der CC auf Managementfunktionen und protollierbare Aktionen. Durchstreichungen in diesen Hinweisen kennzeichnen Aspekte, die für die Erfüllung der Sicherheitsziele nicht relevant sind. Die Hinweise sollen vom ST Autor beachtet werden.

5.1 EVG-Sicherheitsanforderungen

Der Begriff „EVG-Sicherheitsanforderungen“ bezieht sich auf „funktionale EVG-Sicherheitsanforderungen“ und auf „Anforderungen an die Vertrauenswürdigkeit des EVG“.

Tabelle 4 zeigt eine Zuordnung der in den Anforderungen verwendenten englischen Begriffen und den entsprechenden deutschen aus den Kapiteln davor.

english term	**Deutsche Entsprechung**
ballot	Stimmzettel
ballot box	Urne
box handler	Subjekte, die mit elektronischen Urnen umgehen
digital election pen	digitaler Wahlstift
election data	Wahldaten
election district	Wahlbezirk
pen handler	Subjekte, die mit Digitalen Wahlstiften umgehen
recovery	Wiederanlauf
scrutineers	Wahlvorstand
vote casting	Stimmabgabe

Tabelle 4 Zuordnung englisch-deutsche Begriffe

5.1.1 Funktionale EVG-Sicherheitsanforderungen

Die Darlegung der funktionalen EVG-Sicherheitsanforderungen definiert die funktionalen Anforderungen an den EVG in Form funktionaler Komponenten aus Teil 2 der CC, die in Tab. 5 zusammengefasst sind.

Der EVG enthält Betriebsmittel, die zur Verarbeitung und Speicherung von Informationen benutzt werden können. Das Hauptziel der TSF ist die vollständige und korrekte Durchsetzung der TSP für die Betriebsmittel und Informationen, die der EVG kontrolliert.

EVG-Betriebsmittel können auf vielfältige Weise gegliedert und genutzt werden. Teil 2 der CC führt jedoch eine spezielle Gliederung ein, die eine Spezifikation von gewünschten Sicherheitseigenschaften zulässt. Alle Einheiten, die aus Betriebsmitteln gebildet werden können, können zwei Kategorien zugeordnet werden. Die Einheiten können aktiv sein, d.h. diese sind Ursache von Aktionen, die EVG-intern ablaufen und lösen Operationen aus, die mit Informationen ausgeführt werden. Die Einheiten können andererseits passiv sein, d.h. diese sind entweder der Behälter, aus dem Informationen stammen oder der Behälter, in dem Informationen gespeichert werden.

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

a) Subjekte, die mit Digitalen Wahlstiften umgehen (pen handler) und

b) Subjekte, die mit elektronischen Urnen umgehen (box handler).

Passive Einheiten (d.h. Behälter, die Informationen enthalten) werden als ***Objekte*** bezeichnet. Objekte sind die Ziele von Operationen, die von Subjekten ausgeführt werden können. Innerhalb des EVG gibt es folgende Arten von Objekten:

a) aufgezeichnete Stimmen, die im Wahlstift enthalten sein können und

b) gespeicherte Stimmdatensätze, die in den elektronischen Urnen enthalten sein können.

Objekte besitzen bestimmte ***Sicherheitsattribute*** (vgl. Tab. 1 und 2), die Informationen enthalten, welche ein korrektes Verhalten des EVG ermöglichen.

Mindeststärkestufe der Funktionen

Für die funktionalen EVG-Sicherheitsanforderungen wird SOF-Mittel als Mindeststärkestufe der Funktionen postuliert.

Functional Class	Functional component	
FAU: Security Audit	FAU_GEN.1	Audit data generation
FCO: Communication	FCO_NRO.2	Enforced proof of origin
FDP: User Data Protection	FDP_ACC.2A/B	Complete access control
	FDP_ACF.1A/B	Security attribute based access control
	FDP_IFC.2	Complete information flow control
	FDP_IFF.1	Simple security attributes
	FDP_ITT.2	Transmission separation by attribute
	FDP_ITT.4	Attribute-based integrity monitoring
	FDP_RIP.1A/B	Subset residual information protection
	FDP_SDI.2	Stored data integrity monitoring and action
FMT: Security Management	FMT_MSA.3A/B	Static attribute initialisation
	FMT_SMF.1	Specification of Management Functions
FPR: Privacy	FPR_ANO.2	Anonymity without soliciting information
	FPR_UNL.1	Unlinkability
FPT: Protection of the TSF	FPT_AMT.1	Abstract machine testing
	FPT_FLS.1	Failure with preservation of secure state
	FPT_PHP.1	Passive detection of physical attack
	FPT_PHP.3	Resistance to physical attack
	FPT_RCV.1	Manual recovery
	FPT_RCV.4	Function recovery
	FPT_TST.1	TSF testing
FRU: Resource Utilisation	FRU_FLT.1	Degraded fault tolerance

Tabelle 5: Komponenten der funktionalen EVG-Sicherheitsanforderungen

FAU_GEN.1 Audit data generation

“Audit data generation” defines the level of auditable events, and specifies the list of data that shall be recorded in each record.

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps (satisfied by TOE environment)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the {*not specified*} level of audit; and

c) {*the auditable events specified in table 3 and* [assignment: *further specifically defined auditable events*]}.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, {*object identity for the audit events of FDP_ACF.1 components,* [assignment: *further audit relevant information*]}.

APPLICATION NOTE: All auditable events specified in this component should be audited, i.e. the ST author should not include the component FAU_SEL.1.

Operation	Template	Result
Selection, choose one of	*minimum,basic,detailed,not specified*	*not specified*
Assignment	*other specifically defined auditable events*	*the auditable events specified in table 3 and* [assignment: *further specifically defined auditable events*]
Assignment (assigned)	*further specifically defined auditable events*	to be specified by the ST author; The ST author may choose auditable events from the specification of the functional components
Assignment	*other audit relevant information*	*object identity for the audit events of FDP_ACF.1 component,* [assignment: *further audit relevant information*]
Assignment (assigned)	*further audit relevant information*	to be specified by the ST author; possibly: *none*

Management:
There are no management activities foreseen.

Audit:
There are no auditable events foreseen.

FCO_NRO.2 Enforced proof of origin

“Enforced proof of origin” requires that the TSF always generates evidence of origin for transmitted information.

Hierarchical to: FCO_NRO.1 Selective proof of origin

Dependencies: FIA_UID.1 Timing of identification (not applicable)

FCO_NRO.2.1 The TSF shall enforce the generation of evidence of origin for transmitted {*election data*} at all times (i.e. at the successful request to perform the operation ‘establish’ that is controlled by the BSCP).

FCO_NRO.2.2 The TSF shall be able to relate the {*time and election district of origin*} of the originator of the information, and {*all parts*} of the {election data} to which the evidence applies.

FCO_NRO.2.3 The TSF shall provide a capability to verify the evidence of origin of information to {*recipient*} given [assignment: *limitations on the evidence of origin*].

APPLICATION NOTE: If the evidence is generated by the use of a digital signature the capability to verify the evidence can be provided as an indication of the cryptographic key that is needed for verification.

Operation	Template	Result
Assignment	*list of information types*	*election data*
Refinement	at all times	at all times (i.e. at the successful request to perform the operation ‘establish’ that is controlled by the BSCP)
Assignment	*list of attributes*	*time and election district of origin*
Refinement + Assignment	the [assignment: *list of information fields*]	*all parts*
Refinement	information	election data
Selection	*originator, recipient,* [assignment: *list of third parties*]	*recipient*
Assignment	*limitations on the evidence of origin*	to be specified by the ST author; possibly: *indefinite*

Management:
There are no management activities foreseen.

Audit:
The following actions should be auditable:

a) Minimal: The invocation of the non-repudiation service.

~~b) Basic: Identification of the information, the destination, and a copy of the evidence provided.~~

~~c) Detailed: The identity of the user who requested a verification of the evidence.~~

FDP_ACC.2A Complete access control (iteration for digital election pens)

“Complete access control” requires that each identified access control SFP cover all operations on subjects and objects covered by that SFP. It further requires that all objects and operations with the TSC are covered by at least one identified access control SFP.

Hierarchical to: FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control (satisfied by FDP_ACF.1A)

FDP_ACC.2A.1 The TSF shall enforce the {*pen state control policy (PSCP)*} on {*all pen handlers, i.e. activation, cancellation and registration handler, (subjects) and all digital election pens (objects)*} and all operations among subjects and objects covered by the {PSCP}.

{ The PSCP shall adhere to the following security principles:

a) All votes stored on a digital election pen belong to a single voter;

b) Votes are stored on a digital election pen only during an individual voting procedure; otherwise the digital election pen is empty and recording is disabled;

c) There is no charging operation for importing votes in a digital election pen (votes can only be imported using the electronic eye).

}

FDP_ACC.2A.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

Operation	Template	Result
Assignment	*access control SFP*	*pen state control policy (PSCP)*
Assignment	*list of subjects and objects*	*all pen handlers, i.e. activation, cancellation and registration handler, (subjects) and all digital election pens (objects)*
Refinement	SFP	PSCP
Refinement	element FDP_ACC.2A.1: PSCP scope of control	The PSCP shall adhere to the following security principles: a) … b) … c) …

Management:
There are no management activities foreseen.

Audit:
There are no auditable events foreseen.

FDP_ACF.1A Security attribute based access control (iteration for digital election pens)

“Security attribute based access control” allows the TSF to enforce access based upon security attributes and named groups of attributes. Furthermore, the TSF may have the ability to explicitly authorize or deny access to an object based upon security attributes.

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control (satisfied by FDP_ACC.2A)

FMT_MSA.3 Static attribute initialization (satisfied by FMT_MSA.3A)

FDP_ACF.1A.1 **The TSF shall enforce the {*pen state control policy (PSCP)*} to objects based on the following: {*all pen handlers, i.e. activation, cancellation and registration handler, (subjects) and all digital election pens (objects) and the operational state as defined in table 1 (individual object security attribute)*}.**

FDP_ACF.1A.2 **The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: {**

a) activate: Neutral → Aktiv
The activation handler is allowed to perform the operation ‘activate’ if the operational state of the digital election pen is ‘Neutral’. The operation resets the digital election pen, enables recording of votes and changes the operational state to ‘Aktiv’.

b) cancel: Aktiv → Neutral
The cancelation handler is allowed to perform the operation ‘cancel’ if the operational state of a digital election pen is ‘Aktiv’. The operation erases all recorded votes from the digital election pen, disables recording of votes and changes the operational state to ‘Neutral’.

c) register: Aktiv → Neutral
The registration handler is allowed to perform the operation ‘register’ if the operational state of a digital election pen is ‘Aktiv’. The operation discharges and erases all recorded votes from the digital election pen, disables recording of votes and changes the operational state to ‘Neutral’.

}.

FDP_ACF.1A.3 **The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: {*none*}.**

FDP_ACF.1A.4 **The TSF shall explicitly deny access of subjects to objects based on the {*following additional rules: none*}.**

Operation	Template	Result
Assignment	*access control SFP*	*pen state control policy (PSCP)*
Assignment	*list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*	*all pen handlers, i.e. activation, cancellation and registration handler, (subjects) and all digital election pens (objects) and the operational state as defined in table 1 (individual object security attribute)*
Assignment	*rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*	*a) activate …* *b) cancel …* *c) register …*
Assignment	*rules, based on security attributes, that explicitly authorize access of subjects to objects*	*none*
Assignment	*rules, based on security attributes, that explicitly deny access of subjects to objects*	*following additional rules: none*

Management:
There are no management activities foreseen.

Audit:
The following actions should be auditable:

a) Minimal: Successful requests to perform an operation on an object covered by the SFP.
b) Basic: All requests to perform an operation on an object covered by the SFP.
~~c) Detailed: The specific security attributes used in making an access check.~~

FDP_ACC.2B Complete access control (iteration for ballot boxes)

“Complete access control”, requires that each identified access control SFP cover all operations on subjects and objects covered by that SFP. It further requires that all objects and operations with the TSC are covered by at least one identified access control SFP.

Hierarchical to: FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control (satisfied by FDP_ACF.1B)

FDP_ACC.2B.1 The TSF shall enforce the {*box state control policy (BSCP)*} on {*the box handler (subject) and all ballot boxes (objects)*} and all operations among subjects and objects covered by the {BSCP}.

{ The BSCP shall adhere to the following security principle:

Access to a ballot box allowing to compute (intermediate) election results is denied until the vote casting service is irreversibly closed.

