Präsidialdepartement des Kantons Basel-Stadt
Staatskanzlei

Standeskanzlei Graubünden
Chanzlia chantunala dal Grischun
Cancelleria dello Stato dei Grigioni

Kanton St.Gallen
Staatskanzlei

Thurgau
Staatskanzlei

Konzept Vollständige Verifizierbarkeit

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	17.05.2024
Version	1.5
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	27.01.2023	Präzisierung im Abschnitt 4.2.1	Projektleitung E-Voting (BS) Leitung Informatik und Infrastruktur (SG) Fachperson E-Voting (TG)
1.2	28.04.2023	Integration von Graubünden Anpassung in Abschnitt 3.2	Projektleitung E-Voting (BS) E-Voting Beauftragter (GR) Leitung Informatik und Infrastruktur (SG) Fachperson E-Voting (TG)
1.3	14.06.2023	Anpassung in Abschnitt 5	Projektleitung E-Voting (BS) E-Voting Beauftragter (GR) Leitung Informatik und Infrastruktur (SG) Fachperson E-Voting (TG)
1.4	29.09.2023	Formelle Anpassungen	Projektleitung E-Voting (BS) E-Voting Beauftragter (GR) Leitung Informatik und Infrastruktur (SG) Fachperson E-Voting (TG)
1.5	17.05.2024	Anpassungen in Abschnitten 3.3, 3.4 und 4.2.2 / 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 Staatskanzlei (BS) Leitung Staatskanzlei (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 über die politischen Rechte (VPR, SR 161.11) vom 24. Mai 1978	Stand vom 01.07.2022
[2]	Verordnung der BK über die elektronische Stimmabgabe (VEleS, SR 161.116) vom 25. Mai 2022	Stand vom 01.07.2022

Nr.	Dokument	Version
[3]	Verordnung über den Testbetrieb für die elektronische Stimmabgabe (SG 132.150) vom 26. Mai 2009[1]	Stand vom 03.01.2019
[4]	Gesetz über Wahlen und Abstimmungen (Wahlgesetz, SG 132.100) vom 21. April 1994	Stand vom 01.01.2021
[5]	Gesetz über die politischen Rechte im Kanton Graubünden (GPR, BR 150.100) vom 17. Juni 2005	Stand vom 01.01.2024
[6]	Verordnung über die politischen Rechte im Kanton Graubünden (VPR, BR 150.200) vom 20. September 2005	Stand vom 01.01.2024
[7]	Gesetz über Wahlen und Abstimmungen (WAG, sGS 125.3) vom 05. Dezember 2018	Stand vom 01.01.2019
[8]	Verordnung des Regierungsrates zum Gesetz über das Stimm- und Wahlrecht (StWV; RB 161.11) vom 24. Juni 2014	Stand vom 01.08.2014
[9]	Swiss Post Voting System: Verifier specification https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/blob/master/System/Verifier_Specification.pdf	Aktuelle Version auf GitLab
[10]	Notfallplan	Aktuelle Version
[11]	Konzept Schulungen und interne Information	Aktuelle Version
[12]	Glossar	Aktuelle Version

[1] Dieses Dokument ist in Zusammenarbeit der Kantone Basel-Stadt, Graubünden, St.Gallen und Thurgau entstanden. Kantonsspezifische Inhalte werden mit unterschiedlichen Schriftfarben dokumentiert (violett = gilt nur für Basel-Stadt; rot = gilt nur für Graubünden; grün = gilt nur für St.Gallen; blau = gilt nur für Thurgau).

Inhaltsverzeichnis

1 Zweck des Dokumentes

Das vorliegende Dokument beschreibt die Umsetzung der vollständigen Verifizierbarkeit für die elektronische Stimmabgabe in den Kantonen.

2 Einleitung

Gemäss Art. 27i der Verordnung über die politischen Rechte (VPR, siehe *referenziertes Dokument [1]*) stellen die Kantone sicher, dass die korrekte Verarbeitung der Stimmen und die Korrektheit des Ergebnisses des elektronischen Stimmkanals verifiziert werden (Abs. 2). Zusätzlich plausibilisieren sie die Ergebnisse der elektronischen Stimmabgabe (Abs. 1).

Die **Verifizierbarkeit** der elektronischen Stimmabgabe ist die zentrale Massnahme zur Gewährleistung der Sicherheit von E-Voting, da sie die Feststellung von Manipulationen an den elektronisch abgegebenen Stimmen erlaubt. Die Verifizierbarkeit sieht vor, dass überprüft werden können muss, ob:

- die Stimme wie beabsichtigt abgegeben wurde,
- die Stimme so abgespeichert wurde, wie sie abgegeben wurde,
- die Stimme so ausgezählt wurde, wie sie gespeichert wurde.

Die **vollständige Verifizierbarkeit** stellt sicher, dass jede Manipulation, die zu einer Verfälschung des Ergebnisses führt, unter Wahrung des Stimmgeheimnisses erkannt werden kann (siehe Art. 5 Ziff. 1 Verordnung der BK über die elektronische Stimmabgabe, VEleS, *referenziertes Dokument [2]*). Dies ist gegeben, wenn die Anforderungen an die individuelle und an die universelle Verifizierbarkeit erfüllt sind.

