Thurgau

Hardware und Infrastruktur

E-Voting Thurgau

Autor/in	Fachperson E-Voting
Datum	27.07.2023
Version	1.3
Klassifizierung	keine

Kanton Thurgau, Staatskanzlei
Regierungsgebäude, 8510 Frauenfeld
T +41 58 345 53 31, F +41 58 345 53 39
www.staatskanzlei.tg.ch

Änderungskontrolle

Version	Datum	Beschreibung	Name
1.0	21.12.2022	Freigegebene Version	Fachperson E-Voting
1.1	28.04.2023	Anpassungen in Abschnitten 4.1, 4.2, 5.1, 5.1.2, 5.4, 6 und 7	Fachperson E-Voting
1.2	14.06.2023	Anpassungen in Abschnitten 4.2, 5.1.2 und 6	Fachperson E-Voting
1.3	27.07.2023	Anpassungen in Abschnitten 4 und 5.4	Fachperson E-Voting

Prüf- / Freigabestellen

Prüfer/in	Freigeber/in	Datum
Leitung Rechtsdienst	Leitung Rechtsdienst	12.12.2022

Referenzierte Dokumente

Nr.	Dokument	Datum / Version
[1]	Konzept E-Voting	- / Aktuelle Version
[2]	Verordnung der BK über die elektronische Stimmabgabe (VEleS, SR 161.116) vom 25. Mai 2022	Stand vom 01.07.2022
[3]	Basic installation and hardening	- / Aktuelle Version
[4]	SDM Hardening Guidelines der Schweizerischen Post https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/blob/master/Operations/Recommendation_Safety_Measures_Cantonal_Infrastructure.md	- / Aktuelle Version auf GitLab
[5]	Richtlinie Informationssicherheit	- / Aktuelle Version
[6]	Glossar	- / Aktuelle Version

Thurgau

Inhaltsverzeichnis

1. Ziel des Dokuments

Dieses Dokument beschreibt die Vorbereitung sowie den Einsatz der verwendeten Hardware und Infrastruktur während eines Urnengangs. Es definiert auch die Aufbewahrung der einzelnen technischen Mittel sowie den Umgang damit, wenn die Erwahrungsfrist abgelaufen ist.

2. Übersicht der Komponenten und Abgrenzung

Das produktive E-Voting System besteht aus den in *Abbildung 1* aufgeführten Komponenten (siehe *Abschnitt 4.1*).

