Risiken und Mängel des Schweizer E-Voting Systems

Unabhängige Kontrolle und belastbare Wege aus der gegenwärtigen Risikolage

Beat W. Meier *
Buchautor · Unternehmer · Visionär · Ethical Hacker — beat-w-meier.ch, Schweiz

ARTIKELINFO

Artikelhistorie:
Erstellt am 9. Oktober 2026
Datenstand: 9. Oktober 2026
Version 1.1
Quellen: ausschliesslich Originalquellen; eigene Bewertungen ausdrücklich getrennt.
Schlüsselwörter:
E-Voting
Gewaltentrennung
Unabhängige Prüfung
Politische Rechte
Auszählbarkeit
Risikosteuerung

ABSTRACT

Das Schweizer E-Voting befindet sich in einem begrenzten Versuchsbetrieb mit einem einzigen eingesetzten Systemanbieter. Die vorliegende Studie untersucht die institutionellen, technischen, betrieblichen und demokratischen Risiken dieses Modells anhand von Rechtsnormen, amtlichen Originalunterlagen, den Originalberichten der beauftragten Fachleute und versionsgebundener Herstellerdokumentation. Drei Sachverhalte sind auseinanderzuhalten: der produktive Versuchsbetrieb, die Fehlergeschichte früherer Systeme und der noch in Entwicklung befindliche Protokollentwurf für System 2.0. Die Quellen belegen sowohl substanzielle Verbesserungen der Prüfung als auch fortbestehende Abhängigkeiten und neue Fehler im Entwicklungsprozess. Der Auszählungsausfall in Basel-Stadt zeigt, dass korrekte Kryptografie allein das Stimmrecht nicht schützt. Die personelle und organisatorische Trennung zwischen Entwicklung, Projektförderung, Betrieb, Prüfung und Freigabe wird als vorrangiges Querschnittsrisiko bewertet. Externe Prüfungen bestehen; der frei zugängliche, staatsunabhängige Auditweg für jedermann fehlt im dokumentierten Konzept. Empfohlen werden ein vorläufiger Verzicht auf weitere Ausweitung, verbindliche Freigabebedingungen für jeden verbleibenden Einsatz, eine von der Entwicklungsberatung getrennte Schlussprüfung und ein ergebnisoffener Vergleich zwischen Sanierung, Ersatz und geordnetem Verzicht. Die Vorschläge enthalten Zuständigkeiten, überprüfbare Ergebnisse, Abbruchkriterien und einen gestuften Umsetzungsplan.

* Kontakt: beat-w-meier.ch/kontakt · © 2026 Beat W. Meier. Alle Rechte vorbehalten.

Inhaltsverzeichnis

1 Entscheidungsvorlage ... 3
Welche Entscheidungen jetzt erforderlich sind.

2 Auftrag und wissenschaftliche Sorgfalt ... 4
Was die Quellen belegen und wo die Untersuchung endet.

3 Stand des Projekts und historische Lehren ... 6
Versuchsbetrieb, frühere Mängel und neue Entwicklungslinie.

4 Gewaltentrennung und unabhängige Kontrolle ... 8
Rollen, Interessenkonflikte und institutionelle Korrekturen.

5 Technische Risiken, Funktionslücken und Aussagekraft der Prüfungen ... 12
Produktionsstände, Funktionslücken und Must-have-Vergleich mit dem heutigen System.

6 Betrieb und Auszählbarkeit ... 26
Was Basel-Stadt für das Gesamtsystem bedeutet.

7 Stimmgeheimnis und demokratische Wirksamkeit ... 27
Grenzen von E-ID, Prüfcodes und öffentlichen Beweisen.

8 Gesamtrisikoregister ... 30
Prioritäten, Verantwortliche und Freigabebelege.

9 Handlungsoptionen ... 31
Sanieren, ersetzen oder den elektronischen Kanal aufgeben.

10 Verbindliche Freigabebedingungen ... 33
Wann ein Versuch verantwortbar ist und wann er ausgesetzt werden muss.

11 Umsetzungsprogramm ... 35
Konkrete Schritte ab einem politischen Auftrag.

12 Ressourcen und Wirtschaftlichkeit ... 37
Welche Leistungen finanziert und verglichen werden müssen.

13 Beschlussvorschlag und Schlussfolgerung ... 38
Eine belastbare Entscheidung statt eines automatischen Weiterbaus.

14 Anhänge ... 39
Prüfaufträge, Begriffe, Evidenzgrenzen und Personen mit ihren belegten Funktionen.

15 Originalquellen ... 48
Nach Kapiteln und erster Verwendung geordnet.

Abbildungsverzeichnis

1 Heutige Rollen und Prüfaufträge ... 9
2 Zielmodell einer getrennten Schlussprüfung ... 12
3 Funktionslücken im vollständigen Abstimmungsweg ... 18
4 Blockchain-Nachweis und staatsunabhängige Ergebnisprüfung ... 24
5 Nachweise und Entscheidung über eine Freigabe ... 34
6 Projektführung, Gremien und benannte Verantwortliche ... 45
7 Entwicklung, Systembereitstellung und kantonaler Betrieb ... 46
8 Prüfstellen, bekannte Gutachter und behördlicher Entscheid ... 47

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

1 Entscheidungsvorlage

1.1 Das zentrale Urteil

Die kritischste Frage lautet nicht allein, ob die Post sichere Software schreiben kann. Entscheidend ist, ob eine vom Projekterfolg hinreichend unabhängige Instanz das Zusammenwirken von Software, Betriebsorganisation und realem Urnengang prüfen und einen Einsatz wirksam verhindern kann. In einem System mit einem einzigen eingesetzten Anbieter, hoch spezialisiertem Wissen und wiederkehrender Zusammenarbeit wird die Unabhängigkeit der Kontrolle selbst zu einer Sicherheitsvoraussetzung.

Die amtliche Projektorganisation vereint bei der Bundeskanzlei die operative und fachliche Projektleitung mit der Verantwortung für das Zulassungsverfahren. Die Post wirkt im Projektausschuss an der Überwachung des Massnahmenkatalogs mit. Gleichzeitig schreibt Art. 10 VEleS unabhängige Prüfstellen vor; die veröffentlichten Berichte zeigen, dass externe Fachleute tatsächlich prüfen und erhebliche Fragen offen benennen. Die Ausgangsthese dieser Studie ist deshalb präzise: **Die formale Rollentrennung besteht teilweise; ihre wirksame Absicherung gegen Selbstprüfung, Abhängigkeit und Projektdruck muss stärker nachgewiesen und institutionell verbessert werden.** Eine bewiesene Einflussnahme auf konkrete Prüfer oder eine pauschale Befangenheit aller Beteiligten wird damit nicht behauptet.[1,2,3]

Die Bundeskanzlei beurteilt in ihrer Risikobeurteilung 2026-4 die Mehrzahl der verbleibenden Risiken als für den begrenzten Versuchsbetrieb hinreichend gering. Diese offizielle Beurteilung ist ein relevanter Gegenbefund zu einem pauschalen Unsicherheitsurteil. Sie hebt aber selbst unter anderem die Wirksamkeit der Verifizierbarkeit, die Einhaltung der zugelassenen Systemversion, den Expertenmangel, politische Angriffe auf die Verfügbarkeit und neue Technologien als besonders zu beobachtende Risiken hervor. Die vorliegende Studie setzt eine eigene, strengere Priorität bei der institutionellen Kontrolle und der belegbaren Auszählbarkeit. Das ist eine begründete Bewertung, keine angeblich amtliche Gefahreneinstufung.[4]

1.2 Fünf Entscheidungen mit unmittelbarer Wirkung

Erstens: Ausweitung vorläufig an Nachweise binden. Zusätzliche kantonale Einsätze, grössere Elektorate und neue sicherheitsrelevante Integrationen sollen erst nach den Freigabebedingungen in Kapitel 10 erfolgen. Bereits erteilte Bewilligungen dürfen dabei nicht mit einem technischen Eignungsnachweis für jede neue Konfiguration verwechselt werden. Zuständige Behörden müssen die geeignete rechtliche Form eines solchen Vorbehalts bestimmen.

Zweitens: Entwicklung und Schlussabnahme personell trennen. Fachleute dürfen im Entwicklungsprozess beraten und Fehler früh erkennen. Die abschliessende Prüfung eines von ihnen wesentlich mitgestalteten Sicherheitsmechanismus soll jedoch eine andere fachlich qualifizierte Gruppe verantworten. Das gilt auch für die Unterscheidung zwischen operativen Wahlorganen, Schlüsselverantwortlichen und denjenigen, die deren Arbeit prüfen.

Drittens: Für jeden Urnengang ein geschlossenes Nachweispaket verlangen. Auditoren müssen Systemstände, Betrieb und Ergebnisse staatsunabhängig prüfen können. Jede definitiv angenommene Stimme braucht einen bestätigten Blockchain-Eintrag und den Abgleich mit Urne und Auszählung

[1] Q01 · Bundeskanzlei, Projektorganisation, Einleitung und Organe, Abruf 09.10.2026.
[2] Q02 · VEleS, SR 161.116, Stand 01.07.2022; jeweils im Text bezeichnete Artikel und Anhangsziffern.
[3] Q03 · Haines/Pereira, 24.08.2026, S. 1–2 und Anhang B.2.1, S. 22; Entwurf 2.0, Whitepaper 1.1/1.2.
[4] Q04 · Bundeskanzlei, Risikobeurteilung 2026-4, 29.09.2026, S. 2–12, 31 sowie die bezeichneten Einzelrisiken.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

(M15/M16). Fehlt ein kritischer Bestandteil, wird der betroffene Einsatz nicht freigegeben. Bereits geltende Anforderungen an Quellcodeoffenlegung und Produktionsnachweise bilden dafür die Grundlage.[5]

Viertens: System 2.0 als eigenen Zulassungsgegenstand behandeln. Ein neuer Protokollentwurf darf weder die Produktionsfreigabe der bisherigen Linie erben noch allein wegen früherer Schwachstellen verworfen werden. Die im September veröffentlichten Originalberichte und die anschliessende Herstellerkorrektur sind einzeln nachzuverfolgen. Die Korrekturbehauptung eines Herstellers ersetzt keine unabhängige Prüfung.[6,7]

Fünftens: Einen echten Ausstieg offenhalten. Parallel zur Sanierung ist ein begrenzter, unabhängiger Vergleich mit einem Ersatzsystem und mit dem Verzicht auf Remote-E-Voting zu beauftragen. Ein Neubau ist nur dann sinnvoll, wenn er nachweislich Vertrauensannahmen oder Komplexität reduziert. Der Verzicht muss die Bedürfnisse von Auslandschweizerinnen und Auslandschweizern sowie Menschen mit Behinderungen durch konkrete Alternativen berücksichtigen.

1.3 Was daraus nicht folgt

Die öffentlich geprüften Quellen belegen keinen erfolgreichen Angriff, mit dem reale Schweizer Abstimmungsresultate durch das aktuelle Post-System verfälscht wurden. Sie belegen erhebliche historische Fehler, einen realen betrieblichen Verlust der Auszählbarkeit und schwere Befunde an einem neuen Protokollentwurf. Diese Kategorien dürfen nicht vermischt werden. Ebenso wäre es unzulässig, aus nicht entdeckten Angriffen eine Garantie der Fehlerfreiheit abzuleiten.[8,9,10,11]

Ein landesweiter sofortiger Abbruch allein wegen eines noch nicht bestätigten privaten Hinweises wäre mit der hier ausgewerteten Evidenz nicht ausreichend begründet. Für eine konkret betroffene Konfiguration kann eine sofortige Aussetzung dagegen geboten sein, wenn ein plausibler kritischer Fehler nicht rechtzeitig widerlegt oder wirksam abgesichert werden kann. Die Entscheidung muss am Schutz der politischen Rechte ausgerichtet sein und darf nicht von bereits investierten Mitteln abhängen.

2 Auftrag und wissenschaftliche Sorgfalt

2.1 Gegenstand und Betrachtungsebene

Untersucht wird das Schweizer Projekt Vote électronique zum Stichtag 9. Oktober 2026. Der Begriff Gesamtsystem umfasst hier den Weg vom Stimmregister über Erstellung und Versand der Unterlagen, Authentisierung und Stimmabgabe bis zur Aufbewahrung, Auszählung, Prüfung, Beschwerde und geregelten Datenvernichtung. Wenn eine amtliche Mitteilung mit «System der Post» einen engeren Produktumfang meint, wird dieser Unterschied ausdrücklich berücksichtigt.

Die Untersuchung ist eine quellenkritische Risiko- und Governance-Studie. Sie ist kein neuer kryptografischer Sicherheitsbeweis, kein Penetrationstest und keine Vor-Ort-Prüfung kantonaler Abläufe. Die tatsächlichen Vertragsbedingungen, internen Ausstandsentscheidungen, vollständigen Prüfakten und

[5] Q02 · VEleS, SR 161.116, Stand 01.07.2022; jeweils im Text bezeichnete Artikel und Anhangsziffern.
[6] Q05 · Essex, 13.09.2026, Management Summary S. i, Kap. 3–6 und S. 25; Whitepaper 1.2.
[7] Q06 · Post/LORIA, Whitepaper 1.2.1, S. 2, 11–12 und Anhang A.1.3; Änderungsverzeichnis, Commit 6d427c8d6d65, 22.09.2026.
[8] Q05 · Essex, 13.09.2026, Management Summary S. i, Kap. 3–6 und S. 25; Whitepaper 1.2.
[9] Q07 · Bundeskanzlei, Originalmitteilung vom 12.03.2019, Mangel der universellen Verifizierbarkeit.
[10] Q08 · Bundeskanzlei, Originalmitteilung vom 29.03.2019, individuelle Verifizierbarkeit und Standortbestimmung.
[11] Q09 · Regierungsrat Basel-Stadt, Originalmitteilung vom 10.03.2026, Vorfall und Aussetzung.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

produktiven Systemkonfigurationen lagen nicht zur eigenständigen Kontrolle vor. Fehlende öffentliche Belege werden deshalb als Nachweislücke bezeichnet, nicht als Beweis eines Verstosses.

2.2 Ausschliesslich Originalquellen

Als Tatsachengrundlage dienen die geltende VEleS in Fedlex, Originalveröffentlichungen der verantwortlichen Behörden, Berichte der tatsächlich beauftragten Prüfer sowie Originaldokumente der Post. Presseartikel, politische Sekundärdarstellungen und frühere Zusammenfassungen werden nicht als Belege verwendet. Die lokalen Vorarbeiten bestimmen die zu untersuchenden Fragen; belegende Aussagen werden auf ihre Originalquellen zurückgeführt.

Eine Originalquelle ist nicht automatisch unabhängig. Die Bundeskanzlei beschreibt und beurteilt das von ihr koordinierte Projekt; die Post beschreibt ihr eigenes Produkt. Ein Prüfbericht dokumentiert die Untersuchung seines Autors, aber nicht notwendigerweise eine wissenschaftliche Begutachtung durch ein Journal. Die Studie bezeichnet diese Dokumente entsprechend als Behördenbeurteilung, Herstellerangabe oder fachlichen Prüfbericht. Für eine technische Aussage sind untersuchte Version, Bedrohungsmodell, Prüfumfang und Einschränkungen entscheidend.

Bei dynamischen Webseiten gilt der Abrufstand. Bei Berichten gelten deren ausdrücklich bezeichnete Versionen. Für das Whitepaper 1.2.1 und dessen Änderungsverzeichnis wird zusätzlich der Repository-Commit 6d427c8d6d65861af3a330568834997a9758fc8a vom 22. September 2026 verwendet. Damit wird vermieden, dass eine spätere Änderung unter derselben Webadresse die Beleggrundlage unbemerkt verschiebt.[12]

2.3 Vier Evidenzkategorien

Kategorie	Bedeutung	Zulässige Schlussfolgerung
Dokumentierter Vorgang	Amtlich berichtetes Ereignis, Norm oder dokumentierte Rollenverteilung	Der bezeichnete Vorgang ist belegt; Ursachenreichweite bleibt quellengebunden.
Technischer Befund	Originalbericht mit Version, Annahmen und Analyse	Die Aussage gilt für den geprüften Gegenstand und die genannten Voraussetzungen.
Herstellerkorrektur	Nachweis einer Änderung und Erklärung ihres Zwecks	Es liegt eine Korrektur vor; deren Vollständigkeit braucht einen eigenen Nachweis.
Eigene Bewertung oder Empfehlung	Schlussfolgerung aus den Belegen oder vorgeschlagene Sicherheitsanforderung	Keine zusätzliche beobachtete Tatsache und keine bereits geltende amtliche Pflicht.

Die Prioritäten im Risikoregister sind qualitative Handlungsprioritäten. Sie sind keine berechneten Eintrittswahrscheinlichkeiten. Es fehlen belastbare Häufigkeitsdaten für seltene, gezielte Angriffe und für institutionelles Versagen. Auch die Zahlen der Bundeskanzlei für Schadensauswirkungen dürfen nicht als Prozentwerte oder als einfache Produkte von Wahrscheinlichkeit und Schaden gelesen werden; ihre Methodik unterscheidet diese Grössen.[13]

2.4 Umgang mit offenen privaten Meldungen

In den Vorarbeiten wird eine private Sicherheitsmeldung zum Import authentisiert verschlüsselter Daten beschrieben. Die Originalmeldung mit vollständigen Anhängen, versionsgenauem Reproduktionsmaterial und abschliessender fachlicher Stellungnahme liegt in der ausgewerteten Belegbasis nicht vor. Die darin

[12] Q06 · Post/LORIA, Whitepaper 1.2.1, S. 2, 11–12 und Anhang A.1.3; Änderungsverzeichnis, Commit 6d427c8d6d65, 22.09.2026.

[13] Q04 · Bundeskanzlei, Risikobeurteilung 2026-4, 29.09.2026, S. 2–12, 31 sowie die bezeichneten Einzelrisiken.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

beschriebene Hypothese wird deshalb nicht als nachgewiesene Schwachstelle des Produktivsystems, nicht als bestätigter Schweregrad und nicht als erfolgreicher Hack verwendet.

Ein fachgerechter Prüfauftrag bleibt möglich: Originalunterlagen sichern, Komponenten und Bibliotheksstände bestimmen, die Hypothese in einer isolierten Umgebung nachstellen und feststellen, ob eine verletzte lokale Integritätsprüfung durch nachgelagerte Signaturen oder andere Kontrollen wirksam aufgefangen wird. Ein Fehler in einem Teilprozess und die Verfälschung eines gültigen Abstimmungsergebnisses sind unterschiedliche Aussagen. Erst das vollständige Originalmaterial erlaubt eine belastbare Zuordnung. Diese Evidenzgrenze schützt sowohl die meldende Person als auch die sachliche Bewertung des Systems.

3 Stand des Projekts und historische Lehren

3.1 Sechs Grundbewilligungen bedeuten nicht sechs aktive Kantone

Die Bundeskanzlei nennt zum Stichtag Luzern, Basel-Stadt, St.Gallen, Graubünden, Thurgau und Neuenburg als Kantone mit Grundbewilligungen. Alle verwenden das vollständig verifizierbare System der Post. Basel-Stadt hat seinen Versuchsbetrieb nach dem Vorfall vom März bis Ende 2026 ausgesetzt. Eine Grundbewilligung ist deshalb von einer Zulassung und vom tatsächlichen Einsatz an einem bestimmten Urnengang zu unterscheiden.[14,15]

Die amtliche Tabelle vom 29. September 2026 führt für den 29. November Luzern, St.Gallen, Graubünden, Thurgau und Neuenburg auf. Sie weist indikativ rund 221'293 potenziell einbezogene Stimmberechtigte aus. Diese Zahl enthält kantonale Obergrenzen und ist weder eine Zahl abgegebener Stimmen noch die Zahl bereits versandter Stimmrechtsausweise. Für den 27. September weist die Tabelle 39'357 tatsächlich mit E-Voting-Material bediente Inlandschweizer Stimmberechtigte innerhalb der Limite aus; die Auslandschweizer sind eine gesonderte Kategorie. Ein Vergleich dieser unterschiedlichen Bezugsgrössen wäre irreführend.[16]

Die gesetzlichen Versuchslimiten betragen gemäss dieser amtlichen Darstellung 30 Prozent des kantonalen und 10 Prozent des gesamtschweizerischen Inlandelektorats; Auslandschweizer Stimmberechtigte und Stimmberechtigte mit einer Behinderung werden bei der Berechnung dieser Limiten nicht mitgezählt. Begrenzung mindert die maximale Exposition, garantiert aber nicht, dass ein Fehler in einer knappen Gemeinde- oder Kantonsabstimmung folgenlos bleibt.[17]

3.2 Die historische Lehre von 2019

Am 12. März 2019 berichtete die Bundeskanzlei über einen erheblichen Fehler in der universellen Verifizierbarkeit des damals neuen Post-Systems. Forschende hatten ihn durch Analyse von Dokumentation und Quellcode gefunden. Der Mangel erlaubte selbst kein Eindringen, untergrub aber die Aussagekraft der mathematischen Nachweise für Manipulationsfreiheit. Das damals bereits eingesetzte, nur individuell verifizierbare System war von genau diesem Befund nicht betroffen.[18]

[14] Q10 · Bundeskanzlei, Vote électronique, Projektziele und Aktueller Stand, Abruf 09.10.2026.
[15] Q09 · Regierungsrat Basel-Stadt, Originalmitteilung vom 10.03.2026, Vorfall und Aussetzung.
[16] Q11 · Bundeskanzlei, Versuchsbedingungen vom 29.09.2026, Tabellenblätter 29.11.2026 und 27.09.2026 samt Fussnoten.
[17] Q11 · Bundeskanzlei, Versuchsbedingungen vom 29.09.2026, Tabellenblätter 29.11.2026 und 27.09.2026 samt Fussnoten.
[18] Q07 · Bundeskanzlei, Originalmitteilung vom 12.03.2019, Mangel der universellen Verifizierbarkeit.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

Am 29. März folgte die Mitteilung über einen weiteren Mangel bei der individuellen Verifizierbarkeit. Die Post stellte ihr System für den Urnengang vom 19. Mai 2019 nicht bereit. Die Bundeskanzlei erklärte ausdrücklich, keine Hinweise auf eine dadurch verursachte Stimmenverfälschung bei früheren Abstimmungen zu haben. Die Frage «Wurde die Software gehackt?» verlangt deshalb eine differenzierte Antwort: Schwerwiegende Sicherheitsmängel wurden nachgewiesen; eine erfolgreiche Manipulation realer Schweizer Resultate ist damit nicht belegt.[19]

Die institutionelle Lehre ist erheblich. Formale Prüfungen und Zertifikate hatten nicht verhindert, dass externe Quellcodeanalyse fundamentale Fehler aufdeckte. Daraus folgt kein Verzicht auf Audits. Es folgt die Notwendigkeit verschiedener, tatsächlich unabhängiger Erkenntniswege und eines Verfahrens, in dem externe Gegenbeweise stärker wiegen als bestehende Freigaben.

3.3 BFH und die Gefahr falscher Zuschreibungen

Die BFH beschreibt ihre Forschung zu E-Voting seit 2009 und ihre frühere Beteiligung an der Entwicklung eines Systems gemeinsam mit dem Kanton Genf. Für das Post-System dokumentiert sie Prüfaufträge der Bundeskanzlei. Aus der Entwicklungserfahrung an einem anderen System darf nicht geschlossen werden, die BFH sei deshalb Herstellerin des heutigen Post-Systems oder prüfe zwangsläufig ihre eigene Implementierung.[20]

Eine reale Überschneidung entsteht dort, wo Fachleute im laufenden Entwurfsprozess konkrete Konstruktionsvorschläge machen und diese später erneut beurteilen. Die 2026 veröffentlichten Gutachten zu System 2.0 enthalten solche Vorschläge und Rückmeldungen. Das erhöht die Qualität früher Fehlererkennung, verlangt aber Transparenz darüber, wer welche Lösung mitgestaltet und wer danach die unabhängige Schlussprüfung übernimmt.[21,22,23]

3.4 Zwei Entwicklungslinien mit unterschiedlichen Nachweisen

Die produktnahe Prüfung von Release 1.5.4 im Juni 2026, der Intrusionstest von 1.5.4.2 im Juli und die Prüfung des Whitepapers für System 2.0 sind verschiedene Prüfgegenstände. Ein günstiges Urteil über den ersten Gegenstand deckt den zweiten nicht automatisch ab. Ebenso lässt sich ein Entwurfsfehler von System 2.0 nicht ohne technische Herleitung auf einen produktiven Stand der bisherigen Linie übertragen.[24,25,26]

Die aktuelle Lage ist daher weder ein technisch unveränderter Fortbestand von 2019 noch bereits ein bewiesener sicherer Endzustand. Sie ist ein kontrollierter Versuchsbetrieb mit laufender Weiterentwicklung und erheblichen Anforderungen an das Änderungsmanagement. Wer diese Dynamik durch das Wort «zertifiziert» oder «gehackt» verkürzt, verliert die entscheidenden Versions- und Prozessgrenzen.

[19] Q08 · Bundeskanzlei, Originalmitteilung vom 29.03.2019, individuelle Verifizierbarkeit und Standortbestimmung.
[20] Q12 · BFH, BFH-Forschende untersuchen E-Voting-System der Post, 02.06.2022.
[21] Q03 · Haines/Pereira, 24.08.2026, S. 1–2 und Anhang B.2.1, S. 22; Entwurf 2.0, Whitepaper 1.1/1.2.
[22] Q13 · Haenni/Koenig/Locher, Review White Paper 2.0, 14.08.2026, S. 15–16 und 20–23.
[23] Q14 · Müller, Review White Paper 2.0, 23.08.2026, S. 4–7.
[24] Q15 · Haines, Prüfbericht zu Release 1.5.4, 16.06.2026, S. 1–5.
[25] Q16 · Müller, Prüfbericht zu Release 1.5.4, 15.06.2026, S. 1–2.
[26] Q17 · Orange Cyberdefense, P023254, 27.08.2026, S. 4–6 und 10–15; Release 1.5.4.2.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

4 Gewaltentrennung und unabhängige Kontrolle

4.1 Warum dieses Risiko an erster Stelle steht

Mit Gewaltentrennung ist hier die funktionale Trennung von Aufgaben und Entscheidungsmacht gemeint, nicht die Behauptung eines unmittelbar nachgewiesenen Verstosses gegen die verfassungsrechtliche Gewaltenteilung. Entwicklung, Projektauftrag, Betrieb, fachliche Prüfung und öffentlich verantwortete Zulassung verfolgen unterschiedliche Ziele. Werden diese Ziele personell oder organisatorisch vermischt, können Sicherheitsnachweise ihre korrigierende Wirkung verlieren.

Das Risiko wirkt auf alle anderen Risiken: Eine Kontrollstruktur kann eine Schwachstelle erkennen, ihre Bedeutung aber herunterstufen; sie kann notwendige Betriebsmassnahmen erkennen, deren Umsetzung jedoch aus Termindruck als ausreichend behandeln. Solche Fehlentscheidungen benötigen keine böse Absicht. Gemeinsame Annahmen, langjährige Zusammenarbeit, knappe Expertise und die Bindung an einen Projektplan können genügen. Ob sie im Einzelfall tatsächlich wirksam wurden, muss anhand von Entscheidungsakten geprüft werden.

