Glossar

E-Voting Basel-Stadt / Graubünden / St.Gallen / Thurgau

Autoren	**Projektleitung E-Voting (BS)** **E-Voting Beauftragter (GR)** **Leitung der elektronischen Stimmabgabe (SG)** **Fachperson E-Voting (TG)**

Datum	29.09.2023
Version	1.2
Klassifizierung	Keine

Änderungskontrolle

Version	Datum	Beschreibung	Name
1.0	21.12.2022	Freigegebene Version	Projektleitung E-Voting (BS) Leitung Informatik und Infrastruktur (SG) Fachperson E-Voting (TG)
1.1	28.04.2023	Integration von Graubünden Ergänzungen und Anpassungen in Abschnitt 2	Projektleitung E-Voting (BS) E-Voting Beauftragter (GR) Leitung Informatik und Infrastruktur (SG) Fachperson E-Voting (TG)
1.2	29.09.2023	Formelle Anpassungen	Projektleitung E-Voting (BS) E-Voting Beauftragter (GR) Leitung Informatik und Infrastruktur (SG) Fachperson E-Voting (TG)

Prüf-/Freigabestellen

Prüfer	Freigeber	Datum
Leitung Recht und Volksrechte (BS) Leitung Dienst für politische Rechte (SG) Leitung Rechtsdienst (TG)	Leitung Recht und Volksrechte (BS) Leitung Dienst für politische Rechte (SG) Leitung Rechtsdienst (TG)	12.12.2022
Leitung Abteilung Services (GR)	Leitung Abteilung Services (GR)	22.09.2023

Referenzierte Dokumente

Nr.	Dokument	Version
[1]	Verordnung der BK über die elektronische Stimmabgabe (VEleS, SR 161.116) vom 25. Mai 2022	Stand am 1. Juli 2022
[2]	Leitfaden für Risikobeurteilungen der Schweizerischen Bundeskanzlei für das E-Voting-System der Schweizerischen Post ("Leitfaden für Risikobeurteilungen") https://www.bk.admin.ch/dam/bk/de/dokumente/pore/Vote--lectronique/Leitfaden%20BK_Risikobeurteilungen%20Vote%20%C3%A9lectronique,%20Oktober%202022.pdf.download.pdf/Leitfaden%20BK_Risikobeurteilungen%20Vote%20%C3%A9lectronique,%20Oktober%202022.pdf	Version vom 04.10.2022

Inhaltsverzeichnis

1 Zweck des Dokuments

Das vorliegende Dokument beschreibt die im Rahmen der elektronischen Stimmabgabe von den Kantonen verwendeten Begriffe. Werden in den Unterlagen der Post oder in der Verordnung der BK über die elektronische Stimmabgabe (siehe *referenziertes Dokument [1]*) andere Begriffe verwendet, wird darauf hingewiesen.

Das Glossar ist aus Gründen der Übersichtlichkeit in zwei Teilbereiche unterteilt; ein Bereich für die generellen Begrifflichkeiten der elektronischen Stimmabgabe und ein Bereich für die technischen Begrifflichkeiten.

1.1 Quellenangabe zum Ursprung von Definitionen

Wo vorhanden und sinnvoll, wurden die Bedeutungserklärungen aus den Dokumenten "Leitfaden für Risikobeurteilungen" (siehe *referenziertes Dokument [2]*) und "Verordnung der BK über die elektronische Stimmabgabe" (siehe *referenziertes Dokument [1]*) als Basis verwendet. Die Ursprungsdefinitionen der aufgeführten Begriffen sind jeweils mit Sonderzeichen gekennzeichnet.