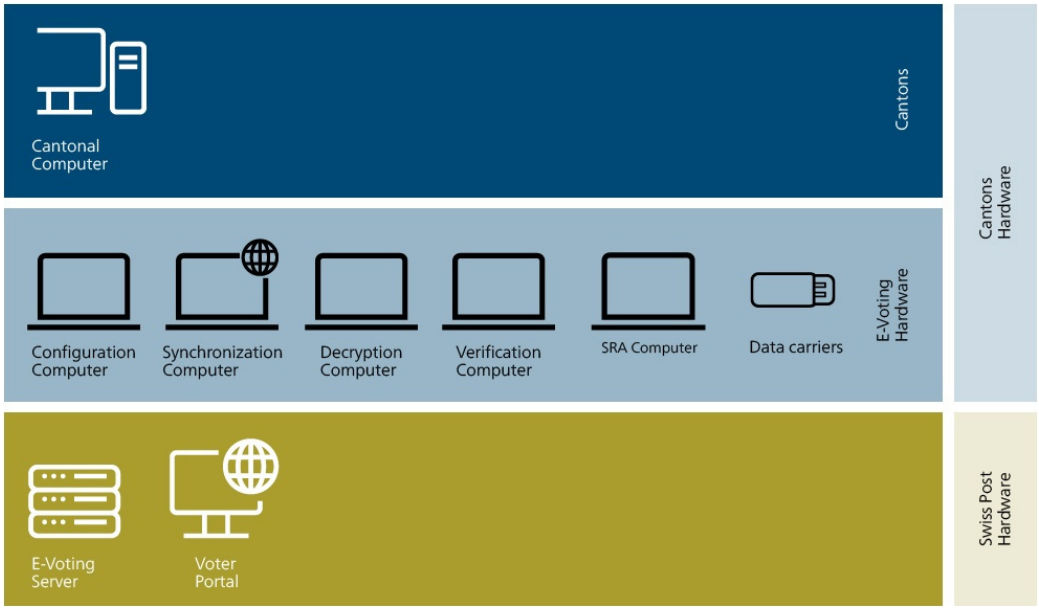

Abbildung 1: Komponenten E-Voting

Das vorliegende Dokument bezieht sich ausschliesslich auf Hardware, die seitens des Kantons für E-Voting und das Durchführen eines Urnengangs eingesetzt wird.

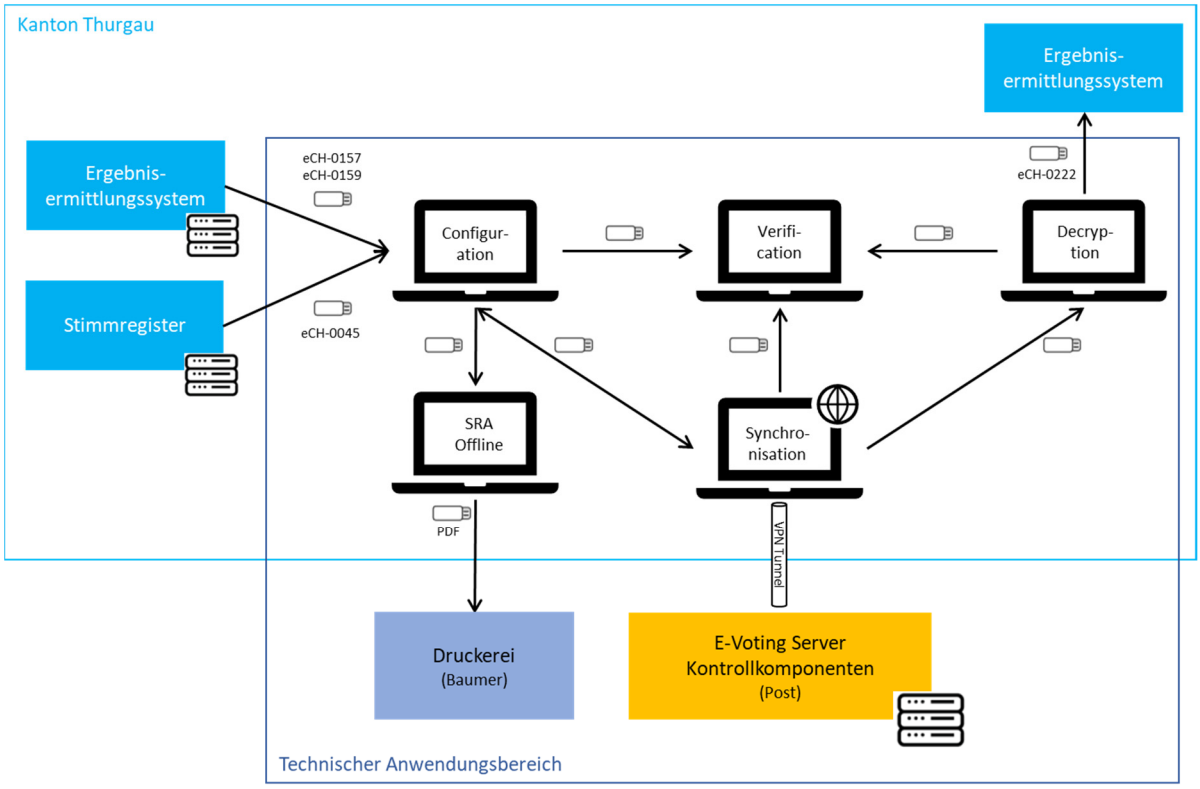

Abbildung 2: Abgrenzung Anwendungsbereich

Die Hardware und Komponenten der Druckerei und des Ergebnisermittlungssystems liegen nicht im Anwendungsbereich des vorliegenden Dokuments.