}

FDP_ACC.2B.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

Operation	Template	Result
Assignment	*access control SFP*	*box state control policy (BSCP)*
Assignment	*list of subjects and objects*	*the box handler (subject) and all ballot boxes (objects)*
Refinement	SFP	BSCP
Refinement	element FDP_ACC.2B.1: BSCP scope of control	The BSCP shall adhere to the following security principle: …

Management:
There are no management activities foreseen.

Audit:
There are no auditable events foreseen.

FDP_ACF.1B Security attribute based access control (iteration for ballot boxes)

“Security attribute based access control” allows the TSF to enforce access based upon security attributes and named groups of attributes. Furthermore, the TSF may have the ability to explicitly authorize or deny access to an object based upon security attributes.

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control (satisfied by FDP_ACC.2B)

FMT_MSA.3 Static attribute initialization (satisfied by FMT_MSA.3B)

FDP_ACF.1B.1 **The TSF shall enforce the {*box state control policy (BSCP)*} to objects based on the following: {*the box handler (subject) and all ballot boxes (objects) and the operational state as defined in table 2 (individual object security attribute)*}.**

FDP_ACF.1B.2 **The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: {**

a) open: Start → Abgabe
The box handler is allowed to perform the operation ‘open’ if the operational state of the ballot box is ‘Start’. The operation ensures that the ballot box contains no ballots and changes the operational state to ‘Abgabe’.

b) store: Abgabe → Abgabe
The box handler is allowed to perform the operation ‘store’ if the operational state of the ballot box is ‘Abgabe’, the type of the registered ballot belongs to the ballot box and the ballot is not already stored. The operation ensures that the ballot is stored in the ballot box and does not change the operational state.

c) close: Abgabe → Bewertung
The box handler is allowed to perform the operation ‘close’ if the operational state of the ballot box is ‘Abgabe’ and the closing time for the vote casting service associated with the ballot box is reached or passed. The operation changes the operational state to ‘Bewertung’.

d) validate: Bewertung → Bewertung
The box handler is allowed to perform the operation ‘validate’ if the operational state of the ballot box is ‘Bewertung’. The operation ensures that the decision is stored in the ballot box. Any user decision overrules the automatic validation result. The operational state remains unchanged.

e) count: Bewertung → Auszählung
The box handler is allowed to perform the operation ‘count’ if the operational state of the ballot box is ‘Bewertung’. The operation ensures that election result is correctly computed based on all validated ballots contained in the ballot box. In addition, it ensures that the number of all valid and all invalid ballots is counted. It changes the operational state to ‘Auszählung’.

f) establish: Auszählung → Ende
The box handler is allowed to perform the operation ‘establish’ if the operational state of the ballot box is ‘Auszählung’. The operation initiates printing of the election result associated with the ballot box and ensures that a proof of origin is generated for the election data including protection against manipulation. The operational state is changed to ‘Ende’.

}.

FDP_ACF.1B.3 **The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: {**

close: Abgabe → Bewertung
The box handler is allowed to perform the operation ‘close’ if the operational state of the ballot box is ‘Abgabe’ and the user confirms the closing of the vote casting service associated with the ballot box. The operation changes the operational state to ‘Bewertung’.

}.

FDP_ACF.1B.4 **The TSF shall explicitly deny access of subjects to objects based on the {*following additional rules: none*}.**

Operation	Template	Result
Assignment	*access control SFP*	*box state control policy (BSCP)*
Assignment	*list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*	*the box handler (subject) and all ballot boxes (objects) and the operational state as defined in table 2 (individual object security attribute)*
Assignment	*rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*	*a) open …* *b) store …* *c) close …* *d) validate …* *e) count …* *f) establish …*
Assignment	*rules, based on security attributes, that explicitly authorize access of subjects to objects*	*close: Abgabe → Bewertung* *The box handler is allowed to perform the operation ‘close’ if the operational state of the ballot box is ‘Abgabe’ and the user confirms the closing of the vote casting service associated with the ballot box. The operation changes the operational state to ‘Bewertung’.*
Assignment	*rules, based on security attributes, that explicitly deny access of subjects to objects*	*following additional rules: none*

Management:
There are no management activities foreseen.

Audit:
The following actions should be auditable:

a) Minimal: Successful requests to perform an operation on an object covered by the SFP.
b) Basic: All requests to perform an operation on an object covered by the SFP.
~~c) Detailed: The specific security attributes used in making an access check.~~

FDP_IFC.2 Complete information flow control

“Complete information flow control” requires that each identified information flow control SFP cover all operations on subjects and information covered by that SFP. It further requires that all information flows and operations with the TSC are covered by at least one identified information flow control SFP.

Hierarchical to: FDP_IFC.1 Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes (satisfied)

FDP_IFC.2.1 **The TSF shall enforce the {*vote casting policy (VCP)*} on {*the registration handler, the box handler (subjects) and the ballots (information)*} and all operations that cause {ballots} to flow to and from subjects covered by the {VCP}.**

FDP_IFC.2.2 **The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by an information flow control SFP.**

Operation	Template	Result
Assignment	*information flow control SFP*	*vote casting policy (VCP)*
Assignment	*list of subjects and information*	*the registration handler, the box handler (subjects) and the ballots (information)*
Refinement	that information	ballots
Refinement	SFP	VCP

Management:
There are no management activities foreseen.

Audit:
There are no auditable events foreseen.

FDP_IFF.1 Simple security attributes

“Simple security attributes” requires security attributes on information, and on subjects that cause that information to flow and on subjects that act as recipients of that information. It specifies the rules that must be enforced by the function, and describes how security attributes are derived by the function.

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control (satisfied)

FMT_MSA.3 Static attribute initialization (not applicable)

FDP_IFF.1.1 **The TSF shall enforce the {*vote casting policy (VCP)*} based on the following types of subject and information security attributes: {*the registration handler, the box handler (subjects without security attributes) and the ballots (information) with ‘type of ballot’ as security attribute*}.**

FDP_IFF.1.2 **The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: {*a ballot flows from the registration handler to the box handler using the storing operation if and only if the type of ballot corresponds to the designated ballot box*}.**

FDP_IFF.1.3 **The TSF shall enforce the {*following additional information flow control rules: none*}.**

FDP_IFF.1.4 **The TSF shall provide the following {*list of additional SFP capabilities: none*}.**

FDP_IFF.1.5 **The TSF shall explicitly authorise an information flow based on the following rules: {*none*}.**

FDP_IFF.1.6 **The TSF shall explicitly deny an information flow based on the following rules: {*none*}.**

APPLICATION NOTE: The security attribute ‘type of ballot’ is supposed to be a unique property of the recorded coordinates contained in each ballot. It is computed by comparing all coordinates with configuration data provided during installation of the TOE. Based on this attribute the TOE is able to store each ballot in its corresponding ballot box (cf. FDP_ITT components).

Operation	Template	Result
Assignment	*information flow control SFP*	*vote casting policy (VCP)*
Assignment	*list of subjects and information controlled under the indicated SFP, and for each, the security attributes*	*the registration handler, the box handler (subjects without security attributes) and the ballots (information) with ‘type of ballot’ as security attribute*
Assignment	*for each operation, the security attribute-based relationship that must hold between subject and information security attributes*	*a ballot flows form the pen handler to the box handler using the storing operation if and only if the type of ballot corresponds to the designated ballot box*
Assignment	*additional information flow control SFP rules*	*following additional information flow control rules: none*
Assignment	*list of additional SFP capabilities*	*list of additional SFP capabilities: none*
Assignment	*rules, based on security attributes, that explicitly authorise information flows*	*none*
Assignment	*rules, based on security attributes, that explicitly deny information flows*	*none*

Management:
There are no management activities foreseen.

Audit:
The following actions should be auditable:

a) Minimal: Decisions to permit requested information flows.

b) Basic: All decisions on requests for information flow.

c) Detailed: The specific security attributes used in making an information flow enforcement decision.

~~d) Detailed: Some specific subsets of the information that has flowed based upon policy goals (e.g. auditing of downgraded material).~~

FDP_ITT.2 Transmission separation by attribute

“Transmission separation by attribute” requires separation of data based on the value of SFP-relevant attributes in addition to the first component.

Hierarchical to: FDP_ITT.1 Basic internal transfer protection

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control (satisfied by FDP_IFC.2)]

FDP_ITT.2.1 The TSF shall enforce the {*vote casting policy (VCP)*} to prevent the {*disclosure, modification and loss of use*} of {ballots} when it is transmitted between physically-separated parts of the TOE.

FDP_ITT.2.2 The TSF shall separate {ballots} controlled by the {VCP} when transmitted between physically-separated parts of the TOE, based on the values of the following: {attribute ‘*type of ballot*’}.

Operation	Template	Result
Assignment	*access control SFP(s) and/or information flow control SFP(s)*	{*vote casting policy (VCP)*}
Selection	*disclosure, modification, loss of use*	*disclosure, modification and loss of use*
Refinement	user data	ballots
Refinement	data	ballots
Refinement	SFP(s)	VCP
Assignment	*security attributes that require separation*	*attribute ‘type of ballot’*

Management:
There are no management activities foreseen.

Audit:
The following actions should be auditable:

a) Minimal: Successful transfers of user data, ~~including identification of the protection method used.~~

b) Basic: All attempts to transfer user data, ~~including the protection method used and any errors that occurred.~~

FDP_ITT.4 Attribute-based integrity monitoring

“Integrity monitoring” requires that the SF monitor user data transmitted between parts of the TOE for identified integrity errors. “Attribute-based integrity monitoring” expands on integrity monitoring by allowing the form of integrity monitoring to differ by SFP-relevant attribute.

Hierarchical to: FDP_ITT.3 Integrity monitoring

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control (satisfied by FDP_IFC.2)]

FDP_ITT.2 Transmission separation by attribute (satisfied)

FDP_ITT.4.1 The TSF shall enforce the {*vote casting policy (VCP)*} to monitor {ballots} transmitted between physically-separated parts of the TOE for the following errors: {*data separation errors, i.e. recorded coordinates do not belong to any configured type of ballot*}, based on the following attributes: {*type of ballot*}.

FDP_ITT.4.2 Upon detection of a data integrity error, the TSF shall {*disable the digital election pen that created the integrity error and inform the scrutineers*}.

Operation	Template	Result
Assignment	*access control SFP(s) and/or information flow control SFP(s)*	*vote casting policy (VCP)*
Refinement	user data	ballots
Assignment	*integrity errors*	*data separation errors, i.e. recorded coordinates do not belong to any configured type of ballot*
Assignment	*security attributes that require separate transmission channels*	*type of ballot*
Assignment	*specify the action to be taken upon integrity error*	*disable the election pen that created the integrity error and inform the scrutineers*

Management:
There are no management activities foreseen.

Audit:
The following actions should be auditable:

a) Minimal: Successful transfers of user data, including identification of the integrity protection method used.

b) Basic: All attempts to transfer user data, including the integrity protection method used and any errors that occurred.

~~c) Basic: Unauthorised attempts to change the integrity protection method.~~

~~d) Detailed: The action taken upon detection of an integrity error.~~

FDP_RIP.1A Subset residual information protection

“Subset residual information protection” requires that the TSF ensure that any residual information content of any resources is unavailable to a defined subset of the objects in the TSC upon the resource's allocation or deallocation.

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1A.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the {*deallocation (operations ‘register’ and ‘cancel’) of the resource from*} the following objects: {*digital election pens*}.

Operation	Template	Result
Selection + Refinement Assignment	*allocation of the resource to, deallocation of the resource from list of objects*	*deallocation (operations ‘register’ and ‘cancel’) of the resource from digital election pens*

Management:
There are no management activities foreseen.

Audit:
There are no auditable events foreseen.

FDP_RIP.1B Subset residual information protection

“Subset residual information protection” requires that the TSF ensure that any residual information content of any resources is unavailable to a defined subset of the objects in the TSC upon the resource's allocation or deallocation.

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1B.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the {*allocation (operation ‘open’) of the resource to*} the following objects: {*ballot boxes*}.

Operation	Template	Result
Selection + Refinement Assignment	*allocation of the resource to, deallocation of the resource from list of objects*	*allocation (operation ‘open’) of the resource to ballot boxes*

Management:
There are no management activities foreseen.

Audit:
There are no auditable events foreseen.

FDP_SDI.2 Stored data integrity monitoring and action

“Stored data integrity monitoring” requires that the SF monitor user data stored within the TSC for identified integrity errors.
“Stored data integrity monitoring and action” adds the additional capability by allowing for actions to be taken as a result of an error detection.