Die **individuelle Verifizierbarkeit** ist die Funktionalität des Systems, die der stimmenden Person ermöglicht durch Beweise (insb. Prüfcodes) zu kontrollieren, ob ihre Stimme unverändert durch den E-Voting Server registriert wurde (siehe Art. 5 Abs. 2 VEleS). Die individuelle Verifizierbarkeit liegt grundsätzlich in der Verantwortung der Stimmberechtigten. Die Stimmberechtigten werden durch den Kanton über die Bedeutung der individuellen Verifizierbarkeit und die Prüfcodes im Besonderen informiert. Sie werden aufgerufen, sich bei falsch angezeigten Prüfcodes beim Kanton zu melden und den Stimmabgabeprozess abzubrechen. Diesbezügliche Meldungen von Stimmberechtigten werden von der Leitung der elektronischen Stimmabgabe gesammelt und den Prüferinnen und Prüfern vorgelegt.

Die **universelle Verifizierbarkeit** ermöglicht es, vorsätzliche oder unbeabsichtigte Manipulationen (Verändern, Hinzufügen, Löschen) in der Infrastruktur zu entdecken. Dafür generiert das System im gesamten Wahl- bzw. Abstimmungsablauf Beweise, die durch die Prüferinnen und Prüfer mit einem technischen Hilfsmittel ausgewertet werden (siehe Art. 5 Abs. 3 VEleS). Die Verantwortung für die universelle Verifizierbarkeit liegt beim Kanton bzw. den vom Kanton mandatierten Prüferinnen und Prüfern.

Für die Beurteilung, ob ein Urnengang korrekt und ohne vorsätzliche oder unbeabsichtigte Manipulation durchgeführt wurde, werden auch allfällige Meldungen / Hinweise der Post berücksichtigt, gestützt auf die Überwachung des Systems (Monitoring). Das Admin-Board erhält von der Post während der Urnenöffnungszeit täglich einen Bericht zu den wichtigsten vom System registrierten Aktivitäten. Der Bericht enthält beispielsweise eine Statistik der abgegebenen Stimmen. Zeigt dieser Bericht Auffälligkeiten, wird diesen nachgegangen. Die Prüferinnen und Prüfer werden über alle Auffälligkeiten bzw. Anomalien informiert.

Zusätzlich zu den Massnahmen im Zusammenhang mit der vollständigen Verifizierbarkeit und dem Monitoring der Post, **plausibilisiert der Kanton die E-Voting-Ergebnisse**. Dazu gehört die Abgabe von Kontrollstimmen an D2 und deren Entschlüsselung und Kontrolle an D3. Des Weiteren werden die Ergebnisse des elektronischen Stimmkanals mit den Ergebnissen der anderen Stimmkanäle verglichen. Die Anzahl der elektronisch ausgezählten Stimmen wird zudem mit den statistischen Berichten der Post abgeglichen.

3 Electoral-Board

3.1 Kantonale Grundlagen und Begriffe

In diesem Dokument wird der Begriff "Electoral-Board" für das nachfolgend kantonal definierte Gremium verwendet. Ausserdem nimmt das Electoral-Board die Aufgaben der Prüferinnen und Prüfer gemäss VEleS (Art. 2 lit. h) wahr.

3.1.1 Kanton Basel-Stadt

In der Verordnung über den Testbetrieb für die elektronische Stimmabgabe (siehe *referenziertes Dokument [3]*) definiert den Kanton Basel-Stadt den Einsatz eines Wahlkomitees (Art. 8a). Das Wahlkomitee besteht aus den Beauftragten des Regierungsrates für Wahlen und Abstimmungen und aus Mitarbeitenden der Staatskanzlei. Gemäss Art. 13 des Wahlgesetzes (siehe *referenziertes Dokument [4]*) werden die Beauftragten vom Regierungsrat gewählt. Die Mitarbeitenden der Staatskanzlei werden durch die Leitung der Staatskanzlei bestimmt.

In Rahmen der elektronischen Stimmabgabe mit der universellen Verifizierbarkeit hat das Wahlkomitee die in Art. 8a der Verordnung definierten Aufgaben, Pflichten und Kompetenzen (siehe *Abschnitte 3.2 und 3.3*). Insbesondere kontrollieren dessen Mitglieder als Prüferinnen und Prüfer die im Zusammenhang mit der universellen Verifizierbarkeit generierten Beweise. Sie setzen dafür ein technisches Hilfsmittel (siehe *Abschnitt 4*) ein. Für die optimale Begleitung der elektronischen Stimmabgabe stellt der Kanton sicher, dass das Wahlkomitee über die notwendigen Kompetenzen verfügt. Im Idealfall sollte das Wahlkomitee mit sechs Personen besetzt werden.

3.1.2 Kanton Graubünden

In Artikel 30e des Gesetzes über die politische Rechte im Kanton Graubünden wird als Grundsatz definiert, dass bei jedem Urnengang die Resultatermittlung überprüft werden muss (GPR; BR 150.100, siehe *referenziertes Dokument [5]*). In der Verordnung über die politischen Rechte im Kanton Graubünden (VPR; BR 150.200, siehe *referenziertes Dokument [6]*) definiert den Kanton den Einsatz einer Wahl- und Abstimmungskommission E-Voting (Art. 21g ff.). Gemäss der Verordnung über die politischen Rechte werden die Mitglieder der Wahl- und Abstimmungskommission E-Voting für die Dauer von vier Jahren durch die Regierung gewählt.