4.2 Die belegte Rollenverteilung

Rolle	Dokumentierter Träger	Sicherheitsrelevante Abgrenzung
Nationaler Projektauftrag	Bundesrat; Umsetzung an Bundeskanzlei übertragen	Politischer Auftrag ist keine technische Abnahme.
Projektleitung und Koordination	Team Vote électronique der Bundeskanzlei	Projektfortschritt und Zulassungsverantwortung liegen institutionell nahe beieinander.
Strategische Beratung	Steuerungsausschuss mit Bund und sechs kantonalen Sitzen	Die Post ist in der veröffentlichten Mitgliederbeschreibung dieses Gremiums nicht aufgeführt.
Massnahmenumsetzung	Projektausschuss mit Bundeskanzlei, Kantonen und Post	Fachliche Mitwirkung des Anbieters muss von Entscheidungen über seine eigene Konformität getrennt werden.
Entwicklung und Systemangebot	Schweizerische Post	Eigene Tests und Herstellerantworten sind notwendig, aber keine unabhängige Schlussabnahme.
Externe Systemprüfung	Unabhängige Stellen im Auftrag der Bundeskanzlei	Auftraggeber ist gemäss VEleS die Bundeskanzlei, nicht die Post.
Prüfung des konkreten Urnengangs	Vom Kanton beauftragte Prüferinnen und Prüfer	Von Entwicklungsaudit, Schlüsselbedienung und Betriebsleitung unterscheiden.

Die ersten vier Zeilen beruhen auf der amtlichen Projektorganisation, die Prüfrollen auf Art. 2, 5 und 10 VEleS. Daraus lässt sich eine reale Mehrfachrolle der Bundeskanzlei ableiten. Nicht ableiten lässt sich, dass die Post allein ihre eigenen Auditoren auswählt, bezahlt oder deren Berichte genehmigt. Für solche weitergehenden Aussagen wären Originalverträge oder andere direkte Nachweise erforderlich.[27,28]

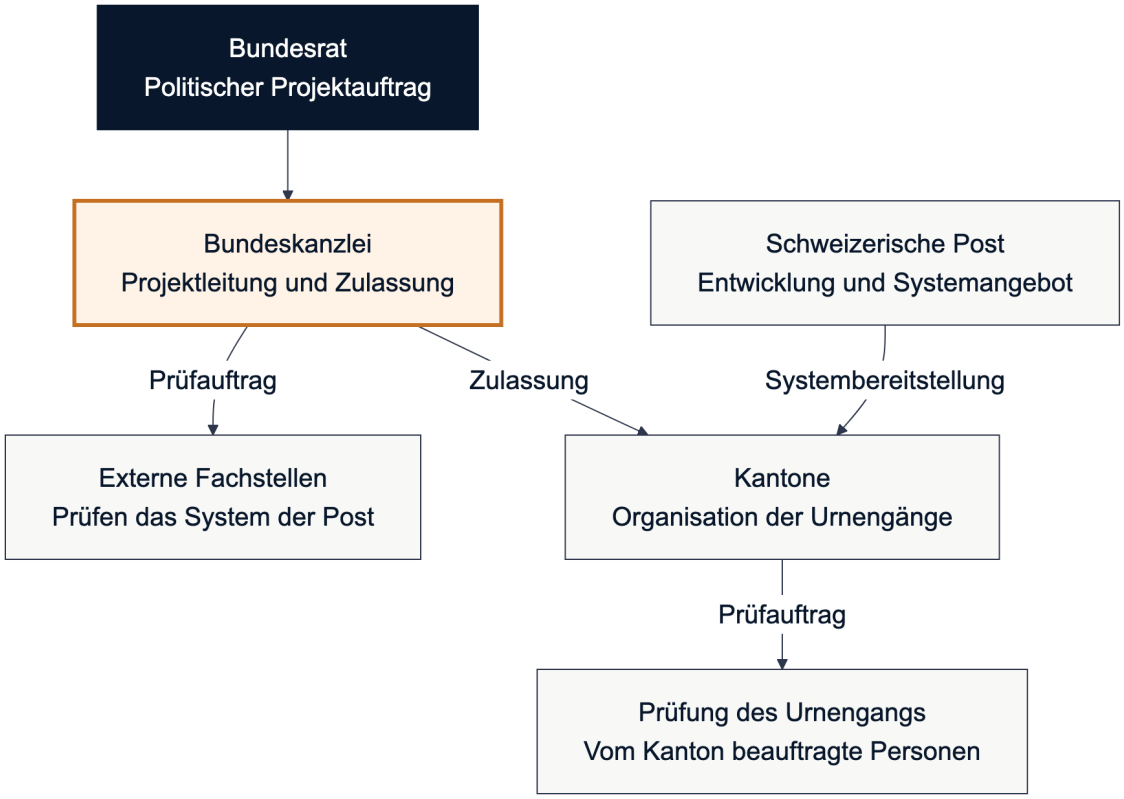
[27] Q01 · Bundeskanzlei, Projektorganisation, Einleitung und Organe, Abruf 09.10.2026.

[28] Q02 · VEleS, SR 161.116, Stand 01.07.2022; jeweils im Text bezeichnete Artikel und Anhangsziffern.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

Abbildung 1 · Heutige Rollen und Prüfaufträge



Eigene Darstellung nach amtlicher Projektorganisation und VEleS. Pfeile zeigen funktionale Beziehungen; Grundbewilligung und beratende Gremien sind ausgelassen (vgl. Kapitel 4.2). Orange markiert die Nähe von Projektleitung und Zulassung, keinen nachgewiesenen Regelverstoss.[29,30]

4.3 Beratung während der Entwicklung und spätere Selbstprüfung

Die Bundeskanzlei erklärt zur Massnahme A.5 ausdrücklich, ihre Fachleute von Beginn an durch regelmässige Whitepaper-Prüfungen in den Entwicklungsprozess eingebunden zu haben. Die Originalberichte dokumentieren sowohl Kritik als auch konkrete Alternativkonstruktionen. Ein solcher Dialog ist fachlich sinnvoll: Ein Fehler im Entwurf lässt sich früher und günstiger beheben als ein Fehler im produktiven Betrieb.[31,32]

Die Grenze liegt bei der abschliessenden Aussage, eine Lösung erfülle alle massgeblichen Anforderungen. Wer eine zentrale Konstruktion wesentlich vorgeschlagen oder entworfen hat, sollte nicht allein die letzte Wirksamkeitsprüfung genau dieser Konstruktion verantworten. Die Aufgabe darf auch nicht bloss einer anderen Person desselben kleinen, gemeinsam arbeitenden Teams übertragen werden, wenn die wesentlichen Annahmen und wirtschaftlichen Abhängigkeiten unverändert bleiben.

Daraus folgt keine pauschale Disqualifikation der BFH oder anderer Forschergruppen. Ein begründetes Ausstandsmodell muss auf konkrete Beiträge und Prüfobjekte bezogen sein. Es muss unterscheiden zwischen Fehlerhinweis, allgemeiner Empfehlung, substanzieller Mitgestaltung und eigener Implementierung. Der Umfang der Mitwirkung entscheidet über den Umfang des nötigen Ausstands.

[29] Q01 · Bundeskanzlei, Projektorganisation, Einleitung und Organe, Abruf 09.10.2026.
[30] Q02 · VEleS, SR 161.116, Stand 01.07.2022; jeweils im Text bezeichnete Artikel und Anhangsziffern.
[31] Q18 · Bundeskanzlei, Massnahmenkatalog, Arbeiten zu A.5, Abruf 09.10.2026.
[32] Q14 · Müller, Review White Paper 2.0, 23.08.2026, S. 4–7.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

4.4 Operative Selbstprüfung ist ein eigenständiges Problem

Haines und Pereira fragen im Anhang B.2.1 ihres Berichts, bezogen auf Whitepaper 1.1, ausdrücklich nach der Rollenvereinbarkeit von Personen, die kritische Schlüsselanteile erzeugen beziehungsweise verwenden und gleichzeitig als Auditoren dieser Vorgänge auftreten. Diese Frage betrifft den Entwurf und dessen Rollenmodell; sie ist kein Nachweis, dass alle Kantone im heutigen Betrieb dieselben Personen unzulässig einsetzen. Das Änderungsverzeichnis zu Whitepaper 1.2 hält bereits fest, dass die Mitwirkung der Wählervertretung bei der Schlüsselerzeugung auf Protokollebene nicht erforderlich sei. Die frühere Kritik darf deshalb nicht unverändert als belegter aktueller Fehler wiederholt werden. Sie zeigt aber, dass organisatorische Unabhängigkeit bereits im technischen Protokoll sauber abgebildet werden muss.[33,34]

Ein Vieraugenprinzip genügt nicht, wenn beide Personen unter derselben operativen Weisung stehen, gemeinsam denselben Fehler vorbereiten und anschliessend ihr eigenes Protokoll freigeben. Für kritische Handlungen braucht es sowohl gegenseitige Kontrolle während der Ausführung als auch eine davon getrennte Ergebnisprüfung. Die technischen Hilfsmittel dieser Ergebnisprüfung müssen gemäss Art. 5 VEleS vom Rest des Systems unabhängig und isoliert sein.[35]

4.5 Sechs verbindliche Trennungsregeln

Unabhängiger Prüfauftrag. Der Auditumfang wird von einer fachlich befähigten Stelle ausserhalb der operativen Projektleitung vorgeschlagen und verbindlich festgelegt. Die Post und kantonale Betreiber liefern Informationen, erhalten aber kein Vetorecht gegen zulässige Prüffragen, gegen kritische Befunde oder gegen die Schlussfolgerung der Prüfenden.

Eigenes Budget und direkte Berichtswege. Die Schlussprüfung erhält ein gesondertes, mehrjährig planbares Budget. Ihre Leitung berichtet direkt an die zuständige Freigabeinstanz und eine geeignete Aufsicht. Die Verlängerung eines Mandats darf nicht von einem günstigen Prüfergebnis abhängen. Gesetzliche Zuständigkeiten bleiben bestehen; eine weitergehende Übertragung von Entscheidungsmacht bedarf der entsprechenden Rechtsgrundlage.

Offenes Interessenregister. Prüfende deklarieren einschlägige Entwicklungs-, Beratungs-, Forschungs- und Finanzierungsbeziehungen. Vorgeschlagen wird ein Rückblick von fünf Jahren, bei eigener Urheberschaft am Prüfobjekt auch darüber hinaus. Diese Frist ist eine Empfehlung dieser Studie. Öffentlich werden die wesentlichen Beziehungen und Ausstandsentscheide, nicht schützenswerte persönliche Vertragsdetails.

Getrennte Schlussprüfung. Für sicherheitsentscheidende Eigenbeiträge gilt ein dokumentierter Ausstand bei der abschliessenden Bewertung. Mindestens eine fachlich unabhängige Gruppe reproduziert die tragenden Gegenbeispiele und die Wirksamkeit der Korrekturen. Eine zweite Unterschrift ohne eigene Prüfarbeit zählt nicht als unabhängige Bestätigung.

Entscheidungshoheit ausserhalb des Lieferantenkreises. Anbieter und operative Projektführung werden angehört. Über die Akzeptanz ihrer eigenen Risiken entscheiden sie nicht allein. Die zuständige Behörde begründet, welche Restunsicherheit sie für welchen Einsatz akzeptiert. Abweichende Fachmeinungen werden dokumentiert und der Aufsicht zugänglich gemacht.

[33] Q03 · Haines/Pereira, 24.08.2026, S. 1–2 und Anhang B.2.1, S. 22; Entwurf 2.0, Whitepaper 1.1/1.2.

[34] Q06 · Post/LORIA, Whitepaper 1.2.1, S. 2, 11–12 und Anhang A.1.3; Änderungsverzeichnis, Commit 6d427c8d6d65, 22.09.2026.

[35] Q02 · VEleS, SR 161.116, Stand 01.07.2022; jeweils im Text bezeichnete Artikel und Anhangsziffern.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

Keine operative Personalunion. Wer kritische Schlüssel erzeugt oder verwendet, Produktionsfreigaben ausführt oder Stimmunterlagen verarbeitet, darf nicht zugleich allein die unabhängige Prüfung derselben Handlung durchführen. Auch gemeinsame Administrationskonten, gemeinsame Wiederherstellungszugänge und Weisungsketten sind auf solche Umgehungen zu untersuchen.

4.6 Ein durchsetzbares Zielmodell

Kurzfristig lässt sich eine organisatorisch getrennte Freigabeprüfung innerhalb der bestehenden Zuständigkeiten mit dokumentierten Berichtswegen, Ausständen und getrennten Budgets etablieren. Mittelfristig ist zu prüfen, ob eine dauerhafte fachliche Zulassungsfunktion institutionell weiter von der operativen Projektförderung getrennt werden soll. Eine neue Behörde ist dafür nicht automatisch erforderlich; eine neue Bezeichnung ohne eigene Ressourcen und Widerspruchsmöglichkeit wäre wirkungslos.

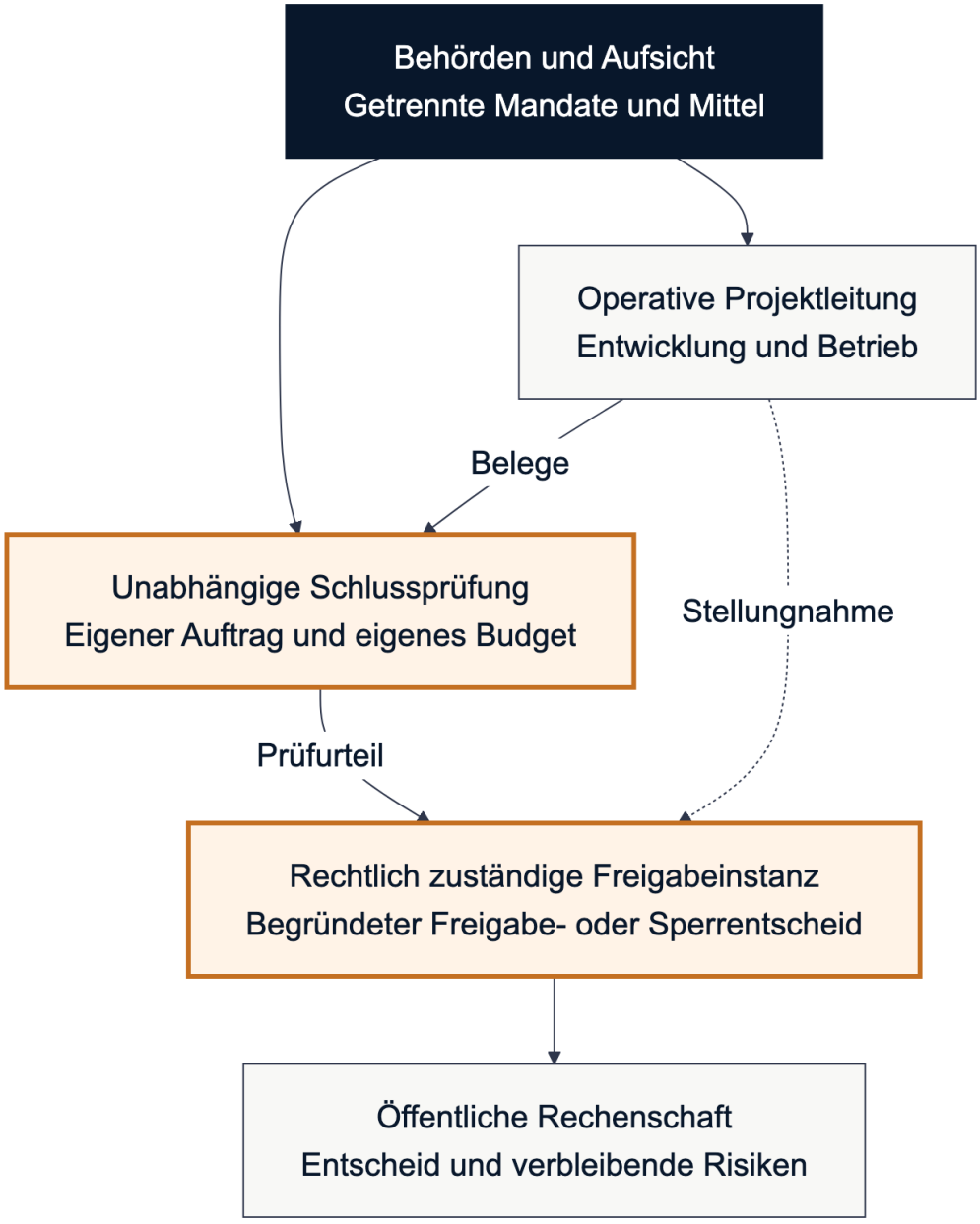
Die politische Verantwortung bleibt beim zuständigen Gemeinwesen. Fachprüfer sollen ein begründetes negatives Urteil abgeben können, ohne selbst zum demokratisch nicht legitimierten Entscheidungsträger zu werden. Ein negatives kritisches Prüfergebnis löst nach dem hier vorgeschlagenen Verfahren eine Freigabesperre aus. Eine politisch gewünschte Abweichung muss sich innerhalb des geltenden Rechts bewegen und öffentlich begründet werden; eine fehlende gesetzliche Sicherheitsvoraussetzung kann nicht durch Mehrheitsentscheid ersetzt werden.

Das erste überprüfbare Ergebnis dieser Reform ist eine Rollen- und Konfliktmatrix für alle aktuellen Mandate. Das zweite ist ein vollständig dokumentierter Freigabeentscheid, an dem erkennbar wird, dass eine unabhängige Stelle einen Einsatz tatsächlich hätte verhindern können. Organigramme allein reichen nicht.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

Abbildung 2 · Zielmodell einer getrennten Schlussprüfung



Vorschlag dieser Studie, abgeleitet aus Kapitel 4.5–4.6. Unabhängige Prüfmandate, eigene Mittel und direkte Berichtswege sollen eine wirksame Schlussprüfung ermöglichen. Die rechtlich zuständigen Behörden behalten die Freigabeverantwortung. Die Darstellung setzt weder eine bereits bestehende neue Behörde noch eine ungeprüfte Verlagerung gesetzlicher Kompetenzen voraus.

5 Technische Risiken, Funktionslücken und Aussagekraft der Prüfungen

5.1 Verifizierbarkeit ist ein bedingter Sicherheitsnachweis

Art. 5 VEleS verlangt, dass Manipulationen, die das Ergebnis verfälschen, unter Wahrung des Stimmgeheimnisses erkannt werden können. Individuelle Verifizierbarkeit betrifft die korrekte Registrierung aus Sicht der stimmenden Person. Universelle Verifizierbarkeit betrifft die korrekte Ergebnisermittlung aus den systemkonform registrierten Stimmen. Die Stichhaltigkeit hängt unter anderem vom

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

vertrauenswürdigen Systemteil, von Generierung und Druck der Unterlagen sowie von den technischen Hilfsmitteln der Prüfer ab.[36]

Das bedeutet: Ein gültiger Beweis bestätigt eine Aussage unter bestimmten Annahmen. Er bestätigt nicht automatisch, dass die Person frei von Druck abgestimmt hat, dass alle Stimmberechtigten teilnehmen konnten oder dass verlorene Schlüssel wiederherstellbar sind. Die vollständige Verifizierbarkeit ist unverzichtbar, aber kein Sammelnachweis für alle demokratischen Eigenschaften.

Für jede Sicherheitsbehauptung ist deshalb eine Kette zu dokumentieren: gesetzliches Schutzziel, Protokollannahme, Spezifikation, implementierte Funktion, eingesetzte Version, betriebliche Voraussetzung und überprüfbares Ergebnis. Ein Bruch zwischen zwei Gliedern lässt sich nicht durch einen guten Nachweis an einer anderen Stelle ausgleichen.

5.2 Was die produktnahen Prüfungen 2026 tatsächlich zeigen

Thomas Haines beurteilt die Änderungen an Release 1.5.4 im Juni 2026 grundsätzlich positiv, kritisiert aber, dass ein einfacher Fehler im Miller-Rabin-Primzahltest fast zwei Jahre unentdeckt blieb. Zugleich hält er die konkrete Fehlerausnutzung in den produktiven Aufrufpfaden für nicht praktikabel, weil die geprüften Kandidaten dort aus dem vorgesehenen deterministischen Verfahren stammen. Johannes Müller beurteilt das praktische Risiko im aktuellen Bedrohungsmodell ebenfalls als vernachlässigbar und beschreibt die Korrektur.[37,38]

Die berechtigte Kritik richtet sich damit vor allem auf die Fehlerentdeckung und die vollständige Prüfung grundlegender Hilfsfunktionen. Es wäre falsch, aus diesem Befund eine bewiesene Möglichkeit zur Manipulation beliebiger realer Stimmen abzuleiten. Ebenso falsch wäre es, ihn wegen der begrenzten Ausnutzbarkeit als bedeutungslos abzutun: Ein einfacher, lange übersehener Fehler gibt Anlass, die Prüfabdeckung und die Ursachen seiner Nichtentdeckung zu untersuchen.

Orange Cyberdefense prüfte im Juli Release 1.5.4.2 mit Quellcodezugang und Testumgebungen. Der Bericht vom 27. August nennt keine relevanten entdeckten Risiken und beurteilt den untersuchten Gegenstand insgesamt als niedriges Risiko. Er dokumentiert aber ausdrücklich 15 Tage Prüfaufwand und schliesst Social Engineering sowie Denial-of-Service-Angriffe aus. Diese Grenzen gehören neben das positive Ergebnis.[39]

Die zwei informatorischen Feststellungen betreffen eine Konfiguration des simulierten eGovernment-Servers und die unzureichende Authentizitätsprüfung beim lokalen Aufbau einer Entwicklungsumgebung. Der Bericht ordnet daraus keine direkte Gefährdung eines Urnengangs ab. Sie sind dennoch nützliche Hinweise auf Schnittstellen und Lieferketten. Ein Fehler im Test-Mock darf nicht als nachgewiesene Schwachstelle eines produktiven kantonalen Behördenportals dargestellt werden.[40]

5.3 Offene Punkte sind versionsgebunden zu verfolgen

Der BFH-Bericht vom 9. Januar 2026 beschreibt die Prüfung mehrerer Releases des Jahres 2025 und enthält weiterhin als geplant oder geklärt geführte Punkte. Der Status «geklärt» bedeutet in dieser Darstellung nicht

[36] Q02 · VEleS, SR 161.116, Stand 01.07.2022; jeweils im Text bezeichnete Artikel und Anhangsziffern.
[37] Q15 · Haines, Prüfbericht zu Release 1.5.4, 16.06.2026, S. 1–5.
[38] Q16 · Müller, Prüfbericht zu Release 1.5.4, 15.06.2026, S. 1–2.
[39] Q17 · Orange Cyberdefense, P023254, 27.08.2026, S. 4–6 und 10–15; Release 1.5.4.2.
[40] Q17 · Orange Cyberdefense, P023254, 27.08.2026, S. 4–6 und 10–15; Release 1.5.4.2.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

automatisch «implementiert und unabhängig wirksam nachgeprüft». Die Veröffentlichung belegt den damaligen Arbeitsstand; sie beweist nicht, dass jeder dieser Punkte am 9. Oktober unverändert offen ist.[41]

Für die Steuerung braucht es eine gemeinsame Befundhistorie mit mindestens folgenden Zuständen: gemeldet, technisch eingeordnet, Korrektur vorgeschlagen, implementiert, unabhängig reproduziert, für bestimmte Releases geschlossen. Eine Herabstufung des Schweregrads muss begründet werden. Ein alter Befund darf nur dann aus der Freigabeentscheidung verschwinden, wenn seine Erledigung oder Nichtanwendbarkeit auf den konkreten Einsatz nachgewiesen ist.

Eine vollständige öffentliche Liste aller technischen Details kann mit Schutzinteressen kollidieren. Mindestens veröffentlicht werden sollen deshalb Gegenstand, betroffene Versionen, zusammengefasste Bedeutung, Zuständigkeit, Entscheidungsstatus und Datum des unabhängigen Abschlusses. Die Prüfstellen und zuständigen Behörden benötigen Zugang zu den vollständigen Belegen.

5.4 System 2.0 und der schwere Befund vom September

Der Originalbericht von Aleksander Essex vom 13. September 2026 untersucht Whitepaper 1.2. Er beschreibt als F-01 einen schweren Fehler in der Stichhaltigkeit des dort vorgeschlagenen Stimmbeweises. Unter den im Bericht analysierten Annahmen könnte ein manipuliertes Abstimmungsgerät Stimmen unbrauchbar machen, obwohl die stimmende Person die erwarteten Prüfcodes sieht. Der Bericht bezieht sich auf den Entwurf; er dokumentiert keinen Angriff auf einen produktiven Schweizer Urnengang.[42]

F-02 betrifft unzureichend festgelegte Kodierungen der Wahloptionen und daraus unter bestimmten Voraussetzungen entstehende Risiken für Integrität und Geheimhaltung. F-03 betrifft fehlende Anforderungen an den Nachweis der Kenntnis von Schlüsselanteilen. Besonders relevant ist die Abgrenzung im Bericht: Eine entsprechende Gegenmassnahme ist für System 1.x beschrieben; ihr Fehlen im Whitepaper 1.2 darf nicht ohne Weiteres als Fehlen im bestehenden System ausgegeben werden.[43]

Die Post veröffentlichte am 22. September Whitepaper 1.2.1. Das Änderungsverzeichnis nennt unter anderem eine Überarbeitung des Beweises in Anhang A.1.3 sowie Präzisierungen zu Schlüsselerzeugung und Vertrauensannahmen. Damit wäre die Aussage, der Hersteller habe bis zum Stichtag überhaupt nicht reagiert, falsch. In den hier ausgewerteten Originalprüfberichten ist jedoch keine eigenständige abschliessende Nachprüfung dieser Fassung 1.2.1 dokumentiert. Der sachgerechte Status lautet: **Herstellerkorrektur vorhanden; unabhängiger Abschluss für die geänderte Fassung in dieser Belegbasis nicht nachgewiesen.**[44]

Auch die Fachurteile müssen mit ihrem Zeitpunkt gelesen werden. Haines und Pereira benennen in ihrem Bericht vom 24. August bereits Zweifel am Stimmbeweis und fordern eine präzisere Festlegung zulässiger Protokollabläufe. Die BFH bewertet die gewählte Entwicklungsrichtung in ihrem Bericht vom 14. August grundsätzlich positiv, hält aber weitere Architektur-, Leistungs- und Spezifikationsfragen offen. Müller beurteilt die Reaktion auf seine Kommentare zu Version 1.2 positiv. Unterschiedliche Schwerpunkte und

[41] Q19 · Haenni/Koenig/Locher, Examination of the Swiss Post Internet Voting System, 09.01.2026, S. 3–9.

[42] Q05 · Essex, 13.09.2026, Management Summary S. i, Kap. 3–6 und S. 25; Whitepaper 1.2.

[43] Q05 · Essex, 13.09.2026, Management Summary S. i, Kap. 3–6 und S. 25; Whitepaper 1.2.