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

Dependencies: No dependencies.

FDP_SDI.2.1 **The TSF shall monitor user data stored within the TSC for *{read errors while discharging a digital election pen and write errors while storing ballots in an ballot box}* on all objects, based on the following attributes: *{exceptions signaled by the underlying software (operating system)}*.**

FDP_SDI.2.2 **Upon detection of a data integrity error, the TSF shall {*stop processing and inform the scrutineers for invoking the recovery and self test mechanisms*}.**

Operation	Template	Result
Assignment	*integrity errors*	*read errors while discharging a digital election pen and write errors while storing ballots in an ballot box*
Assignment	*user data attributes*	*exceptions signaled by the underlying software (operating system)*
Assignment	*action to be taken*	*stop processing and inform the scrutineers for invoking the recovery and self test mechanisms*

Management:
There are no management activities foreseen.

Audit:
The following actions should be auditable:

a) Minimal: Successful attempts to check the integrity of user data, including an indication of the results of the check.

b) Basic: All attempts to check the integrity of user data, including an indication of the results of the check, if performed.

c) Detailed: The type of integrity error that occurred.

d) Detailed: The action taken upon detection of an integrity error.

FMT_MSA.3A Static attribute initialisation (iteration for digital election pens)

“Static attribute initialization” ensures that the default values of security attributes are appropriately either permissive or restrictive in nature.

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes (not applicable)

FMT_SMR.1 Security roles (not applicable)

FMT_MSA.3A.1 The TSF shall enforce the {*pen state control policy (PSCP)*} to provide {*fixed (i.e. pen operational state ‘Neutral’)*} default values for security attributes that are used to enforce the {pen state control policy (PSCP)}.

FMT_MSA.3A.2 The TSF shall allow the {*no role*} to specify alternative initial values to override the default values when an object {} is created.

Operation	Template	Result
Assignment	*access control SFP, information flow control SFP*	*pen state control policy (PSCP)*
Selection, choose one of	*restrictive, permissive,* [assignment: *other property*]	[assignment: *other property*]
Assignment (selected)	*other property*	*fixed (i.e. pen operational state ‘Neutral’)*
Refinement	SFP	pen state control policy (PSCP)
Assignment	*the authorised identified roles*	*no role*
Refinement	or information	—

Management:
There are no management activities foreseen.

Audit:
The following actions should be auditable:

~~a) Basic: Modifications of the default setting of permissive or restrictive rules.~~

~~b) Basic: All modifications of the initial values of security attributes.~~

FMT_MSA.3B Static attribute initialisation (iteration for ballot boxes)

“Static attribute initialization” ensures that the default values of security attributes are appropriately either permissive or restrictive in nature.

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes (not applicable)

FMT_SMR.1 Security roles (not applicable)

FMT_MSA.3B.1 The TSF shall enforce the {*box state control policy (BSCP)*} to provide {*fixed (i.e. box operational state ‘Start’)*} default values for security attributes that are used to enforce the {box state control policy (BSCP)}.

FMT_MSA.3B.2 The TSF shall allow the {*no role*} to specify alternative initial values to override the default values when an object {} is created.

Operation	Template	Result
Assignment	*access control SFP, information flow control SFP*	*box state control policy (BSCP)*
Selection, choose one of	*restrictive, permissive,* [assignment: *other property*]	[assignment: *other property*]
Assignment (selected)	*other property*	*fixed (i.e. box operational state ‘Start’)*
Refinement	SFP	box state control policy (BSCP)
Assignment	*the authorised identified roles*	*no role*
Refinement	or information	—

Management:
There are no management activities foreseen.

Audit:
The following actions should be auditable:

~~a) Basic: Modifications of the default setting of permissive or restrictive rules.~~

~~b) Basic: All modifications of the initial values of security attributes.~~

FMT_SMF.1 Specification of Management Functions

“Specification of Management Functions” requires that the TSF provide specific management functions.

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: {

a) confirmation of the correctness of the system time during initial start-up; and

b) identification of the election district

}.

Operation	Template	Result
Assignment	*list of security management functions to be provided by the TSF*	*a) confirmation of the correctness of the system time during initial start-up and recovery; and* *b) identification of the election district*

Management:
There are no management activities foreseen.

Audit:
The following actions should be auditable:
a) Minimal: Use of the management functions.

FPR_ANO.2 Anonymity without soliciting information

“Anonymity” requires that other users or subjects are unable to determine the identity of a user bound to a subject or operation.
“Anonymity without soliciting information” enhances the requirements of “Anonymity” by ensuring that the TSF does not ask for the user identity.

Hierarchical to: FPR_ANO.1 Anonymity

Dependencies: No dependencies.

FPR_ANO.2.1 The TSF shall ensure that {*all subjects*} are unable to determine the real user name bound to {*digital election pens*}.

FPR_ANO.2.2 The TSF shall provide {*the vote casting service*} to {*the pen handler and the box handler*} without soliciting any reference to the real user name.

APPLICATION NOTE: If no personal data are captured, the confirmation of the lack of such functionality is enough.

Operation	Template	Result
Assignment	*set of users and/or subjects*	*all subjects*
Assignment	*list of subjects and/or operations and/or objects*	*digital election pens*
Assignment	*list of services*	*the vote casting service*
Assignment	*list of subjects*	*the pen handler and the box handler*

Management:
There are no management activities foreseen.

Audit:
The following actions should be auditable:
~~a) Minimal: The invocation of the anonymity mechanism.~~

FPR_UNL.1 Unlinkability

“Unlinkability” requires that users and/or subjects are unable to determine whether the same user caused certain specific operations in the system.

Hierarchical to: No other components.

Dependencies: No dependencies.

FPR_UNL.1.1 The TSF shall ensure that {*all users*} are unable to determine whether {*storing operations*} {*are related as follows: storing operations have been executed in a distinguished sequence or at special point in time*}.

Operation	Template	Result
Assignment	*set of users and/or subjects*	*all users*
Assignment	*list of operations*	*storing operations*
Selection	*were caused by the same user, are related as follows* [assignment: *list of relations*]	*are related as follows* [assignment: *list of relations*]
Assignment (selected)	*list of relations*	*storing operations have been executed in a distinguished sequence*

Management:
There are no management activities foreseen.

Audit:
The following actions should be auditable:
~~a) Minimal: The invocation of the unlinkability mechanism.~~

FPT_AMT.1 Abstract machine testing

“Abstract machine testing” provides for testing of the underlying abstract machine.

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_AMT.1.1 The TSF shall run a suite of tests {*during initial start-up and during recovery*} to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

Operation	Template	Result
Selection	*during initial start-up, periodically during normal operation, at the request of an authorised user,* [assignment: *other conditions*]	*during initial start-up and* [assignment: *other conditions*]
Assignment (selected)	*other conditions*	*during recovery*

Management:
There are no management activities foreseen.

Audit:
The following actions should be auditable:
a) Basic: Execution of the tests of the underlying machine and the results of the tests.

FPT_FLS.1 Failure with preservation of secure state

“Failure with preservation of secure state” requires that the TSF preserve a secure state in the face of the identified failures.

Hierarchical to: No other components.

Dependencies: ADV_SPM.1 Informal TOE security policy model (satisfied)

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: {*any errors during the execution of the controlled operations (PSCP, BSCP and VCP)*}.

APPLICATION NOTE: The ST author shall clearly define the secure state to be preserved as a refinement of this component. The reason why it should be considered secure shall be provided as part of the TOE security policy model (ADV_SPM.1).

Operation	Template	Result
Assignment	*list of types of failures in the TSF*	*any errors during the execution of the controlled operations (PSCP, BSCP and VCP)*

Management:
There are no management activities foreseen.

Audit:
The following actions should be auditable:
a) Basic: Failure of the TSF.

FPT_PHP.1 Passive detection of physical attack

“Passive detection of physical attack” provides for features that indicate when a TSF device or TSF element is subject to tampering. However, notification of tampering is not automatic; an authorised user must perform manual inspection to determining if tampering has occurred.

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.1.1 The TSF shall provide unambiguous detection of {physical tampering with the digital election pens (e.g. modification or substitution) that might compromise the TSF}.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the {digital election pens} has occurred.

Operation	Template	Result
Refinement	physical tampering that might compromise the TSF	physical tampering with the digital election pens (e.g. modification or substitution) that might compromise the TSF
Refinement	TSF's devices or TSF's elements	digital election pens

Management:
There are no management activities foreseen.

Audit:
The following actions should be auditable:
~~a) Minimal: if detection by IT means, detection of intrusion.~~

FPT_PHP.3 Resistance to physical attack

“Resistance to physical attack” provides for features that prevent or resist physical tampering with TSF devices and TSF elements.

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1 The TSF shall resist {*substitution or modification of firmware as tampering scenarios*} to the {*digital election pens*} by responding automatically such that the TSP is not violated.

Operation	Template	Result
Assignment	*physical tampering scenarios*	*Substitution or modification of firmware as tampering scenarios*
Assignment	*list of TSF devices/elements*	*digital election pens*

Management:
There are no management activities foreseen.

Audit:
There are no auditable events foreseen.

FPT_RCV.1 Manual recovery

“Manual recovery” allows a TOE to only provide mechanisms that involve human intervention to return to a secure state.

Hierarchical to: No other components.

Dependencies: AGD_ADM.1 Administrator guidance (satisfied)

ADV_SPM.1 Informal TOE security policy model (satisfied)

FPT_RCV.1.1 After {*system crash/shutdown, media failure*} the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

APPLICATION NOTE: The ST author shall clearly define the secure state to be preserved as a refinement of this component. The reason why it should be considered secure shall be provided as part of the TOE security policy model (ADV_SPM.1).

Operation	Template	Result
Assignment	*list of failures/service discontinuities*	*system crashes/shutdowns, media failures*

Management:
There are no management activities foreseen.

Audit:
The following actions should be auditable:
a) Minimal: the fact that a failure or service discontinuity occurred;
b) Minimal: resumption of the regular operation;
c) Basic: type of failure or service discontinuity.

FPT_RCV.4 Function recovery

“Function recovery” provides for recovery at the level of particular SFs, ensuring either successful completion or rollback of TSF data to a secure state.

Hierarchical to: No other components.

Dependencies: ADV_SPM.1 Informal TOE security policy model (satisfied)

FPT_RCV.4.1 The TSF shall ensure that {*all SFs and the failure scenarios ‘system crash/shutdown’ and ‘media failure’*} have the property that the SF either completes successfully, or for the indicated failure scenarios, recovers to a {consistent and secure state including the consistency constraint that any incompletely stored ballots are removed from the ballot box.}.

APPLICATION NOTE: The ST author shall clearly define the consistent and secure state to be recovered as a further refinement of this component. The reason why it should be considered consistent and secure shall be provided as part of the TOE security policy model (ADV_SPM.1).

Operation	Template	Result
Assignment	*list of SFs and failure scenarios*	*all SFs and the failure scenarios ‘system crash/shutdown’ and ‘media failure’*
Refinement	consistend and secure state	consistent and secure state including the consistency constraint that any incompletely stored ballots are removed from the ballot box.

Management:
There are no management activities foreseen.

Audit:
The following actions should be auditable:

a) Minimal: if possible, the impossibility to return to a secure state after failure of a security function;

b) Basic: if possible, the detection of a failure of a security function.

FPT_TST.1 TSF testing

“TSF testing” provides the ability to test the TSF's correct operation. These tests may be performed at start-up, periodically, at the request of the authorised user, or when other conditions are met. It also provides the ability to verify the integrity of TSF data and executable code.

Hierarchical to: No other components.

Dependencies: FPT_AMT.1 Abstract machine testing (satisfied)

FPT_TST.1.1 The TSF shall run a suite of self tests {*during initial start-up and during recovery*} to demonstrate the correct operation of {*the TSF*}.

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of {*all parts of TSF*}.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

Operation	Template	Result
Selection	*during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions* [assignment: *conditions under which self test should occur*]	*during initial start-up and at the conditions* [assignment: *conditions under which self test should occur*]
Refinement + Assignment (selected)	*at the conditions* [assignment: *conditions under which self test should occur*]	*during recovery*
Selection	[assignment: *parts of TSF*], *the TSF*	*the TSF*
Selection	[assignment: *parts of TSF*], *TSF data*	[assignment: *parts of TSF*]
Assignment (selected)	[assignment: *parts of TSF*]	*all parts of TSF*

Management:
There are no management activities foreseen.