3. Verantwortlichkeiten

Die Leitung der elektronischen Stimmabgabe ist verantwortlich für:

– die Beschaffung der Computer

– die Grundinstallation und das Umsetzen der empfohlenen technischen und organisatorischen Sicherheitsmassnahmen (Hardening)

– die Installation der für die Durchführung eines Urnengangs benötigten E-Voting Software auf den Computern gemäss der Vorgabe der Post

– die Aufbewahrung der Hardware

– die sichere Datenlöschung

Für einzelne Aufgaben (Grundinstallation, Umsetzung Hardening) zieht die Staatskanzlei externe Unterstützung bei (siehe *referenziertes Dokument [1]*).

4. Übersicht Hardware

Die für E-Voting verwendeten Computer und Datenträger werden nachfolgend beschrieben. Gemäss Ziff. 3.20 der Verordnung der BK über die elektronische Stimmabgabe (VEleS, siehe *referenziertes Dokument [2]*) wird der Zugriff und die Verwendung von vertrauenswürdigen Komponenten und Datenträgern protokolliert.

4.1. Computer

Der Kanton Thurgau setzt für E-Voting folgende Computer ein:

– 7 Computer produktiv: 1 Online, 3 Offline, 1 Offline für die Erstellung der Stimmrechtsausweise (SRA) sowie 2 Ersatzgeräte (1 Ersatz Online, 1 Ersatz Offline)

– 2 Computer für Tests: 1 Online, 1 Offline (alle Offline-Schritte werden auf dem gleichen Gerät durchgeführt)

Die Offline-Computer werden nie mit dem Kantonsnetz/Internet verbunden. Alle Computer sind gut sichtbar beschriftet.

Bezeichnung	Umgebung	Zweck	Software
Synchronisation Computer (Online)	Produktion	Administration E-Voting (u.a. Übertragung Abstimmungskonfiguration inkl. anonymisiertem Stimmregister an Abstimmungsportal; Download der elektronischen Urne mit den verschlüsselten Stimmen)	– Secure Data Manager – Voting-Output-Service
Configuration Computer (Offline)	Produktion	Konfiguration Urnengang, Generierung Codes für die Stimmrechtsausweise, Bereitstellung der Urnen durch Electoral-Board	– Data Integration Service – Secure Data Manager – Config Cryptographic Parameters Tool
Decryption Computer (Offline)	Produktion	Mischen der Stimmen, Entschlüsseln der Stimmen durch Electoral-Board, Aufbereitung der Resultate	– Secure Data Manager
Verification Computer (Offline)	Produktion	Überprüfung des Urnengangs	– Verifier
Stimmrechtsausweise Computer (SRA Offline)	Produktion	Erstellung der Stimmrechtsausweise	– VCPS – Voting Card Register

Bezeichnung	Umgebung	Zweck	Software
Ersatz Computer (Online)	Produktion	Ersatz-Computer, falls der produktive Online-Computer ausfällt	– Analog Online-Computer
Ersatz Computer (Offline)	Produktion	Ersatz-Computer, falls ein produktiver Offline-Computer ausfällt	– Analog Offline-Computer
Test Computer (Online)	Test	Verwendung für Testurnengänge	– Analog Online-Computer
Test Computer (Offline)	Test	Verwendung für Testurnengänge	– Analog Offline-Computer

Tabelle 1: Computer

4.2. Datenträger

Der Kanton Thurgau verwendet pro Urnengang verschiedene Datenträger gemäss Vorgaben der Post sowie kantonalen Vorgaben. Es gilt der Grundsatz, dass pro Operation bzw. Prozessschritt ein dedizierter Datenträger verwendet wird. In gewissen Fällen werden PIN-geschützte USB-Sticks mit Datenverschlüsselung auf Hardware-Basis[1] verwendet. Der Kanton führt ein Inventar der Datenträger.