[44] Q06 · Post/LORIA, Whitepaper 1.2.1, S. 2, 11–12 und Anhang A.1.3; Änderungsverzeichnis, Commit 6d427c8d6d65, 22.09.2026.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

Zeitstände erklären einen Teil der Unterschiede; es handelt sich nicht um austauschbare Gesamtzertifikate.[45,46,47]

5.5 Konkrete technische Korrekturen

Spezifikation vor sicherheitskritischer Implementierung. Zustände, erlaubte Übergänge, Fehlerfälle, Wiederholungen, Abbrüche, Kontextbindungen und Schlüsselverwendung sind explizit zu beschreiben. Für jeden kritischen Pfad werden positive und negative Testfälle aus dieser Spezifikation abgeleitet. Ein Protokollbeweis ohne festgelegte Implementierungssemantik bleibt für die Freigabe unvollständig.

Unabhängige Nachprüfung jeder tragenden Korrektur. Für F-01 bis F-03 sind die Gegenbeispiele gegen die alte Fassung und ihr Scheitern gegen die neue Fassung nachzustellen, soweit der jeweilige Befund dies zulässt. Zusätzlich muss geprüft werden, ob die Korrektur neue Annahmen oder Nebenwirkungen einführt. Diese Arbeit soll eine Gruppe verantworten, die den geänderten Mechanismus nicht wesentlich entworfen hat.

Produktionsgleichheit belegen. Die Freigabeunterlagen müssen Quellcode-Commit, Buildwerkzeuge, Abhängigkeiten, Prüfsummen, Konfiguration und produktiv installierte Artefakte verbinden. Reproduzierbare Builds helfen dabei, genügen allein aber nicht: Ein reproduzierbar gebauter falscher oder nicht freigegebener Stand bleibt falsch. Art. 11 und der Anhang der VEleS enthalten bereits Nachweispflichten, an denen diese Forderung ansetzt.[48]

Gemeinsame Ausfallursachen reduzieren. Mehrere Kontrollkomponenten können denselben Fehler enthalten oder von derselben administrativen Infrastruktur abhängen. Zu untersuchen sind deshalb gemeinsame Bibliotheken, Buildsysteme, Administrationszugänge, Identitätsdienste und Wiederherstellungswege. Eine zweite Verifier-Implementierung ist nur dann wertvoll, wenn ihre Unabhängigkeit hinsichtlich Spezifikation, Entwicklung, Betrieb und relevanter Fehlerursachen begründet ist.

Komplexität messbar begrenzen. Neue Schnittstellen und Funktionen werden nur eingeführt, wenn ihr Nutzen einen klar benannten zusätzlichen Prüf- und Betriebsaufwand rechtfertigt. Für den sicherheitskritischen Kern sind unterstützte Wahlformen, Eingabegrenzen und Abhängigkeiten explizit zu inventarisieren. Eine lange Liste von Tests ist weniger aussagekräftig als der Nachweis, dass die wesentlichen Annahmen und Fehlerfälle abgedeckt sind.

5.6 Funktionale Vollständigkeit und tatsächlicher Nutzen

Die Risikobeurteilung darf nicht bei der Frage enden, ob eine abgegebene Stimme kryptografisch geschützt ist. Ebenso wichtig ist, ob eine berechtigte Person den vorgesehenen Vorgang unter realistischen Bedingungen selbständig und erfolgreich abschliessen kann. Ein sicherer Teilprozess genügt nicht, wenn Zugang, Prüfung oder Fehlerbehandlung scheitern. **Funktionale Vollständigkeit ist deshalb ein eigenständiges Abnahmekriterium und ein Bestandteil der Wirtschaftlichkeitsprüfung.**

Die Bundeskanzlei nennt als Ziele eine barrierefreie, mobile und nachvollziehbare Stimmabgabe. Sie führt zudem die Vermeidung ungültiger Stimmen und postalischer Verspätungen sowie die autonome Ausübung politischer Rechte durch Menschen mit Behinderungen als Vorteile an. An diesen öffentlich formulierten

[45] Q03 · Haines/Pereira, 24.08.2026, S. 1–2 und Anhang B.2.1, S. 22; Entwurf 2.0, Whitepaper 1.1/1.2.
[46] Q13 · Haenni/Koenig/Locher, Review White Paper 2.0, 14.08.2026, S. 15–16 und 20–23.
[47] Q14 · Müller, Review White Paper 2.0, 23.08.2026, S. 4–7.
[48] Q02 · VEleS, SR 161.116, Stand 01.07.2022; jeweils im Text bezeichnete Artikel und Anhangsziffern.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

Nutzenversprechen muss sich das tatsächlich angebotene Verfahren messen lassen. Die Aufzählung von Vorteilen ist noch kein Nachweis, dass sie in jeder zugelassenen Konfiguration und für jede Zielgruppe vollständig erreicht werden.[49]

Dabei sind drei Kategorien zu unterscheiden: eine tatsächlich fehlende oder unvollständige Systemfunktion, eine organisatorische beziehungsweise bewilligungsbedingte Zugangsbeschränkung und ein noch fehlender Nachweis der Gebrauchstauglichkeit. Alle drei können den realen Nutzen begrenzen; sie verlangen aber unterschiedliche Korrekturen. Aus einem begrenzten Elektorat folgt beispielsweise keine technische Unfähigkeit des Systems, weitere Stimmen zu verarbeiten. Ebenso belegt eine unterstützte Wahlmaske allein noch keine vollständige und vertrauenswürdige Umsetzung sämtlicher Wahlregeln.

5.7 Belegte Funktions- und Versorgungslücken des heutigen Verfahrens

Unvollständige Durchsetzung bestimmter Wahlregeln bei der Stimmabgabe. Die Post beschreibt im Whitepaper zu System 2.0 ausdrücklich eine Einschränkung des bestehenden Protokolls 1.x: Bei Nationalratswahlen muss eine Stimme mit einer bezeichneten Parteiliste mindestens eine nicht leere Kandidatenauswahl enthalten. Nach dieser Herstellerdokumentation erzwingt bei der Stimmabgabe nur der Voting Client diese Regel; der Client gehört für diesen Nachweis gerade nicht zum vertrauenswürdigen Systemteil. Entsprechende ungültige Stimmen werden in der heutigen Protokolllinie erst während der Auszählung herausgefiltert. Die Durchsetzung durch den vertrauenswürdigen Systemteil bereits bei der Stimmabgabe ist als Anforderung an Protokoll 2.0 und als Massnahme A.26 beschrieben.[50]

Das ist eine konkrete funktionale Lücke an einer sicherheitsrelevanten Grenze. Die normale Benutzeroberfläche kann die falsche Eingabe verhindern, ohne dass das Gesamtsystem dieselbe Garantie gegenüber einem fehlerhaften oder manipulierten Client bietet. Daraus folgt weder, dass alle Stimmen dieses Typs tatsächlich vorkommen, noch dass jede frühere Wahl fehlerhaft war. Kritikwürdig ist vielmehr, dass das pauschale Versprechen, ungültige Stimmen zu verunmöglichen, für diese Konstellation präzisiert werden muss. Auch weitere kantonale Regeln, die mehrere Fragen verbinden, werden laut Whitepaper heute teilweise erst bei der Auszählung durch den vertrauenswürdigen Systemteil behandelt. Ein vollständiger Abnahmekatalog muss deshalb je Wahlregel festhalten, wo sie geprüft wird und was bei einer Verletzung geschieht.[51]

Kein vollständig von der Papierzustellung unabhängiger Zugang. Die aktuelle Herstellerbeschreibung sieht einen Umschlag mit Stimmrechtsausweis und den erforderlichen Codes vor. St.Gallen bestätigt im tatsächlichen Einsatz, dass Zugangsdaten und Codes auf dem Stimmrechtsausweis stehen und den angemeldeten Personen das Stimmmaterial weiterhin zugesendet wird. Elektronische Rückübermittlung kann somit den Postweg der abgegebenen Stimme vermeiden; sie beseitigt nicht die Abhängigkeit vom rechtzeitigen Empfang des Zugangsmaterials. Für Auslandschweizerinnen und Auslandschweizer bleibt damit ein Teil des ursprünglichen Zustellproblems bestehen.[52,53]

Diese Beschränkung ist bei Nutzen- und Kostenangaben ausdrücklich zu berücksichtigen. Das Verfahren ist ein zusätzlicher elektronischer Stimmkanal mit physischem Zugangsmaterial. Ein vollständig digitaler Ablauf wäre eine weitergehende Anforderung. Seine Einführung dürfte allerdings die unabhängige

[49] Q10 · Bundeskanzlei, Vote électronique, Projektziele und Aktueller Stand, Abruf 09.10.2026.
[50] Q06 · Post/LORIA, Whitepaper 1.2.1, S. 2, 11–12 und Anhang A.1.3; Änderungsverzeichnis, Commit 6d427c8d6d65, 22.09.2026.
[51] Q06 · Post/LORIA, Whitepaper 1.2.1, S. 2, 11–12 und Anhang A.1.3; Änderungsverzeichnis, Commit 6d427c8d6d65, 22.09.2026.
[52] Q06 · Post/LORIA, Whitepaper 1.2.1, S. 2, 11–12 und Anhang A.1.3; Änderungsverzeichnis, Commit 6d427c8d6d65, 22.09.2026.
[53] Q22 · Kanton St.Gallen, E-Voting, aktualisiert 08.09.2026, Abschnitte Anmeldung, Stimmabgabe und Helpdesk.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

Übermittlung der Prüfinformationen nicht unbemerkt aufheben: Werden Zugang und Kontrollcodes auf dasselbe möglicherweise kompromittierte Endgerät verlagert, ändern sich die Sicherheitsannahmen.

Fehlender elektronischer Wiederherstellungsweg bei verlorenem Stimmrechtsausweis. St.Gallen erklärt ausdrücklich, dass nach Verlust des Stimmrechtsausweises keine elektronische Stimmabgabe mehr möglich ist. Damit fehlt in diesem veröffentlichten Bedienweg eine elektronische Wiederherstellungsmöglichkeit. Die Aussage betrifft den elektronischen Kanal in St.Gallen; sie belegt weder den Verlust des Stimmrechts insgesamt noch dieselbe Regelung in sämtlichen Kantonen.[54]

Die Folge ist dennoch erheblich: Gerade unterwegs kann eine grundsätzlich berechtigte Person den zugesagten digitalen Zugang verlieren. Eine Wiederherstellung ist keine harmlose Passwortfunktion. Sie müsste eine verlässliche Identitätsprüfung, die sichere Behandlung des bisherigen Zugangsmaterials und den Ausschluss einer Doppelstimmabgabe verbinden. Entweder wird ein solcher Ablauf unabhängig geprüft bereitgestellt, oder es muss vorab ein tatsächlich nutzbarer anderer Stimmweg mit klaren Fristen erklärt werden. Eine allgemeine Helpdesk-Adresse ersetzt diesen Ablauf nicht.

Begrenzte zeitliche und organisatorische Nutzbarkeit. Für die betreffenden Inlandstimmberechtigten berücksichtigt St.Gallen An- und Abmeldungen bis spätestens acht Wochen vor dem Urnengang; bei Erreichen der Limite von 30 Prozent wird die Anmeldung gesperrt. Die elektronische Urne schliesst bei eidgenössischen und kantonalen Urnengängen am Samstag um 12 Uhr. Der publizierte Helpdesk ist montags bis freitags in festgelegten Zeitfenstern erreichbar. Die dort aufgeführten Zeiten weisen somit keine reguläre Unterstützung am letzten Samstagvormittag aus.[55]

Diese Regeln sind keine belegten Softwarefehler. Sie begrenzen aber die Leistung, die Nutzerinnen und Nutzer tatsächlich erhalten: Wer sich spät entscheidet oder kurz vor Kanalschluss Hilfe benötigt, kann auf eine Versorgungslücke stossen. Versuchslimiten und sicherheitsbedingte Vorlaufzeiten sind zu begründen; in einer Nutzenbilanz dürfen sie nicht ausgeblendet werden. Insbesondere ist die digitale Verfügbarkeit des Portals von der Verfügbarkeit wirksamer Hilfe zu unterscheiden.

5.8 Welche Funktionalität vor einer Ausweitung nachzuweisen ist

Die verfügbaren Belege rechtfertigen keine pauschale Behauptung, das heutige System unterstütze keine Wahlen, kein Panaschieren oder keine mobilen Geräte. Die Herstellerdokumentation behandelt ausdrücklich Wahlmodelle und freie Kandidateneinträge. Für eine belastbare Beurteilung braucht es jedoch eine veröffentlichte Funktionsmatrix des zugelassenen Produktionsstands. Künftige Eigenschaften von System 2.0 dürfen nicht als bereits verfügbare Fähigkeiten gezählt werden.[56]

Erforderliche Leistung	Kritischer Prüfpunkt	Verlangter Nachweis
Vollständige Abbildung der vorgesehenen Urnengänge	Wahlmodelle, Kombinationen von Vorlagen, Listen- und Kandidatenregeln sowie zulässige leere Eingaben	Pro Kanton und Wahlart eine freigegebene Testmatrix; Nachweis gegen einen manipulierten Client für Regeln, die vor Aufnahme in die Urne gelten müssen
Selbständige Bedienung und Verifikation	Anmeldung, Auswahl, Codevergleich, Bestätigung und Fehlerbehandlung mit den tatsächlich benötigten Hilfsmitteln	Beobachtete Tests mit betroffenen Nutzergruppen einschliesslich des physischen Stimmmaterials; veröffentlichte Grenzen und behobene Fehler
Mobile Nutzbarkeit	Kleine Displays, unterstützte Browser, Eingabe langer Codes, Verbindungsunterbruch und erneute Anmeldung	Erfolgreiche vollständige Testabläufe auf der veröffentlichten Geräte- und Browserauswahl; kein Verlust eines bereits erreichten Zustands
Verlässlicher Umgang mit Verlust und Störungen	Fehlendes Zugangsmaterial, gesperrter Zugang, widersprüchliche Prüfcodes und unklarer Abschluss	Vorab festgelegter, rechtlich geprüfter Wiederherstellungs- oder Alternativprozess mit Zuständigkeit und Frist

[54] Q22 · Kanton St.Gallen, E-Voting, aktualisiert 08.09.2026, Abschnitte Anmeldung, Stimmabgabe und Helpdesk.

[55] Q22 · Kanton St.Gallen, E-Voting, aktualisiert 08.09.2026, Abschnitte Anmeldung, Stimmabgabe und Helpdesk.

[56] Q06 · Post/LORIA, Whitepaper 1.2.1, S. 2, 11–12 und Anhang A.1.3; Änderungsverzeichnis, Commit 6d427c8d6d65, 22.09.2026.

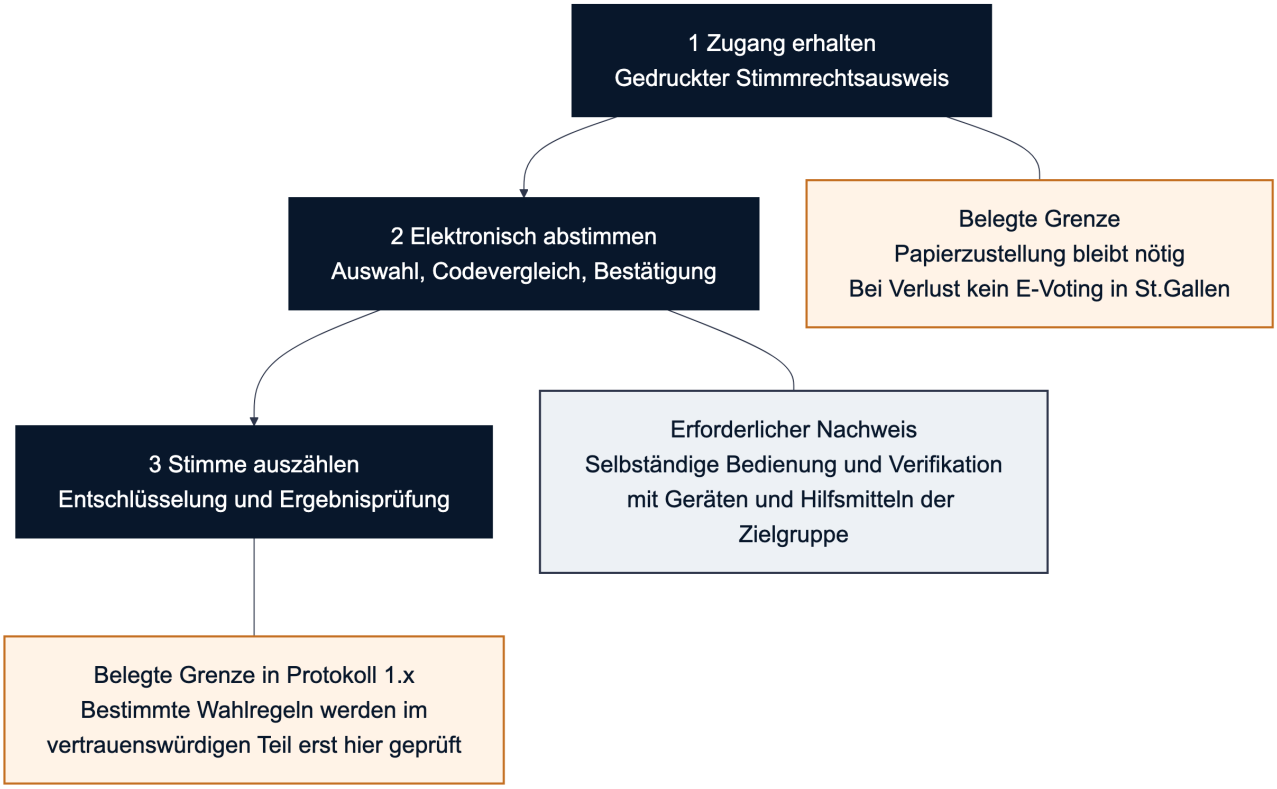
© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

Erforderliche Leistung	Kritischer Prüfpunkt	Verlangter Nachweis
Rechtzeitig erreichbare Hilfe	Öffnungszeiten, Wartezeit und Eskalation während des tatsächlichen Stimmfensters	Unterstützungszeiten bis zum Kanalschluss, geübte Eskalation und nachvollziehbare Bearbeitung dringender Fälle

Diese Tabelle formuliert Abnahmeanforderungen. Sie behauptet nicht, dass sämtliche aufgeführten Fähigkeiten heute fehlen. Besonders bei Barrierefreiheit muss die Untersuchung den ganzen Vorgang erfassen: Eine zugängliche Webseite allein beweist noch nicht, dass eine sehbehinderte Person gedruckte Prüfcodes ohne fremde Hilfe kontrollieren kann. Umgekehrt darf aus dieser Prüfanforderung ohne Untersuchung der angebotenen Hilfsmittel keine pauschale Unzugänglichkeit abgeleitet werden.

Abbildung 3 · Funktionslücken im vollständigen Abstimmungsweg



Eigene Darstellung für den in Kapitel 5 untersuchten Stand. Orange bezeichnet dokumentierte Grenzen: Papierunterlagen und Verlustfolgen am Beispiel St.Gallen sowie die im Whitepaper 1.2.1 beschriebene Prüfung bestimmter Wahlregeln erst bei der Auszählung. Das graue Feld bezeichnet einen erforderlichen Nachweis zur Nutzbarkeit, keine pauschal belegte Abwesenheit barrierefreier Funktionen.[57,58,59]

5.9 Konkrete Konsequenzen für Sanierung und Wirtschaftlichkeit

Bund und Kantone sollen zusammen mit der Post eine versionsgebundene Leistungsbeschreibung veröffentlichen. Sie muss vorhandene Funktionen, bekannte Grenzen, betroffene Nutzergruppen und geplante Ergänzungen sichtbar machen. Die unabhängige Schlussprüfung muss neben kryptografischen Eigenschaften auch den vollständigen Bedienweg und die Fehlerbehandlung bewerten. Die Wahlbehörden verantworten die fachlichen Regeln und den Zugang; die Post verantwortet die nachgewiesenen Produktfunktionen; die Prüfstelle bestätigt den tatsächlich untersuchten Stand.

[57] Q06 · Post/LORIA, Whitepaper 1.2.1, S. 2, 11–12 und Anhang A.1.3; Änderungsverzeichnis, Commit 6d427c8d6d65, 22.09.2026.

[58] Q22 · Kanton St.Gallen, E-Voting, aktualisiert 08.09.2026, Abschnitte Anmeldung, Stimmabgabe und Helpdesk.

[59] Q10 · Bundeskanzlei, Vote électronique, Projektziele und Aktueller Stand, Abruf 09.10.2026.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

Vorrang hat die Beseitigung der konkret belegten Lücken: durchgängige Prüfung kritischer Wahlregeln, eine klar geregelte Behandlung verlorenen Zugangsmaterials und rechtzeitig verfügbare Unterstützung. Neue Komfortfunktionen sind erst dann vorteilhaft, wenn sie die Sicherheit und die selbständige Nutzung nachweislich verbessern. Eine E-ID oder eine neue App ist dafür noch kein hinreichender Nachweis.

Der wirtschaftliche Erfolg ist an zusätzlich ermöglichten, erfolgreich abgeschlossenen und korrekt ausgezählten Stimmabgaben zu messen. Zu erheben sind dafür datensparsam unter anderem Abbrüche, Unterstützungsbedarf, Fehler beim Codevergleich und Fälle nicht rechtzeitig verfügbaren Zugangsmaterials. Eine personenbezogene Verknüpfung mit dem geheimen Stimmverhalten ist dafür weder erforderlich noch zulässig. Kosten für weiterhin notwendige Papierunterlagen, Parallelbetrieb, Support und kantonale Integration gehören in dieselbe Rechnung. Ohne diese Leistungs- und Nutzungsdaten besteht das Risiko, eine technisch aufwendige Ergänzung dauerhaft zu finanzieren, deren entscheidender Zusatznutzen für die vorgesehenen Zielgruppen unzureichend belegt bleibt.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

5.10 Must-have-Vergleich: Was das heutige System liefert

Stand 9. Oktober 2026. «Heutiges System» meint die bestehende Protokolllinie 1.x samt den beschriebenen kantonalen Bedien- und Betriebswegen. Die Matrix enthält 16 von dieser Studie verlangte Mindestleistungen und ein gesondertes Nutzungsziel (Z01). Sie ist ein Abnahmekatalog, keine vollständige Wiedergabe geltenden Rechts. Herstellerentwurf 2.0, Produktivbetrieb und öffentlich belegter Nachweis werden getrennt beurteilt.

A · Stimmfunktionen und überprüfbare Ergebnisse

Must-have / Abnahmemassstab	Status heute	Was das heutige System liefert	Grenze / noch nötige Leistung
M01 · Elektronische Stimmabgabe Berechtigte Personen können im zugelassenen Umfang elektronisch abstimmen.	VORHANDEN	Der elektronische Kanal wird im bewilligten Versuchsbetrieb angeboten. Stimmabgabe aus der Ferne und elektronische Übermittlung sind reale Leistungen. Zugang und Einsatzumfang bleiben begrenzt. [Q10, Q11, Q22]	Eine flächendeckende Verfügbarkeit für alle Stimmberechtigten ist damit nicht zugesagt. Ausweitung und zusätzlicher Nutzen brauchen eigene Nachweise.
M02 · Abbildung der Wahlarten Alle für einen konkreten Einsatz vorgesehenen Vorlagen, Listen- und Kandidatenregeln werden korrekt abgebildet.	NACHWEIS OFFEN	Die Herstellerdokumentation beschreibt Wahlmodelle und freie Kandidateneinträge. Eine pauschale Aussage «keine Wahlen oder kein Panaschieren» wäre falsch. Die vollständige Abdeckung jeder kantonalen Einsatzkonfiguration ist hier nicht belegt. [Q06; Kapitel 5.8]	Freigegebene Funktions- und Testmatrix je Kanton, Wahlart und Produktionsstand. Beschriebene Modelle sind kein Nachweis für jede praktisch eingesetzte Kombination.
M03 · Gültigkeitsprüfung vor Registrierung Kritische Wahlregeln werden im vertrauenswürdigen Systemteil vor Aufnahme in die Urne geprüft.	TEILWEISE	In Protokoll 1.x werden bestimmte Regeln zunächst nur im Client durchgesetzt. Ungültige Kombinationen werden im vertrauenswürdigen Teil teilweise erst bei der Auszählung erkannt. [Q06, S. 11–12]	Konkrete funktionale Lücke. Für Protokoll 2.0 ist die frühere Durchsetzung beschrieben (A.26). Das ist ein Entwurfsziel, kein bereits abgenommener Produktivnachweis.
M04 · Individuelle Verifikation Eine Person kann prüfen, ob ihre Auswahl korrekt übernommen wird, und Abweichungen erkennen.	VORHANDEN	Der veröffentlichte Bedienweg nutzt Auswahl, Vergleich gedruckter Prüfcodes und Bestätigung. Diese Prüffunktion ist Bestandteil des Verfahrens. [Q02, Q06, Q22]	Die Wirksamkeit hängt von korrekter Durchführung und verständlicher Fehlerbehandlung ab. Nutzertests und ein funktionierender Meldeweg bleiben erforderlich; vgl. M06 und M07.
M05 · Universelle Verifikation Berechtigte Prüfpersonen können Registrierung und Ergebnis anhand unabhängiger Hilfsmittel überprüfen.	VORHANDEN	Universelle Verifikation gehört zum System und zu den gesetzlichen Anforderungen. Originalgutachten untersuchen die entsprechenden Protokolle und Softwarestände. Sie wirkt unter bezeichneten Annahmen. [Q02, Q15, Q16, Q19]	Der Mechanismus belegt noch keine staatsunabhängige Prüfung durch beliebige Dritte. Diese weitergehende Mindestanforderung wird in M15 beurteilt; die verbindliche Blockchain-Abbildung jeder angenommenen Stimme in M16.

VORHANDEN: Funktion belegt, kein umfassendes Sicherheitsurteil. TEILWEISE: Leistung vorhanden, konkrete Grenze belegt. FEHLT: bezeichnete Leistung im genannten Umfang nicht angeboten. NACHWEIS OFFEN: Quellen reichen für eine vollständige Bewertung nicht aus; daraus folgt keine bewiesene Funktionsabwesenheit.

Kernaussage: Das heutige System bietet elektronische Stimmabgabe und Verifikationsmechanismen. Eine belegte funktionale Grenze bleibt die verspätete Durchsetzung bestimmter Wahlregeln. Die vollständig passende Abbildung eines konkreten Urnengangs muss versions- und kantonsbezogen nachgewiesen werden.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

5.10 Must-have-Vergleich · Fortsetzung

Bewertung des heutigen Einsatzstands; System 2.0 zählt nicht als bereits gelieferte Funktion. Q-Verweise führen zum Originalquellenverzeichnis in Kapitel 15.