Audit:
The following actions should be auditable:
a) Basic: Execution of the TSF self tests and the results of the tests.

FRU_FLT.1 Degraded fault tolerance

“Degraded fault tolerance” requires the TOE to continue correct operation of identified capabilities in the event of identified failures.

Hierarchical to: No other components.

Dependencies: FPT_FLS.1 Failure with preservation of secure state (satisfied)

FRU_FLT.1.1 The TSF shall ensure the operation of {*the vote casting service*} when the following failures occur: {*malfunction of an individual digital election pen*}.

Operation	Template	Result
Assignment	*list of TOE capabilities*	*the vote casting service*
Assignment	*list of type of failures*	*malfunction of an individual digital election pen*

Management:
There are no management activities foreseen.

Audit:
The following actions should be auditable:

a) Minimal: Any failure detected by the TSF.

b) Basic: All TOE capabilities being discontinued due to a failure.

5.1.2 Anforderungen an die Vertrauenswürdigkeit des EVG

Die Darlegung der Anforderungen an die Vertrauenswürdigkeit des EVG gibt die Vertrauenswürdigkeitsanforderungen als Vertrauenswürdigkeitsstufe (Evaluation Assurance Level – EAL) aus Teil 3 der CC an.

Die Anforderungen an die Vertrauenswürdigkeit des EVG bestehen aus allen Anforderungskomponenten der Vertrauenswürdigkeitsstufe EAL 3. Die Anforderungen werden mit den Komponenten ADV_SPM.1 und AVA_MSU.3 (ersetzt AVA_MSU.1) erweitert.

Assurance Class	Assurance component	
ACM: Configuration management	ACM_CAP.3	Authorisation controls
	ACM_SCP.1	TOE CM coverage
ADO: Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.2	Security enforcing high-level design
	ADV_SPM.1	**Informal TOE security policy model**
	ADV_RCR.1	Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
ALC: Life cycle support	ALC_DVS.1	Identification of security measures
ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	**AVA_MSU.3**	**Analysis and testing for insecure states**
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

Tabelle 6: Komponenten der Anforderungen an die Vertrauenswürdigkeit des EVG

5.2 Sicherheitsanforderungen an die IT-Umgebung

Functional Class	Functional component	
FAU: Security Audit	FAU_SAR.1	Audit review
	FAU_STG.1	Protected audit trail storage
FDP: User Data Protection	FDP_ACC.1	Subset Access Control
	FDP_ACF.1	Security attribute based access control
FIA: Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
	FIA_USB.1	User-subject binding
FMT: Security Management	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_SMF.1E	Specification of Management Functions
	FMT_SMR.1	Security roles
FPT: Protection of the TSF	FPT_STM.1	Reliable time stamps

Tabelle 7: Komponenten der funktionalen Sicherheitsanforderungen an die IT-Umgebung

FAU_SAR.1 Audit review

“Audit review” provides the capability to read information from the audit records.

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation (satisfied)

This component will provide authorised users the capability to obtain and interpret the information. In case of human users this information needs to be in a human understandable presentation. In case of external IT entities the information needs to be unambiguously represented in an electronic fashion.

FAU_SAR.1.1 The {SF of the IT environment} shall provide [assignment: *authorised users*] with the capability to read {*all audit information*} from the audit records.

FAU_SAR.1.2 The {SF of the IT environment} shall provide the audit records in a manner suitable for the user to interpret the information.

Operation	Template	Result
Refinement	TSF	SF of the IT environment
Assignment	*authorised users*	to be specified by the ST author; possibly: *authorised administrators*
Assignment	*list of audit information*	*all audit information*
Refinement	TSF	SF of the IT environment

Management:
The following actions could be considered for the management functions in FMT:

a) maintenance (deletion, modification, addition) of the group of users with read access right to the audit records.

Audit:
The following actions should be auditable if FAU_GEN „Security audit data generation“ is included in the ST as security functional requirement for the IT environment:

a) Basic: Reading of information from the audit records.

FAU_STG.1 Protected audit trail storage

At “Protected audit trail storage” requirements are placed on the audit trail. It will be protected from unauthorised deletion and/or modification.

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation (satisfied)

FAU_STG.1.1 The {SF of the IT environment} shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2 The {SF of the IT environment} shall be able to {*prevent*} unauthorised modifications to the stored audit records in the audit trail.

Operation	Template	Result
Refinement	TSF	SF of the IT environment
Selection, choose one of	*prevent, detect*	*prevent*

Management:
There are no management activities foreseen.

Audit:
There are no auditable events foreseen.

FDP_ACC.1 Subset access control

“Subset access control” requires that each identified access control SFP be in place for a subset of the possible operations on a subset of the objects in the TOE.

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control (satisfied)

FDP_ACC.1.1 **The {SF of the IT environment} shall enforce the {*Discretionary Access Control Policy*} on {*[assignment: list of subjects] acting on the behalf of users, [assignment: list of named objects] and all operations among subjects and objects covered by the DAC policy*}.**

Operation	Template	Result
Refinement	TSF	SF of the IT environment
Assignment	*access control SFP*	*Discretionary Access Control Policy*
Assignment	*list of subjects, objects, and operations among subjects and objects covered by the SFP*	*[assignment: list of subjects] acting on the behalf of users, [assignment: list of named objects] and all operations among subjects and objects covered by the DAC policy*
Assignment (assigned)	*list of subjects*	to be specified by the ST author
Assignment (assigned)	*list of named objects*	to be specified by the ST author

Management:
There are no management activities foreseen.

Audit:
There are no auditable events foreseen.

FDP_ACF.1 Security attribute based access control

“Security attribute based access control” allows the TSF to enforce access based upon security attributes and named groups of attributes. Furthermore, the TSF may have the ability to explicitly authorise or deny access to an object based upon security attributes.

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control (satisfied)

FMT_MSA.3 Static attribute initialization (satisfied)

FDP_ACF.1.1 **The {SF of the IT environment} shall enforce the {*Discretionary Access Control Policy*} to objects based on the following: {**

a) The user identity and group membership(s) associated with a subject; and

b) The following access control attributes associated with an object:
[assignment: List of access control attributes.
The attributes must provide permission attributes with:

i) the ability to associate allowed or denied operations with one or more user identities;

ii) the ability to associate allowed or denied operations with one or more group identities; and

iii) defaults for allowed or denied operations.]

}.

FDP_ACF.1.2 **The {SF of the IT environment} shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: {*[assignment: a set of rules specifying the Discretionary Access Control policy, where:***

i) For each operation there shall be a rule, or rules, that use the permission attributes where the user identity of the subject matches a user identity specified in the access control attributes of the object;

ii) For each operation there shall be a rule, or rules, that use the permission attributes where the group membership of the subject matches a group identity specified in the access control attributes of the object; and

iii) For each operation there shall be a rule, or rules, that use the default permission attributes specified in the access control attributes of the object when neither a user identity nor group identity matches.]

}.

FDP_ACF.1.3 **The {SF of the IT environment} shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects]*.**

FDP_ACF.1.4 **The {SF of the IT environment} shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].**

Operation	Template	Result
Refinement	TSF	SF of the IT environment
Assignment	*access control SFP*	*Discretionary Access Control Policy*
Assignment	*list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*	*a) The user identity and group membership(s) associated with a subject; and* *b) The following access control attributes associated with an object:* *[assignment: List of access control attributes. The attributes must provide permission attributes with:* *i) …* *ii) …* *iii) …]*
Assignment (assigned)	*List of access control attributes. The attributes must provide permission attributes with:* *i) …* *ii) …* *iii) …*	to be specified by the ST author
Refinement	TSF	SF of the IT environment
Assignment	*rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*	*[assignment: a set of rules specifying the Discretionary Access Control policy, where:* *i) …* *ii) …* *iii) …]*
Assignment (assigned)	*a set of rules specifying the Discretionary Access Control policy, where:* *i) …* *ii) …* *iii) …*	to be specified by the ST author
Refinement	TSF	SF of the IT environment
Assignment	*rules, based on security attributes, that explicitly authorise access of subjects to objects*	to be specified by the ST author
Refinement	TSF	SF of the IT environment
Assignment	*rules, based on security attributes, that explicitly deny access of subjects to objects*	to be specified by the ST author

Management:
The following actions could be considered for the management functions in FMT:

a) Managing the attributes used to make explicit access or denial based decisions.

Audit:
The following actions should be auditable:

a) Minimal: Successful requests to perform an operation on an object covered by the SFP.
b) Basic: All requests to perform an operation on an object covered by the SFP.
c) Detailed: The specific security attributes used in making an access check.

FIA_ATD.1 User attribute definition

“User attribute definition” allows user security attributes for each user to be maintained individually.

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 **The {SF of the IT environment} shall maintain the following list of security attributes belonging to individual users: {**

a) User Identifier;
b) Group Memberships;
c) Authentication Data;
d) Security-relevant Roles; and
e) [assignment: other user security attributes].
}

Operation	Template	Result
Refinement	TSF	SF of the IT environment
Assignment	*list of security attributes*	*a)* … *b)* … *c)* … *d)* … *e)* …
Assignment (assigned)	*other user security attributes*	to be specified by the ST author

Management:
The following actions could be considered for the management functions in FMT:

a) if so indicated in the assignment, the authorised administrator might be able to define additional security attributes for users.

Audit:
There are no auditable events foreseen.

FIA_UAU.2 User authentication before any action

“User authentication before any action” requires that users are authenticated before any action will be allowed by the TSF.

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification (satisfied)

FIA_UAU.2.1 The {SF of the IT environment} shall require each user to be successfully authenticated before allowing any other {actions mediated by the SF of the IT environment} on behalf of that user.

Operation	Template	Result
Refinement	TSF	SF of the IT environment
Refinement	TSF-mediated actions	actions mediated by the SF of the IT environment

Management:
The following actions could be considered for the management functions in FMT:
a) management of the authentication data by an administrator;
b) management of the authentication data by the user associated with this data.

Audit:
The following actions should be auditable if FAU_GEN „Security audit data generation“ is included in the ST as security functional requirement for the IT environment:
a) Minimal: Unsuccessful use of the authentication mechanism;
b) Basic: All use of the authentication mechanism.

FIA_UAU.7 Protected authentication feedback

“Protected authentication feedback” requires that only limited feedback information is provided to the user during the authentication.

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication (satisfied)

FIA_UAU.7.1 The {SF of the IT environment} shall provide only {*obscured feedback*} to the user while the authentication is in progress.

Operation	Template	Result
Refinement	TSF	SF of the IT environment
Assignment	*list of feedback*	*obscured feedback*

Management:
There are no management activities foreseen.

Audit:
There are no auditable events foreseen.

FIA_UID.2 User identification before any action

“User identification before any action” requires that users identify themselves before any action will be allowed by the TSF.

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1 The {SF of the IT environment} shall require each user to identify itself before allowing any other {actions mediated by the SF of the IT environment} on behalf of that user.

Operation	Template	Result
Refinement	TSF	SF of the IT environment
Refinement	TSF-mediated actions	actions mediated by the SF of the IT environment

Management:
The following actions could be considered for the management functions in FMT:
a) the management of the user identities.

Audit:
The following actions should be auditable if FAU_GEN „Security audit data generation“ is included in the ST as security functional requirement for the IT environment:
a) Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided;
b) Basic: All use of the user identification mechanism, including the user identity provided.

FIA_USB.1 User-subject binding

“User-subject binding” requires the specification of any rules governing the association between user attributes and the subject attributes into which they are mapped.

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition (satisfied)

FIA_USB.1.1 **The {SF of the IT environment} shall associate the following user security attributes with subjects acting on the behalf of that user: {**

a) The user identity or identities which are used to enforce the Discretionary Access Control Policy;

b) The group membership or memberships used to enforce the Discretionary Access Control Policy;

c) [assignment: any other user security attributes].

}

FIA_USB.1.2 **The {SF of the IT environment} shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: *rules for the initial association of attributes*].**

FIA_USB.1.3 **The {SF of the IT environment} shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: *rules for the changing of attributes*].**

Operation	Template	Result
Refinement	TSF	SF of the IT environment
Assignment	*list of user security attributes*	a) … b) … c) …
Assignment (assigned)	*any other user security attributes*	to be specified by the ST author
Refinement	TSF	SF of the IT environment
Assignment	*rules for the initial association of attributes*	to be specified by the ST author
Refinement	TSF	SF of the IT environment
Assignment	*rules for the changing of attributes*	to be specified by the ST author

Management:
The following actions could be considered for the management functions in FMT:

a) an authorised administrator can define default subject security attributes.
b) an authorised administrator can change subject security attributes.