Die Daten werden nach der Erwahrung oder bei der Vorbereitung auf den nächsten Urnengang mittels 4-Augen-Prinzip gelöscht. Die Ausnahmen von dieser Regel sind nachfolgend aufgelistet. Die Löschung der Datenträger erfolgt mit sDelete (inkl. leerer Speicherplatz), zusätzlich werden die Datenträger neu formatiert. Diese Arbeiten erfolgen auf einem Offline-Gerät.

Hardware	Zweck

Datenträger (SD-Karten)	• Prozess-Datenträger
	  ○ Verwendung für den Hauptprozess (Datentransfer zwischen den Computern; z.B. vom Configuration auf den Synchronisation Computer und umgekehrt).
	• Transfer-Datenträger
	  ○ Verwendung für den Transfer zu den kantonalen Computern bzw. den Umsystemen (z.B. Datentransfer ins Ergebnisermittlungssystem)
	  ○ Der Datenträger (USB-Stick) für die Datenübergabe an die Druckerei wird nach dem Anreichern der Daten durch die Druckerei geschreddert.
	• Verifier-Datenträger
	  ○ Übertragung der Daten auf den Verification Computer

[1] Aktuell: Kingston USB-Stick DataTraveler 200.256-Bit AES-Datenverschlüsselung auf Hardware-Basis (konform zu FIPS-197)

Hardware	Zweck

	• Image-Datenträger
	  ○ Verwendung für die Installation des Image
	• Installations-Datenträger
	  ○ Verwendung für die Installation der E-Voting-Software

Datenträger (PIN-geschützte USB-Sticks)	• Backup-Datenträger
	  ○ Während des Urnengangs werden verschiedene Backups gemacht. Dafür wird pro Computer (Synchronisation Computer, Configuration Computer, Decryption Computer, Verification Computer) ein separater Datenträger verwendet.
	  ○ Die Backupdaten eines Urnengangs werden nach dem Erwahrungsbeschluss des Urnengangs mittels 4-Augen-Prinzip gelöscht.
	• Druckdaten-Datenträger
	  ○ Transfer der Stimmrechtsausweisdaten von Configuration Computer auf SRA Computer
	  ○ Die Daten werden nach dem Transfer der Daten mittels 4-Augen-Prinzip gelöscht.
	• KeePass-Datenträger (online / offline)
	  ○ KeePass-Passwortsafes, für deren Öffnung ein weiteres Passwort erforderlich ist. Die Container enthalten Passwörter und Zertifikate für die Durchführung von E-Voting. Für den Online-Computer und die Offline-Computer werden separate Passwortsafes auf separaten Datenträgern verwendet.
	• Urnengangpasswort-Datenträger
	  ○ Speicherung der Passwörter des Urnengangs (ein Passwort für das Admin-Board und ein Passwort für das Electoral-Board) auf separaten Datenträgern (inkl. Backup; ausgehend von diesen zwei Passwörtern werden an D2 die Sicherheitsschlüssel des Urnengangs für die Ver- und Entschlüsselung der Stimmen generiert). Durch die Verteilung der Datenträger auf unterschiedliche Personen wird sichergestellt, dass die Passwörter nur zum Zeitpunkt der Entschlüsselung wieder zusammenkommen.
	• Direct-Trust-Datenträger
	  ○ Für die Übertragung und Speicherung der im Rahmen des Direct-Trusts generierten Zertifikate und Passwörter.

Tabelle 2: Datenträger (SD-Karten und PIN-geschützte USB-Sticks)

4.3. Weitere Hardware

Hardware	Zweck
Beamer + Leinwand	Ermöglicht Einsicht in das, was auf den Computern passiert.
KVM-Switch	Ermöglicht das Switchen zwischen den verschiedenen Geräten.

Tabelle 3: Weitere Hardware

5. Installation der Computer

Die Computer dürfen in keine Domäne aufgenommen werden und werden auch nicht zentral verwaltet. Die Offline-Computer bleiben immer offline. Sie werden weder mit dem Kantonsnetz noch dem Internet verbunden. Installation und Updates werden offline durchgeführt.