B · Zugang, selbständige Bedienung und Hilfe

Must-have / Abnahmemassstab	Status heute	Was das heutige System liefert	Grenze / noch nötige Leistung
M06 · Barrierefreier Gesamtvorgang Betroffene Personen können Zugang, Auswahl, Codevergleich, Bestätigung und Fehlerbehandlung selbständig bewältigen.	**NACHWEIS OFFEN**	Autonome und barrierefreie Stimmabgabe ist ein öffentliches Projektziel. Die Quellenbasis dieser Studie belegt jedoch keinen vollständigen Nutzungsnachweis für alle betroffenen Gruppen einschliesslich physischer Prüfcodes. [Q10; Kapitel 5.8 und 7.1]	Beobachtete Tests mit Betroffenen und den tatsächlich verwendeten Hilfsmitteln. Fehlender öffentlicher Nachweis bedeutet nicht, dass keine barrierefreien Funktionen existieren.
M07 · Mobiler und fehlertoleranter Bedienweg Der ganze Vorgang funktioniert auf unterstützten Geräten auch bei Unterbruch und unklarem Abschluss.	**NACHWEIS OFFEN**	Mobile Nutzung wird als Ziel genannt. Daraus folgt weder ein generelles Funktionsverbot noch ein belegter vollständiger Ablauf auf jeder Geräte- und Browserkombination. Unterbruch- und Wiederaufnahmefälle sind hier nicht abschliessend nachgewiesen. [Q10; Kapitel 5.8]	Veröffentlichte Geräteliste, erfolgreiche Ende-zu-Ende-Tests und klare Statusmeldungen nach Unterbrüchen; keine unbemerkte Doppelabgabe oder verlorene Auswahl.
M08 · Elektronischer Wiederzugang Verlorenes Zugangsmaterial kann ohne Aufgabe des elektronischen Kanals sicher ersetzt werden.	**FEHLT**	St.Gallen erklärt: Nach Verlust des Stimmrechtsausweises ist keine elektronische Stimmabgabe mehr möglich. Ein elektronischer Wiederherstellungsweg fehlt damit im dort veröffentlichten Verfahren. [Q22]	Geltungsbereich: elektronischer Kanal in St.Gallen. Ein anderer Stimmweg kann bestehen. Wiederherstellung oder Ersatz müssen Identität, Fristen und Ausschluss einer Doppelstimme sichern.
M09 · Reguläre Hilfe bis Kanalschluss Ein veröffentlichter Unterstützungsweg deckt auch die letzte Öffnungsphase des elektronischen Kanals ab.	**FEHLT**	St.Gallen publiziert Helpdesk-Zeiten von Montag bis Freitag; die elektronische Urne schliesst am Samstag um 12 Uhr. Reguläre Hilfe am letzten Samstagvormittag ist in diesen Zeiten nicht vorgesehen. [Q22]	Geltungsbereich: publizierter Regelbetrieb in St.Gallen. Die Versorgungslücke verlangt passende Bereitschafts- und Eskalationswege; ein allfälliger Sonderdienst ist hier nicht belegt.
Z01 · Vollständig papierloser Zugang Zusätzliches Nutzungsziel: Teilnahme ohne vorausgehenden physischen Versand von Zugangsdaten und Prüfcodes.	**FEHLT**	Das heutige Verfahren setzt physisches Stimmmaterial voraus. Es erspart den Postweg der Rücksendung, beseitigt aber nicht die Abhängigkeit vom Empfang der Unterlagen. Das gilt auch für den beschriebenen Entwurf 2.0. [Q06, Q22]	Kein allgemeines gesetzliches Muss dieser Studie. Wer vollständige Unabhängigkeit vom Postweg verspricht, muss einen sicheren Ersatz für Zugang und unabhängige Prüfinformationen nachweisen. 2.0 allein liefert ihn nicht.

VORHANDEN: Funktion belegt, kein umfassendes Sicherheitsurteil. TEILWEISE: Leistung vorhanden, konkrete Grenze belegt. FEHLT: bezeichnete Leistung im genannten Umfang nicht angeboten. NACHWEIS OFFEN: Quellen reichen für eine vollständige Bewertung nicht aus; daraus folgt keine bewiesene Funktionsabwesenheit.

Kernaussage: Die klar belegten Angebotslücken betreffen den elektronischen Wiederzugang und die publizierte Hilfe in St.Gallen sowie den vollständig papierlosen Zugang. Bei Barrierefreiheit und mobiler Fehlertoleranz ist die Aussage enger: Der vollständige Nachweis fehlt in der ausgewerteten Quellenbasis.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

5.10 Must-have-Vergleich · Fortsetzung

Bewertung des heutigen Einsatzstands; System 2.0 zählt nicht als bereits gelieferte Funktion. Q-Verweise führen zum Originalquellenverzeichnis in Kapitel 15.

C · Auszählbarkeit, Geheimhaltung und belastbarer Betrieb

Must-have / Abnahmemassstab	Status heute	Was das heutige System liefert	Grenze / noch nötige Leistung
M10 · Auszählung und Wiederherstellung Registrierte Stimmen bleiben bei plausiblen Geräte- und Personalausfällen vollständig auszählbar.	**TEILWEISE**	Ein regulärer Auszählungsprozess besteht. In Basel-Stadt konnten am 8. März 2026 jedoch 2'048 elektronische Stimmen nicht ausgezählt werden. Zusätzliche Speichermöglichkeiten und Checklisten wurden für weitere Kantone beschrieben. [Q09, Q20]	Die Gegenmassnahmen ersetzen keine beobachtete Wiederherstellungsprobe. Der Vorfall belegt eine betriebliche Lücke im betroffenen Ablauf, keinen generellen Ausfall sämtlicher Kantone.
M11 · Stimmgeheimnis im Gesamtbetrieb Identität, Stimmzugang, Protokolle und Auszählung dürfen keine unzulässige Zuordnung zur konkreten Stimme ermöglichen.	**NACHWEIS OFFEN**	Kryptografische Schutzmechanismen und gesetzliche Anforderungen bestehen. Ihre vollständige Umsetzung in sämtlichen aktuellen Betriebs-, Druck-, Administrations- und Aufbewahrungsprozessen ist öffentlich nicht vollständig rekonstruierbar. [Q02, Q04; Kapitel 7 und 14.4]	Versions- und einsatzbezogener Nachweis der Datenflüsse, Zugriffe, Aufbewahrung und Löschung. Der Status behauptet keinen belegten Bruch des Stimmgeheimnisses.
M12 · Sichere Störfälle und Kanalwechsel Unklare Registrierung, Abbruch und allfällige Ersatzabgabe werden ohne Doppelstimmen oder Rechtsverlust behandelt.	**NACHWEIS OFFEN**	Die Quellenbasis liefert kein vollständig geprüftes, kantonsübergreifendes Ersatzverfahren für alle Zustände vor und nach Registrierung. Ein pauschaler Rückfall auf Papier genügt nach Registrierung nicht. [Q02, Q04; Kapitel 6.3]	Je Einsatz festgelegte Status-, Sperr-, Abgleich- und Entscheidungsregeln, rechtlich geprüft und praktisch geübt. Offener Nachweis ist keine Behauptung beobachteter Doppelstimmen.
M13 · Identischer geprüfter und betriebener Stand Version, Build, Konfiguration und installierte Artefakte stimmen mit Prüfung und Zulassung überein.	**NACHWEIS OFFEN**	Die VEleS verlangt entsprechende Nachweise; die Risikobeurteilung behandelt Abweichungen zwischen geprüftem und eingesetztem Stand. Die Studie hat keine Produktionsinstallation selbst verifiziert. [Q02, Q04; Kapitel 5.5 und 14.4]	Geschlossene Zuordnung von Quellcode, Build, Prüfsummen, Konfiguration und produktiver Installation. Ein veröffentlichtes Repository oder eine Versionsnummer allein liefert sie nicht.
M14 · Nachprüfbares Freigabe- und Ergebnispaket Befunde, Korrekturen, Prüfungen, Zuständigkeiten und Ergebnisnachweise sind für berechtigte Kontrollstellen nachvollziehbar verbunden.	**NACHWEIS OFFEN**	Es gibt öffentliche Prüfberichte und behördliche Risikobeurteilungen. Vollständige aktuelle Mandats-, Ausstands-, Betriebs- und Erledigungsnachweise sind aus der ausgewerteten Belegbasis nicht rekonstruierbar. [Q01, Q04; Kapitel 14.4–14.6]	Ein konsistentes Paket pro Version und Urnengang; öffentliche Begründung und kontrollierter Zugang zu geschützten Belegen. Quelloffenheit und Einzelberichte ersetzen dieses Paket nicht.

VORHANDEN: Funktion belegt, kein umfassendes Sicherheitsurteil. TEILWEISE: Leistung vorhanden, konkrete Grenze belegt. FEHLT: bezeichnete Leistung im genannten Umfang nicht angeboten. NACHWEIS OFFEN: Quellen reichen für eine vollständige Bewertung nicht aus; daraus folgt keine bewiesene Funktionsabwesenheit.

Kernaussage: Der entscheidende Betriebsnachweis betrifft den vollständigen Ablauf. Die vorhandenen öffentlichen Berichte belegen ernsthafte Prüfarbeit, erlauben aber keine lückenlose Abnahme aller heutigen Produktions- und Betriebszustände. Eine neue Systemversion muss dieselben Anforderungen erneut erfüllen.

Lieferperspektive: Eine heute fehlende Leistung wird nicht allein durch eine angekündigte neue Version zur zugesagten Lieferung. Für M03 ist ein konkretes Entwurfsziel dokumentiert. Für die übrigen offenen Punkte ersetzt die ausgewertete Belegbasis weder einen verbindlichen Lieferplan noch eine Abnahme. Auch Entwurf 2.0 bleibt auf physisches Stimmmaterial angewiesen; Z01 ist dadurch nicht erfüllt.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

5.10 Must-have-Vergleich · Fortsetzung

D · Staatsunabhängige Prüfung und Blockchain

Must-have / Abnahmemassstab	Status heute	Was das heutige System liefert	Grenze / noch nötige Leistung
M15 · Staatsunabhängige Ergebnisprüfung Dritte prüfen den konkreten Urnengang ohne staatliche Prüfinfrastruktur, Organisation oder fallweise Mitwirkung.	**NICHT VORGESEHEN**	Der dokumentierte Prüfweg richtet sich an vom Kanton ausgewählte Auditoren. Ein vollständiges öffentliches Audit des realen Urnengangs durch jedermann ohne staatliche Mitwirkung ist darin nicht vorgesehen. Externe Systemgutachten bestehen. [Q02; Q06, S. 13, 15; Q30]	Offene Spezifikation, vollständige authentische Belege, unabhängige Datenkopien und eigene Prüferprogramme. Kein Behördenkonto, Behördenportal oder staatliches Einzelmandat als Voraussetzung.
M16 · Blockchain-Eintrag für jede angenommene Stimme Definitive Aufnahme in die Urne und bestätigter, eindeutig zugehöriger Blockchain-Eintrag bilden einen verbindlichen Vorgang.	**NICHT VORGESEHEN**	Im dokumentierten heutigen Konzept ist keine Blockchain mit einem Eintrag je angenommener Stimme vorgesehen. Auch Whitepaper 2.0, Version 1.2.1, plant diesen Annahmeweg nicht. M16 verlangt eine Änderung des Konzepts. [Q06, Kapitel 3; Kapitel 5.12 dieser Studie]	Je Stimme ein geschützter Eintrag; Annahme erst nach festgelegter Bestätigung. Externe Auditoren gleichen Blockchain, vollständigen Urnenbestand und Auszählung ab. Eine nachträgliche Sammelverankerung genügt nicht.

NICHT VORGESEHEN bewertet den beschriebenen Planungsumfang: Ein frei zugängliches Vollaudit und eine Blockchain je angenommener Stimme fehlen darin. M15 und M16 sind verbindliche Ziel- und Abnahmeanforderungen dieser Studie, keine Behauptung bereits geltenden Rechts.

Annahmeregel. Vor der Blockchain-Bestätigung bleibt die Stimme ausstehend. Die elektronische Urne wird aus den bestätigten, fachlich gültigen Einträgen abgeleitet. Ein lokaler Schreibfehler darf keine angenommene Stimme verlieren; ein Wiederholungsversuch darf keine zweite erzeugen.

Prüfunabhängigkeit. Auditoren betreiben eigene Knoten, beziehen Belege auch aus unabhängigen Replikaten und prüfen lokal, nach Datenübernahme auch offline. Auswahl, Organisation und Veröffentlichung ihrer Prüfung hängen weder von einer Behörde noch vom Anbieter ab.

Vollständigkeit. Jeder gültige Annahmeeintrag gehört genau einmal zum auswertbaren Bestand, jede ausgewertete Stimme zu genau einem solchen Eintrag. Reine Anzahlengleichheit genügt nicht. Signierte Manifeste und kryptografische Beweise müssen auch Austausch, Auslassung und widersprüchliche Datenstände erkennbar machen.

Nachweis vor Einsatz. Mindestens zwei organisatorisch unabhängige Auditorenteams reproduzieren den gesamten Abgleich mit unabhängig entwickelten Prüfprogrammen, ohne Zugang zu staatlichen Diensten. Manipulierte, doppelte und fehlende Belege müssen zu konkreten Fehlermeldungen führen.

Freigabefolge: Fehlt der praktische Gesamtnachweis, ist die Anforderung nicht erfüllt. Eine Herstellerzusage, ein Blockchain-Explorer oder eine formale Auditorenrolle ersetzt ihn nicht. G5 übernimmt diese Sperre.

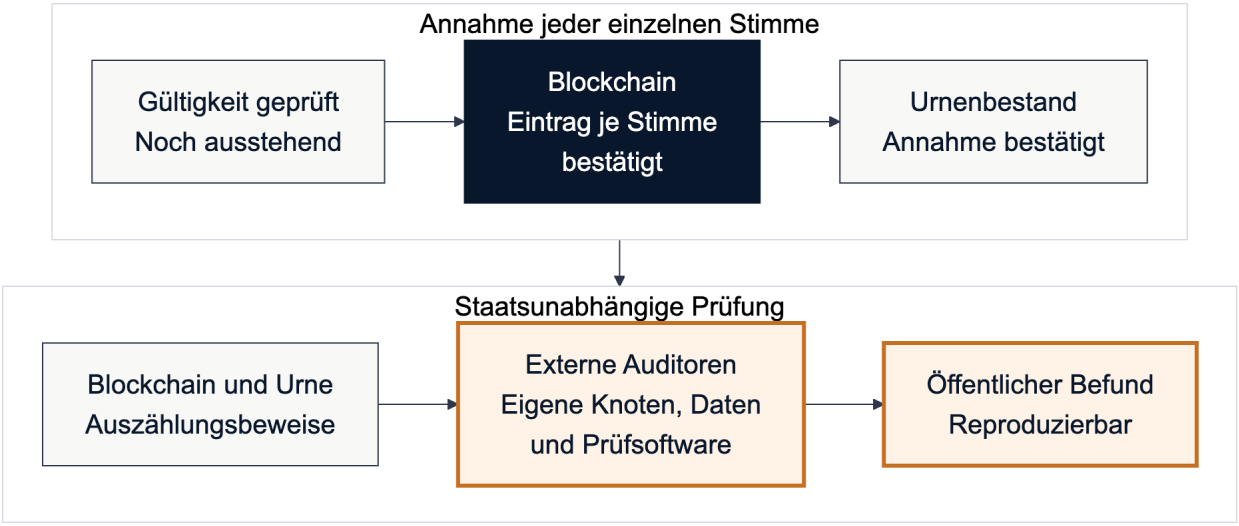
© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

5.11 Blockchain als verbindlicher Annahmenachweis

Im heutigen dokumentierten Plan ist diese Blockchain nicht vorgesehen. Die Studie verlangt sie als zusätzlichen öffentlichen Annahmenachweis: Jede definitiv angenommene Stimme erhält einen eigenen bestätigten Eintrag. Daraus muss der Urnenbestand unabhängig rekonstruierbar sein. Zweck und demokratische Bedeutung erläutert Kapitel 5.12.

Abbildung 4 · Blockchain-Nachweis und staatsunabhängige Ergebnisprüfung



Eigene Darstellung der Zielanforderungen M15/M16. Externe Auditoren erhalten keine Entschlüsselungsschlüssel für individuelle Stimmen. Die behördliche Verantwortung für den Urnengang bleibt vom eigenständigen technischen Prüfweg getrennt.

Geschützter Eintrag. Vorgesehen sind die Urnengang-ID, eine kryptografisch bindende und verbergende Referenz auf den randomisiert verschlüsselten Stimmzettel sowie die nötigen Gültigkeits- und Einmaligkeitsbeweise. Keine Identität, Klartextwahl oder einfach erratbare Prüfsumme von «Ja/Nein» gehört in die Kette. Die Zuordnung zu den Auszählungsbeweisen muss prüfbar bleiben.

Bestätigung und Störfall. Protokoll, Bestätigungsregel und verbindlicher Annahmeschluss sind vorab festzulegen. Bitcoin zeigt, dass Bestätigungen ein verbleibendes Reorganisationsrisiko vermindern, keine absolute Endgültigkeit schaffen. Bei Unterbruch, Verzögerung oder Kettenwechsel braucht es einen wiederholbaren Abgleich; eine wartende Transaktion darf nicht als definitiv angenommen erscheinen.[60]

Unabhängige Belege. Die benötigten verschlüsselten Daten und Beweise müssen neben der Blockchain vollständig bei unabhängigen Stellen verfügbar sein. Ein Hash allein ermöglicht keine Auszählungsprüfung. ElectionGuard beschreibt öffentliche Ergebnisbelege und Drittprüfer als Ansatz; dies belegt keine fertige Schweizer Integration.[61]

Grenze der Aussage. Die Blockchain beweist für sich weder den ursprünglichen Stimmwillen noch die Richtigkeit des Stimmregisters oder die Freiheit von Zwang. Individuelle Verifikation, überprüfbare Berechtigung und Geheimhaltung bleiben eigene Anforderungen. Staat und Anbieter dürfen Konsens und Prüfdatenzugang nicht beherrschen. Netzwerk, Leistung, Fristen, Kosten und Datenschutz sind vor Einsatz nachzuweisen.[62]

60 Q27 · Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, Abschnitte 5, 8 und 11. Übertragen wird das Prüfprinzip, nicht die Behauptung eines fertigen Abstimmungssystems.

61 Q28 · ElectionGuard, Creating a Verifiable Election und Election Record, Abschnitte Publishing Verifiable results und Election Record, Abruf 09.10.2026.

62 Q29 · National Academies, Securing the Vote, 2018, Kapitel 5, S. 103–105, Abschnitt Blockchains. Grenzen der Technik, kein Audit des heutigen Schweizer Systems.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

5.12 Vertrauen durch öffentliche Kontrolle

Vertrauen muss eine Prüfung aushalten. In einer Demokratie entscheidet die Auszählung darüber, welcher politische Wille verbindlich wird. Auch wer eine Abstimmung verliert, muss ihre Korrektheit mit selbst gewählten Fachleuten überprüfen können. Eine belastbare Kontrolle stärkt die Akzeptanz eines Ergebnisses gerade dann, wenn Vertrauen in Behörden, Parteien oder Anbieter fehlt. Jede Person soll sagen können: Ich kann die Belege selbst prüfen oder jemanden damit beauftragen, dem ich vertraue.

Im heutigen Plan fehlt dieser offene Prüfweg. Die untersuchte Systembeschreibung sieht keine Blockchain vor, in der jede angenommene Stimme öffentlich nachvollziehbar verankert wird. Auch der Entwurf für System 2.0 übernimmt diese Funktion nicht. Sein Whitepaper beschreibt vom Kanton ernannte Wählervertretungen und ausgewählte Auditoren. Der hier vorgeschlagene Blockchain-Nachweis ist deshalb eine zusätzliche Architektur- und Demokratieanforderung, keine bereits zugesagte Leistung des laufenden Projekts.[63]

Die Kritik betrifft den Zugang zur Kontrolle. Das heutige dokumentierte Konzept ermöglicht kein frei zugängliches, vollständiges externes Audit eines realen Urnengangs durch jedermann ohne staatliche Mitwirkung. Es organisiert die Ergebnisprüfung innerhalb eines kantonal bestimmten Verfahrens. Die Bundeskanzlei beauftragt zudem unabhängige Systemprüfungen; Quellcodeoffenlegung und Bug-Bounty-Programme ermöglichen öffentliche Fehleranalysen. Diese Leistungen sind wertvoll. Sie geben der Öffentlichkeit aber noch keinen selbständig nutzbaren Beweisweg vom angenommenen Urnenbestand bis zum Ergebnis. Das ist ein erhebliches demokratisches Kontrolldefizit.[64]

Die Blockchain soll einen gemeinsamen Prüfbestand schaffen. Jede definitiv angenommene Stimme erhält einen geschützten Eintrag. Unabhängige Knoten bewahren denselben überprüfbaren Verlauf; Änderungen und widersprüchliche Fassungen müssen nach den festgelegten Konsensregeln erkennbar sein. Mit den zugehörigen Beweisen lässt sich kontrollieren, ob Stimmen fehlen, ersetzt oder mehrfach berücksichtigt wurden und ob die Auszählung genau auf diesem Bestand beruht. Staat und Anbieter dürfen diesen Prüfbestand weder nachträglich umschreiben noch den alleinigen Zugang dazu kontrollieren.

Jedermann erhält denselben Zugang. Bürgerinnen und Bürger, Hochschulen, Medien, Parteien und private Auditoren sollen die Daten herunterladen, eigene Knoten betreiben und die Prüfung mit eigener Software wiederholen können. Dafür braucht es weder ein staatliches Einzelmandat noch Unterstützung durch die Betreiber. Die Durchführung ist organisatorisch und technisch eigenständig. Offene Spezifikationen und vollständige Belegpakete machen auch konkurrierende Prüfprogramme möglich. Fachkenntnis bleibt nötig; die Erlaubnis zur Kontrolle darf kein Privileg sein.[65]

Der Verlauf wird prüfbar, die Stimmwahl bleibt geheim. Öffentlich nachvollziehbar werden die geschützte Annahme jeder Stimme, die Vollständigkeit des Bestands und die korrekte Auswertung. Politische Einzelentscheidungen, personenbezogene Zugänge und vorzeitige Teilergebnisse bleiben verborgen. Kryptografische Beweise müssen die Prüfung ermöglichen, ohne einen vorzeigbaren Beleg für den Inhalt der eigenen Stimme zu schaffen. Die Aussagen über Berechtigung, Stimmwillen und Zwang benötigen weiterhin die in Kapitel 5.11 bezeichneten zusätzlichen Nachweise.

Demokratische Wirkung. So erhält Vertrauen eine überprüfbare Grundlage. Fehler können unabhängig benannt, unbegründete Manipulationsvorwürfe anhand gemeinsamer Belege zurückgewiesen und Ergebnisse auch gegen politische Interessen bestätigt werden. Dieses Ziel muss die Architektur bestimmen. Solange der offene Auditweg im Konzept fehlt, bleibt die Öffentlichkeit bei der entscheidenden Ergebnisprüfung auf die organisierte Kontrolle anderer angewiesen.

63 Q06 · Post/LORIA, Whitepaper 1.2.1, Kapitel 2.4.4, S. 13, und Kapitel 3.1, S. 14–15: kantonale Ernennung und Auswahl der Auditoren; beschriebenes Protokoll ohne Blockchain-Annahmeweg. Bewertung des dokumentierten Planungsumfangs.

64 Q02 · VEleS, Art. 2 und 5; Q30 · Bundeskanzlei, Überprüfung von Systemen, Abschnitte Voraussetzungen und Überprüfung des Post-Systems, Abruf 09.10.2026. Die Bewertung betrifft den offenen Ergebnis-Auditweg, nicht das Fehlen externer Systemprüfungen.

65 Q28 · ElectionGuard, Creating a Verifiable Election und Election Record: Drittprüfer anhand veröffentlichter Belege als technisches Beispiel. Daraus folgt keine bereits bestehende Schweizer Umsetzung.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

6 Betrieb und Auszählbarkeit

6.1 Der reale Schaden in Basel-Stadt

Am 8. März 2026 konnten in Basel-Stadt 2'048 elektronisch abgegebene Stimmen nicht entschlüsselt und ausgezählt werden. Der Regierungsrat berichtete am 10. März von erfolglosen Wiederherstellungsversuchen, ordnete eine externe Analyse an und setzte den Versuchsbetrieb bis Ende 2026 aus. Er führte den Vorfall auf die Handhabung einer externen USB-Komponente zurück und grenzte ihn ausdrücklich vom bereitgestellten Post-Produkt ab.[66]

Die Bundeskanzlei konkretisierte am 17. April den Umgang mit PIN-geschützten USB-Sticks als Ursache. Für die weiter beteiligten Kantone wurden Abläufe überprüft und unter anderem zusätzliche Speicherarten und Checklisten vorgesehen. Sie hielt einen gleichartigen erneuten Vorfall aufgrund der geprüften Abläufe für sehr unwahrscheinlich.[67]

Diese amtliche Ursachenzuordnung ist ernst zu nehmen. Für die politische Rechteausübung bleibt jedoch der gesamte Ablauf massgeblich: Eine Stimme, die wegen eines externen Datenträgers nicht gezählt werden kann, ist für die betroffene Person ebenso verloren wie eine Stimme, die wegen eines Softwarefehlers nicht gezählt wird. Die Studie ordnet den Fall deshalb als Versagen der betrieblichen Auszählbarkeit ein, ohne ihn fälschlich zu einem nachgewiesenen Fehler der Post-Kryptografie oder zu einem Hackerangriff umzudeuten.

6.2 Vieraugenkontrolle braucht eine Wiederherstellungsprobe

Eine Checkliste kann verhindern, dass Arbeitsschritte vergessen werden. Sie belegt nicht, dass Daten nach einem Gerätefehler, einer PIN-Sperre oder dem Ausfall einer Schlüsselperson tatsächlich verfügbar bleiben. Ein Wiederherstellungsplan wird erst durch eine praktisch durchgeführte Übung belastbar.

Vor jedem Einsatzzyklus sollen die Kantone mit der tatsächlich vorgesehenen Hardware, den Rollen und den gesicherten Verfahrensständen einen vollständigen Testlauf mit Teststimmen durchführen. Dabei wird mindestens ein primärer Datenträger absichtlich als nicht verfügbar angenommen; ebenso wird der Ausfall einer berechtigten Person simuliert. Der Lauf muss vom versiegelten Ausgangsmaterial bis zu einem vollständig überprüfbaren Ergebnis führen. Die reale geheime Stimmabgabe darf dabei weder vorzeitig entschlüsselt noch für Trainingszwecke kopiert werden.

Redundanz darf die Geheimhaltung nicht unterlaufen. Ein zentraler Hauptschlüssel als bequeme Sicherung würde die Trennung der Schlüsselverantwortung schwächen. Sicherungen müssen deshalb innerhalb des jeweiligen kryptografischen Schwellen- und Rollenmodells gestaltet, getrennt verwahrt und kontrolliert wiederhergestellt werden. Eine technische Lösung, die nur verfügbar oder nur vertraulich ist, genügt nicht.

6.3 Ein Ausfall ist auch eine Frage des Wahlrechts

Für den Ausfall vor der Stimmabgabe, während der Öffnungszeit und nach der elektronischen Registrierung sind unterschiedliche Verfahren erforderlich. Vor Registrierung kann unter geeigneten rechtlichen und organisatorischen Bedingungen ein anderer Kanal angeboten werden. Nach Registrierung darf eine zusätzliche Papierstimme nicht ohne geregelte Sperr- und Abgleichlogik angenommen werden: Sonst entstehen Doppelstimmen oder widersprüchliche Gültigkeitsentscheidungen.