In Rahmen der elektronischen Stimmabgabe hat die Wahl- und Abstimmungskommission E-Voting Aufgaben, Pflichten und Kompetenzen (siehe *Abschnitte 3.2 und 3.3*). Insbesondere kontrollieren dessen Mitglieder als Prüferinnen und Prüfer die im Zusammenhang mit der universellen Verifizierbarkeit generierten Beweise. Sie setzen dafür ein technisches Hilfsmittel (siehe *Abschnitt 4*) ein. Für die optimale Begleitung der elektronischen Stimmabgabe stellt der Kanton sicher, dass die Wahl- und Abstimmungskommission E-Voting über die notwendigen Kompetenzen verfügt. Im Idealfall sollte die Kommission mit mind. fünf Personen besetzt werden.

3.1.3 Kanton St.Gallen

Im Gesetz über Wahlen und Abstimmungen (WAG, siehe *referenziertes Dokument [7]*) definiert der Kanton St.Gallen den Einsatz eines kantonalen Stimmbüros (Art. 11 ff.). Gemäss WAG werden die Mitglieder des kantonalen Stimmbüros für die Dauer von vier Jahren (eine Legislatur-Periode) durch die Regierung gewählt. Die Regierung bestimmt zudem eine Präsidentin oder einen Präsidenten sowie eine Schreiberin oder einen Schreiber aus dessen Mitgliedern.

In Rahmen der elektronischen Stimmabgabe hat das Stimmbüro zusätzliche Aufgaben, Pflichten und Kompetenzen (siehe *Abschnitte 3.2 und 3.3*). Insbesondere kontrollieren dessen Mitglieder als Prüferinnen und Prüfer die im Zusammenhang mit der universellen Verifizierbarkeit generierten Beweise. Sie setzen dafür ein technisches Hilfsmittel (siehe *Abschnitt 4*) ein. Für diese Aufgabe wird ein Ausschuss des Stimmbüros definiert, der die Aufgaben mit Blick auf die elektronische Stimmabgabe wahrnimmt. Für die optimale Begleitung der elektronischen Stimmabgabe stellt der Kanton sicher, dass der Ausschuss des Stimmbüros über die notwendigen Kompetenzen verfügt. Im Idealfall sollte der Ausschuss mit mind. sechs Personen besetzt werden.

3.1.4 Kanton Thurgau

Im Kanton Thurgau bestimmt der Regierungsrat mindestens fünf Mitglieder des Stimmbüros für Auslandschweizerinnen und Auslandschweizer (Art. 26 Abs. 1 der Verordnung zum Gesetz über das Stimm- und Wahlrecht StWV; siehe *referenziertes Dokument [8]*). Das Stimmbüro überwacht den Ablauf, die Entschlüsselung und die Auswertung der elektronisch abgegebenen Stimmen (Art. 26 Abs. 2 StWV). Es kann zur Ermittlung der Ergebnisse zusätzliche Personen beiziehen (Art. 26 Abs. 3 StWV).

In Rahmen der elektronischen Stimmabgabe hat das Stimmbüro zusätzliche Aufgaben, Pflichten und Kompetenzen (siehe *Abschnitte 3.2 und 3.3*). Insbesondere kontrollieren dessen Mitglieder als Prüferinnen und Prüfer die im Zusammenhang mit der universellen Verifizierbarkeit generierten Beweise. Sie setzen dafür ein technisches Hilfsmittel (siehe *Abschnitt 4*) ein. Für die Begleitung der elektronischen Stimmabgabe stellt der Kanton sicher, dass das Stimmbüro oder ein Ausschuss aus Mitgliedern des Stimmbüros über die notwendigen Kompetenzen verfügen.

3.2 Rechte und Pflichten der Mitglieder des Electoral-Boards

In Rahmen ihrer Tätigkeiten haben die Mitglieder des Electoral-Boards die folgenden Rechte:

- Sie dürfen alle Schritte der elektronischen Stimmabgabe (D0 bis D4) verfolgen und beobachten.
- Sie haben Einsicht in alle Protokolle und Unterlagen im Zusammenhang mit E-Voting und dürfen Fragen stellen.
- Sie erhalten von der Staatskanzlei / Standeskanzlei alle Informationen, die für die Beurteilung der Korrektheit des Ergebnisses relevant sind (insbesondere die Zahl und Art von Anomalien, die durch stimmberechtigte Personen gemeldet werden; Meldungen und Hinweise der Post oder von Dritten).
- Sie haben das Recht, über die wichtigsten Prozesse im Zusammenhang mit der Verifizierbarkeit angemessen informiert und geschult zu werden.
- Sie dürfen externe Unterstützung anfragen (siehe *Abschnitt 3.4*).
- Sie dürfen in Abstimmung mit der Regierung als leitende Behörde bei eidgenössischen und kantonalen Wahlen und Abstimmungen öffentlich über ihre Tätigkeit kommunizieren.

Grundsätzlich muss die Staatskanzlei / Standeskanzlei gegenüber dem Electoral-Board eine vollständige Transparenz über die Tätigkeiten für die elektronische Stimmabgabe sicherstellen.