Für die Installation und Konfiguration wird ein Installationsmedium verwendet, das die zu installierende Software und die Konfigurationsdateien enthält.

Die Installation ist in mehrere Schritte aufgeteilt:

1. Erstellen eines Images/Installationsmediums pro Urnengang:
   Für die Computer wird ein Image erstellt, das vor dem Urnengang mit den Updates und neuen Softwareversionen versorgt wird. Das Image beinhaltet die Systeminstallation (Betriebssystem, Treiber, Sicherheitsupdates etc.), die notwendige Zusatzsoftware sowie die Scripts für das Hardening. Von allen Komponenten wird der Hashwert oder die Signatur geprüft. Das Image ist so strukturiert, dass der Aufbau einfach nachvollzogen werden kann. Das Image wird im Auftrag und gemäss den Vorgaben der Kantone zentral durch einen externen Dienstleister erstellt und an die Kantone verteilt.

2. Installation des Images (mit lokalen Administratorenrechten):
   Das Image wird durch den Kanton auf einen Datenträger (USB-Stick) gespeichert. Die Computer werden aus dem Tresor geholt und von Null auf mit dem neuen Image aufgesetzt (Zero-Touch-Installation). Alle Computer werden im 4-Augen-Prinzip mit dem gleichen Image aufgesetzt.

3. Prüfung der Installation und des Hardenings:
   Der Kanton prüft die Installation und das Hardening im 4-Augen-Prinzip.

4. Installation der E-Voting-Software gemäss Anleitung Post (ohne Administratorenrechte):
   Der Kanton prüft und installiert die von der Post gelieferte Software (SDM, DIS, Verifier, etc.) gemäss Anleitung im 4-Augen-Prinzip. Hierzu sind keine Administratorenrechte nötig.

Die Computer werden nie direkt aktualisiert, sondern immer mit einem aktualisierten Image frisch installiert.

5.1. Definition des Images pro Urnengang

Der Kanton gibt die Erstellung des Images ungefähr elf bis zwölf Wochen vor dem Urnengang beim externen Dienstleister in Auftrag. Dieser setzt für die Erstellung des Images ein Gerät (kein E-Voting-Computer) mit dem Image des vorangegangenen Urnengangs auf (siehe *referenziertes Dokument [3]*). Der Computer wird mit dem Internet verbunden, und es wird auf den Servern von Microsoft nach Updates gesucht. Die Update-Nummern werden notiert, und die entsprechenden Updates werden einzeln vom Updatekatalog von Microsoft heruntergeladen und in das Image integriert. Der Computer wird anschliessend mit dem aktualisierten Image neu aufgesetzt. Der Prozess wird so lange wiederholt, bis keine Updates mehr gefunden werden.

Falls Updates von Applikationen notwendig sind, werden diese heruntergeladen und in das Software-Verzeichnis des Images integriert. Die Treiberupdates für die Computermodelle und die Antivirus-Definition werden ebenfalls in das Image integriert.

Jede Software, die installiert wird, wird von der offiziellen Quelle oder im Ausnahmefall von der Post bezogen (siehe *Abschnitt 5.1.2*). Es wird die letzte verfügbare Version oder die von der Post vorgegebene Version verwendet. Wird nicht die letzte verfügbare Version verwendet, so wird dies begründet.

Bei allen Installationsdateien werden die Hashwerte oder die Signaturen geprüft. Alle Dateien werden zudem mit einem Antivirenscanner geprüft.

5.1.1. Betriebssystem

Als Betriebssystem wird Windows 10 LTSC 2021 (unverändertes Windows-Image von Microsoft) verwendet. Es werden keine Microsoft-Accounts angelegt und es dürfen keine weitere Software oder weiteren Apps installiert werden.

5.1.2. Zusatzsoftware

Folgende Software wird gemäss der Vorgabe der Post in das Image integriert:

– sTunnel: Stellt die sichere Verbindung zur Post via VPN her.

– OpenSSL: Wird benötigt, um Dateien zu signieren oder Signaturen zu kontrollieren.