[66] Q09 · Regierungsrat Basel-Stadt, Originalmitteilung vom 10.03.2026, Vorfall und Aussetzung.
[67] Q20 · Bundeskanzlei, Zulassungen für 14.06.2026, Originalmitteilung vom 17.04.2026.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

Ein pauschales Versprechen, bei technischen Schwierigkeiten auf Papier zurückzufallen, ist deshalb unzureichend. Die Unterlagen müssen festlegen, ab wann eine Stimme registriert ist, welche Alternative zu welchem Zeitpunkt noch zulässig ist und wer bei widersprüchlichen Zuständen entscheidet. Diese Regeln sind vor dem Ereignis rechtlich und betrieblich zu prüfen und den Stimmberechtigten verständlich mitzuteilen.

Ob ein Ausfall eine Wiederholung oder Aufhebung eines Ergebnisses verlangt, hängt vom anwendbaren Recht und vom konkreten Fall ab. Ein mathematisch möglicherweise entscheidender Stimmenumfang ist ein wichtiger Prüfpunkt, aber keine automatisch geltende Aufhebungsregel. Die Bundeskanzlei behandelt diesen Zusammenhang im Risiko des Verlusts abgegebener Stimmen.[68]

6.4 Zuständigkeit und überprüfbare Verbesserung

Der Kanton verantwortet den Urnengang und seine betrieblichen Abläufe. Die Post muss die sichere Bedienbarkeit und Dokumentation ihres Produkts unterstützen. Die unabhängige Prüfung bewertet, ob die gemeinsame Prozessgestaltung einzelne plausible Fehlhandlungen abfängt. Keine dieser Verantwortungen darf durch den Hinweis aufgehoben werden, ein anderer Beteiligter habe den letzten Bedienfehler begangen.

Als Erfolg gilt nicht «alle Mitarbeitenden geschult», sondern ein unabhängig beobachteter, fehlerbehafteter Probelauf mit erfolgreicher Wiederherstellung und vollständig erklärbaren Prüfergebnissen. Für Basel-Stadt ist zusätzlich ein nachvollziehbarer Abschluss der Ursachen- und Massnahmenprüfung erforderlich. Die ausgewerteten Mitteilungen über die angeordnete Untersuchung ersetzen keinen Abschlussbericht; dessen vollständige Ergebnisse werden hier nicht vorweggenommen.

7 Stimmgeheimnis und demokratische Wirksamkeit

7.1 Menschen sind Teil des Nachweises

Die individuelle Verifizierbarkeit setzt voraus, dass Stimmberechtigte die vorgesehenen Prüfschritte verstehen, tatsächlich ausführen und bei Abweichungen wirksam reagieren können. Ein technisch korrekter Vergleichscode schützt wenig, wenn die Benutzeroberfläche zum unbesehenen Bestätigen verleitet, der Vergleich abgebrochen wird oder eine Meldung im Support als gewöhnliches Bedienproblem verschwindet. Die Bundeskanzlei führt die ungenügende Wirksamkeit der Verifizierbarkeit als eigenes Risiko R2.[69]

Erforderlich sind beobachtete Nutzungsstudien mit realistischen Aufgaben und verschiedenen Zielgruppen. Gemessen werden sollen Verständnis, tatsächliche Prüfung, Fehlinterpretationen, Barrieren und die erfolgreiche Bearbeitung eines simulierten Widerspruchs. Die Studie soll auch zeigen, ob die Instruktionen in allen eingesetzten Sprachen und mit assistiven Technologien funktionieren. Eine reine Zufriedenheitsbefragung oder ein barrierefrei lesbarer Startbildschirm reicht nicht.

Aus diesen Ergebnissen sind Mindestanforderungen an die Bedienung abzuleiten. Dabei dürfen keine individuellen politischen Präferenzen erfasst werden. Testvorlagen und Teststimmen ermöglichen die Untersuchung ohne reale Wahlentscheidungen. Wie hoch eine ausreichende Erkennungsleistung sein muss, ist vor der Studie anhand des Bedrohungsmodells festzulegen; eine nachträglich dem Ergebnis angepasste Schwelle wäre kein belastbarer Nachweis.

[68] Q04 · Bundeskanzlei, Risikobeurteilung 2026-4, 29.09.2026, S. 2–12, 31 sowie die bezeichneten Einzelrisiken.
[69] Q04 · Bundeskanzlei, Risikobeurteilung 2026-4, 29.09.2026, S. 2–12, 31 sowie die bezeichneten Einzelrisiken.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

7.2 Authentisierung und E-ID lösen verschiedene Probleme

Starke Authentisierung kann bestimmte Formen des Missbrauchs fremder Zugangsdaten erschweren. Sie beweist nicht, dass eine Person unbeobachtet und ohne Druck abstimmt. Auch ein erfolgreich authentisiertes Gerät kann kompromittiert sein. Deshalb darf eine E-ID nicht als universelle Lösung für Integrität, freie Willensbildung und Auszählbarkeit präsentiert werden.

Haines und Müller diskutieren 2026 die Einführung eines eGovToken als zusätzliche Authentisierungsmöglichkeit. Müller empfiehlt, auch eine direkte SSO-Anbindung zu prüfen, um starke Authentisierung nicht unnötig in ein schwächeres, von Menschen zu übertragendes Geheimnis zu verwandeln. Solche Änderungen bringen zugleich neue Schnittstellen, Abhängigkeiten und Datenschutzfragen mit sich.[70,71]

Für eine E-ID-Integration sind mindestens die Trennung von Identität und Stimmabgabe, Datenminimierung, Protokollierung, Ausfall des Identitätsdienstes, Kontowiederherstellung und alternative Zugänge zu prüfen. Die Identitätsprüfung soll die Berechtigung bestätigen, ohne einen nachträglich verknüpfbaren Nachweis der konkreten Stimme zu erzeugen. Eine dauerhafte Identitätssignatur über den politischen Inhalt wäre gerade kein geeigneter Sicherheitsgewinn.

Die Bundesverwaltung teilte Ende Juni 2026 eine Verzögerung der E-ID-Einführung mit; für die Vertrauensinfrastruktur wurde das erste Halbjahr 2027 als voraussichtlicher Termin genannt. Eine sofortige Sanierung des E-Votings darf daher nicht von einer vermeintlich bereits allgemein verfügbaren E-ID abhängen. Die VEleS erlaubt unabhängige Authentisierungsmittel, verlangt aber eine vertiefte Risikoprüfung ihrer Auswirkungen auf Stimmrechtsprüfung und Geheimhaltung.[72,73]

Eine obligatorische biometrische Prüfung wird hier nicht empfohlen. Ihre Wirksamkeit gegen Zwang, Identitätsmissbrauch und kompromittierte Endgeräte wäre gesondert zu belegen. Zugleich wären Ausschlussrisiken, Datenschutz, Fehlerquoten und Wiederherstellungsverfahren zu bewerten. Eine zusätzliche sensible Datenverarbeitung ist kein Sicherheitsnachweis aus sich selbst heraus.

7.3 Freie Stimmabgabe und organisierter Missbrauch

Remote-E-Voting findet ausserhalb einer kontrollierten Wahlkabine statt. Personen können unter Druck stehen, Zugangsdaten weitergeben oder Geräte Dritter verwenden. Briefliche Stimmabgabe kennt ebenfalls Risiken ausserhalb der Wahlkabine. Der relevante Vergleich betrifft deshalb Reichweite, Automatisierbarkeit, Erkennbarkeit und Möglichkeiten der Abhilfe, nicht ein idealisiertes risikoloses Papierverfahren.

Die Bundeskanzlei berücksichtigt systematisches Sammeln beziehungsweise missbräuchliches Nutzen von Stimmzugängen als eigenes Risiko. Eine technische Massnahme, die Identität strenger prüft, kann einen Teil des Missbrauchs erschweren und gleichzeitig neue Möglichkeiten der Überwachung schaffen. Sicherheitsziele müssen deshalb gemeinsam bewertet werden.[74]

Für die Praxis sind verständliche Hinweise zur persönlichen Verfügung über die Zugangsmittel, unabhängige Meldestellen und ein klar geregeltes Verfahren bei vermutetem Missbrauch erforderlich. Mechanismen wie

[70] Q15 · Haines, Prüfbericht zu Release 1.5.4, 16.06.2026, S. 1–5.
[71] Q16 · Müller, Prüfbericht zu Release 1.5.4, 15.06.2026, S. 1–2.
[72] Q21 · Bundesverwaltung E-ID, Neuer Zeitplan, veröffentlicht 30.06.2026.
[73] Q02 · VEleS, SR 161.116, Stand 01.07.2022; jeweils im Text bezeichnete Artikel und Anhangsziffern.
[74] Q04 · Bundeskanzlei, Risikobeurteilung 2026-4, 29.09.2026, S. 2–12, 31 sowie die bezeichneten Einzelrisiken.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

erneute Stimmabgabe oder Kanalwechsel dürfen nur nach vollständiger Prüfung ihrer rechtlichen, kryptografischen und betrieblichen Folgen eingeführt werden. Sie sind keine beiläufige Erweiterung der Benutzeroberfläche.

7.4 Öffentliche Nachprüfbarkeit ohne Beweis der eigenen Wahl

Mehr Transparenz bedeutet nicht, sämtliche Daten eines Urnengangs unterschiedslos zu veröffentlichen. Identifikatoren, Zeitstempel, individuelle Belege und verschlüsselte Stimmen können in Kombination Rückschlüsse ermöglichen oder langfristige Geheimhaltungsrisiken schaffen. Ein öffentlich vorzeigbarer Nachweis der gewählten Option würde zudem Druck und Stimmenkauf erleichtern. Art. 4 VEleS führt den Schutz vor missbräuchlicher Verwendung von Beweisen zum Stimmverhalten ausdrücklich als Sicherheitsziel auf.[75]

Empfohlen wird ein abgestuftes Nachweismodell. Öffentlich sind das freigegebene Systeminventar, zusammengefasste Prüfberichte, nachvollziehbare Freigabeentscheide und solche kryptografischen Belege zugänglich, deren Veröffentlichung unabhängig auf Geheimhaltungs- und Verknüpfungsrisiken geprüft wurde. Besonders sensible Rohdaten bleiben während der zulässigen Frist kontrolliert zugänglich für legitimierte Prüf- und Rechtsmittelstellen.

Das Prüfwerkzeug allein schafft noch keine unabhängige Nachprüfbarkeit. Es braucht authentische Eingangsdaten, eine vollständige Spezifikation der zu beweisenden Aussage und eine vom Hersteller hinreichend unabhängige Durchführung. Wenn dieselbe Organisation Daten auswählt, das einzige Prüfprogramm liefert und das Ergebnis abschliessend erklärt, bleibt die Kontrolle institutionell schwach. M15/M16 verlangen deshalb einen eigenständigen Prüfweg mit unabhängig verfügbaren Belegen, eigenen Blockchain-Knoten und eigener Prüfsoftware; siehe Kapitel 5.11.

7.5 Beweissicherung und Löschung sorgfältig vereinbaren

Die Aussage, sämtliche Abstimmungsdaten würden unmittelbar und unterschiedslos gelöscht, ist zu pauschal. Anhang Ziffer 12.8 VEleS betrifft nach der Erwahrung die Vernichtung der als vertraulich klassifizierten Daten mit Bezug zu einzelnen eingegangenen Stimmen. Ziffer 3.12 regelt kritische Daten nach Verwendung und erlaubt bei guten Gründen auch eine sichere Aufbewahrung des Datenträgers. Aus diesen Regeln lässt sich kein Verbot jeder späteren öffentlichen Verfahrensdokumentation ableiten.[76]

Ein Aufbewahrungskonzept muss Datenarten, rechtliche Fristen, Zugriffsberechtigte, Integritätsschutz und Löschereignisse getrennt festlegen. Öffentliche Prüfberichte und unkritische Nachweise können anders behandelt werden als geheime Schlüssel oder individuelle Stimmbezüge. Bei offenen Rechtsmitteln oder Vorfällen ist vor der Löschung zu klären, welche Sicherung rechtlich geboten und zulässig ist. Eine pauschale Vorratsspeicherung zur angeblichen Sicherheit würde das Geheimhaltungsrisiko unnötig vergrössern.

7.6 Langfristige Geheimhaltung

Die Bundeskanzlei berücksichtigt neue Technologien und die daraus entstehenden Risiken für das Stimmgeheimnis, einschliesslich der Entwicklung leistungsfähiger Quantencomputer. Ein heute vertraulich gespeicherter Datensatz kann langfristig anders zu bewerten sein. Daraus folgt eine Pflicht zur

[75] Q02 · VEleS, SR 161.116, Stand 01.07.2022; jeweils im Text bezeichnete Artikel und Anhangsziffern.
[76] Q02 · VEleS, SR 161.116, Stand 01.07.2022; jeweils im Text bezeichnete Artikel und Anhangsziffern.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

Datenminimierung und zu einem vorbereiteten Migrationskonzept, aber kein Beleg dafür, dass die gegenwärtige Verschlüsselung bereits gebrochen sei.[77]

Eine Migration auf neue kryptografische Verfahren ist selbst sicherheitskritisch. Sie verlangt neue Spezifikationen, Beweise, Implementierungsprüfungen und Leistungsnachweise. Die Bezeichnung «post-quanten-sicher» darf nicht als Beschaffungsversprechen genügen. Für den konkreten Wahlprozess müssen auch Verifizierbarkeit, Schlüsselverwaltung und die Folgen gemischter Verfahren untersucht werden.

8 Gesamtrisikoregister

8.1 Bewertungslogik

Das Register bündelt die eigenen Bewertungen dieser Studie. **Priorität A** bedeutet: vor Ausweitung beziehungsweise vor Einsatz einer betroffenen Konfiguration verbindlich entscheiden und nachweisen. **Priorität B** bedeutet: mit festem Auftrag bearbeiten und in die Freigabeprüfung einbeziehen. Die Einstufung behauptet keine statistisch bekannte Eintrittswahrscheinlichkeit. Ein B-Risiko wird zum unmittelbaren Freigabehindernis, sobald konkrete Hinweise auf eine Verletzung eines massgeblichen Sicherheitsziels vorliegen.

«Nachweis offen» bedeutet, dass die ausgewerteten öffentlichen Quellen die vollständige Erledigung für den bezeichneten Gegenstand nicht zeigen. Es bedeutet nicht zwingend, dass intern kein Nachweis existiert. Die jeweils zuständige Stelle muss diese Lücke durch überprüfbare Unterlagen schliessen.

ID und Priorität	Risiko und Evidenzlage	Verantwortung und geforderter Nachweis
R01 · A	Rollenkumulation und Selbstprüfung. Institutionelle Nähe ist dokumentiert; konkrete unzulässige Einflussnahme ist nicht bewiesen.	Bund und Kantone: Rollenmatrix, Interessenregister, Ausstandsentscheide, unabhängige Schlussabnahme.
R02 · A	Verlust der Auszählbarkeit. In Basel-Stadt real eingetreten; amtliche Gegenmassnahmen beschrieben.	Kanton mit Post: beobachtete Wiederherstellung trotz Datenträger- und Personalausfall.
R03 · A	Entwurfsfehler in System 2.0. Originalbefunde zu 1.2; Herstellerkorrektur 1.2.1 vorhanden.	Post und getrennte Prüfergruppe: unabhängiger Abschluss aller sicherheitskritischen Befunde vor Einsatz.
R04 · A	Abweichung zwischen geprüftem, zugelassenem und betriebenem Stand. Von der BK als relevantes Risiko geführt.	Anbieter, Betreiber und Freigabestelle: durchgehende Zuordnung von Quellcode, Build, Konfiguration und Installation.
R05 · A	Unwirksame Verifizierbarkeit im tatsächlichen Ablauf. Als BK-Risiko erfasst; kein pauschaler Nachweis des Versagens.	Kantone und unabhängige Usability-Prüfung: gemessene Fehlererkennung und funktionierender Meldeweg.
R06 · A	Gemeinsame Fehlerursachen in Kontrollkomponenten und Prüfhilfsmitteln. Strukturelles Risiko trotz formaler Mehrfachheit.	Architektur- und Betriebsprüfung: dokumentierte technische und administrative Unabhängigkeit.
R07 · B	Kompromittierte Endgeräte, Phishing und Behördenportal-Schnittstellen. Prüfumfänge decken nicht jeden realen Angriffspfad ab.	Kanton und Anbieter: vollständiges Schnittstellenmodell, eigene Prüfung neuer Authentisierung und klarer Zuständigkeitsübergang.
R08 · B	Offenlegung des Stimmgeheimnisses durch Druck, Datensammlung oder unbedachte Transparenz. Vertrauensannahmen amtlich anerkannt.	Kantone, Druckstellen und Datenschutzprüfung: Datenflussmodell, Datenminimierung und getestete Vertraulichkeitskontrollen.
R09 · B	Zwang und organisierter Zugangsmissbrauch. Im Fernwahlumfeld relevant; E-ID allein beseitigt das Risiko nicht.	Bund und Kantone: rechtlich geprüftes Schutz- und Meldekonzept, Vergleich mit anderen Stimmkanälen.
R10 · B	Politisch motivierter Ausfall, insbesondere Verfügbarkeitsangriffe. In der BK-Beurteilung besonders hervorgehoben.	Betreiber und Kanton: unabhängige Last- und Ausfallprüfung, klare Ersatz- und Kommunikationsverfahren.
R11 · B	Anbieter- und Expertenabhängigkeit. Ein eingesetzter Anbieter und knappe Fachkompetenz sind dokumentiert.	Auftraggeber: Wissenstransfer, nutzbare Dokumentation, vertraglicher Exit und unabhängige Befähigung.
R12 · B	Lieferketten- und Administrationsrisiken. Produktcode ist nur ein Teil des betriebenen Systems.	Anbieter und Betreiber: Abhängigkeitsinventar, authentische Artefakte, getrennte Zugänge und Nachweise für Änderungen.
R13 · B	Unzureichende Beweissicherung oder übermässige Aufbewahrung. Rechtliche Schutzgüter können kollidieren.	Kanton mit Rechts- und Datenschutzstellen: differenzierter Aufbewahrungs- und Löschplan für Normal- und Störfälle.

[77] Q04 · Bundeskanzlei, Risikobeurteilung 2026-4, 29.09.2026, S. 2–12, 31 sowie die bezeichneten Einzelrisiken.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

ID und Priorität	Risiko und Evidenzlage	Verantwortung und geforderter Nachweis
R14 · B	Kostenbindung und automatischer Weiterbau. Ohne Vergleich kann ein schwacher Pfad aus Gewohnheit fortgeführt werden.	Politische Auftraggeber: vollständige Kostenrechnung, Nutzenvergleich und finanzierter Ausstiegspfad.
R15 · B	Langfristiger Bruch kryptografischer Annahmen. Anerkanntes Zukunftsrisiko ohne belastbaren Eintrittstermin.	Anbieter und Bund: Datenminimierung, beobachtete Entwicklung und unabhängig geprüfter Migrationsplan.
R16 · A	Unvollständige Prüfung bestimmter Wahlregeln vor Registrierung und begrenzte Nutzbarkeit. Hersteller- und kantonale Originalangaben, Kapitel 5.7.	Wahlbehörden und Anbieter: vollständige Funktionsmatrix, fachlich geprüfte Regeln und nachgewiesene Fehlerbehandlung vor einer Ausweitung.

Die tatsächlichen Grundlagen für R01 bis R06 stehen in Kapitel 4 bis 6, für R07 bis R10 und R13 bis R15 in Kapitel 7 und der amtlichen Risikobeurteilung. R11 und R14 sind zusätzlich eine eigene wirtschaftliche und institutionelle Bewertung des dokumentierten Einanbieterbetriebs.[78,79]

8.2 Drei gekoppelte Krisenszenarien

Szenario A: Ein plausibler Fehler kurz vor Öffnung des Kanals. Die Post hält ihn für lokal begrenzt, ein externer Prüfer für potenziell ergebnisrelevant. Ohne getrennte Entscheidungsbefugnisse entsteht Druck, den geplanten Urnengang nicht zu gefährden. Abhilfe: Originalbefund und Gegenargumente gehen gleichzeitig an eine unabhängige Fachgruppe und die zuständige Freigabestelle. Bleibt ein kritischer Widerspruch bis zur Freigabe ungeklärt, wird die betroffene Konfiguration nicht eingesetzt.

Szenario B: Ein gemeinsamer Dienst fällt während der Stimmabgabe aus. Mehrere Kantone nutzen dieselbe technische Grundlage. Ein geringer schweizweiter Nutzungsanteil begrenzt nicht zwingend die lokale Bedeutung. Abhilfe: getrennte Fehlerbereiche, vorab geübte Betriebsentscheidungen, klare Mitteilungen und ein rechtlich geprüftes Verfahren für Personen, deren Registrierung unklar ist. Ein spontan eingeführter zweiter Stimmkanal ist keine sichere Lösung.

Szenario C: Ein Ergebnis ist technisch prüfbar, öffentlich aber nicht erklärbar. Widersprüchliche Aussagen über Versionen, Prüfdaten oder offene Befunde erschweren die Nachvollziehbarkeit. Abhilfe: ein gemeinsam referenziertes Nachweispaket und eine öffentliche, verständliche Begründung des Freigabeentscheids. Vertrauliche Details bleiben geschützt; die Begründung der Entscheidung darf deshalb nicht verschwinden.

Diese Szenarien sind analytische Konstruktionen, keine Behauptungen über bereits eingetretene Ereignisse. Sie zeigen, weshalb Governance, Technik und Betrieb nicht in voneinander isolierten Risikoregisterzeilen abgearbeitet werden dürfen.

9 Handlungsoptionen

9.1 Vier Wege im Vergleich

Option	Nutzen und Voraussetzung	Hauptrisiko und Entscheidung
A · Unverändert fortsetzen und ausweiten	Geringer kurzfristiger Umstellungsaufwand; nutzt vorhandene Organisation.	Erhöht Exposition, bevor kritische Nachweise geschlossen sind. Diese Studie empfiehlt die Option nicht.
B · Stabilisieren und unabhängig nachweisen	Bestehende Investitionen bleiben nutzbar; klar begrenzte Versuche liefern überprüfbare Erkenntnisse.	Scheitert, wenn Nachweislücken wiederholt ohne Abschluss vertagt werden. Empfohlener erster Schritt mit verbindlichen Sperren.

[78] Q04 · Bundeskanzlei, Risikobeurteilung 2026-4, 29.09.2026, S. 2–12, 31 sowie die bezeichneten Einzelrisiken.

[79] Q10 · Bundeskanzlei, Vote électronique, Projektziele und Aktueller Stand, Abruf 09.10.2026.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

Option	Nutzen und Voraussetzung	Hauptrisiko und Entscheidung
C · Grundlegend neu entwerfen oder Anbieter wechseln	Kann strukturelle Vertrauensannahmen und Komplexität reduzieren.	Neuer Entwicklungs- und Nachweisaufwand; ein Neubau kann dieselben Fehler wiederholen. Nur nach unabhängigem Vergleich freigeben.
D · Remote-E-Voting geordnet beenden	Entfernt die spezifische digitale Angriffs- und Betriebsfläche.	Verliert bestimmte Zugangs- und Komfortvorteile. Alternative Stimmwege müssen gezielt verbessert werden.

Die Optionen sind nicht symmetrisch teuer oder gleich weit entwickelt. Ohne belastbare Angebote, Betriebskosten und Nutzungsdaten wäre eine zahlenmässige Rangfolge Scheingenauigkeit. Der Vergleich muss dieselben Schutzziele und denselben Zeithorizont verwenden. Versunkene Entwicklungskosten dürfen eine künftige unsichere Fortführung nicht rechtfertigen.

9.2 Warum Stabilisierung zuerst sinnvoll ist

Eine zeitlich begrenzte Stabilisierung kann die wichtigsten Unsicherheiten klären, ohne sofort einen weiteren langfristigen Entwicklungspfad festzuschreiben. Sie finanziert vor allem unabhängige Prüfung, betrieblichen Nachweis, Dokumentation und sichere Fehlerbehebung. Funktionsausbau und zusätzliche Abhängigkeiten werden zurückgestellt, soweit sie nicht für die Behebung eines nachgewiesenen Sicherheitsproblems erforderlich sind.

Der Vorschlag ist nur glaubwürdig, wenn er ein Ende besitzt. Nach der in Kapitel 11 vorgeschlagenen ersten Nachweisphase muss eine öffentliche Entscheidung vorliegen: Welche Bedingungen sind erfüllt, welche nicht, und rechtfertigt der verbleibende Nutzen die verbleibenden Risiken? Ein wiederholtes Verschieben desselben kritischen Nachweises ist ein Argument für Aussetzung oder Ausstieg, nicht für eine automatische nächste Verlängerung.

9.3 Voraussetzungen für einen Neustart

Ein Ersatzprojekt beginnt mit Anforderungen und Bedrohungsmodell, nicht mit der Wahl einer Programmiersprache. Es muss zeigen, welche bisher nötigen Vertrauensannahmen entfallen, welche neuen Annahmen hinzukommen und wie sich der Nachweisaufwand verändert. Herstellerunabhängige Schnittstellen, offen prüfbare Spezifikationen und praktisch nutzbare Rechte an den relevanten Artefakten sind bereits bei der Beschaffung zu regeln.

Eine neue Implementierung allein beseitigt keine strukturelle Selbstprüfung. Dieselbe Organisation, die eine bevorzugte Architektur auswählt und entwickelt, darf nicht allein über deren endgültige Eignung entscheiden. Auch ein staatliches oder vollständig quelloffenes System benötigt eine getrennte Abnahme. Offenlegung verbessert Prüfbarkeit, ersetzt aber weder fachliche Kapazität noch betriebliche Beweise.

System 2.0 ist daher als mögliche technische Option zu bewerten, nicht als bereits entschiedene Rettung. Vor einer produktiven Einführung müssen die Erkenntnisse der Whitepaper-Prüfung in Spezifikation, Implementierung und Betrieb vollständig durchgearbeitet werden. Der Wechsel einer Versionshauptnummer ist kein eigenständiger Sicherheitsnachweis.

9.4 Ein geordneter Ausstieg ist eine vollwertige Option

Ein Ausstieg muss die laufenden Urnengänge, die Beweissicherung, gesetzliche Aufbewahrung und Geheimhaltung sowie bestehende Verträge berücksichtigen. Er bedeutet keine ungeplante Abschaltung während der Stimmabgabe. Zunächst wird die sichere Abwicklung oder Beendigung der jeweils betroffenen Verfahren geregelt, dann die Infrastruktur zurückgebaut.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

Für Auslandschweizerinnen und Auslandschweizer sind die tatsächlichen Ursachen verspäteter Stimmabgabe zu erheben und die rechtlich möglichen Verbesserungen des physischen Stimmwegs zu prüfen. Für Menschen mit Behinderungen sind autonome und geheime Alternativen gemeinsam mit Betroffenen zu entwickeln. Ein Wegfall des digitalen Kanals ist politisch nur tragfähig, wenn solche Nachteile offen ausgewiesen und nach Möglichkeit konkret vermindert werden.