In Rahmen ihrer Tätigkeiten haben die Mitglieder des Electoral-Boards die folgenden Pflichten:

- Sie müssen am D2 (Bereitstellung der Urne) und D3 (Entschlüsselung der Stimmen und Ergebnisermittlung) teilnehmen.
- Sie sind für den Betrieb des technischen Hilfsmittels zuständig und können die Ausführung der operativen Schritte an die Staatskanzlei / Standeskanzlei delegieren.
- Sie wahren das Amtsgeheimnis.
- Sie wahren das Stimmgeheimnis.
- Sie behandeln die Ergebnisse der elektronischen Urne bis zur offiziellen Publikation der Ergebnisse als vertraulich.
- Alle Daten und Dateien, die für die elektronische Stimmabgabe notwendig sind, dürfen die Infrastruktur des Kantons nicht verlassen und müssen sicher und gemäss den Vorgaben aufbewahrt werden (dies gilt insb. für die Dateien, die für die universelle Verifizierbarkeit notwendig sind). Ausnahmen sind möglich, wenn die Staatskanzlei / Standeskanzlei oder das Electoral-Board mit der Post oder unabhängigen Experten zusammenarbeiten (siehe *Abschnitt 3.4).*

- Sie müssen an den Schulungen teilnehmen und sich in die Prozesse der universellen Verifizierbarkeit einarbeiten. Sie müssen in der Lage sein, die Vorgänge und ihre Bedeutung rund um das technische Hilfsmittel in den Kernpunkten zu verstehen.

3.3 Aufgaben des Electoral-Boards

Das Electoral-Board wird bei D2 (Bereitstellung der Urne) und D3 (Entschlüsselung der Stimmen und Ergebnisermittlung) eingesetzt. Sie haben ausserdem das Recht während den anderen Aufgaben anwesend sein.

Die folgende Tabelle fasst die wichtigsten Aufgaben des Electoral-Boards zusammen und stellt sie den Aufgaben der Prüferinnen und Prüfer gemäss VEleS gegenüber:

Prozessschritt	**Aufgaben des Electoral-Boards gemäss kantonalem Recht**	**Aufgaben des Electoral-Boards als Prüferinnen und Prüfer gemäss VEleS**
D2 (Bereitstellung der Urnen)	• Das Electoral-Board und das Admin-Board definieren je ein komplexes Passwort und speichern dieses separat voneinander auf PIN-geschützen Datenträgern (mit je mind. einem Backup). Mit diesen zwei Passwörtern werden die Sicherheitsschlüssel des Urnengangs generiert. • Jedes Mitglied des Electoral-Boards gibt eine Stimme in die Kontrollurne ab. Die Stimmabgabe wird protokolliert und das Protokoll in einem Kuvert versiegelt. Die Staatskanzlei / Standeskanzlei bewahrt dieses bis zum Abstimmungs-/Wahlsonntag sicher auf. • Das Electoral-Board bestätigt per Unterschrift, dass die Schritte im D2 korrekt durchgeführt wurden.	• Prüfung, dass die richtige Version des Verifiers im Einsatz ist • Kontrolle der Ergebnisse des Verifiers bei der Überprüfung der Konfiguration des Urnengangs
D3 (Entschlüsselung der Stimmen und Ergebnisermittlung)	• Nach dem Mischen geben je ein Mitglied des Electoral-Boards und des Admin-Boards das auf ihrem Datenträger gespeicherte Passwort ein, um die Stimmen mit dem rekonstruierten Sicherheitsschlüssel zu entschlüsseln. • Die Kontrollurne wird elektronisch ausgezählt und mit dem Protokoll "Abgabe Kontrollstimmen" verglichen. Die beiden Ergebnisse müssen identisch sein. • Die EV-Ergebnisse werden ausgezählt und ins Ergebnisermittlungssystem eingespielt. Das Electoral-Board kontrolliert, dass die EV-Ergebnisse im Ergebnisermittlungssystem korrekt eingespielt wurden und den mittels Verifier überprüften Ergebnissen entsprechen.	• Beobachtung alle Prozessschritten während D3 • Prüfung, dass die richtige Version des Verifiers im Einsatz ist • Prüfung der Informationen über den Ablauf des Urnengangs, die vom Admin-Board geliefert werden • Beobachtung der Überprüfung des Urnengangs anhand des Verifiers und Kontrolle der Ergebnisse. Jegliche Feststellungen werden den Prüferinnen und Prüfern erklärt. • Bei Bedarf geben die Prüferinnen und Prüfer eine Untersuchung in Auftrag.

Prozessschritt	Aufgaben des Electoral-Boards gemäss kantonalem Recht	Aufgaben des Electoral-Boards als Prüferinnen und Prüfer gemäss VEleS
	• Das Electoral-Board bestätigt per Unterschrift, dass die Schritte im D3 korrekt durchgeführt wurden, und die EV-Ergebnisse korrekt sind.	

Tabelle 1: Aufgaben des Electoral-Boards und der Prüferinnen und Prüfer

3.4 Technische Begleitung

Die Untersuchung von festgestellten Problemen oder Unregelmässigkeiten erfolgt in erster Linie in Zusammenarbeit mit den Spezialistinnen und Spezialisten der Post. Der Kanton erstellt einen Bericht, in dem die Analyse und die Ursache beschrieben wird.

Für die Analyse von Ereignissen und/oder für die Bestätigung der Analyse durch die Post können die Staatskanzlei / Standeskanzlei oder das Electoral-Board auf von der Post unabhängige Experten zugreifen. Die Kantone arbeiten zu diesem Zweck mit ausgewählten Experten zusammen.