Audit:
The following actions should be auditable if FAU_GEN „Security audit data generation“ is included in the ST as security functional requirement for the IT environment:

a) Minimal: Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject).
b) Basic: Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject).

FMT_MSA.1 Management of security attributes

“Management of security attributes” allows authorised users (roles) to manage the specified security attributes.

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control (satisfied), or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles (satisfied)

FMT_SMF.1 Specification of Management Functions (satisfied by FMT_SMF.1E)

FMT_MSA.1.1 **The {SF of the IT environment} shall enforce the {*Discretionary Access Control Policy*} to restrict the ability to {*modify*} the security attributes {*access control attributes associated with a named object*} to [assignment: *the authorised identified roles*].**

Operation	Template	Result
Refinement	TSF	SF of the IT environment
Assignment	*access control SFP, information flow control SFP*	*Discretionary Access Control Policy*
Selection	*change_default, query, modify, delete,* [assignment: *other operations*]	*modify*
Assignment	*list of security attributes*	*access control attributes associated with a named object*
Assignment	*the authorised identified roles*	to be specified by the ST author

Management:
The following actions could be considered for the management functions in FMT:

a) Managing the group of roles that can interact with the security attributes.

Audit:
The following actions should be auditable:

a) Basic: All modifications of the values of security attributes.

FMT_MSA.3 Static attribute initialisation

“Static attribute initialization” ensures that the default values of security attributes are appropriately either permissive or restrictive in nature.

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes (satisfied)

FMT_SMR.1 Security roles (satisfied)

FMT_MSA.3.1 The {SF of the IT environment} shall enforce the {*Discretionary Access Control Policy*} to provide {*restrictive*} default values for security attributes that are used to enforce the {Discretionary Access Control Policy}.

FMT_MSA.3.2 The {SF of the IT environment} shall allow the [assignment: *the authorised identified roles*] to specify alternative initial values to override the default values when an object or information is created.

Operation	Template	Result
Refinement	TSF	SF of the IT environment
Assignment	*access control SFP, information flow control SFP*	*Discretionary Access Control Policy*
Selection, choose one of	*restrictive, permissive,* [assignment: *other property*]	*restrictive*
Refinement	SFP	Discretionary Access Control Policy
Refinement	TSF	SF of the IT environment
Assignment	*the authorised identified roles*	to be specified by the ST author

Management:
The following actions could be considered for the management functions in FMT:

a) managing the group of roles that can specify initial values;
b) managing the permissive or restrictive setting of default values for a given access control SFP.

Audit:
The following actions should be auditable:

a) Basic: Modifications of the default setting of permissive or restrictive rules.
b) Basic: All modifications of the initial values of security attributes.

FMT_SMF.1E Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1E.1 The {SF of the IT environment} shall be capable of performing the following security management functions: [assignment: list of security management functions to be provided by the TSF].

Operation	Template	Result
Refinement	TSF	SF of the IT environment
Assignment	*list of security management functions to be provided by the TSF*	to be specified by the ST author

Management:
There are no management activities foreseen.

Audit:
The following actions should be auditable:
a) Minimal: Use of the management functions.

FMT_SMR.1 Security roles

“Security roles” specifies the roles with respect to security that the TSF recognises.

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification (satisfied)

FMT_SMR.1.1 The {SF of the IT environment} shall maintain the roles {

a) authorized administrator;
b) users authorized by the Discretionary Access Control Policy to modify object security attributes;
c) users authorized to modify their own authentication data; and
d) [assignment: other roles]
}.

FMT_SMR.1.2 The {SF of the IT environment} shall be able to associate users with roles.

Operation	Template	Result
Refinement	TSF	SF of the IT environment
Assignment	*the authorised identified roles*	a) … b) … c) … d) *[assignment: other roles]*
Assignment (assigned)	*other roles*	to be specified by the ST author
Refinement	TSF	SF of the IT environment

Management:
The following actions could be considered for the management functions in FMT:
a) Managing the group of users that are part of a role.

Audit:
The following actions should be auditable:
a) Minimal: modifications to the group of users that are part of a role;
b) Detailed: every use of the rights of a role.

FPT_STM.1 Reliable time stamps

“Reliable time stamps” requires that the TSF provide reliable time stamps for TSF functions.

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 The {SF of the IT environment} shall be able to provide reliable time stamps for {use within the TSF}.

Operation	Template	Result
Refinement	TSF	SF of the IT environment
Refinement	its own use	use within the TSF

Management:
The following actions could be considered for the management functions in FMT:

a) management of the time.

Audit:
The following actions should be auditable if FAU_GEN „Security audit data generation“ is included in the ST as security functional requirement for the IT environment:

a) Minimal: changes to the time;
b) Detailed: providing a timestamp.

6 PP-Anwendungsbemerkungen

Dieser optionale Teil des PP enthält zusätzliche Anwenderinformationen, die für die Erstellung, die Prüfung und Bewertung oder den Gebrauch des EVG relevant bzw. nützlich sein können.

6.1 Zugriffskontrollpolitiken

Der ST-Autor wird darauf hingewiesen, dass eine Erweiterung der beiden Zugriffskontrollpolitiken PSCP und BSCP mit zusätzlichen Attributen oder Operationen grundsätzlich zulässig ist. Allerdings muss jede solche Erweiterung folgende Beschränkungen beachten:

1) Die Erweiterung muss konsistent sein mit den Sicherheitscharakteristiken von PSCP und BSCP, die in den Regeln der Komponenten FDP_ACF.1A/B beschrieben sind.
2) Die Erweiterung muss die Sicherheitsprinzipien von PSCP und BSCP respektieren, die als Verfeinerung der Komponenten FDP_ACC.2A/B beschrieben sind.

6.2 EVG-Sicherheitsmodell

Im informellen EVG-Sicherheitsmodell soll der Hersteller eine strukturelle Darstellung der EVG-Sicherheitspolitik, die aus der Gesamtheit aller funktionalen EVG-Sicherheitsanforderungen besteht, bereitstellen. Der Schwerpunkt des Modells soll in einer klaren und begründeten Definition der von den Komponenten FPT_FLS.1, FPT_RCV.1 und FPT_RCV.4 geforderten sicheren Zustände liegen. Das EVG-Sicherheitsmodell muß insbesondere die Wechselwirkungen mit den Objekten und zugehörigen Attributen der Zugriffskontrollpolitiken PSCP und BSCP darstellen.

Es wird empfohlen, das EVG-Sicherheitsmodell (Element ADV_SPM.1.2C) als Ergänzung der funktionalen EVG-Sicherheitsanforderungen in die Sicherheitsvorgaben zu integrieren. Der Nachweis der Konsistenz und Vollständigkeit des EVG-Sicherheitsmodells (Element ADV_SPM.1.3C) soll die Erklärung der gegenseitigen Unterstützung der Sicherheitsanforderungen ergänzen.

6.3 Controled Access Protection Profile (CAPP)

Die Komponenten

- FAU_SAR.1, FAU_STG.1,
- FDP_ACC.1 ,FDP_ACF.1,
- FIA_ATD.1, FIA_UAU.2, FIA_UAU.7, FIA_UID.2, FIA_USB.1 und
- FMT_MSA.1, FMT_MSA.3, FMT_SMR.1

sind Sicherheitsanforderungen an die IT-Umgebung, die vom unterliegenden Betriebssystem erfüllt werden können. Sie sind konform zu den entsprechenden Anforderungen des Conroled Access Protection Profile [CAPP] formuliert. Weil eine breite Auswahl an zertifizierten Betriebssystemen diesen Anforderungen genügt, wird dem ST-Autor empfohlen, ihre Erfüllung durch die Verwendung eines solchen Bestriebssystems nachzuweisen.

7 Erklärung

Dieser Teil des PP stellt den Nachweis zur Prüfung und Bewertung des PP dar. Dieser Nachweis unterstützt die Postulate, dass das PP eine vollständige und in sich geschlossene Menge von Anforderungen ist und dass ein zu diesem PP konformer EVG eine wirksame Menge von IT-Sicherheitsgegenmaßnahmen in der Sicherheitsumgebung bereitstellt.

7.1 Erklärung der Sicherheitsziele

Die Erklärung der Sicherheitsziele weist nach, dass die dargelegten Sicherheitsziele auf alle Aspekte, die in der EVG-Sicherheitsumgebung identifiziert werden, zurückverfolgbar sind und dass sie geeignet sind, diese abzudecken.

Die Rückverfolgung der Sicherheitsziele auf die Bedrohungen und organisatorischen Sicherheitspolitiken ist in Tabelle 8 dargestellt. Die Eignung zur Abdeckung dieser Aspekte der EVG-Sicherheitsumgebung wird im Folgenden nachgewiesen. Die Abdeckung der Annahmen ist durch deren erneute Darlegung als Sicherheitsziele für die Umgebung offensichtlich. Die Identifier wurden entsprechend gleich gewählt (A.* entspricht OE.*).

T.Anonymität Der allgemeine Verzicht auf die Erfassung von Daten, die die Anonymität der Wähler gefährden (OT.Anonymität) wird durch das Verbot der Erzeugung von Belegen für die Stimmabgabe (OT.Quittungsfreiheit) ergänzt. Außerdem stellt das Ziel der IT-Umgebung OE.Schadsoftware sicher, dass keine Schadsoftware auf den Rechnern ist, insbesondere auch keine, mit deren Hilfe die Anonymität gebrochen werden kann. Damit wird die Bedrohung für alle potentiellen Angreifer, einschließlich des Wählers selbst, vollständig entfernt.

T.Beweis Das Verbot der Erzeugung von Belegen für die Stimmabgabe (OT.Quittungsfreiheit) nimmt allen potentiellen Angreifern, einschließlich des Wählers selbst, die Möglichkeit zum Beweis der Stimmabgabe. Zwar können während des Wahlvorgangs Daten aus dem Stift ausgelesen werden. Diese sind aber als Beweis für die Stimmabgabe nicht geeignet, weil sie keinen Beleg für die Registrierung der Stimmen enthalten. Damit wird die Bedrohung vollständig entfernt.

T.Betriebsstörung Technischen Betriebsstörungen wird durch die Behandlung von Störungen und Fehlern und die sichere Wiederanlauffunktion (OT.Robustheit) in Zusammenhang mit der Feststellbarkeit und Erkennbarkeit des EVG-Zustandes (OT.Verifikation) begegnet. Die Wirksamkeit dieser Ziele wird durch materielle (OE.Schadsoftware, OE.Speicherung, OE.Zugang, OE.Zutritt), personelle (OE.Personal, OE.Wahlvorstand) und Vernetzbarkeitsziele (OE.Verbindung) der Umgebung unterstützt. Damit werden die Auswirkungen der Bedrohung auf ein akzeptables Niveau abgeschwächt.

T.ManipulationStift Einer versuchten Manipulation der Firmware des Digitalen Wahlstifts wird durch den EVG widerstanden (OT.Verifikation). Soweit eine materielle Manipulation nicht vom Digitalen Wahlstift selbst verhindert wird, tragen materielle Ziele (OE.Verbindung, OE.Zutritt, OE.Schadsoftware) der Umgebung zur Wirksamkeit dieses Widerstands bei. Dieser Aspekt der Bedrohung wird damit vollständig entfernt.

Materielle Manipulationen an der Hardware des Digitalen Wahlstifts können grundsätzlich nicht verhindert werden. Sie sind jedoch erkennbar (OT.Verifikation) und entsprechende Handlungen sind durch personnelle Ziele der Umgebung (OE.Personal, OE.Wahlvorstand) gewährleistet. Die Auswirkungen dieses Aspekts der Bedrohung werden damit auf ein akzeptables Niveau abgeschwächt.

T.ManipulationErgebnis Dem Versuch, die Wahldaten nach dem Ende der Wahl auszutauschen oder zu verändern, wird mit einer manipulationssicheren Speicherung der Wahldaten begegnet (OT.Ergebnisfeststellung). Dem Versuch, die Wahldaten gegen echte Wahldaten eines anderen Wahllokals auszutauschen, wird durch die Kennzeichnung mit einem eindeutigen Nachweis des Ursprungs (zugehöriges Wahllokal) begegnet (OT.Ergebnisfeststellung). Die Wirksamkeit dieses Ziels wird durch materielle (OE.Schadsoftware, OE.Zugang, OE.Zugriff, OE.Zutritt) und personelle (OE.Personal, OE.Wahlvorstand) Ziele der Umgebung unterstützt. Damit werden die Auswirkungen der Bedrohung auf ein akzeptables Niveau abgeschwächt.