– Notepad++: Wird benötigt, um XML-Files editieren zu können.

– KeePass: Wird zur Verwaltung der Zertifikate und Passwörter benötigt, die für die Durchführung eines Urnengangs notwendig sind, inkl. Generierung der Passwörter des Urnengangs.

– WMGJ "Verificatum Multiplicative Groups Library for Java" (wird von der Post geliefert): Wird durch den SDM verwendet.

Zusätzlich wird folgende Software installiert:

– sDelete: Erlaubt ein sicheres Löschen von Daten.

– HP Hotkey Manager: Erlaubt die Konfiguration von Tastaturkurzbefehlen für HP Geräte.

– 7-zip: Erlaubt das Erstellen und Entpacken von Archivdateien mit verschiedenen Formaten.

– TotalCommander: Zweispaltiger Dateimanager für Windows.

Es wird keine weitere Software installiert.

5.1.3. Hardening

Das Hardening deckt die folgenden Ziele ab:

– Es sind nur die zwingend benötigten Benutzer vorhanden.
– Es sind nur die zwingend notwendigen Programme installiert.
– Die Hardening-Empfehlungen der Post sind umgesetzt, soweit dies für die E Voting-Computer möglich ist.
– Die „Microsoft-recommended security configuration baselines for Windows and other Microsoft products“ sind umgesetzt, soweit dies für die E Voting-Computer möglich ist (https://www.microsoft.com/en-us/download/details.aspx?id=55319).
– Alle Netzwerkadapter sind deaktiviert mit Ausnahme desjenigen Netzwerkadapters des Synchronisation Computers (Online), der für die Kommunikation mit den Servern der Post zwingend erforderlich ist.

Die Hardening-Empfehlungen der Post sind auf GitLab publiziert (siehe *referenziertes Dokument [4]*). Das Script für das Hardening wird veröffentlicht.

5.2. Prüfung Installation und Hardening

Nach der Installation des Images wird die Installation und das Hardening im 4-Augen-Prinzip durch den Kanton anhand einer Checkliste geprüft.

5.3. Accounts

Jeder Computer verfügt über zwei Accounts: (1) Administrator-Account, der für die Installation des Images verwendet wird und nur dem Kanton bekannt ist und von diesem definiert wird; (2) User-Account für den Urnengang. Für die beiden Accounts werden unterschiedliche, genügend sichere Passwörter gemäss den Vorgaben der Richtlinie Informationssicherheit (siehe *referenziertes Dokument [5]*) gesetzt.

5.4. Installation E-Voting Software

Die von der Post gelieferte Software wird gemäss den Release-Anleitungen der Post installiert. Die Hashwerte der von der Post gelieferten Software werden gegenüber den Ergebnissen der beobachteten Kompilierung gemäss dem Akzeptanz-Protokoll des Trusted Build und der Releasenote geprüft. Nachfolgend findet sich eine Auflistung der Applikationen mit einer Zuteilung auf welchen Geräten diese zu installieren sind.

Software	Typ	Beschreibung	Installiert auf				
			C	S	D	V	SRA
Secure Data Manager (SDM)	Applikation	Das Hauptprogramm, um einen Urnengang aufzusetzen. Um die Sicherheit der Daten zu gewährleisten, werden Operationen mit dem Secure Data Manager auf den unterschiedlichen Geräten ausgeführt. Der Secure Data Manager stellt sicher, dass die Daten, die auf einem der Geräte bearbeitet werden, mit den anderen Geräten synchronisiert werden. Er ermöglicht dem Online-Computer zudem die Synchronisierung der Daten mit den E-Voting Servern bei der Post.	X	X	X		
Config Cryptographic Parameters Tool	Applikation	Tool, welches nach Eingabe des Seeds die Verschlüsslungsparameter des Urnengangs konfiguriert. Zusätzlich werden damit einmal pro Jahr die Direct-Trust-Keystores erstellt. Das Config Cryptographic Parameter Tool greift auf die Bibliothek der Crypto-Primitives[2] zu.	X				
Data Integration Service (DIS)	Applikation	Der Data Integration Service ist ein Tool, das die Stammdaten des Urnengangs (wie eCH-Dateien) für den Secure Data Manager konvertiert.	X				
Verifier	Applikation	Der Verifier ist die Software, die die Überprüfung des Urnenganges ermöglicht.				X	