Die Tätigkeiten, Rechte und Pflichten sowie Verfügbarkeit (insb. während oder kurz nach jedem Urnengang) werden vertraglich zwischen den Kantonen und den Experten festgehalten.

4 Technisches Hilfsmittel

4.1 Verifier der Post als technisches Hilfsmittel

Der Kanton stellt dem Electoral-Board den Verifier der Post als technisches Hilfsmittel der Prüferinnen und Prüfer (im Sinne der VEleS) zur Verfügung. Es handelt sich dabei um eine Software, die es erlaubt, die Konfiguration des Urnengangs sowie das Mischen und Entschlüsseln zu überprüfen.

Der Verifier wurde von der Post auf der Plattform GitLab offengelegt[2]. Der Verifier ist unter der permissiven Open Source Lizenz Apache 2 lizenziert. Der Verifier ist in folgendem Sinn unabhängig vom E-Voting System der Post:

- Der Code des Verifiers ist eine eigenständige Software der Post mit separatem Code.
- Der Verifier nutzt die Library Crypto-Primitives[3]. Diese beinhaltet kryptographische Algorithmen und wird auch durch das E-Voting-System genutzt. Wie der Verifier ist auch die Crypto-Primitives-Library unter der permissiven Open Source Lizenz Apache 2 lizenziert.

[2] Siehe swisspost-evoting / Verifier / Verifier · GitLab
[3] Siehe https://gitlab.com/swisspost-evoting/crypto-primitives/crypto-primitives

Die Qualität und der Funktionsumfang des Verifiers wird mit folgenden Massnahmen sichergestellt:

- Durch die Offenlegung der Dokumentation (Spezifikationen) und des Codes kann der Verifier öffentlich überprüft werden.
- Der Verifier ist ebenfalls Teil des Bug-Bounty-Programms der Post. Somit besteht ein Anreiz, Fehler zu melden.
- Der Verifier gehört zum Gegenstand der unabhängigen Überprüfung im Auftrag der Bundeskanzlei.
- Der Verifier wird durch die Post technisch und funktional getestet.
- Der Verifier wird durch die Kantone fachlich getestet.

Mittels Hashwerte prüft das Electoral-Board, ob der eingesetzte Verifier dem veröffentlichten Quellcode entspricht und damit die richtige Version des Verifiers im Einsatz ist.

4.2 Prüfpunkte im Verifier der Post

Zur Umsetzung der universellen Verifizierbarkeit umfasst der Verifier der Post eine Vielzahl von Prüfpunkten. Die vollständige Liste der Prüfpunkte kann der Spezifikation entnommen werden (siehe *referenziertes Dokument [9]*).

4.2.1 Blöcke der Prüfpunkte

Die Prüfpunkte sind in zwei Blöcke gruppiert:

Block	**Beschreibung**	**Wann**
Überprüfung Konfigurationsphase	In diesem Block wird geprüft, ob der Urnengang korrekt vorbereitet wurde. Dies beinhaltet sowohl die Konfiguration des Urnenganges als auch die kryptographische Konfiguration.	D2
Überprüfung Auszählung und Resultatermittlung	In diesem Block wird die Korrektheit der kryptographischen Operationen (Bereinigen, Mischen und Entschlüsseln) überprüft. Der Verifier prüft zudem, dass alle bestätigten Stimmen und nur gültig abgegebene Stimmen entschlüsselt wurden, und dass die EV-Ergebnisse mit den einzelnen entschlüsselten Stimmen übereinstimmen.	D3

Tabelle 2: Prüfpunktblöcke des Verifiers

4.2.2 Ergebnis der Prüfpunkte

Pro Prüfpunkt gibt der Verifier eines der folgenden Ergebnisse aus:

Ergebnis	Beschreibung
Erfolgreich (weiss)	Der Prüfpunkt wurde erfolgreich getestet. Keine Fehler oder Anomalien wurden festgestellt.
Fehler (gelb)	Der Prüfpunkt konnte aufgrund eines Fehlers nicht durchgeführt werden.
Anomalie (rot)	Der Prüfpunkt konnte durchgeführt werden, aber die Kontrolle entspricht nicht dem erwarteten Ergebnis.