T.Verkettbarkeit Eine Ermittlung der Zeit und/oder der Reihenfolge der Speicherung der Stimmdatensätze in der Urne ist nicht möglich, da der EVG für die Speicherung einen Mechanismus verwendet, der gewährleistet, dass weder die Zeit noch die Reihenfolge der Speicherung rekonstruierbar sind (OT.Unverkettbarkeit). Die Wirksamkeit dieses Ziels wird durch materielle Ziele der Umgebung (OE.Schadsoftware, OE.Verbindung, OE.Zugang, OE.Zugriff, OE.Zutritt) unterstützt. Damit werden die Auswirkungen der Bedrohung auf ein akzeptables Niveau abgeschwächt.

T.Wahlvorgang Dem Versuch, vor Beginn des Wahlvorgangs Daten, die als Bestandteil der Stimme abgegeben werden, in den Digitalen Wahlstift zu bringen, wird durch den EVG entgegengewirkt, da nur die während des Wahlvorgangs in den Digitalen Wahlstift eingebrachten Stimmen abgegeben werden können und nur über das elektronische Auge Stimmen in den Digitalen Wahlstift eingebracht werden können (OT.Aufzeichnung). Dem Versuch, während des Wahlvorgangs Daten, die als Bestandteil der Stimme abgegeben werden, in den Digitalen Wahlstift zu bringen, wird entgegengewirkt, da zu Beginn jedes Wahlvorgangs der Speicher des Digitalen Wahlstifts gelöscht und der Stift für die Aufzeichnung von Stimmen freigeschaltet wird (OT.Wahlvorgang). Darüber hinaus wird diesem Versuch dadurch entgegengewirkt, dass zum Ende jedes Wahlvorgangs die aufgezeichneten Stimmen vom Digitalen Wahlstift gelöscht werden und der Stift für die Aufzeichnung von Stimmen gesperrt wird (OT.Wahlvorgang). Die Wirksamkeit dieser Ziele wird durch materielle Ziele der Umgebung (OE.Schadsoftware, OE.Verbindung, OE.Zutritt) und personelle Ziele (OE.Wahlvorstand) der Umgebung unterstützt. Damit werden die Auswirkungen der Bedrohung auf ein akzeptables Niveau abgeschwächt.

P.Ergebnisermittlung Diese Sicherheitspolitik fordert zunächst, dass die in der Urne gespeicherten Stimmdatensätze ausgewertet werden. Dies ist abgedeckt, da in OT.Bewertung das Ziel formuliert ist, dass die Bewertung grundsätzlich automatisch erfolgt. Außerdem fordert die Politik, dass der Wahlvorstand über unklare Stimmen entscheidet. Dies wird durch das Ziel OT.Bewertung erreicht. Die Sicherheitspolitik P.Ergebnisermittlung fordert außerdem, dass die Anzahl der gültigen und ungültigen Stimmdatensätze ermittelt wird. Dies wird durch das Ziel OT.Auszählung erreicht. Außerdem fordert die Politik, dass für alle gültigen Stimmdatensätze das summarische Ergebnis berechnet wird. Dies wird durch das Ziel OT.Auszählung erreicht. Die Wirksamkeit dieser Ziele wird durch materielle (OE.Schadsoftware, OE.Speicherung, OE.Konfiguration, OE.Zugang, OE.Zugriff, OE.Zutritt) und personelle Ziele (OE.Administrator, OE.Wahlvorstand, OE.Personal) der Umgebung unterstützt.

P.Ergebnisfeststellung Die Sicherheitspolitik wird mit dem Ziel OT.Ergebnisfeststellung erreicht, da hier der Ausdruck des Ergebnisses gefordert wird. Die Wirksamkeit dieses Ziel wird durch materielle (OE.Schadsoftware, OE.Zugang, OE.Zugriff, OE.Zutritt) und personelle Ziele (OE.Wahlvorstand, OE.Personal) der Umgebung unterstützt.

P.Protokollierung Die Abdeckung dieser Sicherheitspolitik ist durch deren erneute Darlegung als Sicherheitsziel in OT.Protokollierung offensichtlich Die Wirksamkeit dieses Ziels wird durch materielle Ziele der Umgebung unterstützt (OE.Protokollschutz, OE.Schadsoftware, OE.Speicherung, OE.Zugang).

P.Wahlhandlung Diese Sicherheitspolitik fordert zunächst, dass die Anzeige, Bewertung und die Auszählung von Stimmdatensätzen erst nach dem Schluss der Wahlhandlung erfolgen darf. Diese Forderung ist für den Fall der Bewertung und Auszählung durch die Ziele OT.Bewertung und OT.Auszählung erreicht sowie für den Fall der Anzeige durch das Ziel OT.Quittungsfreiheit. Außerdem fordert diese Politik, dass der Schluss der Wahlhandlung nicht rückgängig gemacht werden darf. Dies wird durch das Ziel OT.Wahlhandlung erreicht. Des Weiteren fordert diese Sicherheitspolitik, dass der Schluss der Wahlhandlung vom Wahlvorstand explizit bestätigt werden muss. Dies wird durch das Ziel OT.Wahlhandlung erreicht. Die Wirksamkeit dieser Ziele wird durch materielle (OE.Schadsoftware, OE.Systemzeit, OE.Zugang, OE.Zutritt) und personelle Ziele (OE.Administrator, OE.Wahlvorstand, OE.Personal) der Umgebung unterstützt.

	T.Anonymität	T.Beweis	T.Betriebsstörung	T.ManipulationStift	T.ManipulationErgebnis	T.Verkettbarkeit	T.Wahlvorgang	P.Ergebnisermittlung	P.Ergebnisfeststellung	P.Protokollierung	P.Wahlhandlung
OT.Anonymität	×										
OT.Aufzeichnung							×				
OT.Auszählung								×			×
OT.Bewertung								×			×
OT.Ergebnisfeststellung					×				×		
OT.Protokollierung										×	
OT.Quittungsfreiheit	×	×									×
OT.Robustheit			×								
OT.Unverkettbarkeit						×					
OT.Verifikation			×	×							
OT.Wahlhandlung											×
OT.Wahlvorgang							×				
OE.Beobachtung											
OE.Berechtigung											
OE.Identifikation											
OE.Notfallvorsorge											
OE.Stimmzettel											
OE.Administrator								×			×
OE.Konfiguration								×			
OE.Personal			×	×	×			×	×		×
OE.Protokollschutz										×	
OE.Schadsoftware	×		×	×	×	×	×	×	×	×	×
OE.Speicherung			×					×		×	
OE.Systemzeit										×	×
OE.Verbindung			×	×		×	×				
OE.Wahlvorstand			×	×	×		×	×	×		×
OE.Zugang			×		×	×		×	×	×	×
OE.Zugriff					×	×		×	×		
OE.Zutritt			×	×	×	×	×	×	×		×

Tabelle 8: Rückverfolgung der Sicherheitsziele

7.2 Erklärung der Sicherheitsanforderungen

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

1) Die Kombination aus den einzelnen Komponenten der funktionalen und Vertrauenswürdigkeitsanforderungen für den EVG und dessen IT-Umgebung zusammen erfüllt die dargelegten Sicherheitsziele.
2) Die Menge der Sicherheitsanforderungen zusammen bildet ein sich gegenseitig unterstützendes und in sich konsistentes Ganzes.
3) 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.
4) Die ausgewählte funktionale Stärkestufe des PP, zusammen mit jedem Postulat der expliziten funktionalen Stärke einer Funktion ist konsistent mit den Sicherheitszielen des EVG.

7.2.1 Erfüllung der Sicherheitsziele

Die Rückverfolgung der Sicherheitsanforderungen auf die Sicherheitsziele für den EVG ist in Tabelle 9 dargestellt. Die Rückverfolgung der Sicherheitsanforderungen auf die Sicherheitsziele für die IT-Umgebung ist in Tabelle 10 dargestellt. Die Eignung zur Abdeckung aller Aspekte der EVG-Sicherheitsumgebung wird im Folgenden nachgewiesen.

OT.Anonymität Die Komponente FDP_RIP.1A gewährleistet, dass der Digitale Wahlstift nach der Stimmabgabe keine Stimmen mehr enthält. Daher kann anhand des digitalen Stiftes keine Zuordnung zwischen Wähler und seiner Stimme hergestellt werden. Die Komponente FPR_ANO.2 gewährleistet, dass anhand der gespeicherten Daten keine Zuordnung zwischen Wähler und seiner Stimme möglich ist.

OT.Aufzeichnung Die Zugriffskontrollpolitik PSCP (FDP_ACC.2A, FDP_ACF.1A) gewährleistet in Kombination mit der Informationsflusskontrollpolitik VCP (FDP_IFC.2, FDP_IFF.1), dass nur die während eines Wahlvorgangs in den Digitalen Wahlstift eingebrachten Stimmen abgegeben werden können. Sie stellt außerdem sicher, dass nur über das elektronische Auge Stimmen in den Stift gelesen werden können. Die Komponente FDP_RIP.1A gewährleistet, dass der Digitale Wahlstift nach der Stimmabgabe keine Stimmen mehr enthält, die sonst möglicherweise nochmals abgegeben werden könnten. Die Sicherheitspolitiken werden durch die Überwachung der fehlerfreien Funktion des Digitalen Wahlstifts (FDP_SDI.2, FPT_PHP.1) unterstützt.

OT.Auszählung Die Zugriffskontrollpolitik BSCP (FDP_ACC.2B) gewährleistet, dass vor dem Ende der Wahlhandlung keine Ergebnisse berechnet werden können. Die Zugriffskontrollpolitik BSCP (FDP_ACF.1B) gewährleistet, dass auf der Basis aller gültigen Stimmdatensätze durch Auszählung das summarische Ergebnis sowie die Anzahl der gültigen und der ungültigen Stimmdatensätze ermittelt werden.

OT.Bewertung Die Zugriffskontrollpolitik BSCP (FDP_ACC.2B) gewährleistet, dass vor dem Ende der Wahlhandlung keine Ergebnisse und Bewertungen durchführbar sind. Die Zugriffskontrollpolitik BSCP (FDP_ACF.1B) gewährleistet, dass bei unklaren Stimmen die Entscheidung des Wahlvorstandes in der Urne gespeichert wird.

OT.Ergebnisfeststellung Die Komponenten FCO_NRO.2 und FMT_SMF.1 gewährleisten, dass zur Feststellung des Ergebnisses der EVG unter Kontrolle der Zugriffskontrollpolitik BSCP (FDP_ACF.1B.2 Buchstabe f) die Wahldaten vor unbemerkter Manipulation schützt und sie mit einem eindeutigen Nachweis ihres Ursprungs (zugehöriges Wahllokal) kennzeichnet. Die Zugriffskontrollpolitik BSCP (FDP_ACF.1B Buchstabe f) gewährleistet auch, dass nach der Auszählung ein Ausdruck des festgestellten Ergebnisses erfolgt.

OT.Protokollierung Die Komponenten FAU_GEN.1 gewährleisten, dass die in Tabelle 3 aufgelisteten Ereignisse vom EVG protokolliert werden. Durch die Komponente FMT_SMF.1 wird diese Anforderung unterstützt, da hier die korrekte Systemzeit gefordert wird, die für die Protokollierung erforderlich ist.

OT.Quittungsfreiheit Die Komponente FDP_RIP.1A gewährleistet, dass der Digitale Wahlstift nach der Stimmabgabe keine Stimmen mehr enthält. Daher kann anhand des digitalen Stiftes keine Zuordnung zwischen Wähler und seiner Stimme hergestellt werden. Die Komponente FPR_ANO.2 gewährleistet, dass anhand der gespeicherten Daten keine Zuordnung zwischen Wähler und seiner Stimme möglich ist. Damit können die gespeicherten Daten nicht genutzt werden, um einen Beweis zu erzeugen. Dies wird durch die Informationsflusskontrollpolitik VCP (FDP_IFC.2, FDP_IFF.1) unterstützt. Durch die Komponente FDP_ITT.2 wird gewährleistet, dass bei der Übertragung der Stimme in die Urne keine Information über den Inhalt fließen kann. Daher kann auch hier kein Beweis erzeugt werden. Durch die Komponente FPR_UNL.1 wird gewährleistet, dass anhand der im EVG gespeicherten Daten kein Beweis erzeugt werden kann, da niemand in der Lage ist, den Zusammenhang zwischen Stimmen und Wähler herzustellen (weder über die Zeit noch über die Reihenfolge).