Der Optionsvergleich soll deshalb nicht nur Kosten je elektronischer Stimme berechnen. Er soll auch fragen, für welche Personengruppen der Kanal einen nachgewiesenen zusätzlichen Zugang schafft und wie teuer gleichwertige Alternativen wären. Die Bundeskanzlei nennt Barrierefreiheit und das Verhindern postalischer Verspätungen als Projektziele; deren tatsächliche Erfüllung ist empirisch zu prüfen.[80]

10 Verbindliche Freigabebedingungen

10.1 Bestehendes Recht und vorgeschlagene Verschärfung

Art. 3 VEleS verlangt unter anderem eine sichere, vertrauenswürdige und nachvollziehbare elektronische Stimmabgabe. Art. 9 fordert zusätzliche Massnahmen, wenn die Risiken trotz Einhaltung der Anhangsanforderungen nicht hinreichend gering sind. Die Erfüllung einer Checkliste befreit somit nicht von der Gesamtbeurteilung.[81]

Die folgenden Bedingungen sind ein Vorschlag dieser Studie zur operativen Umsetzung und teilweise zur Verschärfung des Nachweises. Sie werden nicht als bereits vollständig geltender Verordnungstext ausgegeben. Ihre rechtsverbindliche Einführung ist durch die zuständigen Stellen zu prüfen.

Bedingung	Erforderlicher Nachweis	Folge bei Nichterfüllung
G1 · Unabhängige Entscheidung	Interessenregister, Ausstände und getrennte Schlussprüfung sind dokumentiert.	Keine Freigabe der betroffenen neuen Version oder Ausweitung.
G2 · Geschlossener kritischer Befund	Kritische Gegenbeispiele sind versionsgenau bewertet; Korrekturen unabhängig bestätigt.	Betroffene Konfiguration aussetzen; kein Einsatz auf Basis einer blossen Herstellerzusage.
G3 · Identischer Systemstand	Zugelassener, geprüfter und installierter Stand samt relevanter Konfiguration stimmen nachweislich überein.	Öffnung des Kanals unterbleibt bis zur Klärung.
G4 · Auszählbarkeit	Wiederherstellung bei plausiblen Geräte- und Personalausfällen erfolgreich geübt.	Kein Einsatz des nicht ausreichend abgesicherten Ablaufs.
G5 · Wirksame Verifikation	M15/M16: Drittprüfung auf eigener Infrastruktur; bestätigter Blockchain-Eintrag je angenommener Stimme; vollständiger Abgleich mit Urne und Auszählung.	Keine Freigabe, solange das Sicherheitsziel nicht nachgewiesen ist.
G6 · Geheimhaltung und Rechtsmittel	Datenflüsse, Aufbewahrung, Löschung und Beweissicherung sind gemeinsam geprüft.	Keine zusätzliche Datenerhebung oder Veröffentlichung ohne ausreichende Grundlage.
G7 · Sicherer Störfall	Entscheidungen, Kommunikationswege und rechtlich zulässige Alternativen sind vorab geübt.	Kein Betrieb mit ungeklärter Doppelstimmen- oder Registrierungsproblematik.
G8 · Begründete Risikoakzeptanz	Zuständige Stelle benennt verbleibende Risiken, Umfang, Dauer und Widerrufsauslöser.	Keine pauschale oder stillschweigende Verlängerung.
G9 · Vollständiger Vorgang	Wahlregeln, Zugang, mobile Bedienung, Barrierefreiheit und Fehlerbehandlung sind für den Einsatzstand geprüft.	Keine Ausweitung mit unbelegten Funktions- oder Nutzenversprechen.

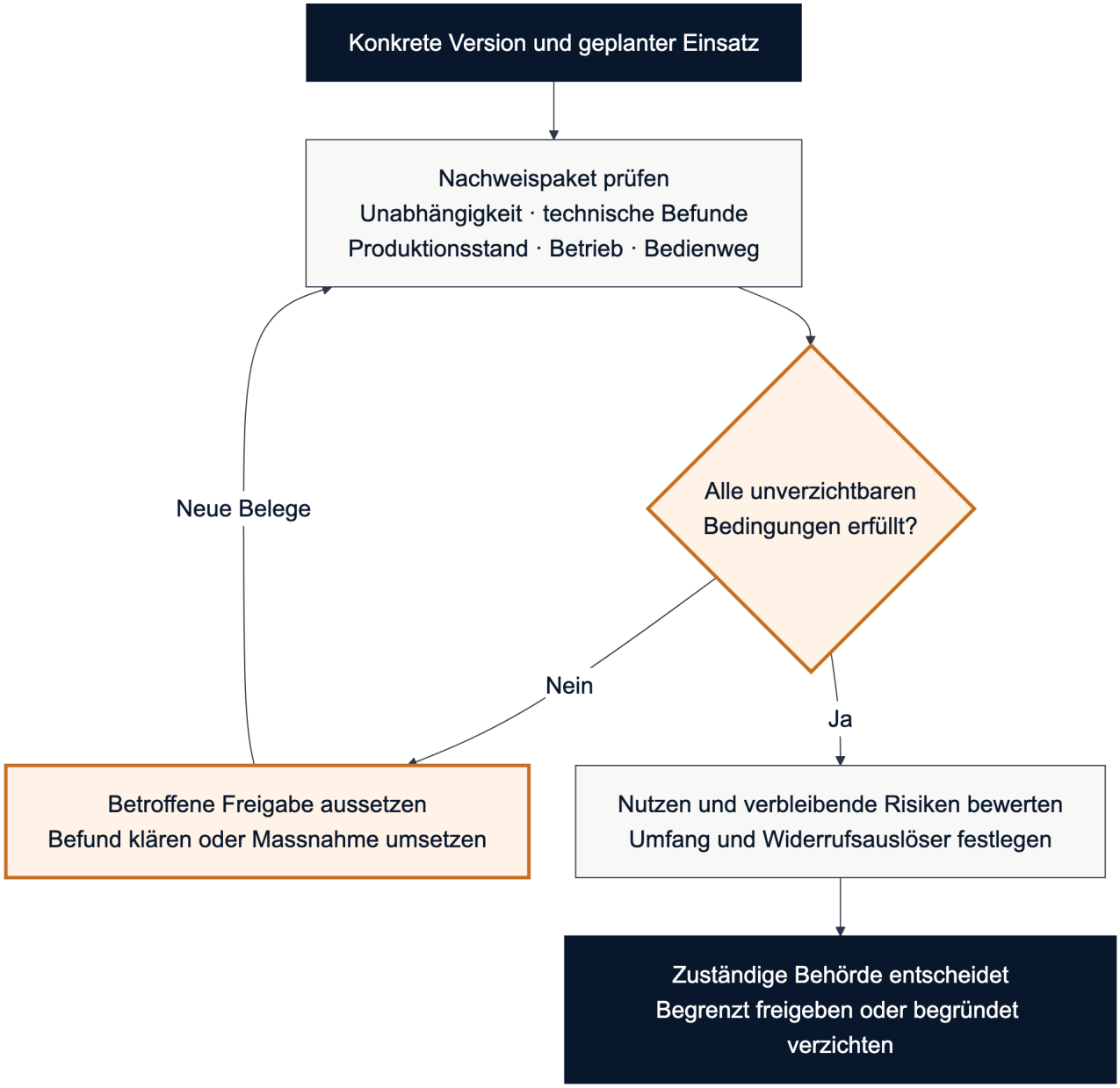
[80] Q10 · Bundeskanzlei, Vote électronique, Projektziele und Aktueller Stand, Abruf 09.10.2026.

[81] Q02 · VEleS, SR 161.116, Stand 01.07.2022; jeweils im Text bezeichnete Artikel und Anhangsziffern.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

Abbildung 5 · Nachweise und Entscheidung über eine Freigabe



Vorgeschlagener Entscheidungsweg zu den Bedingungen G1 bis G9 in Kapitel 10.1. Unverzichtbare Sicherheits- und Rechtsvoraussetzungen können nicht durch Vorteile in anderen Bereichen verrechnet werden. Ein positives fachliches Prüfergebnis ermöglicht die begründete Behördenentscheidung; es bewirkt keine automatische Zulassung.

10.2 Kein Mittelwert über unverzichtbare Sicherheitsziele

Integrität, Geheimhaltung und eine rechtmässige Auszählung sind keine austauschbaren Qualitätsmerkmale. Ein sehr gutes Ergebnis in der Benutzbarkeit darf eine fehlende Geheimhaltung nicht kompensieren. Deshalb eignet sich ein gewichteter Gesamtpunktwert nicht als alleinige Freigaberegel. Zuerst müssen die unverzichtbaren Bedingungen erfüllt sein; erst danach dürfen Nutzen, Kosten und verbleibende Risiken verglichen werden.

Ein Nachweis besitzt ausserdem einen Geltungsbereich. Ändert sich eine wichtige Bibliothek, ein Authentisierungsdienst, der Druckprozess oder die Rollenverteilung, ist zu prüfen, welche früheren Belege weiterhin tragen. Es ist weder nötig, nach jeder kleinen Änderung das gesamte System von null zu prüfen, noch zulässig, alte Freigaben ohne Auswirkungsanalyse auf neue Konfigurationen zu übertragen.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

10.3 Sperren und Eskalation vorab vereinbaren

Jeder sicherheitsrelevante Hinweis erhält eine zuständige fachliche Person, einen nachvollziehbaren Bearbeitungsstatus und eine Frist bis zum nächsten Einsatzentscheid. Als organisatorische Zielwerte werden eine Eingangsbestätigung innerhalb von zwei Arbeitstagen, eine erste fachliche Einordnung innerhalb von zehn Arbeitstagen und ein begründeter Zwischenentscheid innerhalb von 30 Kalendertagen vorgeschlagen. Bei unmittelbar möglicher schwerer Auswirkung muss die Beurteilung schneller erfolgen. Dies sind vorgeschlagene Prozessziele, keine Zusage einer technischen Behebung innert dieser Fristen.

Bei Dissens entscheidet nicht die meldende Person und auch nicht der Hersteller allein. Eine unabhängige fachliche Stelle bewertet die Originalbelege, dokumentiert Gegenargumente und empfiehlt gegebenenfalls eine vorläufige Einsatzsperre. Die rechtlich zuständige Behörde trifft und verantwortet den Entscheid. Die Dringlichkeit eines Wahltermins verändert nicht die technische Gültigkeit eines Gegenbeweises.

11 Umsetzungsprogramm

11.1 Die ersten 30 Tage nach Mandatserteilung

Die folgenden Zeiträume sind vorgeschlagene Arbeitsfenster ab einem künftigen verbindlichen Auftrag. Sie sind keine bereits beschlossenen Termine und keine Prognose, bis wann die Schweiz alle Risiken beseitigt haben wird.

Massnahme	Federführung	Konkretes Ergebnis und Abnahme
M01 · Umfang begrenzen	Zuständige Bundes- und Kantonsstellen	Dokumentierter Vorbehalt für Ausweitungen; laufende Einsätze einzeln anhand kritischer Nachweise beurteilt.
M02 · Rollen offenlegen	Auftraggeber ausserhalb der operativen Projektleitung	Personen- und organisationsbezogene Rollenmatrix; Interessenbindungen und Ausstände bewertet.
M03 · Befunde zusammenführen	Unabhängige fachliche Koordination	Versionsgebundenes Register mit Originalbelegen, Gegenpositionen, Korrekturstand und nächstem Entscheid.
M04 · Originalmeldungen sichern	Zuständige Meldestelle mit Prüfern	Vollständige Belegpakete für strittige Hinweise; keine Einstufung allein aufgrund von Zusammenfassungen.
M05 · Betriebsnachweise sichten	Jeder beteiligte Kanton	Aktuelle Abläufe, Sicherungen, Rollen und letzte Wiederherstellungsübung geprüft; Lücken priorisiert.
M06 · Freigabeprozess festlegen	Rechtlich zuständige Behörde	Bedingungen G1 bis G9 in einem genehmigten Verfahren mit klaren Sperr- und Eskalationswegen umgesetzt.

Der Erfolg dieser ersten Phase liegt in Klarheit und Durchsetzbarkeit. Noch nicht jeder technische Befund muss behoben sein. Es muss aber feststehen, was für den nächsten Einsatz unverzichtbar ist, wer den Nachweis liefert und wer ihn unabhängig beurteilt. Ein unvollständiges Register darf nicht als abgeschlossene Sicherheitsprüfung ausgegeben werden.

11.2 Tage 31 bis 90

Unabhängige technische Abschlussprüfung. Für die in Kapitel 5 bezeichneten sicherheitskritischen Änderungen werden getrennte Prüfaufträge vergeben. Das Ergebnis enthält untersuchte Artefakte, Annahmen, Reproduktionsbelege, verbleibende Unsicherheiten und eine eindeutige Zuordnung zu den Einsatzständen. Eine reine Literaturzusammenfassung ist keine Abnahme.

Kantonale Wiederherstellungsübungen. Jeder künftig eingesetzte Ablauf wird mit repräsentativen Testdaten und real vorgesehenen Rollen durchgespielt. Beobachtet werden Schlüsselzugriff,

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

Datenträgerausfall, Personalausfall, Protokollierung, Verifikation und Entscheidung bei Widersprüchen. Wiederholt wird nur, was nach Korrekturen tatsächlich neu zu prüfen ist.

Prüfung der Selbstprüfungsrisiken. Für jedes Audit wird festgestellt, ob die Gruppe den Prüfgegenstand wesentlich mitgestaltet hat. Gegebenenfalls wird die Schlussprüfung neu zugeteilt. Bestehendes Wissen bleibt nutzbar: Die ursprüngliche Gruppe erklärt Entwurfsentscheidungen und frühere Befunde, erhält aber nicht die alleinige letzte Entscheidung über deren Erledigung.

Erste öffentliche Zwischenbilanz. Veröffentlicht werden die erreichten Nachweise, die verbleibenden Sperren und die begründeten Entscheidungen zum Versuchsumfang. Sensible technische Details werden geschützt. Die Öffentlichkeit muss dennoch erkennen können, ob das Programm tatsächlich Risiken schliesst oder lediglich neue Termine setzt.

11.3 Monate 3 bis 6

In dieser Phase wird der unabhängige Optionsvergleich abgeschlossen. Die Projektleitung liefert Kosten- und Betriebsdaten; mindestens eine vom bisherigen Entwicklungspfad unabhängige Gruppe beurteilt die Alternativen. Vertreter der betroffenen Nutzergruppen wirken an der Nutzenbewertung mit. Die Entscheidungsmatrix enthält unverzichtbare Sicherheitsziele, erwarteten Nutzen, Gesamtkosten, Abhängigkeiten und Rückzugsmöglichkeiten.

Parallel werden die rechtlich und organisatorisch nötigen Anpassungen für eine dauerhafte Trennung von Projektförderung und Freigabe vorbereitet. Dazu gehören Mandatsbedingungen, Publikationsregeln, Ausstandsverfahren und Zugriff auf vollständige Prüfunterlagen. Reine Empfehlungen ohne zuständige Stelle und Finanzierung gelten nicht als umgesetzt.

Am Ende steht ein begründeter Grundsatzentscheid: begrenzt fortsetzen, den Entwicklungspfad ändern oder aussteigen. Bei fortbestehenden kritischen Nachweislücken wird nicht automatisch eine weitere sechsmonatige Phase beschlossen. Der Entscheid muss erklären, welche neuen Erkenntnisse eine Verlängerung überhaupt erwarten lässt und weshalb die verbleibende Exposition verantwortbar ist.

11.4 Monate 6 bis 12

Nur für eine nach den vorherigen Bedingungen gewählte Option beginnt die nächste Umsetzungsphase. Bei Sanierung stehen die nachgewiesene Schliessung verbleibender Befunde und ein begrenzter praktischer Einsatz im Vordergrund. Bei Ersatz folgt ein klar abgegrenzter Entwicklungs- und Prüfauftrag mit eigenem Nachweisplan. Bei Ausstieg werden Verträge, Daten, Infrastruktur und alternative Zugangswege geordnet bearbeitet.

Eine Ausweitung erfolgt schrittweise und an Erkenntnisziele gebunden. Für jeden Schritt ist vorher festzulegen, was gelernt werden soll, wie sich ein unerwarteter Befund auswirkt und wann zum vorherigen Zustand zurückgekehrt wird. Das Ziel ist eine überprüfbare Entscheidung über Eignung, nicht eine steigende Nutzerzahl als Selbstzweck.

11.5 Kennzahlen für die Aufsicht

Kennzahl	Sinnvolle Interpretation	Missverständnis vermeiden
Anteil kritischer Befunde mit unabhängigem Abschluss	Für jeden freizugebenden Stand müssen alle entscheidenden Befunde behandelt sein.	Viele geschlossene Bagatellen kompensieren keinen offenen kritischen Punkt.
Vollständige Zuordnung von Zulassung und Betrieb	Für jeden Einsatz sind Artefakte und relevante Konfiguration nachgewiesen.	Eine Versionsnummer allein beweist keine Produktionsgleichheit.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

Kennzahl	Sinnvolle Interpretation	Missverständnis vermeiden
Erfolgreiche Wiederherstellungsübungen	Alle vorgesehenen kantonalen Abläufe bestehen die definierten Fehlerszenarien.	Eine Vorführung durch den Anbieter ersetzt keine kantonale Übung.
Dauer strittiger Sicherheitsentscheide	Überfällige Fälle lösen Eskalation aus; Gründe bleiben sichtbar.	Kurze Bearbeitungsdauer ist kein Qualitätsbeweis, wenn Hinweise vorschnell verworfen werden.
Nachgewiesene Prüfkompetenz und Ausstände	Jede Schlussprüfung besitzt ausreichende Kompetenz und angemessene Unabhängigkeit.	Rotierende Namen ohne eigene Facharbeit schaffen keine Kontrolle.
Tatsächlicher zusätzlicher Zugang	Nutzen für Zielgruppen ist mit geeigneten Vergleichsdaten belegt.	Registrierungen oder allgemeine Zufriedenheit sind kein Ersatz für wirksame Rechteausübung.

12 Ressourcen und Wirtschaftlichkeit

12.1 Wofür Mittel erforderlich sind

Unabhängigkeit kostet Zeit und fachliche Kapazität. Die Sanierung lässt sich nicht glaubwürdig als zusätzliche Aufgabe derselben bereits ausgelasteten Personen organisieren. Benötigt werden getrennt beauftragte Leistungen für Kryptografie und Protokollanalyse, sichere Software und Lieferketten, kantonale Betriebsprüfung, Gebrauchstauglichkeit und Barrierefreiheit sowie Wahlrecht und Datenschutz. Eine Person muss die Nachweiskette über diese Fachgebiete hinweg koordinieren, ohne dadurch die unabhängige Schlussentscheidung zu ersetzen.

Die Studie setzt bewusst keinen scheinpräzisen Gesamtbetrag an. Die ausgewerteten Originalquellen liefern keine konsolidierte Vollkostenrechnung aller Kantone, des Bundes und des Anbieters für das hier vorgeschlagene Programm. Ein seriöser Budgetbeschluss erfordert Leistungsbeschreibungen, vorhandene Kapazitäten, Angebote, Umstellungsaufwand und einen definierten Zeithorizont.

12.2 Ein prüfbares Kostenmodell

Die Rechnung trennt einmalige Entwicklung und Migration, wiederkehrenden Betrieb, kantonales Personal, unabhängige Prüfung, Druck und Versand, Sicherheitsmanagement, Störfallvorsorge sowie Ausstiegskosten. Dieselben Kategorien werden auf alle Optionen angewandt. Kosten, die auch ohne E-Voting anfallen, sind als gemeinsame Grundkosten kenntlich zu machen.

Zu berichten sind Gesamtkosten, Zusatzkosten gegenüber der Vergleichsoption und Kosten für den nachgewiesenen zusätzlichen Zugang der Zielgruppen. Eine Division durch die Anzahl elektronischer Stimmen kann ergänzen, darf aber den demokratischen Nutzen für kleine Gruppen nicht verdecken. Ebenso wenig darf ein unbestimmter Digitalisierungsnutzen jede Kostensteigerung rechtfertigen.

Eine Sensitivitätsanalyse soll mindestens geringe, mittlere und hohe Nutzung, zusätzlichen Prüfaufwand, Lieferantenwechsel und eine vorzeitige Beendigung untersuchen. Es werden Szenarien ausgewiesen, keine behaupteten Prognosen. Die Entscheidung muss auch dann tragfähig sein, wenn der elektronische Kanal kleiner bleibt als erhofft.

12.3 Vertragsgestaltung und Ausstiegsmöglichkeiten

Auftraggeber müssen prüfen, ob sie über hinreichende Rechte und tatsächlich nutzbare Unterlagen verfügen, um unabhängig zu prüfen, den Betrieb zu verstehen und einen Wechsel oder Ausstieg durchzuführen. Dazu gehören Spezifikationen, Datenformate, Buildanleitungen, Abhängigkeitsstände,

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

betriebliche Dokumentation und die Mitwirkung bei einer geordneten Übergabe. Das Vorliegen veröffentlichter Quelltexte allein beantwortet diese Vertragsfragen nicht.

Ein zweiter Anbieter ist nicht automatisch die Lösung. Zwei Anbieter mit denselben technischen Abhängigkeiten können ähnliche Fehler haben und den Prüfaufwand verdoppeln. Zunächst ist die Fähigkeit der Auftraggeber zu stärken, den bestehenden Anbieter fachlich zu kontrollieren und eine Alternative überhaupt beurteilen zu können. Erst dann lässt sich Wettbewerb sinnvoll gestalten.

13 Beschlussvorschlag und Schlussfolgerung

13.1 Vorschlag für einen politischen Auftrag

Die zuständigen Bundes- und Kantonsstellen sollen ein befristetes Programm zur unabhängigen Neubewertung und Stabilisierung von E-Voting beschliessen. Der Auftrag umfasst die Prüfung der institutionellen Rollentrennung, die versionsgenaue Schliessung kritischer technischer Befunde, praktisch beobachtete Betriebsnachweise und einen ergebnisoffenen Vergleich der Handlungsoptionen. Über zusätzliche Einsätze und Ausweitungen wird erst nach den dazu erforderlichen Nachweisen entschieden.

Die operative Projektleitung und die Post liefern alle notwendigen Unterlagen und wirken an der Fehlerbehebung mit. Die unabhängige Schlussprüfung erhält getrennte Verantwortliche und einen direkten Berichtsweg. Zusätzlich sind die staatsunabhängige Prüfung jedes Urnengangs und der Blockchain-Nachweis jeder definitiv angenommenen Stimme gemäss M15/M16 verbindlich vorzusehen. Die zuständige Behörde veröffentlicht den begründeten Freigabe- oder Sperrentscheid sowie die massgeblichen Restunsicherheiten. Gesetzliche Geheimhaltungs- und Datenschutzpflichten werden durch eine abgestufte Veröffentlichung gewahrt.

Für System 2.0 ist ausdrücklich ein eigener Nachweisweg festzulegen. Die Herstellerkorrektur von Whitepaper 1.2.1 wird unabhängig geprüft, bevor daraus eine tragende Grundlage für weitere Implementierung und spätere Zulassung wird. Ein positiver Entwurfsentscheid ist von der späteren Freigabe implementierter Software und realer Betriebsabläufe zu trennen.

13.2 Wann ein Ausstieg angezeigt ist

Ein geordneter Verzicht ist angezeigt, wenn wesentliche Schutzziele nur mit nicht überprüfbaren Annahmen erreichbar bleiben, kritische Fehler nicht unabhängig geschlossen werden können oder die Auftraggeber auf Dauer keine wirksame Kontrolle aufbauen können. Er ist ebenfalls ernsthaft zu erwägen, wenn der belegte zusätzliche Nutzen die verbleibenden Risiken und Vollkosten gegenüber realistischen Alternativen nicht rechtfertigt.

Ein Neustart ist nur dann eine bessere Entscheidung, wenn sein Vorteil konkret nachgewiesen wird. Der blosse Wunsch nach einem neuen System, einer E-ID oder einer vollständig digitalen Abwicklung ist kein solcher Nachweis. Neue Technik kann einen Teil der heutigen Probleme lösen und zugleich neue Abhängigkeiten schaffen.

13.3 Schlussfolgerung

Die Schweizer E-Voting-Lage verlangt eine institutionelle und technische Korrektur zugleich. Die Quellen zeigen vorhandene unabhängige Prüfungen, substanzielle Verbesserungen und offene wissenschaftliche

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

Kritik. Sie zeigen aber auch, wie stark Sicherheit von der Qualität der Nachprüfung, der realen Rollenverteilung und fehlerverträglichen Betriebsabläufen abhängt.

Die fehlende oder unzureichend abgesicherte Trennung zwischen Entwicklung, Auftrag, Betrieb, Prüfung und Freigabe ist deshalb eines der wichtigsten Querschnittsrisiken. Ihr Gewicht entsteht daraus, dass sie die Behandlung aller anderen Risiken beeinflusst. Wirksame Trennung muss sich an konkreten Entscheidungen zeigen: an einem dokumentierten Ausstand, einem unabhängig widerlegten Fehler, einer verweigerten Freigabe und einer tatsächlich erfolgreichen Wiederherstellungsübung.

Demokratisches Vertrauen verlangt überprüfbare Ergebnisse. Eine Ausweitung ist erst vertretbar, wenn auch frei gewählte Dritte den Urnengang ohne staatliche Hilfe auditieren können. Die fehlende öffentliche Prüfbarkeit ist eine zentrale Lücke des heutigen Konzepts.

14 Anhänge

14.1 Prüfauftrag zur institutionellen Unabhängigkeit

Die unabhängige Untersuchung soll für jeden Beteiligten erfassen, wer Anforderungen formuliert, Architekturentscheidungen trifft, Code entwickelt, Prüfaufträge vergibt, Prüfberichte bezahlt, kritische Befunde bewertet, Ausstände entscheidet, Ergebnisse veröffentlicht und den Einsatz freigibt. Zusätzlich sind tatsächliche technische Befugnisse wie Administrationsrechte, Zugriff auf Schlüsselanteile und Zugriff auf Prüfdaten zu erfassen.

Prüfbare Unterlagen sind Mandatsverträge, Leistungsbeschreibungen, Rollenverzeichnisse, Interessenangaben, Freigabeprotokolle, Befundhistorien und begründete Ausnahmeentscheide. Nicht erforderlich ist eine pauschale Veröffentlichung vertraulicher Personaldaten. Erforderlich ist, dass eine legitime Aufsicht die vollständigen Unterlagen einsehen und die Öffentlichkeit die wesentlichen Schlussfolgerungen nachvollziehen kann.

Das Ergebnis muss konkrete Risiken und konkrete Abhilfen enthalten. Formulierungen wie «enge Zusammenarbeit ist etabliert» oder «alle Beteiligten sind unabhängig» genügen ohne Bezugsobjekt nicht. Für jeden wesentlichen Entwicklungsbeitrag ist zu zeigen, welche andere Stelle dessen abschliessende Prüfung verantwortet.