Sonderzeichen	Quelle der Ursprungsdefinition
*	"Leitfaden für Risikobeurteilungen" der Schweizerischen Bundeskanzlei
**	Verordnung der BK über die elektronische Stimmabgabe

Tabelle 1: Zuordnung der Sonderzeichen gemäss Quelle

1.2 Kantonale Unterschiede

In gewissen Fällen unterscheiden sich die kantonalen Gegebenheiten. Diese Unterschiede sind in diesem und allen anderen gemeinsamen Dokumenten farblich gekennzeichnet:

Farbe	Kanton
violett	Violett geschriebener Text gilt nur für den Kanton Basel-Stadt
rot	Rot geschriebener Text gilt nur für den Kanton Graubünden
grün	Grün geschriebener Text gilt nur für den Kanton St.Gallen
blau	Blau geschriebener Text gilt nur für den Kanton Thurgau

Tabelle 2: Farbliche Kennzeichnung der kantonalen Unterschiede

2 Glossar – Generelle Begriffe

Die folgende Tabelle liefert eine Übersicht der relevanten generellen Begrifflichkeiten im Zusammenhang mit der elektronischen Stimmabgabe.

Begriff	Beschreibung
Admin-Board	Personen, die für die technische Durchführung des Urnengangs verantwortlich sind.
Bug-Bounty-Programm	Ein Bug-Bounty-Programm ist ein "Kopfgeld-Programm" für das Entdecken und Melden von Schwachstellen. Bug-Bounty-Programme setzen Anreize für die öffentliche Überprüfung (insbesondere durch sogenannte ethische Hacker) und tragen zur Sicherheit von E-Voting bei, indem Schwachstellen frühzeitig gefunden und behoben werden können. Die Post hat den Quellcode sowie die Dokumentation zu System und Betrieb ab 2021 auf der Fachplattform GitLab veröffentlicht. Im Rahmen ihres Bug-Bounty-Programms belohnt sie Meldungen, die zur Verbesserung des Systems beitragen, mit bis zu CHF 250'000.
Briefliche Stimmabgabe, Stimmabgabe an der Urne*	Gesamtheit der Stimm- und Wahlzettel, die per brieflicher Stimmabgabe oder an der Urne abgegeben worden sind.
Container	Begriff aus der "OCTAVE Allegro"-Methodologie: Mittel (physisch oder technisch), die Informationsressourcen bearbeiten, speichern oder übermitteln.
D0*	Zeiteinheit innerhalb des Prozesses: Vorbereitung des Urnengangs.
D1*	Zeiteinheit innerhalb des Prozesses: Tag, an dem die elektronischen Urnen konfiguriert, diese an das Online-System der Post übermittelt und die Stimmrechtsausweise generiert werden.
D2*	Zeiteinheit innerhalb des Prozesses: Tag, an dem die Sicherheitsschlüssel des Urnengangs (vgl. Begriff "Sicherheitsschlüssel") festgelegt werden, die Konfiguration des Urnengangs überprüft wird und die elektronischen Urnen bereitgestellt werden.
D3*	Zeiteinheit innerhalb des Prozesses: Tag, an dem die elektronischen Stimmen entschlüsselt, die Ergebnisse der elektronischen Stimmabgabe ermittelt und der Urnengang durch die Prüferinnen und Prüfer geprüft wird.
D4*	Zeiteinheit innerhalb des Prozesses: Nachbearbeitung des Urnengangs, inkl. Vernichtung der Daten.