OT.Robustheit Die Komponenten FPT_RCV.1 und FPT_RCV.4 gewährleisten, dass der EVG nach einer Betriebsstörung oder -unterbrechung in einen konsistenten und sicheren Betriebszustand zurückkehrt, einschließlich der Entfernung unvollständig gespeicherter Stimmdatensätze aus der Urne. Durch die Komponente FDP_SDI.2 wird sichergestellt, dass Lese- und Schreibfehler erkannt und gemeldet werden. Die Komponenten FPT_AMT.1 und FPT_TST.1 stellen sicher, dass nach einem Wiederanlauf die Funktionsfähigkeit überprüft wird. Diese Eigenschaft wird durch die Zugriffskontrollpolitik BSCP (FDP_ACC.2B, FDP_ACF.1B) und die Komponente FPT_FLS.1 unterstützt, da damit gewährleistet wird, dass durch eine Betriebsstörung oder -unterbrechung kein Wiederanlauf in einem anderen oder inkonsistenten Zustand möglich ist. Fehler bei der Übertragung der Stimme vom Wahlstift werden durch die Komponente FDP_ITT.4 behandelt. Diese Eigenschaften werden durch die Komponenten FPT_PHP.3 und FRU_FLT.1 unterstützt, da hierdurch sichergestellt wird, dass modifizierte bzw. fehlerhafte Wahlstifte erkannt werden. Schließlich wird die doppelte Speicherung von Stimmdatensätzen von der kontrollierten Operation ‚store’ (FDP_ACF.1B) verhindert. Die klare und begründete Definition der sicheren Zustände im EVG-Sicherheitsmodell (Komponente ADV_SPM.1) schafft zusätzliches Vertrauen in die wirksame Erfüllung des Sicherheitsziels.

OT.Unverkettbarkeit Durch die Komponente FPR_UNL.1 wird gewährleistet, dass anhand der im EVG gespeicherten Daten kein Beweis erzeugt werden kann, da niemand in der Lage ist den Zusammenhang zwischen Stimmen und Wähler herzustellen (weder über die Zeit noch über die Reihenfolge). Dies wird durch die Informationsflusskontrollpolitik VCP (FDP_IFC.2, FDP_IFF.1) unterstützt. Für die Übertragung wird die Unverkettbarkeit durch die Komponente FDP_ITT.2 gewährleistet.

OT.Verifikation Durch die Komponente FPT_PHP.1 wird gewährleistet, dass materielle Manipulationen an der Hardware des Digitalen Wahlstifts erkannt werden. Durch die Komponente FPT_PHP.3 ist gewährleistet, dass Manipulationsversuche an der Firmware des Digitalen Wahlstifts erkannt werden. Die Erkennung von fehlerhaften Wahlstiften ist durch die Komponente FRU_FLT.1 abgedeckt. Die Komponente FDP_SDI.2 gewährleistet, dass Integritätsfehler bei der Speicherung von Daten entdeckt werden. Zusammen mit der Komponente AVA_MSU.3 gewährleistet damit der EVG, dass zu jedem Zeitpunkt im Wahllokal der Zustand des EVG eindeutig feststellbar ist und die Wähler und der Wahlvorstand angemessene Hinweise bei Störungen des technischen Betriebs und bei entdeckten Manipulationen von Wahlstiften erhalten. Durch die Verwendung der Komponenten FPT_RCV.1 und FPT_RCV.4 gilt dies auch für den Zustand nach einem Wiederanlauf. Durch die Zugriffskontrollpolitik BSCP (FDP_ACC.2B, FDP_ACF.1B) wird schließlich sichergestellt, dass bei jedem Wahlvorgang eindeutig erkennbar ist, ob die Stimmen gelöscht (Annullierung) oder in der Urne gespeichert (Registrierung) wurden. Dies wird durch die Komponenten FDP_SDI.2 und FDP_ITT.4 unterstützt. Die klare und begründete Definition der sicheren Zustände im EVG-Sicherheitsmodell (Komponente ADV_SPM.1) schafft zusätzliches Vertrauen in die wirksame Erfüllung des Sicherheitsziels.

OT.Wahlhandlung Die Zugriffskontrollpolitik BSCP (FDP_ACC.2B, FDP_ACF.1B) gewährleistet, dass der Dienst der Stimmabgabe auf den Zeitraum der Wahlhandlung beschränkt ist und insbesondere die Komponente FDP_ACF.1B stellt sicher, dass der Schluss der Wahlhandlung nicht umkehrbar ist und erst explizit durch den Wahlvorstand bestätigt werden muss. Dies wird durch die Komponente FDP_SDI.2 unterstützt. Dass dies auch für den Startzeitraum gilt, stellt die Komponente FMT_MSA.3B sicher.

OT.Wahlvorgang Die Zugriffskontrollpolitik BSCP (FDP_ACC.2B, FDP_ACF.1B) und die Zugriffspolitik PSCP (FDP_ACC.2A, FDP_ACF.1A) gewährleisten zusammen mit der Informationsflusskontrolle aus FDP_IFC.2 und FDP_IFF.1, dass der EVG zu Beginn jedes Wahlvorgangs nach erfolgreicher Funktionsprüfung den Speicher des Digitalen Wahlstifts löscht und den Stift für die Aufzeichnung von Stimmen freigibt (Aktivierung). Außerdem stellt sie sicher, dass der EVG zum Ende des Wahlvorgangs die aufgezeichneten Stimmen vom Digitalen Wahlstift löscht und den Stift für die Aufzeichnung von Stimmen sperrt (Registrierung bzw. Annullierung). Dies wird durch die Komponenten FDP_RIP.1A, FDP_SDI.2 und FMT_MSA.3A unterstützt.

	OT.Anonymität	OT.Aufzeichnung	OT.Auszählung	OT.Bewertung	OT.Ergebnisfeststellung	OT.Protokollierung	OT.Quittungsfreiheit	OT.Robustheit	OT.Unverkettbarkeit	OT.Verifikation	OT.Wahlhandlung	OT.Wahlvorgang
ADV_SPM.1								×		×		
AVA_MSU.3										×		
FAU_GEN.1						×						
FCO_NRO.2					×							
FDP_ACC.2A		×										×
FDP_ACF.1A		×										×
FDP_ACC.2B			×	×				×		×	×	×
FDP_ACF.1B			×	×	×			×		×	×	×
FDP_IFC.2		×					×		×			×
FDP_IFF.1		×					×		×			×
FDP_ITT.2							×		×			
FDP_ITT.4								×		×		
FDP_RIP.1A	×	×					×					×
FDP_RIP.1B											×	
FDP_SDI.2		×						×		×	×	×
FMT_MSA.3A												×
FMT_MSA.3B											×	
FMT_SMF.1					×	×						
FPR_ANO.2	×						×					
FPR_UNL.1							×		×			
FPT_AMT.1								×				
FPT_FLS.1								×				
FPT_PHP.1		×								×		
FPT_PHP.3								×		×		
FPT_RCV.1								×		×		
FPT_RCV.4								×		×		
FPT_TST.1								×				
FRU_FLT.1								×		×		

Tabelle 9: Rückverfolgung der EVG-Sicherheitsanforderungen

Im Folgenden werden nur die Sicherheitsziele an die IT-Umgebung betrachtet, nicht aber solche, die den beabsichtigen Gebrauch des EVG betreffen.

OE.Administrator Die Zugangs- und Zugriffskontrollpolitiken (FDP_ACC.1, FDP_ACF.1) der IT-Umgebung ermöglichen dem Administrator die Vergabe der Zugangs- und Zugriffsberechtigungen in der IT-Umgebung und die Beschränkung dieser Berechtigungen auf den Wahlvorstand bzw. die an ihn gebundenen Subjekte in der IT-Umgebung. Diese Funktionalität der IT-Umgebung wird von den Komponenten FIA_ATD.1, FIA_USB.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1E und FMT_SMR.1 unterstützt. Bei der Vergabe der Zugangs- und Zugriffskontrolle für die Protokolldaten wird der Administrator von der IT-Umgebung durch die Komponente FAU_SAR.1 unterstützt.

OE.Konfiguration Die Zugangs- und Zugriffskontrollpolitik (FDP_ACC.1, FDP_ACF.1) gewährleistet, dass die für die Bewertung benötigten Stimmzetteldaten nicht verändert werden können. Die restlichen Teilziele sind organisatorischer oder personeller Natur.

OE.Protokollschutz Durch die Komponente FAU_SAR.1 wird sichergestellt, dass nur autorisierte Benutzer auf die Protokolldaten zugreifen können und die Komponente FAU.STG.1 gewährleistet eine sichere Speicherung der Protokolldaten, so dass die IT-Umgebung die vom EVG erzeugten Protokolldaten vor unberechtigtem Löschen und vor unberechtigter Modifikation schützen kann.

OE.Systemzeit Die IT-Umgebung stellt dem EVG durch die Komponente FMT_STM.1 verlässliche Zeitstempel zur Verfügung.

OE.Zugang Der Zugang zum EVG kann auf den Wahlvorstand und den Administrator beschränkt werden, da die IT-Umgebung durch die Komponenten FDP_ACC.1, FDP_ACF.1 eine Identifikation und Authentisierung der Benutzer in der IT-Umgebung ermöglicht. Diese wird durch die Komponenten FIA_ATD.1, FIA_UAU.2, FIA_UAU.7, FIA_UID.2, FIA_USB.1 unterstützt. Für die Protokolldaten wird die Zugangskontrolle über FAU_SAR.1 geregelt.

OE.Zugriff Der Zugriff auf Objekte (bspw. Dateien) in der IT-Umgebung, die vom EVG gespeicherte Wahldaten enthalten, kann von der IT-Umgebung durch die Verwendung der Komponenten FDP_ACC.1, FDP_ACF.1 auf Subjekte (bspw. Prozesse) beschränkt werden, die an den Wahlvorstand oder den Administrator gebunden sind. Diese wird durch die Komponenten FIA_ATD.1, FIA_UAU.2, FIA_UAU.7, FIA_UID.2, FIA_USB.1 unterstützt. Für die Protokolldaten wird die Zugangskontrolle über FAU_SAR.1 geregelt.

Die folgenden Ziele stellen ausschließlich personelle und organisatorische Ziele dar. Daher korrespondieren diese mit keinen Anforderungen an die IT-Umgebung: OE.Beobachtung, OE.Berechtigung, OE.Identifikation, OE.Notfallvorsorge, OE.Stimmzettel, OE.Personal, OE.Schadsoftware, OE.Wahlvorstand, OE.Zugriff, OE.Verbindung und OE.Speicherung.

	OE.Administrator	OE.Konfiguration	OE.Protokollschutz	OE.Systemzeit	OE.Zugang	OE.Zugriff
FAU_SAR.1	×		×		×	×
FAU_STG.1			×			
FDP_ACC.1	×	×			×	×
FDP_ACF.1	×	×			×	×
FIA_ATD.1	×				×	×
FIA_UAU.2					×	×
FIA_UAU.7					×	×
FIA_UID.2					×	×
FIA_USB.1	×				×	×
FMT_MSA.1	×					
FMT_MSA.3	×					
FMT_SMF.1E	×					
FMT_SMR.1	×					
FMT_STM.1				×		

Tabelle 10: Rückverfolgung der Sicherheitsanforderungen an die IT-Umgebung

7.2.2 Gegenseitige Unterstützung der Sicherheitsanforderungen

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.

Die funktionalen Komponenten wurden aus den vordefinierten CC Komponenten ausgewählt. Die Verwendung der Verfeinerungsoperationen erfüllen die CC Richtlinien. Insbesondere werden die Sicherheitsprinzipien der Komponenten FDP_ACC.2A/B von in den Regeln der Komponenten FDP_ACF.1A/B beschriebenen Sicherheitscharakteristiken respektiert.

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.

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.

7.2.3 Rechtfertigung der Auswahl von Sicherheitsanforderungen

Alle ausgewählten Sicherheitsforderungen sind in Teil 2 oder Teil 3 der CC enthalten.

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

Die folgenden nicht erfüllten Abhängigkeiten von funktionalen Sicherheitsanforderungen sind nicht anwendbar:

FCO_NRO.2 → FIA_UID.1 Für den Ursprungsnachweis ist die Identität des Urhebers unerheblich. An seine Stelle tritt die Bezeichnung des Wahlbezirks.