[2] Siehe dazu https://gitlab.com/swisspost-evoting/crypto-primitives

Software	Typ	Beschreibung	Installiert auf				
			C	S	D	V	SRA
Voting Card Register (VCR)	Applikation	Das VCR erstellt eine Liste aller IDs der Stimmrechtsausweise mit Wählerkreis, Namen der Stimmberechtigten und Stati. Wird benötigt für die Doppelstimmprüfung.					X
Voting Card Manager (VCM)	Web-Applikation	Mit dem VCM können während dem Urnengang Massen- oder Einzelsperrungen von Stimmrechtsausweisen gemacht werden (im Rahmen der Doppelstimm-prüfung). Der Zugriff erfolgt via kantonale Computer.					
Voting Output Service (VOS)	Applikation	Das Tool ermöglicht es zusätzlich zu den Ergebnisdateien (eCH0110 und eCH0222) die Ergebnisse des Urnengangs in PDF-Form und damit in einfacher lesbarer Form darzustellen.		X			
Voting Card Print Service (VCPS)	Applikation	Software zur Erstellung der druckfertigen Stimmrechtsausweise.					X

Tabelle 4: E-Voting Software

In der obigen Tabelle wurden die folgenden Abkürzungen für die Geräte verwendet. C=Configuration Computer, S=Synchronisation Computer, D=Decryption Computer, V=Verification Computer, SRA=Stimmrechtsausweise Computer

6. Räumlichkeiten und Schutzmassnahmen

Die Hardware wird ausschliesslich im zugangsgesicherten Regierungsgebäude verwendet und aufbewahrt. Zugang zum Regierungsgebäude haben nur Kantonsmitarbeitende mit einem Badge oder Besucher in Begleitung. Der Zutritt zu den Büros ist jeweils nur mit Schlüssel möglich. Weitere Informationen zur Aufbewahrung sind unter *Abschnitt 7* zu finden.

Während eines Urnenganges wird die Hardware aus dem Tresor entnommen und im definierten Sitzungszimmer für die Verwendung aufgebaut und vorbereitet. Während der Verwendung darf die Hardware nie unbeaufsichtigt zugänglich sein und muss jederzeit überwacht werden.

Wird die Hardware (Computer, Datenträger) längere Zeit nicht verwendet, ist sie gemäss *Abschnitt 7* im Tresor wegzuschliessen. Zubehör wie Stromversorgung, Dockingstation, Beamer etc. müssen nicht zwingend abgebaut werden.

Alle Vorgänge (Entnahmen und Einschlüsse Tresor, Raumschliessungen und Öffnungen, etc.) sind in einem Protokoll durch zwei Personen festzuhalten.

7. Aufbewahrung

Die Hardware (Computer, Datenträger) wird in einem Tresor aufbewahrt. Der Tresor befindet sich in einem abgeschlossenen Büro des Regierungsgebäudes. Der Zugang zum Tresor ist nur im 4-Augen-Prinzip möglich durch die Eingabe von zwei Codes[3].

8. Kommunikationssicherheit

Die Computer, die im Rahmen eines Urnenganges eine Online-Verbindung zum E-Voting System der Post benötigen, dürfen ausschliesslich über das separierte, für E-Voting konfigurierte Netzwerksegment eine Verbindung aufbauen. Dies wird mit einer Regel im Hardening durchgesetzt. Eine WLAN-Anbindung ist nicht möglich, da beim Hardening die WLAN-Funktionalität deaktiviert wird.

Die Verbindung zum E-Voting Server der Post erfolgt über VPN (sTunnel).

[3] Datenträgerschrank mit eingebautem Doppelcode-Programm, 4-Augen-Prinzip

9. Tabellenverzeichnis

10. Abbildungsverzeichnis