14.2 Mindestinhalt eines technischen Belegpakets

Bestandteil	Inhalt
Identität	Prüfgegenstand, Versionen, Commits, Prüfsummen, Datum und verantwortliche Personen.
Aussage	Das konkrete Sicherheitsziel und die Behauptung, die geprüft werden soll.
Annahmen	Vertrauenswürdige Komponenten, Angreiferfähigkeiten und betriebliche Voraussetzungen.
Methode	Reproduktionsweg in isolierter Umgebung, Testumfang, Beweisprüfung und Grenzen.
Ergebnis	Beobachtung, Gegenargumente, betroffene Einsatzstände und verbleibende Unsicherheit.
Korrektur	Geänderte Artefakte und Erklärung, weshalb die Ursache behoben wird.
Abschluss	Unabhängige Nachprüfung, Zuständigkeit und begründeter Freigabeentscheid.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

14.3 Begriffe

Vollständige Verifizierbarkeit: Verbindung individueller und universeller Verifizierbarkeit gemäss VEleS. Sie setzt definierte Vertrauensannahmen und eine wirksame Durchführung voraus.

Kontrollkomponenten: Nach VEleS unabhängig ausgestaltete und betriebene Komponenten. Entscheidend ist die begründete Unabhängigkeit, nicht allein ihre Anzahl.

System 1.x und System 2.0: In dieser Studie Bezeichnungen für die bisherige Systemlinie und den gesondert untersuchten neuen Protokollentwurf. Eine Whitepaper-Version ist keine produktive Softwareversion.

Selbstprüfung: Beurteilung der eigenen wesentlichen Gestaltung oder Handlung. Sie ist von zulässiger fachlicher Zusammenarbeit und von einem blossen früheren Kontakt zu unterscheiden.

Freigabebedingung: Vorab definierter Nachweis, ohne den der bezeichnete Einsatz nicht stattfinden soll. Die rechtliche Zuständigkeit für die Entscheidung bleibt gesondert zu bestimmen.

Produktionsgleichheit: Nachweis, dass der tatsächlich eingesetzte Stand den geprüften und zugelassenen Artefakten und relevanten Konfigurationen entspricht.

Querschnittsrisiko: Risiko, das mehrere technische oder betriebliche Risiken gleichzeitig beeinflusst, etwa eine unwirksame unabhängige Kontrolle.

14.4 Grenzen und offene Nachweise

Die Studie hat keine produktive Installation untersucht und keine eigene Angriffssimulation durchgeführt. Sie hat die veröffentlichten Prüfberichte nicht durch neue mathematische Beweise ersetzt. Der vollständige interne Erledigungsstand aller Meldungen, die tatsächlichen Ausstandsregeln und sämtliche kantonalen Betriebsnachweise sind öffentlich nicht vollständig aus der ausgewerteten Belegbasis rekonstruierbar.

Es wurde kein vollständiger Abschlussbericht der Basler Ursachenanalyse als Grundlage verwendet. Die Aussagen zum Ereignis und zu den Gegenmassnahmen beruhen auf den bezeichneten Originalmitteilungen. Ebenso ist der private Importbefund mangels vorliegendem Originalbeleg ausdrücklich von den bestätigten technischen Befunden getrennt.

Die Untersuchung belegt keine Manipulation realer Schweizer Abstimmungsresultate durch das aktuelle Post-System. Diese Aussage beschreibt die Reichweite der geprüften Quellen, nicht die beweisbare Abwesenheit jedes unentdeckten Angriffs. Empfehlungen und vorgeschlagene Fristen sind eigene Schlussfolgerungen der Studie.

14.5 Wichtige Personen und ihre belegten Funktionen

Stichtag: 9. Oktober 2026. Die folgende Übersicht erfasst 21 für Steuerung, Entwicklung und Prüfung wichtige Personen anhand öffentlich zugänglicher Originalquellen. Sie unterscheidet aktuelle Amts- und Leitungsangaben von der belegten Mitarbeit an einem bestimmten Entwicklungs- oder Prüfbericht. Ein Bericht aus dem Jahr 2026 belegt den dort genannten Beitrag; er beweist für sich allein weder ein heute fortlaufendes Vertragsverhältnis noch eine heutige Weisungs- oder Freigabebefugnis. Die Übersicht ist deshalb keine vollständige Personal- oder Mandatsliste aller beteiligten Stellen.

Bund und strategische Steuerung. Die Projektorganisation nennt die Bundessitze im Steuerungsausschuss nach Funktionen. Die Zuordnung zu Personen erfolgt durch Abgleich mit den amtlichen Amtsprofilen beziehungsweise der aktuellen Risikobeurteilung. Die Teilnahme an einzelnen

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

Sitzungen und allfällige Stellvertretungen sind damit nicht nachgewiesen. Der Bundesrat bleibt der kollektive nationale Auftraggeber; die einzelnen aufgeführten Personen ersetzen dessen Zuständigkeit nicht.[82,83]

Person	Belegte Funktion am Stichtag	Bezug zum E-Voting und Grenze der Aussage
Viktor Rossi	Bundeskanzler	Leitet den Steuerungsausschuss Vote électronique. In der Genehmigungsrubrik der Risikobeurteilung 2026-4 genannt; strategische Führung und behördliche Risikoverantwortung. [84,85]
Barbara Perriard	Leiterin der Sektion Politische Rechte der Bundeskanzlei	Das Projekt ist in ihrer Sektion angesiedelt; ihre Funktion besitzt einen Bundessitz im Steuerungsausschuss. In der Genehmigungsrubrik der Risikobeurteilung 2026-4 genannt. [86,87]
Aurore Borer	Teilprojektleiterin Vote électronique, Bundeskanzlei	In dieser Funktion in der Genehmigungsrubrik der Risikobeurteilung 2026-4 aufgeführt. Daraus folgt keine belegte alleinige Gesamtprojektleitung oder alleinige Zulassungsbefugnis. [88]
Michael Schöll	Direktor des Bundesamtes für Justiz	Seine Amtsfunktion ist als Bundessitz im Steuerungsausschuss vorgesehen; strategische Mitwirkung. Kein Nachweis eines persönlichen technischen Prüfmandats. [89,90]
Florian Schütz	Direktor des Bundesamtes für Cybersicherheit	Seine Amtsfunktion ist als Bundessitz im Steuerungsausschuss vorgesehen. Dieser Sitz ist von einem konkreten unabhängigen Systemaudit zu unterscheiden. [91,92]
Martina Hirayama	Staatssekretärin für Bildung, Forschung und Innovation	Ihre Amtsfunktion ist als Bundessitz im Steuerungsausschuss vorgesehen; strategische Mitwirkung. Keine daraus ableitbare operative Entwicklungsrolle. [93,94]

Die Risikobeurteilung bezeichnet Rossi, Perriard und Borer in der Rubrik «Durch die Bundeskanzlei genehmigt». Die öffentliche Textfassung enthält Unterschriftsfelder. Die Nennung wird hier als amtliche Funktions- und Zuständigkeitsangabe verwendet, ohne daraus eine eigenständige Prüfung der tatsächlichen Unterzeichnung oder internen Kompetenzordnung abzuleiten.[95]

Post und Entwicklung des Protokollentwurfs. Die aktuelle Karriereseite der Post nennt Baptiste Lanoix als Leiter E-Voting. Die übrigen sieben Namen nennt das Vorwort des Whitepapers 1.2.1 ausdrücklich als Beteiligte an der Zusammenarbeit zwischen Post und LORIA. Das ist ein versionsgebundener Entwicklungsnachweis. Die Tabelle schreibt diesen Personen keine darüber hinausgehenden Personalführungs- oder Zulassungsbefugnisse zu.[96,97]

[82] Q01 · Bundeskanzlei, Projektorganisation, Einleitung und Organe, Abruf 09.10.2026.
[83] Q04 · Bundeskanzlei, Risikobeurteilung 2026-4, 29.09.2026, S. 2–12, 31 sowie die bezeichneten Einzelrisiken.
[84] Q01 · Bundeskanzlei, Projektorganisation, Einleitung und Organe, Abruf 09.10.2026.
[85] Q04 · Bundeskanzlei, Risikobeurteilung 2026-4, 29.09.2026, S. 2–12, 31 sowie die bezeichneten Einzelrisiken.
[86] Q01 · Bundeskanzlei, Projektorganisation, Einleitung und Organe, Abruf 09.10.2026.
[87] Q04 · Bundeskanzlei, Risikobeurteilung 2026-4, 29.09.2026, S. 2–12, 31 sowie die bezeichneten Einzelrisiken.
[88] Q04 · Bundeskanzlei, Risikobeurteilung 2026-4, 29.09.2026, S. 2–12, 31 sowie die bezeichneten Einzelrisiken.
[89] Q01 · Bundeskanzlei, Projektorganisation, Einleitung und Organe, Abruf 09.10.2026.
[90] Q24 · Bundesamt für Justiz, Michael Schöll, Direktor, amtliches Profil, Abruf 09.10.2026.
[91] Q01 · Bundeskanzlei, Projektorganisation, Einleitung und Organe, Abruf 09.10.2026.
[92] Q25 · Bundesamt für Cybersicherheit, Der Direktor des BACS, amtliches Profil, Abruf 09.10.2026.
[93] Q01 · Bundeskanzlei, Projektorganisation, Einleitung und Organe, Abruf 09.10.2026.
[94] Q26 · SBFI, Martina Hirayama, Staatssekretärin, amtliches Profil, Abruf 09.10.2026.
[95] Q04 · Bundeskanzlei, Risikobeurteilung 2026-4, 29.09.2026, S. 2–12, 31 sowie die bezeichneten Einzelrisiken.
[96] Q23 · Schweizerische Post, Informatik und Digital Services, Porträt Baptiste Lanoix, Abruf 09.10.2026.
[97] Q06 · Post/LORIA, Whitepaper 1.2.1, S. 2, 11–12 und Anhang A.1.3; Änderungsverzeichnis, Commit 6d427c8d6d65, 22.09.2026.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

Person	Organisation und belegte Funktion	Bedeutung und Nachweisstand
Baptiste Lanoix	Schweizerische Post; Leiter E-Voting	Aktuelle Funktionsbezeichnung auf der Originalseite der Post, abgerufen am 9. Oktober 2026. Anbieterführung; daraus ergibt sich kein behördlicher Zulassungsentscheid. [98]
Olivier Esseiva	Schweizerische Post; Mitwirkung am Protokollentwurf	Im Vorwort des Whitepapers 1.2.1 als Beteiligter an der Entwicklung mit LORIA genannt. Die Quelle benennt hier keinen übergeordneten Leitungstitel. [99]
Audhild Høgåsen	Schweizerische Post; Mitwirkung am Protokollentwurf	Namentlich genannte Beteiligte an der Entwicklung von System 2.0 im Whitepaper 1.2.1. Entwicklungsseite, keine unabhängige Schlussprüfung dieses eigenen Beitrags. [100]
Chiara Spadafora	Schweizerische Post; Mitwirkung am Protokollentwurf	Namentlich genannte Beteiligte an der Entwicklung von System 2.0 im Whitepaper 1.2.1. Entwicklungsseite, keine unabhängige Schlussprüfung dieses eigenen Beitrags. [101]
Véronique Cortier	LORIA; Mitwirkung am Protokollentwurf	Im Vorwort als wissenschaftliche Beteiligte an der Zusammenarbeit genannt; Forschungs- und Entwicklungsbeitrag. [102]
Alexandre Debant	LORIA; Mitwirkung am Protokollentwurf	Im Vorwort als wissenschaftlicher Beteiligter an der Zusammenarbeit genannt; Forschungs- und Entwicklungsbeitrag. [103]
Henri Devillez	LORIA; Mitwirkung am Protokollentwurf	Im Vorwort als wissenschaftlicher Beteiligter an der Zusammenarbeit genannt; Forschungs- und Entwicklungsbeitrag. [104]
Pierrick Gaudry	LORIA; Mitwirkung am Protokollentwurf	Im Vorwort als wissenschaftlicher Beteiligter an der Zusammenarbeit genannt; Forschungs- und Entwicklungsbeitrag. [105]

Das Whitepaper ordnet die vier LORIA-Beteiligten dem Umfeld von Université de Lorraine, CNRS und Inria zu. Daraus werden hier keine individuell überprüften arbeitsrechtlichen Anstellungen bei allen drei Einrichtungen abgeleitet. Auch die Nennung im Whitepaper ist keine persönliche Garantie für sämtliche Eigenschaften einer späteren produktiven Implementierung.[106]

Externe fachliche Prüfung. Die folgenden Namen sind durch Originalgutachten aus dem Jahr 2026 belegt. Aufgeführt ist der konkrete Prüfbeitrag, nicht eine unbelegte dauerhafte Funktion als «oberster Auditor». Die rechtliche Einsatzfreigabe bleibt bei den zuständigen Behörden. Soweit ein Gutachter technische Verbesserungsvorschläge entwickelt, ist dessen Beitrag bei der späteren Unabhängigkeitsprüfung gemäss Kapitel 4 gesondert zu bewerten.

Person	Belegter Prüfbeitrag 2026	Fundstelle und Reichweite
Thomas Haines	Externer Gutachter zu Release 1.5.4 sowie gemeinsam mit Olivier Pereira zum Whitepaper 1.1 und 1.2	Berichte vom 16. Juni und 24. August 2026. Belegt Analyse der bezeichneten Softwareänderungen und Protokollentwürfe. [107,108]

[98] Q23 · Schweizerische Post, Informatik und Digital Services, Porträt Baptiste Lanoix, Abruf 09.10.2026.
[99] Q06 · Post/LORIA, Whitepaper 1.2.1, S. 2, 11–12 und Anhang A.1.3; Änderungsverzeichnis, Commit 6d427c8d6d65, 22.09.2026.
[100] Q06 · Post/LORIA, Whitepaper 1.2.1, S. 2, 11–12 und Anhang A.1.3; Änderungsverzeichnis, Commit 6d427c8d6d65, 22.09.2026.
[101] Q06 · Post/LORIA, Whitepaper 1.2.1, S. 2, 11–12 und Anhang A.1.3; Änderungsverzeichnis, Commit 6d427c8d6d65, 22.09.2026.
[102] Q06 · Post/LORIA, Whitepaper 1.2.1, S. 2, 11–12 und Anhang A.1.3; Änderungsverzeichnis, Commit 6d427c8d6d65, 22.09.2026.
[103] Q06 · Post/LORIA, Whitepaper 1.2.1, S. 2, 11–12 und Anhang A.1.3; Änderungsverzeichnis, Commit 6d427c8d6d65, 22.09.2026.
[104] Q06 · Post/LORIA, Whitepaper 1.2.1, S. 2, 11–12 und Anhang A.1.3; Änderungsverzeichnis, Commit 6d427c8d6d65, 22.09.2026.
[105] Q06 · Post/LORIA, Whitepaper 1.2.1, S. 2, 11–12 und Anhang A.1.3; Änderungsverzeichnis, Commit 6d427c8d6d65, 22.09.2026.
[106] Q06 · Post/LORIA, Whitepaper 1.2.1, S. 2, 11–12 und Anhang A.1.3; Änderungsverzeichnis, Commit 6d427c8d6d65, 22.09.2026.
[107] Q15 · Haines, Prüfbericht zu Release 1.5.4, 16.06.2026, S. 1–5.
[108] Q03 · Haines/Pereira, 24.08.2026, S. 1–2 und Anhang B.2.1, S. 22; Entwurf 2.0, Whitepaper 1.1/1.2.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

Person	Belegter Prüfbeitrag 2026	Fundstelle und Reichweite
Olivier Pereira	Externer Gutachter zum Whitepaper 1.1 und 1.2 gemeinsam mit Thomas Haines	Bericht vom 24. August 2026 mit eigenem Berichtsteil. Keine daraus abgeleitete Betriebs- oder Entwicklungsleitung bei der Post. [109]
Johannes Müller	Externer Gutachter zu Release 1.5.4 und zum Whitepaper 1.1 und 1.2	Berichte vom 15. Juni und 23. August 2026. Der Whitepaper-Bericht enthält auch konstruktive Alternativvorschläge. [110,111]
Aleksander Essex	Externer Gutachter zum Entwurf System 2.0, Massnahme A.5	Bericht vom 13. September 2026 zu Whitepaper 1.2 und früheren Empfehlungen; Quelle der Befunde F-01 bis F-03. 112
Rolf Haenni	BFH; Mitautor der fachlichen System- und Whitepaper-Prüfungen	Gemeinsam mit Koenig und Locher: Bericht vom 9. Januar sowie Whitepaper-Prüfung vom 14. August 2026. [113,114]
Reto E. Koenig	BFH; Mitautor der fachlichen System- und Whitepaper-Prüfungen	Dieselben gemeinsamen BFH-Berichte. Die Autorenschaft belegt die Mitwirkung, keine persönliche alleinige Freigabeverantwortung. [115,116]
Philipp Locher	BFH; Mitautor der fachlichen System- und Whitepaper-Prüfungen	Dieselben gemeinsamen BFH-Berichte. Frühere institutionelle Entwicklungserfahrung ist getrennt vom aktuellen Prüfgegenstand zu beurteilen. [117,118]

Nicht öffentlich ausreichend aufgelöste Rollen. Die amtliche Organisationsseite nennt sechs kantonale Sitze im Steuerungsausschuss, veröffentlicht dort aber keine vollständige namentliche Besetzung. Auch die konkrete personelle Besetzung des Projektausschusses, die Verantwortlichen aller kantonalen Schlüsselzeremonien und die persönlichen Ausstandsentscheidungen lassen sich daraus nicht rekonstruieren. Der veröffentlichte Orange-Bericht bezeichnet Orange Cyberdefense Switzerland SA beziehungsweise das SCRT-Team als Prüfstelle, ohne in der Autorenübersicht einzelne Auditorinnen und Auditoren zu nennen. Diese Lücken werden nicht mit vermuteten Namen gefüllt.[119,120]

Konsequenz für die Gewaltentrennung. Für jede der genannten Rollen muss eine zuständige Aufsicht zusätzlich Mandat, Finanzierung, Weisungsweg, Entwicklungsbeiträge und Freigaberechte kennen. Die öffentlich belegte Mehrfachrolle der Bundeskanzlei ist ein institutioneller Prüfpunkt. Die benannte Zusammenarbeit von Post und LORIA gehört zur Entwicklungsseite. Die unabhängige Schlussprüfung muss ihre wesentlichen Beiträge von aussen beurteilen. Die blosse Nennung einer Person in einem Gremium oder Gutachten beweist weder Befangenheit noch wirksame Unabhängigkeit. Der in Kapitel 11 vorgeschlagene Auftrag zur Offenlegung der Rollen soll deshalb gerade die noch fehlenden Mandats- und Ausstandsnachweise beschaffen.

[109] Q03 · Haines/Pereira, 24.08.2026, S. 1–2 und Anhang B.2.1, S. 22; Entwurf 2.0, Whitepaper 1.1/1.2.
[110] Q16 · Müller, Prüfbericht zu Release 1.5.4, 15.06.2026, S. 1–2.
[111] Q14 · Müller, Review White Paper 2.0, 23.08.2026, S. 4–7.
[112] Q05 · Essex, 13.09.2026, Management Summary S. i, Kap. 3–6 und S. 25; Whitepaper 1.2.
[113] Q19 · Haenni/Koenig/Locher, Examination of the Swiss Post Internet Voting System, 09.01.2026, S. 3–9.
[114] Q13 · Haenni/Koenig/Locher, Review White Paper 2.0, 14.08.2026, S. 15–16 und 20–23.
[115] Q19 · Haenni/Koenig/Locher, Examination of the Swiss Post Internet Voting System, 09.01.2026, S. 3–9.
[116] Q13 · Haenni/Koenig/Locher, Review White Paper 2.0, 14.08.2026, S. 15–16 und 20–23.
[117] Q19 · Haenni/Koenig/Locher, Examination of the Swiss Post Internet Voting System, 09.01.2026, S. 3–9.
[118] Q13 · Haenni/Koenig/Locher, Review White Paper 2.0, 14.08.2026, S. 15–16 und 20–23.
[119] Q01 · Bundeskanzlei, Projektorganisation, Einleitung und Organe, Abruf 09.10.2026.
[120] Q17 · Orange Cyberdefense, P023254, 27.08.2026, S. 4–6 und 10–15; Release 1.5.4.2.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

14.6 Projektübersicht: Wer ist wofür verantwortlich?

Diese Übersicht verbindet die belegte Projektorganisation mit den Namen aus Kapitel 14.5. Sie trennt politische Verantwortung, Projektarbeit, Entwicklung, Betrieb, Prüfung und Zulassung. Die Tabelle ist eine funktionale Zuordnung nach der ausgewerteten Quellenbasis; eine interne Kompetenz- oder Unterschriftenordnung ersetzt sie nicht.[121,122,123]

Aufgabe	Zuständige Stelle / bekannte Personen	Verantwortung und Abgrenzung
Politischer Auftrag und Grundbewilligung	Bundesrat	Legt den nationalen Auftrag fest und entscheidet über die Grundbewilligung für Versuche. Keine persönliche technische Abnahme durch einzelne Mitglieder.
Strategische Beratung	Steuerungsausschuss; Vorsitz Viktor Rossi	Bundessitze nach Amtsfunktion: Barbara Perriard, Michael Schöll, Florian Schütz und Martina Hirayama; dazu sechs kantonale Sitze. Berät die Projektführung.
Projektführung und Koordination	Bundeskanzlei; Sektion Politische Rechte unter Barbara Perriard; Team Vote électronique	Institutionelle Projektleitung und Koordination. Aurore Borer ist als Teilprojektleiterin belegt; ihre genaue interne Kompetenzdelegation bleibt gesondert nachzuweisen.
Gemeinsame Massnahmen	Projektausschuss mit Bundeskanzlei, Kantonen und Post	Zusammenarbeit bei der Umsetzung. Öffentliche Quellen liefern keine vollständige namentliche Besetzung oder persönliche Zuständigkeitsmatrix.
Produkt und Herstellerkorrekturen	Schweizerische Post; Baptiste Lanoix als Leiter E-Voting	Entwicklung und Bereitstellung des Systems sowie Dokumentation und Korrekturen. Die Leitung auf Anbieterseite ersetzt keine behördliche Zulassung.
Protokollentwurf System 2.0	Post und LORIA; benannte Mitwirkende in Abbildung 6	Versionsgebundener Forschungs- und Entwicklungsbeitrag zu Whitepaper 1.2.1. Keine daraus abgeleitete alleinige Sicherheits- oder Freigabeverantwortung.
Unabhängige Systemprüfung	Bundeskanzlei als Auftraggeberin; externe Prüfstellen in Abbildung 7	Gutachter prüfen bezeichnete Versionen und Prüfgegenstände. Umfang, Ausstände und abschliessende Nachprüfung sind je Mandat offenzulegen.
Urnengang, Betrieb und Auszählung	Jeweils einsetzender Kanton	Organisiert den konkreten Urnengang und dessen betriebliche Durchführung. Verantwortliche für Schlüssel, Wiederherstellung und Auszählung müssen kantonal benannt sein.
Prüfung des konkreten Urnengangs	Vom Kanton beauftragte Prüfpersonen	Prüfen den konkreten Ablauf und die Ergebnisse mit den verlangten unabhängigen Hilfsmitteln. Die Namen sind aus der untersuchten zentralen Quellenbasis nicht vollständig ermittelbar.
Zulassung und Risikoentscheid	Rechtlich zuständige Behörden; Bundeskanzlei für die Zulassung	Entscheidet im gesetzlichen Zuständigkeitsrahmen auf Basis der erforderlichen Nachweise. Herstellerantwort und positives Gutachten sind noch kein Zulassungsentscheid.

Leseschlüssel: Die folgenden drei Organigramme vertiefen dieselbe Zuordnung. Genannte Personen sind anhand ihrer belegten Funktion oder ihres konkreten Beitrags eingeordnet; offene kantonale oder interne Besetzungen bleiben sichtbar.

[121] Q01 · Bundeskanzlei, Projektorganisation, Einleitung und Organe, Abruf 09.10.2026.

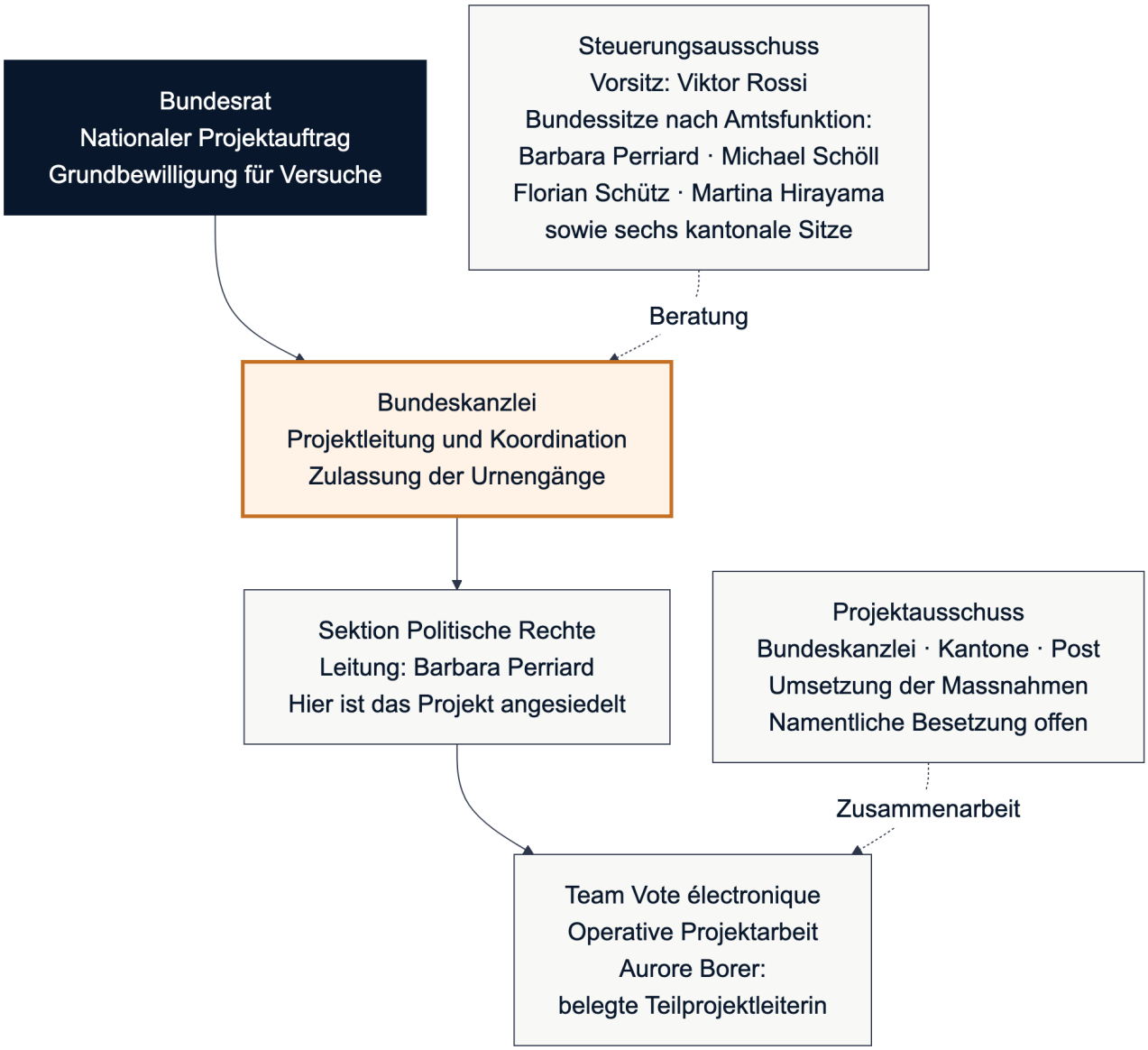
[122] Q02 · VEleS, SR 161.116, Stand 01.07.2022; jeweils im Text bezeichnete Artikel und Anhangsziffern.

