



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK
Sektion Politische Rechte

Neuausrichtung und Wiederaufnahme der Versuche

Schlussbericht des Steuerungsausschusses Vote électronique (SA VE)

30. November 2020

Inhalt

1. Ausgangslage	3
1.1 E-Voting in der Schweiz.....	3
1.2 Rahmenbedingungen des bisherigen Versuchsbetriebs	3
1.2.1 Aufgaben und Rollen von Bund und Kantonen	3
1.2.2 Schrittweise Einführung als dritter Stimmkanal	3
1.2.3 Kontrolle und Aufsicht.....	3
1.2.4 Sicherheitsanforderungen.....	4
1.2.5 Risiko- und Krisenmanagement	5
1.2.6 Transparenzmassnahmen	5
1.3 Situation 2019	5
1.3.1 System der Schweizerischen Post	5
1.3.2 System des Kantons Genf	5
1.3.3 Überführung in den ordentlichen Betrieb.....	6
1.3.4 Schlussfolgerungen zur Situation 2019	6
1.4 Situation Ende 2020.....	7
1.5 Neuausrichtung des Versuchsbetriebs	7
1.5.1 Auftrag des Bundesrates und Zielsetzung.....	7
1.5.2 Zusammenarbeit von Bund und Kantonen	8
2. Dialog mit der Wissenschaft	9
2.1 Einbezug von Expertinnen und Experten	9
2.2 Vorgehen und Ausgestaltung des Dialogs.....	9
2.3 Zusammenfassung der Ergebnisse des Dialogs	10
2.3.1 Allgemeine Einschätzung	10
2.3.2 Bereitstellung eines sicheren Systems.....	10
2.3.3 Mandatierte und öffentliche Prüfung.....	11
2.4 Einschätzungen zum Dialog mit der Wissenschaft.....	12
3. Beschreibung der Massnahmen	13
A. Weiterentwicklung der Systeme.....	13
B. Wirksame Kontrolle und Aufsicht.....	20
C. Stärkung der Transparenz und des Vertrauens.....	28
D. Stärkere Vernetzung mit der Wissenschaft	34
4. Gesamtbeurteilung und weiteres Vorgehen	37
4.1 Zusammenfassung der Stossrichtungen und Etappierung der Massnahmen.....	37
4.2 Auswirkungen auf Bund und Kantone	38
4.2.1 Massnahmen für den Wiedereinsatz und die erste Etappe nach dem Wiedereinsatz... 38	
4.2.2 Mittel- bis langfristige Entwicklungen.....	38
4.2.3 Langfristige Sicherstellung der Finanzierung	39
5. Schlussfolgerungen	41
Anhang: Massnahmenkatalog	42

1. Ausgangslage

1.1 E-Voting in der Schweiz

Die elektronische Stimmabgabe in der Schweiz befindet sich seit 2004 in einer Versuchsphase.¹ E-Voting ist Teil der E-Government-Strategie Schweiz von Bund und Kantonen. Die rechtlichen Grundlagen für die Versuche bilden Artikel 8a des Bundesgesetzes über die politischen Rechte (BPR; SR 161.1), die Artikel 27a-27q der Verordnung vom 24. Mai 1978 über die politischen Rechte (VPR; SR 161.11) sowie die Verordnung der Bundeskanzlei (BK) vom 13. Dezember 2013 über die elektronische Stimmabgabe (VEleS; SR 161.116). Es gilt seit Beginn des Projekts unverändert das Motto «Sicherheit vor Tempo». In der Schweiz werden nur E-Voting-Systeme zugelassen, welche die hohen bundesrechtlichen Sicherheitsanforderungen erfüllen.