Begriff	Beschreibung
Electoral-Board (VEleS: Prüferinnen und Prüfer)	Personen, die nach kantonalem Recht für die Beaufsichtigung des ordnungsgemässen Ablaufs des elektronischen Urnengangs verantwortlich sind und die in der VEleS vorgesehene Rolle der Prüferinnen und Prüfern übernehmen. Sie generieren die Sicherheitsschlüssel des Urnengangs (vgl. Begriff "Sicherheitsschlüssel"). Im Kanton Basel-Stadt agiert das Wahlkomitee (Verordnung über den Testbetrieb für die elektronische Stimmabgabe, Art. 8a) als Electoral-Board. Im Kanton Graubünden agiert die Wahl- und Abstimmungskommission E-Voting (Verordnung über die politischen Rechte im Kanton Graubünden, Art. 21g) als Electoral-Board. Im Kanton St.Gallen agiert ein Ausschuss des kantonalen Stimmbüros (WAG, Art. 11 ff) als Electoral-Board. Im Kanton Thurgau agiert das Stimmbüro für Auslandschweizerinnen und -schweizer (StWV, Art. 26) als Electoral-Board.
EV-Stimmregister*	Kantonales Register der Stimmberechtigten, die zur elektronischen Stimmabgabe zugelassen sind.
EV-Ergebnisse*	Ergebnisse der Auszählung der elektronischen Urnen.
Gegenstand des Urnengangs*	Abstimmungsfragen, die den Stimmberechtigten bei Abstimmungen unterbreitet werden, bzw. Listen mit den Kandidatinnen und Kandidaten bei Wahlen.
Hilfsmittel für die Stimmberechtigten	Bereitgestellte Unterlagen und Inhalte zur Information der Stimmberechtigten (z.B. Stimmmaterial, Informationsplattform etc.).
Informationsressourcen*	Begriff aus der "OCTAVE Allegro"-Methodologie: Besonders wichtige Datenelemente, deren Integrität, Vertraulichkeit und/oder Verfügbarkeit geschützt werden muss.
Kontrollurne	Urne, welche die Kontrollstimmen der Mitglieder des Electoral-Boards enthält, um die Integrität der Urne vom Electoral-Board prüfen zu lassen.
Stimmrechtsausweis (SRA)*	Ein Dokument, welches den Stimmberechtigten erlaubt, ihr Stimmrecht wahrzunehmen.

Begriff	Beschreibung
Testurnen	Urnen, die es erlauben, die Funktionsfähigkeit des Systems zu testen. Es kommen während des Prozesses verschiedene Testurnen zum Einsatz, beispielsweise werden am D2 in Anwesenheit des Electoral-Boards Teststimmen abgegeben und entschlüsselt, um sicherzustellen, dass der gesamte Prozess ordnungsgemäss funktioniert.

Tabelle 3: Generelle Begriffe

3 Glossar – Technische Begriffe

Die folgende Tabelle liefert eine Übersicht der relevanten technischen Begrifflichkeiten im Zusammenhang mit der elektronischen Stimmabgabe.

Begriff	Beschreibung
Backend*	Das Backend der E-Voting-Umgebung wird von der Post betrieben und umfasst den E-Voting Server sowie die Kontrollkomponenten.
Cantonal Computer	Normaler Büroarbeitsplatz eines Kantonsmitarbeitenden.
Configuration Computer (Offline) (VEleS: Setup-Komponente) (Post: Setup SDM)	Offline Gerät, welches für die Konfiguration eines Urnengangs benötigt wird (vgl. Begriff "Offline Geräte"). Auf diesem Gerät werden beispielweise die Codes für die Stimmrechtsausweise generiert. Insbesondere wird die Software SDM auf diesem Gerät installiert.
Datenträger	USB-Sticks oder SD-Karten, die für den Austausch von Daten zwischen den verschiedenen Geräten verwendet werden.
Decryption Computer (Offline) (VEleS: Kontrollkomponente beim Kanton) (Post: Tally SDM)	Offline Gerät, welches für das Mischen und Entschlüsseln der Stimmen benötigt wird (vgl. Begriff "Offline Geräte"). Insbesondere wird die Software SDM auf diesem Gerät installiert.
DIS (Data Integration Service)*	Tool der Post zur Generierung der Konfigurationsdateien eines Urnengangs.
Entropie	In der Kryptographie versteht man unter Entropie die Unvorhersehbarkeit von Daten. Je grösser die Entropie ist, desto komplexer und unvorhersehbarer sind die Daten. Damit wird es schwieriger, sie zu entschlüsseln. Für die Sicherheit von E-Voting ist es wichtig, dass Werte, die zufällig sein müssen, genügend zufällig sind und somit über ausreichend Entropie verfügen.
Ergebnisermittlungssystem	Kantonales System zur Auszählung und Konsolidierung der Ergebnisse aus allen Stimmkanälen.
E-Voting Landing Page	Internet-Seite, die den Kantonen von der Post zur Verfügung gestellt wird. Die Landing Page enthält verschiede Informationen für die Stimmberechtigten sowie Links zu den aktiven Urnengängen im Wahl- und Abstimmungsportal.