Tabelle 3: Ergebnis der Prüfpunkte

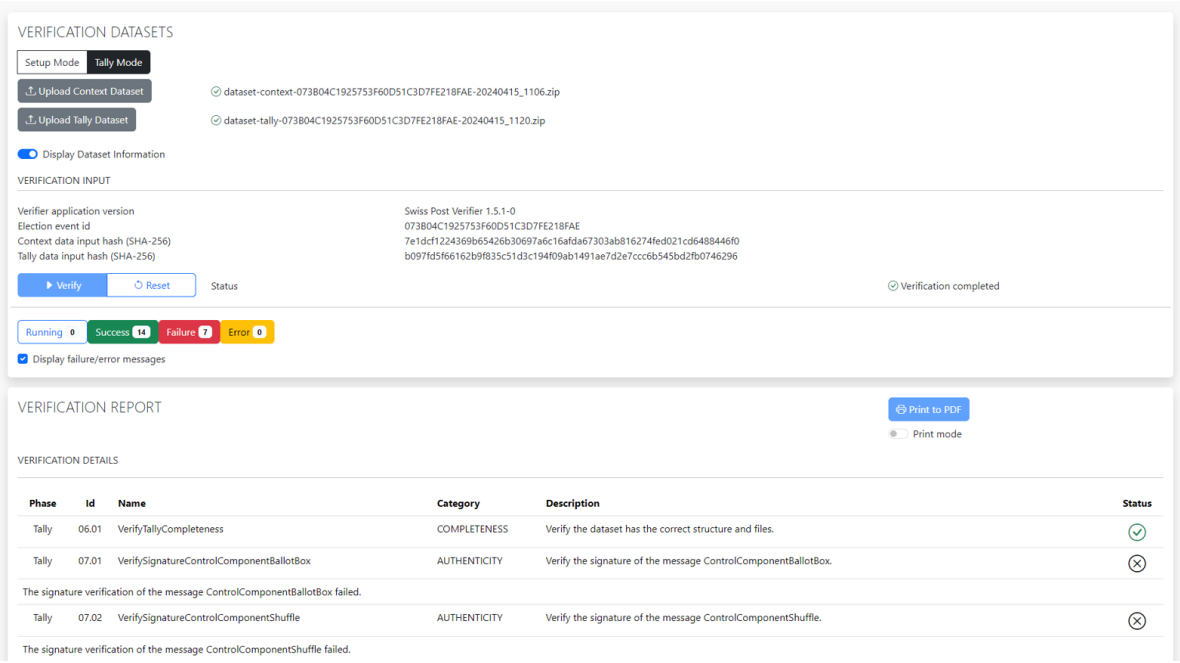

Abbildung 1: Oberfläche des Verifiers

4.2.3 Kategorien der Prüfpunkte

Die folgende Tabelle zeigt die Kategorisierung der Prüfpunkte, die durch den Verifier automatisiert geprüft werden. Die Prüfpunkte sind je nach Kategorie unterschiedlich komplex in der Analyse.

	Kategorie der Prüfpunkte	**Beschreibung**
Tiefe Komplexität	Vollständigkeit	Sind die zu prüfenden Daten vollständig? Erlauben die Datenelemente eine vollständige Prüfkette? Beispiel: Wenn eine Datei fehlt, ist der Test nicht erfolgreich.
	Authentizität	Können die Datenelemente eindeutig demjenigen zugeordnet werden, der berechtigt ist? Beispiel: Wenn eine Datei geändert wurde, ist die elektronische Signatur der Datei nicht mehr gültig. Der Test ist nicht erfolgreich.
	Konsistenz	Sind zusammengehörige Datenelemente konsistent zueinander? Beispiel: Die Anzahl von bestätigten Stimmen in jeder Kontrollkomponente muss gleich sein.
	Integrität	Stimmen alle Datenelemente mit der Spezifikation überein? Sind sie alle innerhalb der angegebenen Bereiche? Beispiel: Die Liste der Stimmrechtausweisnummern, die von einer Kontrollkomponente bestätigt wurde, ist eine Unterliste der Stimmrechtausweisnummern, die in D1 generiert wurden.
Hohe Komplexität	Beweise	Sind die in den Wahl- und Abstimmungsdaten enthaltenen kryptographischen Beweise alle gültig? Liefern sie die notwendigen Beweise, um auf die Korrektheit der entsprechenden Protokollschritte zu schliessen? Beispiel: Wenn es beim Mischen einer elektronischen Urne zu Änderungen des Inhalts der Urne kommt, werden die Beweise des Mischens dies bemerken, und eine Anomalie wird festgestellt.

Tabelle 4: Arten der Prüfpunkte des Verifiers

Zusätzlich zu diesen Prüfungen zeigt der Verifier verschiedene Datenelemente an, die durch das Electoral-Board manuell kontrolliert werden müssen. So zeigt der Verifier beispielsweise die Anzahl Stimmberechtigte an. Das Electoral-Board prüft, ob die Angaben mit der ursprünglichen Konfiguration des Urnengangs übereinstimmen.

5 Umgang mit Fehlern und/oder Anomalien

Der Kanton antizipiert mögliche Probleme und erstellt für die wichtigsten Szenarien einen Notfallplan. Dieser Notfallplan beinhaltet auch die wichtigsten Szenarien im Zusammenhang mit der Verifizierbarkeit und der Plausibilisierung der Ergebnisse. Der Notfallplan (siehe *referenziertes Dokument [10]*) wird nach jedem Urnengang anhand der neusten Erfahrungen überprüft und nötigenfalls überarbeitet. Im Notfallplan wird auch definiert, wann der gemeinsame Krisenstab informiert bzw. aktiviert wird.

Zeigt das Monitoring des Urnengangs, der Verifier oder die Plausibilisierung eine Anomalie oder einen Fehler, erfolgt eine Analyse durch die Leitung der elektronischen Stimmabgabe und das Electoral-Board, um die Kritikalität festzustellen und die Massnahmen zu definieren. Dabei lässt sich die Leitung der elektronischen Stimmabgabe von folgenden Fragestellungen und Kriterien leiten.

5.1 Wann tritt die Anomalie und/oder der Fehler auf?

Wird der Fehler oder die Anomalie während der Prüfung in D2 festgestellt, wird die Ursache untersucht. Nach Möglichkeit kann der Urnengang neu aufgesetzt werden, um ein korrekte Konfiguration des Urnengangs sicherzustellen.

5.2 Wie schnell kann die Anomalie und/oder der Fehler untersucht und/oder behoben werden?

Kann das entdeckte Problem durch eine Wiederholung gewisser Prozessschritte behoben werden?