Seit 2004 haben insgesamt 15 Kantone die kantonalrechtlichen Grundlagen geschaffen und in über 300 erfolgreichen Versuchen einem Teil ihrer Stimmberechtigten die elektronische Stimmabgabe ermöglicht. In allen Kantonen wurden die Auslandschweizer Stimmberechtigten zu den Versuchen zugelassen, in einigen Kantonen zusätzlich ein Teil der in der Schweiz wohnhaften Stimmberechtigten. Den Kantonen standen in den letzten Jahren zwei Systeme für die elektronische Stimmabgabe zur Verfügung: Das System des Kantons Genf sowie jenes der Schweizerischen Post. Da beide Anbieter ihre Systeme Mitte 2019 zurückgezogen haben, steht E-Voting in der Schweiz derzeit nicht zur Verfügung (vgl. dazu Kapitel 1.3.1 und 1.3.2).

1.2 Rahmenbedingungen des bisherigen Versuchsbetriebs

1.2.1 Aufgaben und Rollen von Bund und Kantonen

Bei der Ausübung der politischen Rechte besteht eine föderalistische Kompetenzaufteilung. Für eidgenössische Urnengänge werden auf Bundesebene die Rahmenbedingungen festgelegt und die Kantone sind für die Durchführung zuständig. Diese Kompetenzaufteilung gilt auch im Bereich der elektronischen Stimmabgabe und ist in den bestehenden Rechtsgrundlagen zu den Versuchen mit E-Voting abgebildet. Demnach entscheiden die Kantone, ob sie ihren Stimmberechtigten die elektronische Stimmabgabe im Rahmen eines Versuchs zur Verfügung stellen wollen. Sie können dafür ein eigenes System betreiben oder das System eines anderen Kantons oder eines privaten Unternehmens nutzen (Art. 27k^{bis} Abs. 1 Bst. b VPR). Der Bund ist für die Bewilligung und Zulassung der Versuche zuständig, unterstützt die Kantone in rechtlichen, organisatorischen und technischen Belangen und koordiniert die Vorhaben auf nationaler Ebene.

1.2.2 Schrittweise Einführung als dritter Stimmkanal

Seit Beginn des Projekts gilt der Grundsatz «Sicherheit vor Tempo». E-Voting soll schrittweise eingeführt werden. In den Rechtsgrundlagen des Bundes werden hohe Sicherheitsanforderungen an die E-Voting-Systeme und deren Betrieb gestellt. Diese sind strukturell an die schrittweise Weiterentwicklung der elektronischen Stimmabgabe gebunden. Die abgestuften Anforderungen sehen eine Limitierung des Elektorats vor, das für die elektronische Stimmabgabe zugelassen werden kann. Diese Limiten sehen eine Zulassung bis zu 30, 50 oder 100 Prozent des kantonalen Elektorats sowie bis zu 10, 30 oder 100 Prozent des gesamtschweizerischen Elektorats vor. Die stimmberechtigten Auslandschweizerinnen und -schweizer werden bei der Berechnung der Limiten nicht mitgezählt.

1.2.3 Kontrolle und Aufsicht

Bewilligungsverfahren

Die Kantone benötigen für den Einsatz der elektronischen Stimmabgabe eine Grundbewilligung des Bundesrates sowie für jeden Urnengang eine Zulassung der BK. Im Rahmen des Bewilligungsverfahrens prüft die BK die Konformität mit den Rechtsgrundlagen des Bundes.

¹ Der Kanton Genf hat die ersten Versuche mit E-Voting auf kantonaler Ebene bereits 2003 durchgeführt.

Für Kantone, die erstmals Versuche mit der elektronischen Stimmabgabe durchführen, kann die Grundbewilligung für höchstens fünf Urnengänge erteilt werden (Art. 27a Abs. 2 VPR). Danach kann der Bundesrat eine Grundbewilligung für eine längere Dauer erteilen (Art. 27a Abs. 3 VPR). In der Praxis beträgt die Höchstdauer zwei Jahre (BBI 2013 5194). Für den Einsatz des elektronischen Stimmkanals bei den Nationalratswahlen bedarf es jeweils einer besonderen Grundbewilligung (Art. 27a Abs. 4 VPR).