ANWENDUNGSBEMERKUNG: Die technische Umsetzung des Ursprungsnachweises für die Wahldaten und des damit verbundenen Manipulationsschutzes (FCO_NRO.2) bleibt in diesem Schutzprofil offen. Der ST-Autor wird darauf hingewiesen, daß abhängig von der technischen Ausgestaltung die Ergänzung weiterer Anforderungskomponenten erforderlich sein kann (vgl. CC Part 2, Par. 638f). Insbesondere bei Verwendung einer digitalen Signatur sind geeignete Komponenten aus der Klasse FCS (Cryptographic Support) zu ergänzen.

FDP_IFF.1 → FMT_MSA.3 Der verwendete Attribut ‚type of ballot’ muss zur Anwendung der Kontrollregel aus den konfigurierten Koordinaten der zulässigen Stimmzettel berechnet werden. Eine Initialisierung mit einem Anfangswert ist nicht sinnvoll.

FMT_MSA.3A/B → FMT_MSA.1 Die Sicherheitsattribute werden innerhalb der Zugriffskontrollpolitiken PSCP und BSCP für die Steuerung von Zustandsübergängen verwendet. Eine Verwaltung der Attribute durch Benutzer des EVG ist nicht sinnvoll.

FMT_MSA.3A/B → FMT_SMR.1 Die Sicherheitsattribute werden innerhalb der Zugriffskontrollpolitiken PSCP und BSCP für die Steuerung von Zustandsübergängen verwendet. Die Spezifikation alternativer Anfangswerte für diese Attribute ist nicht sinnvoll und daher keiner Rolle erlaubt.

7.2.4 Erklärung der Vertrauenswürdigkeitsstufe

Das Schutzprofil wurde entwickelt für ein Produkt, das in Wahllokalen unter ständiger Aufsicht des Wahlvorstands und in einer IT-Umgebung ohne externe Verbindung betrieben wird. Sachkundige Angriffe müssen somit auf den Digitalen Wahlstift in der Wahlkabine konzentriert sein oder sie müssen außerhalb des Wahllokals durchgeführt werden (vgl. die Bedrohungen in Kap. 3.2). Vor diesem Hintergrund ist die gewählte Vertrauenswürdigkeitsstufe EAL 3 zusammen mit der Augmentierung mit den Komponenten ADV_SPM.1 und AVA_MSU.3 zur wirksamen Überwachung des sicheren Betriebs durch den Wahlvorstand als angemessen zu betrachten. Sie gewährleistet insbesondere angemessene Vertrauenswürdigkeit, dass der EVG während Entwicklung, Auslieferung und Installation nicht manipuliert wird. Für die Zulassung von Produkten, die konform mit diesem Schutzprofil sind, werden ergänzend eine angemessene Durchsicht und/oder eine Veröffentlichung der Darstellung der Implementierung empfohlen.

7.2.5 Erklärung der Mindest-Stärkestufe

Die gewählte Mindest-Stärkestufe SOF-mittel ist konsistent zu den Sicherheitszielen des EVG, weil dadurch zusätzlich zur Vertrauenswürdigkeitsstufe EAL 3 einem direkten Angriff auf die Sicherheitsmechanismen des EVG auch nach der Wahl und außerhalb des Wahllokals mit angemessener Widerstandskraft begegnet wird.

A Glossar – Wahlspezifisch

Mandatsrelevanz Als Mandatsrelevanz wird die Erheblichkeit eines – z.B. in einem Wahlprüfungsverfahren beanstandeten – Wahlfehlers auf das Wahlergebnis bezeichnet. Mandatsrelevant ist dabei jeder Fehler, der Einfluss auf den Ausgang der Wahl (bei Mehrheitswahlen) oder die Sitzverteilung (bei Verhältniswahlen) zumindest eines Wahlbewerbers hat oder haben könnte.

Stimmabgabevermerk Jeder Wahlberechtigte, der im Urnenwahllokal gewählt hat, wird vom Wahlvorstand im Wählerverzeichnis in der dafür vorgesehenen Spalte mit einem Stimmabgabevermerk (rotes Kreuz) gekennzeichnet. Dadurch wird ausgeschlossen, dass ein Wahlberechtigter zweimal wählt.

Stimme (Gültig/Ungültig) Der Wille des Wählers muss erkennbar sein. Bei der Stimmabgabe ist der Wähler an die zugelassenen Wahlvorschläge gebunden. Die Stimmabgabe erfolgt dadurch, dass mit dem Digitalen Wahlstift deutlich kenntlich gemacht wird, welchem Wahlvorschlag die Stimme gelten soll. Die Form der Kennzeichnung ist weitgehend dem Wähler überlassen. In der Regel erfolgt die Kennzeichnung durch ein Kreuz im aufgedruckten Kreis. Eine ähnliche eindeutige und neutrale Kenntlichmachung z.B. durch ein Doppelkreuz oder durch Abhaken ist ebenso möglich.

Stimmzettel Hierbei handelt es sich um ein vorgedrucktes Blatt Papier oder vergleichbare Abbildflächen, die die zu einer Wahl zugelassenen Wahlvorschläge (Kandidaten und/oder Parteien) in einer vorgegebenen Reihenfolge und mit vorgegebenen Informationen (z.B. Familiennamen, Vornamen, Stadtteil, Geburtsjahr und Beruf der im Wahlvorschlag angegebenen Personen) auflistet. Die Stimmzettel enthalten ferner eine kurze allgemeinverständliche Erläuterung der Regeln zur Stimmabgabe. Der oder die Wahlvorschläge werden dann z.B. durch Ankreuzen ausgewählt. Der Stimmzettel wird danach in eine Wahlurne geworfen und damit anonymisiert. Nach Schluss der Wahlhandlung werden die abgegebenen Stimmzettel bewertet und das Ergebnis im Wahllokal ermittelt und festgestellt.

SOF (Stärke der Funktionen) Eine Charakterisierung einer EVG-Sicherheitsfunktion, die den geringsten angenommenen Aufwand beschreibt, der notwendig ist, um deren erwartetes Sicherheitsverhalten durch einen direkten Angriff auf die zugrunde liegenden Sicherheitsmechanismen außer Kraft zu setzen.

Wählerverzeichnis Im Wählerverzeichnis sind alle Personen eingetragen, die wahlberechtigt sind. Es wird zu einem festgelegten Termin aus den Daten des Einwohnermeldeamtes angelegt. Hierbei werden dann alle jeweils wahlberechtigten Personen erfasst. Für jeden Wahlbezirk wird ein eigenes (Teil-) Wählerverzeichnis mit den dort gemeldeten Wahlberechtigten angelegt.

Wahlbezirk Der Wahlbezirk ist eine geografisch zusammenhängende Verwaltungseinheit, zur konkreten, lokalen Durchführung von Wahlen mit Zuordnung auf ein Wahllokal bzw. einen Wahlraum. Es wird zwischen Urnenwahlbezirken und Briefwahlbezirken unterschieden.

Wahlergebnis Ein Wahlergebnis ist ein vom Wahlleiter verkündetes amtliches Ergebnis, das von den Wahlausschüssen festgestellt wurde. Als vorläufiges Ergebnis wird das in der Wahlnacht ermittelte Ergebnis bezeichnet, das unter Vorbehalt der vor der Sitzung dieser Ausschüsse stattfindenden Wahlprüfung steht.

Wahlhandlung Während der Wahlhandlung können Stimmen abgegeben werden. Die Wahlhandlung bezeichnet also den Zeitraum, in dem Wahlvorgänge stattfinden können.

Wahlhelfer Ein Wahlhelfer bekleidet ein Ehrenamt und nimmt dieses in einem Wahlvorstand in einer bestimmten Funktion wahr.

Wahlkabine Die Wahlkabine oder Wahlzelle ist ein für Dritte nicht einsehbarer Raum oder Verschlag, der eine geheime Wahl ermöglichen soll. Daher darf sie jeweils nur von einer Person betreten werden, worüber der Wahlvorstand zu wachen hat. Die Wähler können an einem Tisch den Stimmzettel unbeobachtet ankreuzen, bevor sie ihn in die Wahlurne werfen.

Wahlniederschrift Über die Wahlhandlung sowie über die Ermittlung und Feststellung des vorläufigen Wahlergebnisses ist vom Schriftführer des Wahlvorstandes eine Wahlniederschrift auszufüllen. Diese ist anschließend von den Mitgliedern des Wahlvorstandes zu unterzeichnen. Zur Darstellung des vorläufigen Wahlergebnisses in der Wahlniederschrift und im Wahllokal für die Öffentlichkeit wird ein Papierausdruck benötigt.

Wahlprüfung Wahlprüfung nennt man das Verfahren, in dem die Rechtmäßigkeit und Gültigkeit einer Wahl durch den Wahlausschuss festgestellt wird, um das endgültige Wahlergebnis verkünden zu können.

Wahlurne Die Wahlurne ist ein geschlossener Behälter mit abschließbarem Deckel und Einwurfschlitz zur Durchführung einer geheimen Wahl mit Stimmzetteln. Die Wähler kreuzen in einer Wahlkabine unbeobachtet und unbeeinflusst einen oder mehrere Stimmzettel an und werfen diese danach gefaltet in die Wahlurne. Die verschlossene Wahlurne wird nach Schluss der Wahlhandlung geöffnet und ausgeleert, damit die Stimmzettel bewertet und ausgezählt werden können.

Wahlvorgang Für jeden Wähler besteht der Wahlvorgang aus folgenden Schritten:

1. Vorprüfung der Wahlberechtigung, Ausgabe der Stimmzettel, Aktivierung und Ausgabe des Digitalen Wahlstifts
2. Freie und Geheime Stimmabgabe in der Wahlkabine
3. Prüfung der Wahlberechtigung ggf. Annullierung der Stimmabgabe und Vernichtung der Stimmzettel
4. Registrierung der Stimmabgabe (bei bestehender Wahlberechtigung) und Einwurf der Stimmzettel in die Wahlurne

Wahlvorstand Jedem Wahlbezirk ist ein Wahlvorstand zugeordnet. Der Wahlvorstand besteht aus dem Wahlvorsteher, dem Schriftführer, deren Stellvertretungen und weiteren Beisitzern. Der Wahlvorstand ist ein eigenständiges Wahlorgan. Er nimmt ein eingeschränktes Hausrecht im Wahllokal wahr, hat für die Einrichtung des Wahlraumes zu sorgen, überwacht die Stimmabgabe, bewertet die Stimmen und zählt sie aus. Er stellt das vorläufige Ergebnis fest und sorgt für dessen Übermittlung an die zuständige Wahlzentrale.

Wahlzentrale Am Wahltag werden Wahlzentralen eingerichtet, die nach Wahlende die Ergebnisse aus den Wahllokalen entgegennehmen und an die Wahlleitung weitermelden.

B Abkürzungen

ANSI American National Standards Institute

BSI Bundesamt für Sicherheit in der Informationstechnik

CAPP Controled Access Protection Profile

CC Common Criteria for IT Security Evaluation (Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik)

CEM Common Methodology for IT Security Evaluation (Gemeinsame Methodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik)

EAL Evaluation Assurance Level (Vertrauenswürdigkeitsstufe)

EVG Evaluationsgegenstand

FIPS Federal Information Processing Standards

IEC International Electrotechnical Commision

ISO International Organisation for Standardization

IT Information Technology (Informationstechnik)

PKCS Public-Key Cryptography Standards

PP Protection Profile (Schutzprofil)

SFP Security Functional Policy

ST Security Target (Sicherheitsvorgaben)

TOE Target of Evaluation (Evaluationsgegenstand – EVG)

TSF TOE Security Functions (EVG-Sicherheitsfunktionen)

TSP TOE Security Policy (EVG-Sicherheitspolitik)

C Literatur

[CAPP] U.S. National Security Agency (NSA), Information Systems Security Organization: *Controled Access Protection Profile*, Version 1.d, 8 October 1999

[VoVo06] Roland Vogt, Melanie Volkamer: *Requirements Engineering for eVoting*, in 7th International Common Criteria Conference (ICCC), Sept. 2006

[VoKr06a] Melanie Volkamer, Robert Krimmer: *Overview Online-Wahlen*, in D*A*CH Sicherheit, 2006

[VoKr06b] Melanie Volkamer, Robert Krimmer: *Die Online-Wahl auf dem Weg zum Durchbruch*, in Informatikspektrum, April 2006