Es ist möglich, dass gewisse Vollständigkeitsprüfungen fehlschlagen, weil Input-Dateien nicht vollständig vorliegen. Durch die Beschaffung der fehlenden Daten (z.B. mittels Backups oder erneuter Sammlung) kann die Verifizierung erfolgreich wiederholt werden. Für die Verifizierung ist nur die Verfügbarkeit und die Korrektheit dieser Daten wichtig und nicht, wann sie generiert oder beschafft werden. Dieses „Recovery-Szenario“ kommt, wenn immer möglich, zur Anwendung. Wenn das Problem innert nützlicher Frist am Abstimmungs- oder Wahlsonntag behoben werden kann, ist eine erfolgreiche Verifikation des Urnengangs möglich. Das Ergebnis kann zweifelsfrei bestätigt werden. Bis zum nächsten Einsatz des Systems wird zusammen mit der Post analysiert, welche Massnahmen notwendig sind, damit das Problem nicht mehr auftritt. Ansonsten sind aber keine weiteren Massnahmen notwendig.

Zeitliche Abhängigkeit mit den anderen Prozessen am oder nach Wahl-/Abstimmungssonntag:

Am Abstimmungs- oder Wahlsonntag steht eine begrenzte Zeit für die Analyse zur Verfügung. Die Fristen hängen von den internen Abläufen des Kantons ab und werden auch mit der Bundeskanzlei abgestimmt. Die Bundeskanzlei erwartet die finalen Ergebnisse bis Mittwoch nach dem Wahl-/Abstimmungssonntag.

Im Kanton Basel-Stadt werden am Sonntag Anfang Nachmittag zuerst Zwischenergebnisse publiziert. Die Zwischenergebnisse beinhalten die Ergebnisse des brieflichen Stimmkanals. Nach dem Abschluss der Auszählung werden die Endergebnisse (als vorläufige Ergebnisse) publiziert und der Bundeskanzlei und dem Bundesamt für Statistik übermittelt. Die Ergebnisse des elektronischen Stimmkanals werden erst bei der Publikation der Endergebnisse miteinbezogen. Die finalen Ergebnisse werden am Mittwoch nach dem Wahl-/Abstimmungssonntag im Kantonsblatt publiziert (Redaktionsschluss ist der Dienstag; die Rechtsmittelfrist ab Publikation beträgt drei Tage bei Bundesvorlagen und fünf Tage bei kantonalen Vorlagen).

Im Kanton St.Gallen werden am Sonntag im Laufe des Nachmittags Zwischenergebnisse publiziert. Nach dem Abschluss der Auszählung werden die Endergebnisse (als vorläufige Ergebnisse) publiziert und der Bundeskanzlei und dem Bundesamt für Statistik übermittelt. Die finalen Ergebnisse werden am Montag (acht Tage nach dem Urnengang) im Kantonsblatt publiziert (Redaktionsschluss ist der Donnerstag nach dem Wahl-/Abstimmungssonntag; die Rechtsmittelfrist ab Publikation beträgt drei Tage).

Im Kanton Graubünden werden die Zwischenergebnisse am Wahl-/Abstimmungssonntag nach 12:00 Uhr auf der Webseite des Kantons publiziert und dem Bundesamt für Statistik übermittelt. Die Publikation der provisorischen Schlussresultate erfolgt nach dem Abschluss der Auszählung in allen Gemeinden (in der Regel ca. um 14:00 Uhr bzw. bei Proporzwahlen zu einem späteren Zeitpunkt). Die Gemeinden liefern die Wahl-/Stimmzettel sowie die Protokolle an die Standeskanzlei, die die Eingangskontrolle vornimmt. Die finalen Ergebnisse werden am Donnerstag nach dem Wahl-/Abstimmungssonntag im Kantonsamtsblatt publiziert. Beschwerden sind spätestens am dritten Tage nach der amtlichen Bekanntgabe der Ergebnisse einzureichen.

Im Kanton Thurgau werden am Sonntag im Laufe des Nachmittags Zwischenergebnisse publiziert. Nach dem Abschluss der Auszählung werden die Endergebnisse (als vorläufige Ergebnisse) publiziert und der Bundeskanzlei und dem Bundesamt für Statistik übermittelt. In seiner Sitzung vom Dienstagvormittag nimmt der Regierungsrat die Ergebnisse zur Kenntnis. Die finalen Ergebnisse werden am Freitag im Amtsplatt publiziert (Redaktionsschluss ist der Dienstag; die Rechtsmittelfrist ab Publikation beträgt drei Tage).

Wenn der Fehler oder die Anomalie rechtzeitig analysiert und behoben werden kann, werden die Ergebnisse als Endergebnisse publiziert. Bleibt die Unsicherheit bestehen, muss beurteilt werden, ob und wie sie sich allenfalls auf das Endergebnis auswirken könnten (insb. abhängig von der Einschätzung zu *Abschnitt 5.4*). Ist ein Einfluss gering oder sehr unwahrscheinlich, werden die Ergebnisse als Endergebnisse publiziert. Könnte der Einfluss erheblich sein, wird von der Leitung der Staatskanzlei / Standeskanzlei in Absprache mit der Bundeskanzlei (bei eidg. Abstimmungen / Wahlen) entschieden, was mit den Ergebnissen passiert (im schlimmsten Fall muss die Abstimmung / Wahl wiederholt werden).