Unabhängige Überprüfung

Die Kantone sorgen gemäss Artikel 7 VEeS dafür, dass die Erfüllung der Anforderungen von unabhängiger Stelle überprüft wird. Möchte ein Kanton den elektronischen Stimmkanal für mehr als 30 bzw. 50 Prozent seines kantonalen Elektorats anbieten, so sind erhöhte Anforderungen an die Prüfung des Systems zu erfüllen. Solche Überprüfungen sind in der Regel von Stellen durchzuführen, die von der schweizerischen Akkreditierungsstelle (SAS) akkreditiert worden sind. Die Einzelheiten der Zertifizierung sind in der VPR und in der VEeS geregelt.

Ergänzend wurden im Rahmen der Bewilligungsverfahren jeweils sogenannte «Begleitgruppen» eingesetzt, die sich aus Vertretenden der Kantone zusammensetzten. Die Begleitgruppen führten Benutzer-tests durch, konnten Rückfragen zu den Gesuchsunterlagen stellen und dienten dem Informationsaustausch.

1.2.4 Sicherheitsanforderungen

Die technischen und betrieblichen Anforderungen sind in der VEeS sowie deren Anhang festgelegt. Die zentralen Anforderungen zur Einhaltung hoher Sicherheitsstandards bei E-Voting sind folgende:

- Verifizierbarkeit: Die Verifizierbarkeit erlaubt es, Manipulationen unter Einhaltung des Stimmgeheimnisses festzustellen. Die VEeS unterscheidet zwischen individueller und vollständiger Verifizierbarkeit:
 - Die individuelle Verifizierbarkeit erlaubt es den Stimmenden festzustellen, ob ihre Stimme durch das System korrekt registriert wurde, namentlich so wie sie der Stimmende abgegeben hat. Damit können sie ausschliessen, dass ihre Stimme auf der zur Stimmabgabe verwendeten Plattform oder im Internet missbräuchlich verändert wurde.
 - Die vollständige Verifizierbarkeit gewährleistet, dass systematische Fehlfunktionen infolge von Softwarefehlern, menschlichen Fehlleistungen oder Manipulationsversuchen im gesamten Wahl- bzw. Abstimmungsablauf dank unabhängiger Mittel erkannt werden. Zum Schutz des Stimmgeheimnisses ist sichergestellt, dass die Stimmen vom Zeitpunkt der Stimmabgabe bis zur Entschlüsselung der kryptografisch gemischten Stimmen zu keinem Zeitpunkt in unverschlüsselter Form vorliegen und nicht entschlüsselt werden können. Um den scheinbaren Widerspruch zwischen der Nachvollziehbarkeit und der Wahrung des Stimmgeheimnisses aufzulösen, müssen kryptografische Verfahren zum Einsatz kommen, die speziell für die elektronische Stimmabgabe konzipiert werden.
- Verteilung der Verantwortung: Die E-Voting-Systeme müssen auf eine Vielzahl von verschieden ausgestalteten Computern verteilt sein, wovon ein Teil nicht ans Internet angeschlossen sein darf. Auch muss technisch und organisatorisch sichergestellt sein, dass keine Einzelpersonen ohne Mehr-Augen-Kontrolle auf kritische Daten oder auf Stimmen zugreifen können.
- Überprüfung: Die Systeme werden regelmässig durch unabhängige Organisationen geprüft (externe Audits, Zertifizierung, Wiederholungsaudits für die Rezertifizierung). Das kryptografische Protokoll wird von hochspezialisierten Fachpersonen im Bereich Kryptografie geprüft.
- Beste Praktiken: Gemäss dem obligatorischen, kontinuierlichen Verbesserungsprozess müssen die Systeme stets angepasst und laufend gegen die neuesten Sicherheitslücken geschützt werden.