[123] Q04 · Bundeskanzlei, Risikobeurteilung 2026-4, 29.09.2026, S. 2–12, 31 sowie die bezeichneten Einzelrisiken.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

Abbildung 6 · Projektführung, Gremien und benannte Verantwortliche



Stand 9. Oktober 2026. Durchgezogene Pfeile zeigen Auftrag und organisatorische Zuordnung; gepunktete Pfeile Beratung oder Zusammenarbeit. Die Bundessitze sind über Amtsfunktionen zugeordnet, nicht über nachgewiesene Sitzungsteilnahme. Aurore Borer ist als Teilprojektleiterin belegt; eine alleinige Gesamtprojektleitung wird ihr nicht zugeschrieben. Die Namen und Einzelnachweise stehen in Kapitel 14.5.[124,125]

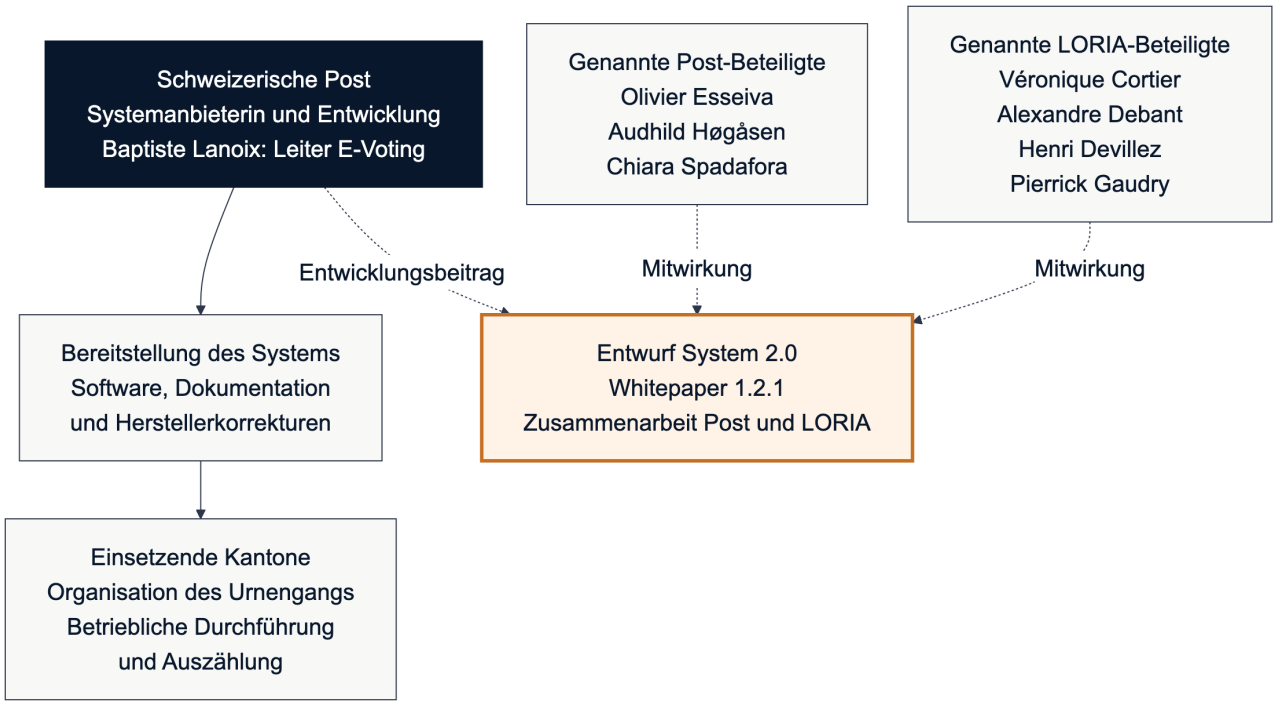
[124] Q01 · Bundeskanzlei, Projektorganisation, Einleitung und Organe, Abruf 09.10.2026.

[125] Q04 · Bundeskanzlei, Risikobeurteilung 2026-4, 29.09.2026, S. 2–12, 31 sowie die bezeichneten Einzelrisiken.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

Abbildung 7 · Entwicklung, Systembereitstellung und kantonaler Betrieb



Durchgezogene Pfeile zeigen den funktionalen Weg vom Anbieter zum kantonalen Einsatz, keine Personalhierarchie zwischen Post und Kantonen. Gepunktete Pfeile bezeichnen die im Whitepaper 1.2.1 belegte Entwicklungsmitwirkung. Die sieben genannten Mitwirkenden sind damit nicht als Abteilungsleitende oder Verantwortliche jeder späteren Produktivversion ausgewiesen. Baptiste Lanoix ist als Leiter E-Voting der Post belegt.[126,127]

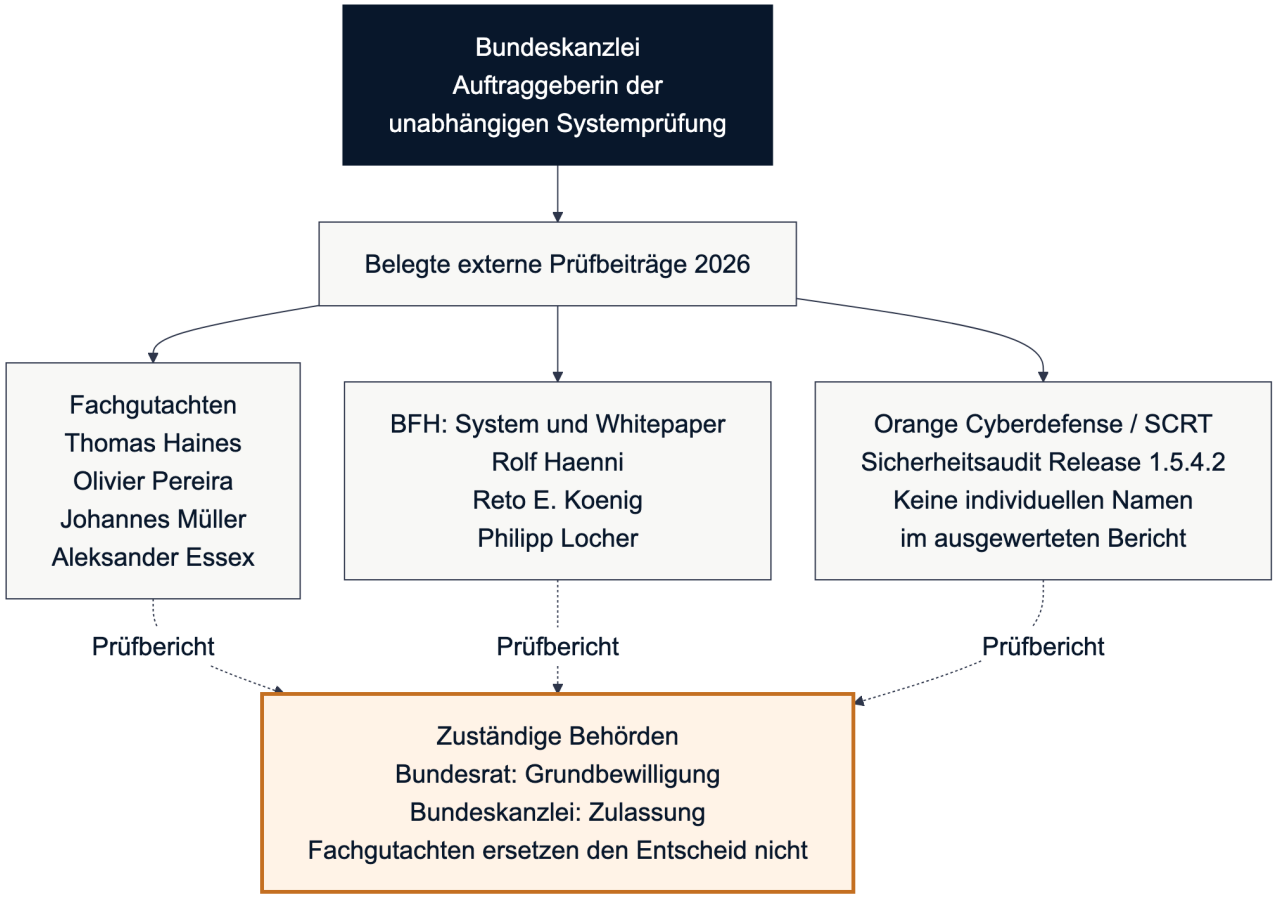
[126] Q06 · Post/LORIA, Whitepaper 1.2.1, S. 2, 11–12 und Anhang A.1.3; Änderungsverzeichnis, Commit 6d427c8d6d65, 22.09.2026.

[127] Q23 · Schweizerische Post, Informatik und Digital Services, Porträt Baptiste Lanoix, Abruf 09.10.2026.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

Abbildung 8 · Prüfstellen, bekannte Gutachter und behördlicher Entscheid



Die Prüfbeiträge beziehen sich auf die in Kapitel 14.5 genannten Berichte und Versionen. Die Zuordnung begründet weder ein unbegrenzt laufendes Mandat noch eine persönliche Zulassungsbefugnis. Gepunktete Pfeile zeigen, dass Berichte die Behördenentscheidung fachlich stützen. Zusätzlich beauftragt jeder Kanton die Prüfung des konkreten Urnengangs; deren namentliche Besetzung ist gesondert nachzuweisen. Einzelbelege zu allen Gutachtern und Orange stehen in Kapitel 14.5.[128,129]

[128] Q01 · Bundeskanzlei, Projektorganisation, Einleitung und Organe, Abruf 09.10.2026.

[129] Q02 · VEleS, SR 161.116, Stand 01.07.2022; jeweils im Text bezeichnete Artikel und Anhangsziffern.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

15 Originalquellen

Alle folgenden Quellen sind Originalveröffentlichungen der jeweils bezeichneten Institutionen oder Verfasser. Online-Abruf am 9. Oktober 2026. Die Reihenfolge folgt der ersten Verwendung im Text; die Kapitelzuordnung erleichtert die Nachprüfung. Kurze Belege stehen in den Fussnoten. Dynamische Übersichtsseiten sind als solche gekennzeichnet. Auf längere wörtliche Zitate wird zugunsten quellengebundener Paraphrasen verzichtet.

15.1 Grundlagen und zentrale Entscheidung

Q01 · Bundeskanzlei — Projektorganisation. Undatierte, laufend gepflegte Organisationsdarstellung; Abrufstand 9. Oktober 2026. Fundstellen: Einleitung, Abschnitte Steuerungsausschuss und Projektausschuss. Belegt Auftrag, Projektleitung, Zulassungsverantwortung und Gremienzusammensetzung. Behördenquelle über die eigene Organisation; kein Nachweis gelebter Ausstandsverfahren. Verwendet in Kapitel 1 und 4. Zusätzlich verwendet in Kapitel 14.5. Original.

Q02 · Schweizerische Bundeskanzlei — Verordnung über die elektronische Stimmabgabe. VEleS vom 25. Mai 2022, Stand 1. Juli 2022, SR 161.116, AS 2022 336. Fundstellen: Art. 2–11; Anhang Ziff. 3.12, 4.12, 12.8 sowie Vorgaben zu Entwicklung, Produktionsnachweisen und Prüfung. Geltender Originalnormtext in Fedlex; Rechtsgrundlage, kein Nachweis tatsächlicher Einhaltung. Verwendet in Kapitel 1, 2, 4–7 und 10. Amtlicher Originaltext.

Q03 · Thomas Haines und Olivier Pereira — Report on the White Paper on the Swiss Post Voting System 2.0 Versions 1.1 and 1.2. 24. August 2026; veröffentlicht durch die Bundeskanzlei am 22. September 2026. Fundstellen: S. 1–2, technische Analyse und Anhang B.2.1, S. 22. Originalgutachten zum Entwurf; enthält Fragen zu Protokollabläufen und zur Personalunion von Schlüsselverantwortlichen und Auditoren. Kein Befund eines produktiven Angriffs. Verwendet in Kapitel 1, 3–5. Zusätzlich verwendet in Kapitel 14.5. Originalbericht.

Q04 · Bundeskanzlei — Risikobeurteilung Vote électronique 2026-4. Veröffentlicht am 29. September 2026. Fundstellen: S. 2–3 Zusammenfassung und Matrix; S. 5–12 Risiken, Kontext und Methodik; S. 31 Genehmigungsrubrik; Einzelbewertungen insbesondere R2, R5, R8, R11, R13, R14 und R15. Originalbeurteilung der zuständigen Projekt- und Zulassungsbehörde. Belegt die amtliche Einschätzung, nicht eine unabhängige Eintrittswahrscheinlichkeit. Verwendet in Kapitel 1, 2 und 5–8. Zusätzlich verwendet in Kapitel 14.5. Originalbericht.

Q05 · Aleksander Essex — Swiss Post Voting System 2.0 Measure A.5 Addendum Disposition of White Paper v1.1 Recommendations and New Findings in v1.2. Version 2 vom 13. September 2026; publiziert am 22. September 2026. Fundstellen: Management Summary S. i; Kap. 3–6; Schlussfolgerung S. 25. Gedruckte Seitenzählung; das PDF hat 29 Seiten. Originalgutachten mit Befunden F-01 bis F-03 zum Whitepaper 1.2. Die Bezeichnung Severe stammt vom Gutachter und wird nicht auf einen produktiven Stand übertragen. Verwendet in Kapitel 1 und 5. Zusätzlich verwendet in Kapitel 14.5. Originalbericht.

Q06 · Schweizerische Post in Zusammenarbeit mit LORIA — White Paper on the Swiss Post Voting System 2.0 Measure A.5 und Änderungsverzeichnis. Whitepaper-Version 1.2.1; Repository-Commit 6d427c8d6d65861af3a330568834997a9758fc8a vom 22. September 2026. Fundstellen: Deckblatt und Vorwort S. 2 mit Beteiligtenliste, Abschnitte 2.4.1–2.4.2, S. 11–12, Anhang A.1.3 und Abschnitt Changes in version 1.2.1 im Änderungsverzeichnis. Originale Herstellerdokumentation über Korrekturen; keine unabhängige Bestätigung ihrer vollständigen Wirksamkeit. Verwendet in Kapitel 1, 2, 5 und 13. Zusätzlich verwendet in Kapitel 14.5. Versionsgebundenes Whitepaper, versionsgebundenes Änderungsverzeichnis.

Q07 · Bundeskanzlei — Offenlegung des Quellcodes führt zur Entdeckung eines Mangels im neuen E-Voting-System der Post. 12. März 2019. Fundstellen: Abschnitte zum Mangel der universellen Verifizierbarkeit und zur Abgrenzung vom damals eingesetzten System. Zeitgenössische amtliche Originalmitteilung; belegt die Feststellung und behördliche Einordnung, ersetzt nicht den mathematischen Originalbeweis. Verwendet in Kapitel 1 und 3. Originalmitteilung.

Q08 · Bundeskanzlei — Bundeskanzlei nimmt Standortbestimmung zum E-Voting vor. 29. März 2019. Fundstellen: weiterer Mangel der individuellen Verifizierbarkeit, Nichtverfügbarkeit am 19. Mai 2019 und fehlende Hinweise auf frühere Stimmenverfälschung. Zeitgenössische amtliche Originalmitteilung. Verwendet in Kapitel 1 und 3. Originalmitteilung.

Q09 · Regierungsrat Basel-Stadt — E-Voting Basel-Stadt gibt Analyse zu den Umständen und Ursachen des Vorfalls bei der Abstimmung vom 8. März 2026 in Auftrag. 10. März 2026. Fundstellen: 2'048 nicht auszählbare Stimmen, erfolglose Entschlüsselung, Aussetzung bis Ende 2026 und Abgrenzung zur externen Komponente. Originalmitteilung über den eigenen Vorfall, kein abschliessender Untersuchungsbericht. Verwendet in Kapitel 1, 3 und 6. Originalmitteilung.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

15.2 Projektstand und fachliche Prüfungen

Q10 · Bundeskanzlei — Vote électronique. Undatierte, fortgeschriebene Projektübersicht; Abrufstand 9. Oktober 2026. Fundstellen: Projektziele und Aktueller Stand. Belegt sechs Grundbewilligungen und den eingesetzten Anbieter; keine Aussage, dass alle sechs Kantone an jedem Urnengang teilnehmen. Verwendet in Kapitel 3, 8 und 9. Originalseite.

Q11 · Bundeskanzlei — Einsatz E-Voting Versuchsbedingungen. Amtliche Excel-Datei vom 29. September 2026. Fundstellen: Tabellenblätter 29.11.2026 und 27.09.2026, Summenzeilen und Fussnoten 1–6. Belegt indikative Zulassungsgrössen, effektiven Materialversand innerhalb der Limite und unterschiedliche Bezugsgrössen. Die gerundete Novemberzahl wird in dieser Studie ausdrücklich als Obergrösse, nicht als Nutzung ausgewiesen. Verwendet in Kapitel 3. Originaldatei.

Q12 · Berner Fachhochschule — BFH-Forschende untersuchen E-Voting-System der Post. 2. Juni 2022. Fundstellen: Prüfauftrag und Abschnitt Jahrelange Erfahrung im Bereich E-Voting. Institutionelle Originalquelle zur eigenen Forschungs- und früheren Genfer Entwicklungsrolle. Kein Nachweis eigener Entwicklung der aktuellen Post-Implementierung. Verwendet in Kapitel 3. Originalseite.

Q13 · Rolf Haenni, Reto E. Koenig und Philipp Locher — Review of White Paper on the Swiss Post Voting System 2.0. BFH, 14. August 2026, Version 1.1 mit Addendum zu 1.2. Fundstellen: Schlussfolgerung S. 15–16, Addendum S. 20–23. Originalgutachten mit positiver Beurteilung wesentlicher Änderungen und fortbestehenden Architektur- und Skalierungsfragen. Verwendet in Kapitel 3 und 5. Zusätzlich verwendet in Kapitel 14.5. Originalbericht.

Q14 · Johannes Müller — Review White Paper on Swiss Post Voting System 2.0 Measure A.5 version 1.1 and 1.2. 23. August 2026. Fundstellen: S. 4–6 mit eigenen Alternativvorschlägen und S. 7 mit Bewertung von 1.2. Originalgutachten; dokumentiert konstruktive Mitwirkung, aber weder einen vollständigen Produktivnachweis noch einen nachgewiesenen persönlichen Interessenkonflikt. Verwendet in Kapitel 3–5. Zusätzlich verwendet in Kapitel 14.5. Originalbericht.

Q15 · Thomas Haines — Report on Release 1.5.4. 16. Juni 2026, Scopes 1 und 2, publiziert durch die Bundeskanzlei. Fundstellen: fünfseitiger Bericht, insbesondere Miller-Rabin, Kontextbindung, Authentisierung und Grenzen der Codeanalyse. Originalgutachten zur bezeichneten Version; die praktische Nichtausnutzbarkeit wird auf die beschriebenen Aufrufpfade begrenzt. Verwendet in Kapitel 3, 5 und 7. Zusätzlich verwendet in Kapitel 14.5. Originalbericht.

Q16 · Johannes Müller — Review of Version 1.5.4 of the Swiss Post Voting System. 15. Juni 2026, Scopes 1 und 2, publiziert durch die Bundeskanzlei. Fundstellen: zweiseitiger Bericht zu eGovToken, SSO, Primzahltest und Spezifikationsreferenzen. Originalgutachten; keine pauschale Bewertung späterer Releases. Verwendet in Kapitel 3, 5 und 7. Zusätzlich verwendet in Kapitel 14.5. Originalbericht.

Q17 · Orange Cyberdefense Switzerland SA — E-voting 1.5.4.2 Security Audit Report. Referenz P023254, Prüfung Juli 2026, öffentliche Version 1.0 vom 27. August 2026. Fundstellen: S. 4–6 Zusammenfassung, Aufwand, Prüfumfang und Ausschlüsse; S. 10–15 informatorische Befunde. Originalbericht der beauftragten Prüfstelle. Positive Aussage gilt für den angegebenen Umfang; Social Engineering und Denial of Service waren ausgeschlossen. Verwendet in Kapitel 3 und 5. Zusätzlich verwendet in Kapitel 14.5. Originalbericht.

Q18 · Bundeskanzlei — Massnahmenkatalog von Bund und Kantonen. Fortgeschriebene Originalseite; Abrufstand 9. Oktober 2026. Fundstelle: Arbeiten zu Massnahme A.5, einschliesslich Beschreibung der Vertrauensannahmen beim Druck und der regelmässigen Einbindung der Experten in die Whitepaper-Prüfung. Die Seite enthält die am 22. September publizierten Originalgutachten. Verwendet in Kapitel 4. Originalseite.

Q19 · Rolf Haenni, Reto E. Koenig und Philipp Locher — Examination of the Swiss Post Internet Voting System. BFH, Final Version vom 9. Januar 2026; Releases 1.5.0, 1.5.1, 1.5.2, 1.5.2.1 und 1.5.2.2. Fundstellen: S. 3–9 Prüfauftrag, Arbeitsweise und damalige Befundzustände; anschliessende Einzelbefunde. Originalgutachten zum Untersuchungszeitraum Juni bis Dezember 2025. Dessen offene Punkte werden nicht ohne aktuellen Nachweis als im Oktober 2026 weiterhin offen behauptet. Verwendet in Kapitel 5. Zusätzlich verwendet in Kapitel 14.5. Originalbericht.

Q22 · Kanton St.Gallen — E-Voting. Dienst für Politische Rechte, letzte Aktualisierung 8. September 2026; Abruf 9. Oktober 2026. Fundstellen: Anmeldung, Zusendung des Stimmmaterials, Öffnung der elektronischen Urne, Verlust des Stimmrechtsausweises und Helpdesk-Zeiten. Amtliche Originalbeschreibung des kantonalen Bedienwegs; die Grenzen werden nicht auf sämtliche Kantone übertragen. Verwendet in Kapitel 5. Originalseite.

Q27 · Satoshi Nakamoto — Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Fundstellen: Abschnitte 3–5, 8 und 11. Originalentwurf für ein verteiltes Transaktionsprotokoll; erklärt Konsens und bestätigungsabhängige Sicherheit. Kein Nachweis für die Eignung als Abstimmungssystem. Verwendet in Kapitel 5.11. Originalpaper.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.

Q28 · ElectionGuard — Creating a Verifiable Election und Election Record. Undatierte technische Originaldokumentation; Abruf 9. Oktober 2026. Fundstellen: Publishing Verifiable results und Election Record. Beschreibt Drittprüfer und ein veröffentlichbares Belegpaket. Dient als technisches Beispiel; keine Behauptung einer Schweizer Produktivintegration. Verwendet in Kapitel 5.11. Verifizierbarkeit. Belegpaket.

Q29 · National Academies of Sciences, Engineering, and Medicine — Securing the Vote: Protecting American Democracy. 2018, DOI 10.17226/25120. Fundstelle: Kapitel 5, S. 103–105, Abschnitt Blockchains. Wissenschaftlicher Konsensbericht über die Grenzen von Blockchain bei Wahlen; kein aktuelles Schweizer Systemgutachten. Verwendet in Kapitel 5.11. Originalkapitel.

Q30 · Bundeskanzlei — Überprüfung von Systemen. Undatierte amtliche Originalseite; Abruf 9. Oktober 2026. Fundstellen: Voraussetzungen und Überprüfung des vollständig verifizierbaren Post-Systems. Beschreibt beauftragte unabhängige Prüfungen, Offenlegung und öffentliche Fehleranalyse. Belegt diese Prüfwege, keinen voraussetzungslosen öffentlichen Auditdienst für jeden realen Urnengang. Verwendet in Kapitel 5.10 und 5.12. Originalseite.

15.3 Betrieb und Identität

Q20 · Bundeskanzlei — E-Voting Zulassungen für die Abstimmung vom 14. Juni 2026. 17. April 2026. Fundstellen: Einordnung des Basler Vorfalls, PIN-geschützte USB-Sticks und Überprüfung der Abläufe in den anderen Kantonen. Amtliche Originalmitteilung über Zulassung und Gegenmassnahmen; keine eigene praktische Wiederherstellungsprüfung durch den Verfasser dieser Studie. Verwendet in Kapitel 6. Originalmitteilung.

Q21 · Bundesverwaltung E-ID — Neuer Zeitplan für die Einführung der E-ID und der Vertrauensinfrastruktur. Auf der Originalseite als veröffentlicht am 30. Juni 2026 ausgewiesen. Fundstelle: Mitteilung über Verzögerung und voraussichtlichen Start der Vertrauensinfrastruktur im ersten Halbjahr 2027. Zeitgebundene Planungsangabe, keine Zusage über eine fertige E-Voting-Integration. Verwendet in Kapitel 7. Originalmitteilung.

15.4 Personen und aktuelle Amtsfunktionen

Q23 · Schweizerische Post — Informatik und Digital Services. Undatierte, am 9. Oktober 2026 abgerufene Karriereseite. Fundstelle: Mitarbeitendenporträt Baptiste Lanoix, Funktionsbezeichnung «Leiter E-Voting». Originalangabe des Arbeitgebers; belegt den veröffentlichten Leitungstitel, nicht Mandatsbeginn, interne Vollmachten oder eine behördliche Prüfrolle. Verwendet in Kapitel 14.5. Originalseite.

Q24 · Bundesamt für Justiz — Michael Schöll, Direktor. Amtliches Personenprofil, veröffentlicht am 1. September 2021; Abrufstand 9. Oktober 2026. Fundstelle: Überschrift und letzter Absatz zur Amtsleitung seit 1. September 2021. Belegt die aktuelle veröffentlichte Amtsfunktion; der Bezug zum Steuerungsausschuss ergibt sich erst zusammen mit Q01. Verwendet in Kapitel 14.5. Amtliches Profil.

Q25 · Bundesamt für Cybersicherheit — Der Direktor des BACS. Undatiertes amtliches Personenprofil; Abrufstand 9. Oktober 2026. Fundstelle: erster Absatz zur Direktion durch Florian Schütz seit 1. Januar 2024. Belegt die aktuelle veröffentlichte Amtsfunktion; kein Nachweis eines persönlichen E-Voting-Prüfmandats. Verwendet in Kapitel 14.5 zusammen mit Q01. Amtliches Profil.

Q26 · Staatssekretariat für Bildung, Forschung und Innovation — Martina Hirayama, Staatssekretärin für Bildung, Forschung und Innovation. Undatiertes amtliches Personenprofil; Abrufstand 9. Oktober 2026. Fundstelle: Überschrift und erster Absatz zur Direktion seit 1. Januar 2019. Belegt die aktuelle veröffentlichte Amtsfunktion; der Gremienbezug wird durch Q01 hergestellt. Verwendet in Kapitel 14.5. Amtliches Profil.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Public.