Begriff	Beschreibung
E-Voting Server (VEleS: Nicht vertrauenswürdiger Systemteil) (Post: Voting Server)	Kernkomponente der E-Voting Plattform, auf der der Kanton über den SDM den Urnengang einrichtet. Der E-Voting Server ist Teil des Backends (vgl. Begriff "Backend"), wird durch die Post betrieben und speichert die elektronischen Urnen.
Hashwert (Fingerabdruck)	Ein Hashwert (auch als Prüfsumme bezeichnet) ist ein Wert, der durch eine kryptographische Funktion aus Daten generiert wird. Er ist eine Art Fingerabdruck der Daten, der sich aus einer festen Anzahl von Bytes zusammensetzt und als eindeutige Kennung der Daten dient. Hashwerte werden eingesetzt, um die Integrität von Daten sicherzustellen. Jede Veränderung an den Daten führt zu einem vollständig anderen Hashwert. Ist der Hashwert identisch, weiss man, dass keine Veränderung vorgenommen worden ist. Hashwerte spielen beispielsweise bei der Herstellung der für E-Voting notwendigen Software (Build) eine wichtige Rolle. Anhand der Hashwerte können die Kantone prüfen, dass sie die richtige und unveränderte Software ausführen (vgl. Begriff "Trusted Build und Trusted Deployment").
Initialisierungscode auf dem Stimmrechtsausweis	Der Initialisierungscode besteht aus einer Reihe von Zahlen und Buchstaben, die sich auf dem Stimmrechtsausweis befinden. Die Stimmberechtigten müssen den Initialisierungscode sowie ein zusätzliches Authentifizierungsmerkmal auf dem Startbildschirm des Wahl- und Abstimmungsportals eingeben, um sich zu identifizieren und den Stimmabgabeprozess zu starten.
KeePass	Passwort-Manager, der für die sichere Verwaltung der Passwörter verwendet wird.
Kontrollkomponenten**	Die Kontrollkomponenten sind unabhängige Elemente des Systems, die unterschiedlich ausgestaltet sind, von unterschiedlichen Personen betrieben werden und durch besondere Massnahmen gesichert sind. Gewisse Kontrollkomponenten sind Teil des Backends (vgl. Begriff "Backend"), werden durch die Post betrieben und kommen insb. bei der Erstellung der Prüfcodes, der Prüfung der Prüfcodes bei der Stimmabgabe und der Mischung der Urnen zum Einsatz. Bei der Mischung der Urnen fungiert der Decryption Computer als Kontrollkomponente, die beim Kanton betrieben wird.
Logs*	Daten, mit denen das korrekte Funktionieren des Stimmvorgangs festgestellt werden kann oder anhand deren eine allfällige Fehlfunktion untersucht werden kann.