1.2.5 Risiko- und Krisenmanagement

Der Kanton ist für die Durchführung von eidgenössischen Urnengängen verantwortlich und trägt die Risiken beim Einsatz der elektronischen Stimmabgabe. Er muss mit einer Risikobeurteilung darlegen, dass sich jegliche Sicherheitsrisiken in einem ausreichend tiefen Rahmen bewegen. Die Anforderungen an die Risikobeurteilungen sind in Artikel 3 in Verbindung mit Artikel 6 VEeS festgehalten.

In einer Krisenvereinbarung legen Bund und Kantone fest, wie die Information, Zusammenarbeit und Kommunikation bei einem Vorfall mit der elektronischen Stimmabgabe erfolgen soll.

1.2.6 Transparenzmassnahmen

Das Vertrauen der Öffentlichkeit in die Stimmkanäle ist zentral. Deshalb sind im Bereich der elektronischen Stimmabgabe verschiedene transparenzfördernde Massnahmen vorgesehen. So fordert das Bundesrecht insbesondere, dass der Quellcode und die Dokumentation von vollständig verifizierbaren Systemen veröffentlicht werden muss (Art. 7a und 7b VEeS). Ausserdem haben sich der Bund und die Kantone 2017 in einer Absichtserklärung dazu bekannt, dass vor dem ersten Einsatz eines Systems mit vollständiger Verifizierbarkeit ein öffentlicher Intrusionstest (PIT) durchgeführt werden soll, bei dem interessierte Personen versuchen können, die Systeme zur elektronischen Stimmabgabe anzugreifen.

1.3 Situation 2019

1.3.1 System der Schweizerischen Post

Die Schweizerische Post bietet seit 2016 ein E-Voting-System mit individueller Verifizierbarkeit an, das von verschiedenen Kantonen eingesetzt worden ist. Zusätzlich hat sie ein neues System mit vollständiger Verifizierbarkeit entwickelt und im Februar 2019 dessen Quellcode gegenüber der Öffentlichkeit offengelegt. Zudem wurde dieses System vom 25. Februar bis am 24. März 2019 einem von Bund, Kantonen und Post organisierten öffentlichen Intrusionstest (PIT) unterzogen. Die Rückmeldungen der Teilnehmenden lieferten Hinweise zu Verbesserungspotenzial bei der Einhaltung von gewissen besten Praktiken im Bereich der Sicherheitstechnik. Ein Eindringen in die Infrastruktur, eine Manipulation von Stimmen oder ein Brechen des Stimmgeheimnisses konnte im Rahmen des PIT nicht festgestellt werden.²

Im offengelegten Quellcode wurden aber erhebliche Sicherheitsmängel im Bereich der Verifizierbarkeit entdeckt. Einer der Mängel betraf die individuelle Verifizierbarkeit und damit das System der Post, das bis dahin in Betrieb war. Die BK hat in der Folge eine unabhängige Überprüfung des individuell verifizierbaren Systems der Post in Auftrag gegeben. Dabei wurden auf der einen Seite die betrieblichen Abläufe bei der Post als positiv beurteilt, auf der anderen Seite wurden jedoch im System weitere Mängel festgestellt.³

Die Post hat im Juli 2019 kommuniziert, dass das individuell verifizierbare System nicht mehr eingesetzt wird und sie sich auf die Weiterentwicklung des vollständig verifizierbaren Systems konzentrierte.

1.3.2 System des Kantons Genf

Der Kanton Genf gehört zu den Pilotkantonen, die ihren Stimmberechtigten E-Voting bei eidgenössischen Urnengängen bereits 2004 anboten. Dazu hat der Kanton Genf ein eigenes System, das System CHVote, entwickelt und betrieben. Neben dem Kanton Genf haben mehrere Kantone dieses System eingesetzt, das die individuelle Verifizierbarkeit aufwies. Der Kanton Genf arbeitete seit 2016 an der Entwicklung eines Systems mit vollständiger Verifizierbarkeit.