5.3 Kann der Kanton die festgestellte Anomalie oder den Fehler selbst untersuchen, oder benötigt er die Unterstützung der Post oder von externen Expertinnen und Experten?

Der Kanton orientiert sich für seine Analyse an der Spezifikation des Verifiers (siehe *referenziertes Dokument [9]*). Er zieht für seine Analyse die Spezialistinnen und Spezialisten der Post bei.

Kann eine Manipulation nicht ausgeschlossen werden, ziehen die Kantone unabhängige Expertinnen und Experten bei. Die Untersuchung erfolgt zudem in Absprache mit der Bundeskanzlei bzw. des gemeinsamen Krisenstabs.

5.4 Was ist das Problem und wie gravierend ist es?

Wo bzw. bei welchen Kontrollmassnahmen tritt die Anomalie und/oder der Fehler auf?

Betroffenes Sicherheitsziel: Entweder ist das Stimmgeheimnis betroffen oder die Integrität der Stimmen bzw. die Korrektheit des Ergebnisses. Es ist auch möglich, dass beide Sicherheitsziele betroffen sind. Eine Verletzung des Stimmgeheimnisses muss untersucht werden, hat aber keine Auswirkungen auf das Resultat. Das Ergebnis der Wahl oder der Abstimmung ist nicht in Frage gestellt und kann bestätigt werden. Gibt es Fehler oder Anomalien, die einen Einfluss auf die Korrektheit des Ergebnisses haben könnten, muss anhand der nachfolgenden Kriterien untersucht werden, ob das Resultat bestätigt werden kann oder nicht.

Anzahl potenziell betroffener Stimmen / Einfluss auf das Ergebnis: Wie viele Stimmen können vom festgestellten Problem potenziell betroffen sein? Könnte durch die Anzahl potenziell betroffener Stimmen das Resultat der Wahl oder der Abstimmung kippen (dies unter Berücksichtigung der via die anderen Stimmkanäle abgegebenen Stimmen)? Hat das festgestellte Problem keinen Einfluss auf das Ergebnis, so kann dieses bestätigt werden. Hat es möglicherweise einen Einfluss auf das Ergebnis, so können die Ergebnisse nicht bestätigt werden. Bis zum Abschluss der Untersuchung kann der Kanton keine oder nur provisorische Ergebnisse publizieren.

Sicherheitsziel / **Ausmass**	**Stimmgeheimnis**	**Korrektheit der Ergebnisse**
Keine Stimmen betroffen	Untersuchung wird lanciert. Die Ergebnisse können publiziert und bestätigt werden.	Untersuchung wird lanciert. Die Ergebnisse können publiziert und bestätigt werden.
Betroffene Stimmen haben keinen Einfluss auf die finalen Ergebnisse	Untersuchung wird lanciert. Die Ergebnisse können bestätigt und publiziert werden.	Untersuchung wird lanciert. Die Ergebnisse können mit Vorbehalt publiziert werden. Die Ergebnisse werden nach der Untersuchung bestätigt.
Betroffene Stimmen könnten Einfluss auf die finalen Ergebnisse haben	Untersuchung wird lanciert. Die Ergebnisse können bestätigt und publiziert werden.	Untersuchung wird lanciert. Die Ergebnisse können erst nach der Untersuchung publiziert werden.

Tabelle 5: Umgang mit Fehlern oder Anomalien während D3

5.5 Wer muss wann informiert werden?

Interne Information

Sobald sich abzeichnet, dass ein Problem besteht, das den ordentlichen Ablauf am Abstimmung- oder Wahlsonntag beeinträchtigt (z.B. durch eine zeitliche Verzögerung), informiert die Leitung der elektronischen Stimmabgabe die Leitung der Staatskanzlei / Standeskanzlei und die nötigen internen Stellen (inkl. Gemeinden).

Information der anderen E-Voting-Kantone

Bei einem Problem werden die anderen Kantone umgehend informiert. Wenn mehrere oder alle Kantone betroffen sind, werden die Analyse und die Massnahmen zwischen den Kantonen koordiniert.

Information der Bundeskanzlei

Die Bundeskanzlei wird gemäss der Krisenvereinbarung informiert.

Information des Krisenstabs

Der Krisenstab wird gemäss der Krisenvereinbarung informiert und aktiviert.

Information der Öffentlichkeit

Die Öffentlichkeit wird in Abstimmung mit der Leitung der Staatskanzlei / Standeskanzlei, der Medienstelle des Kantons, der Bundeskanzlei und der Post über den Sachverhalt informiert.

5.6 Kann das System beim nächsten Urnengang eingesetzt werden?

Abhängig davon, wie gravierend ein Problem war und wie schnell es analysiert oder behoben werden kann, entscheidet der Kanton, ob er das System beim nächsten Urnengang einsetzen will oder nicht. Dazu tauscht er sich mit der Bundeskanzlei als Zulassungsbehörde, den anderen Kantonen und der Post aus.

6 Schulung für das Electoral-Board

Die Schulung für das Electoral-Board soll die folgenden Themen abdecken:

- Prozesse E-Voting
- Rolle und Einsatz des Verifiers
- Notfallplan und Krisenvereinbarung

Die Details der Schulung sind im "Konzept Schulungen und interne Information" definiert (siehe *referenziertes Dokument [11]*).

7 Abbildungsverzeichnis

8 Tabellenverzeichnis