Begriff	Beschreibung
Offline Geräte	Isolierte Geräte, die für die Durchführung und die Überprüfung eines Urnengangs benötigt werden. Die Offline Geräte haben zu keinem Zeitpunkt Zugang zu einem Netzwerk oder dem Internet. Die Daten werden ausschliesslich verschlüsselt über Datenträger übertragen (vgl. Begriffe "Configuration Computer" und "Decryption Computer").
Parameter des Urnengangs*	Basisdaten des Urnengangs, beispielsweise das Datum des Urnengangs, die Daten und die Zeiten, zu denen die Stimmabgabe möglich ist, die Art der Abstimmung und/oder Wahl sowie die Sicherheitsparameter (z.B. die Anzahl der Mitglieder des Electoral-Boards).
Passwörter des Urnengangs	Passwörter zur Generierung der Sicherheitsschlüssel des Urnengangs an D2 (die Sicherheitsschlüssel werden benötigt für die Ver- und Entschlüsselung der Stimmen).
Passwörter der Mitglieder des Admin-Boards	Passwörter, die es einem Mitglied des Admin-Boards erlauben, sich beim SDM (vgl. Begriff "SDM (Secure Data Manager)") zu authentifizieren.
SDM (Secure Data Manager)*	Zentrale Software der Post, damit die Kantone einen Urnengang aufsetzen und durchführen können. Diese Software wird auf den E-Voting-Computern der Kantone installiert. Mit dieser Software werden beispielsweise an D1 und D2 die Codes für die Stimmberechtigten und die Sicherheitsschlüssel für die Verschlüsselung der Stimmen generiert und die Stimmen an D3 gemischt und entschlüsselt.
Seed	Seed (Englisch für Saat, Keim, säen, setzen) bezeichnet in der Kryptographie den Startwert (Initialisierungswert) für einen Verschlüsselungsalgorithmus. Basierend auf der Eingabe des Seeds durch den Kanton werden die Verschlüsselungsparameter berechnet.
Sicherheitsschlüssel	Kryptographischer Grundstein, um ein digitales Asset zu schützen. Im Kontext von der elektronischen Stimmabgabe wird basierend auf der Eingabe von zwei Passwörtern der Sicherheitsschlüssel für die Ver- und Entschlüsselung der Stimmen generiert.
Software der Einwohnerdienste	Software-Anwendung der Gemeinden / der Kantone zur Verwaltung und Pflege der Daten der Stimmberechtigten. Die Anwendung wird zudem dazu verwendet, die eCH0045-Dateien (Stimmregister) für den Urnengang zu generieren (vgl. Begriff "EV-Stimmregister").

Begriff	Beschreibung
Software zur Generierung der Stimmrechtsausweise*	Software, die für die Generierung der Stimmrechtsausweise verwendet wird.
Stimmrechtsausweise (SRA) Computer (Offline)	Offline Gerät, das für Generierung der Stimmrechtsausweise verwendet wird.
Synchronisation Computer (Online) (VEleS: Nicht vertrauenswürdiger Systemteil) (Post: Online SDM)	Online Gerät, das für die Synchronisation des Urnengangs mit den Servern der Post benötigt wird. Insbesondere wird die Software SDM auf diesem Gerät installiert.
Trusted Build und Trusted Deployment	Der Begriff Trusted Build und Trusted Deployment (kurz "Trusted Build und Deployment") steht für eine vertrauenswürdige Herstellung (Build) und Installation (Deployment) der für E-Voting notwendigen Software. Durch den Trusted Build und Trusted Deployment-Prozess wird sichergestellt, dass die von der Post und den Kantonen eingesetzte Software dem publizierten Quellcode entspricht, der einer öffentlichen Kontrolle und unabhängigen Überprüfung unterzogen wurde. Dieser Prozess wird durch eine von den Kantonen mandatierte Fachperson sowie einem Vertreter der Kantone aktiv begleitet. Die entsprechenden Protokolle werden veröffentlicht.
Verification Computer (Offline)	Offline Gerät, dass dem Electoral-Board zur Überprüfung des Urnengangs zur Verfügung gestellt wird (vgl. Begriff "Offline Geräte"). Insbesondere wird die Software Verifier auf diesem Gerät installiert.
Verifier* (VEleS: Technisches Hilfsmittel der Prüferinnen und Prüfer)	Software der Post. Der Verifier dient den Prüferinnen und Prüfer als technisches Hilfsmittel, um die Konfiguration des Urnengangs sowie das Mischen und Entschlüsseln zu überprüfen.
Verifizierungscodes auf dem Stimmrechtsausweis*	Die auf dem Stimmrechtsausweis aufgedruckten Codes (Bestätigungs- und Finalisierungscode sowie die Prüfcodes).
Wahl- und Abstimmungsportal*	Web-Portal der Post, das von den stimmenden Personen zur Stimmabgabe genutzt wird.

Tabelle 4: Technische Begriffe

4 Tabellenverzeichnis