² Vgl. dazu den Schlussbericht des Steuerungsausschusses «Vote électronique - Öffentlicher Intrusionstest 2019», August 2019 unter www.bk.admin.ch > Politische Rechte > Vote électronique > Öffentlicher Intrusionstest.

³ Mitglieder der E-Voting-Gruppe der Berner Fachhochschule (BFH) haben die Umsetzung des kryptografischen Protokolls in der Systemspezifikation und im Quellcode untersucht und die Forschenden Olivier Pereira (Université de Louvain) und Vanessa Teague (University of Melbourne) haben die Umsetzung des Protokolls aufgrund der Systemspezifikation geprüft. Ausserdem hat die Firma Oneconsult ausgehend von den Risikobeurteilungen der Kantone die Umsetzung der technisch-organisatorischen Sicherheitsmassnahmen begutachtet. Die Berichte sind auf der Webseite der BK publiziert: www.bk.admin.ch > Politische Rechte > Vote électronique > Berichte und Studien.

Im November 2018 hat der Kanton Genf darüber informiert, sein System CHVote nicht mehr weiterzuentwickeln, da es nicht in der Aufgabe eines Kantons liege, ein IT-System von solcher Komplexität und Grösse alleine zu entwickeln, zu betreiben und zu finanzieren.⁴ Im Juni 2019 hat der Kanton Genf kommuniziert, dass der Bundesratsentscheid zur Bewilligung von E-Voting bei den Nationalratswahlen aufgrund einer Verschiebung auf Mitte August zu spät erfolge und er den Betrieb seines bisherigen Systems per sofort einstellt.⁵ Somit wurde das Genfer System am Urnengang vom 19. Mai 2019 zum letzten Mal eingesetzt.

Der Kanton Genf hat 2016 Teile des Quellcodes des individuell verifizierbaren Systems unter Open-Source-Lizenz publiziert. 2019 erfolgte die Quellcode-Publikation des noch nicht fertig entwickelten Systems mit vollständiger Verifizierbarkeit.

1.3.3 Überführung in den ordentlichen Betrieb

Der Bundesrat hat am 19. Dezember 2018 das Vernehmlassungsverfahren für die Überführung des elektronischen Stimmkanals in den ordentlichen Betrieb eröffnet. Die in der Vernehmlassung unterbreitete Teilrevision des BPR hätte die Beendigung der Versuchsphase und die Verankerung der elektronischen Stimmabgabe als dritter Stimmkanal vorgesehen. Mit der Vorlage wären die wichtigsten Anforderungen im Gesetz geregelt worden, d.h. namentlich die Verifizierbarkeit der Stimmabgabe und der Ergebnisermittlung, die Öffentlichkeit von Informationen zum verwendeten System und dessen Betrieb, die Barrierefreiheit sowie die Pflicht der Kantone, für den Einsatz des elektronischen Stimmkanals über eine Bewilligung des Bundes zu verfügen. Die Kantone hätten immer noch frei entscheiden können, ob sie die elektronische Stimmabgabe einführen wollen oder nicht.

Aus der Vernehmlassung ging hervor, dass eine deutliche Mehrheit der Kantone und der Parteien die Einführung von E-Voting grundsätzlich begrüssen. Die Konferenz der Kantonsregierungen sowie 19 Kantone befürworteten die Überführung in den ordentlichen Betrieb. Diejenigen Parteien, die sich grundsätzlich für E-Voting aussprachen, erachteten die Zeit aber noch nicht als reif für diesen Schritt. Daher hat der Bundesrat am 26. Juni 2019 beschlossen, vorerst auf die Teilrevision des BPR zu verzichten.⁶

1.3.4 Schlussfolgerungen zur Situation 2019

Aus der im Jahre 2019 erfolgten Umsetzung der Transparenzmassnahmen und insbesondere aus der damit verbundenen Entdeckung von erheblichen Sicherheitsmängeln im bisherigen und zukünftigen Post-System lassen sich die folgenden Schlussfolgerungen ziehen:

- Die durchgeführten Transparenzmassnahmen haben wertvolle Beiträge zur Verbesserung der E-Voting-Systeme geleistet, indem wichtige Erkenntnisse gewonnen und Mängel aufgedeckt werden konnten.
- Mit der Offenlegung des Quellcodes und dem PIT konnten Erfahrungen im Bereich der «public scrutiny» und dem breiten Einbezug von externen Fachpersonen gesammelt werden. Diese Erfahrung zeigte auch den Handlungsbedarf bei der Ausgestaltung der Offenlegung und der Qualität des Quellcodes auf.
- Die Entdeckung erheblicher Mängel liess auf grössere Unzulänglichkeiten beim bisherigen Entwicklungsprozess schliessen und zeigte Handlungsbedarf im Bereich der Qualitätssicherung auf.
- Die festgestellten Mängel und Unzulänglichkeiten wurden mit den bisherigen Kontroll- und Zertifizierungsprozessen nicht erkannt. Die bestehenden Prozesse haben zu wenig gegriffen.

⁴ Medienmitteilung des Kantons Genf vom 28. November 2018, abrufbar unter www.ge.ch/document/point-presse-du-conseil-etat-du-28-novembre-2018#extrait-12897.

⁵ Medienmitteilung des Kantons Genf vom 19. Juni 2019, abrufbar unter www.ge.ch/document/point-presse-du-conseil-etat-du-19-juin-2019.

⁶ Medienmitteilung des Bundesrates vom 27. Juni 2019; abrufbar unter www.bk.admin.ch > Politische Rechte > E-Voting > Medienmitteilungen.

Die Entwicklungen im Projekt Vote électronique haben zu parlamentarischen Vorstössen auf Ebene des Bundes wie auch der Kantone geführt. Einerseits geht es um die Anforderungen an die Systemanbieter.⁷ Andererseits wird insgesamt die Sicherheit der elektronischen Stimmabgabe in Frage gestellt oder es werden Bedingungen an die Weiterführung des Versuchsbetriebs formuliert.⁸ Die Diskussion rund um E-Voting wird auch durch Mutmassungen zur Einflussnahme durch Drittstaaten bei Wahlen und durch Berichterstattungen über diverse Vorfälle im Bereich der Cyber-Sicherheit und des Datenschutzes unabhängig von der unmittelbaren Relevanz für E-Voting beeinflusst. Damit ist E-Voting Teil einer Grundsatzdebatte über Chancen und Risiken der Digitalisierung.⁹

1.4 Situation Ende 2020

Die Entwicklungen in den letzten Jahren haben auch dazu geführt, dass sich die Marktsituation auf der Anbieter- wie auch der Nachfrageseite verändert hat. Von den bisherigen Systemanbietern verbleibt momentan nur die Schweizerische Post. Sie ist die einzige Anbieterin, die in die Weiterentwicklung eines E-Voting-Systems investiert. Das im Jahre 2017 von Bund und Kantonen formulierte Ziel einer Mehrproduktstrategie ist nicht wie gewünscht erreicht worden. Vom E-Voting-System des Kantons Genf verbleibt der durch die Berner Fachhochschule fertiggestellte und unter einer Open-Source-Lizenz publizierte Kern des Systems mit vollständiger Verifizierbarkeit. Es hat sich gezeigt, dass Entwicklung und Betrieb eines Systems mit vollständiger Verifizierbarkeit ein anspruchsvolles und aufwändiges Unterfangen sind. Es ist davon auszugehen, dass sich an dieser Situation so rasch nichts ändern wird.

Auf der Nachfrageseite hat sich die Situation ebenfalls stark verändert. Während bei der Abstimmung vom 14. Juni 2015 in 14 Kantonen Versuche mit E-Voting durchgeführt wurden, boten bei der Abstimmung vom 10. Februar 2019 noch zehn Kantone den elektronischen Stimmkanal an. Es streben momentan nur wenige Kantone eine rasche Wiederaufnahme der Versuche an. Die anderen Kantone setzen bei der Digitalisierung auf andere Vorhaben. Dies führt auch dazu, dass zum Teil langjährige E-Voting-Verantwortliche in den Kantonen andere Aufgaben übernehmen und Know-how verloren geht. Ob und wie die Neuausrichtung bei E-Voting gelingt, hängt entscheidend davon ab, dass die verbleibende Systemanbieterin sowie die verbleibenden Kantone weiterhin bereit sind, in die Weiterentwicklung des Post-Systems und die Wiederaufnahme der Versuche zu investieren, und dass in den nächsten Jahren wieder neue Kantone dazu stossen.

1.5 Neuausrichtung des Versuchsbetriebs

1.5.1 Auftrag des Bundesrates und Zielsetzung

Im Juni 2019 beauftragte der Bundesrat die BK, gemeinsam mit den Kantonen bis Ende 2020 eine Neuausrichtung des Versuchsbetriebs von E-Voting zu konzipieren.¹⁰ Dieser Entscheid stützte sich auf die Ergebnisse der Vernehmlassung zu einer Überführung von E-Voting in den ordentlichen Betrieb sowie auf die entdeckten Mängel im System der Post.

Die Neuausrichtung des Versuchsbetriebs hat sich gemäss Auftrag des Bundesrats an den folgenden Zielen zu orientieren:

1. Weiterentwicklung der Systeme
2. Wirksame Kontrolle und Aufsicht

⁷ Bund: Mo. 18.4225 Wehrli «Elektronische Stimmabgabe in den Grundversorgungsauftrag der Post aufnehmen»; Mo. 18.4375 Sommaruga «E-Voting. Ein schneller und entschlossener Einsatz für ein System auf Open-Source-Basis und in öffentlicher Hand»; Kantone: u.a. Annahme eines Gesetzesentwurfs durch den Genfer Kantonsrat, der fordert, dass das vom Kanton eingesetzte System in seiner Konzeption, seiner Führung und seinem Betrieb vollständig in öffentlicher Hand sein muss.

⁸ Bund: Parl. Initiative Müller 18.427 «Ja zu E-Voting, aber Sicherheit kommt vor Tempo»; parl. Initiative Zanetti 18.468 «Marschhalt beim E-Voting»; Mo. 19.3294 Zanetti «E-Versand statt E-Voting»; Kantone: u.a. Kantonsrat St. Gallen: Ablehnung der Motion 42.19.07, die einen sofortigen Übungsabbruch für E-Voting fordert; Kantonsrat Luzern: Ablehnung der Motion 683 über ein Moratorium für E-Voting im Kanton Luzern.

⁹ Vgl. dazu u.a. Forschungsstelle Sotomo (2018): Digitale Lebensvermessung und Solidarität, Verhalten und Einstellungen der Schweizer Bevölkerung, Zürich; digitalswitzerland (2019): Am digitalen Puls der Bevölkerung, Ein Bericht über die Einstellung der Bevölkerung zum Thema Digitalisierung, aufgenommen im Rahmen des Digitaltags 2019.

¹⁰ Medienmitteilung des Bundesrates vom 27. Juni 2019; abrufbar unter www.bk.admin.ch > Politische Rechte > E-Voting > Medienmitteilungen.

3. Stärkung der Transparenz und des Vertrauens

4. Stärkere Vernetzung mit der Wissenschaft

Im Rahmen der Neuausrichtung ist gemäss Auftrag des Bundesrates zu prüfen, inwiefern die Anforderungen des Bundesrechts angepasst werden müssen. Diese müssen geeignet sein, um die Qualität und Sicherheit der eingesetzten Systeme wirksam zu messen und sicherzustellen. Die Anforderungen müssen zudem die Erwartungen der Politik und Öffentlichkeit bezüglich Sicherheit und Transparenz erfüllen, um das Vertrauen stärken zu können.

1.5.2 Zusammenarbeit von Bund und Kantonen

Gestützt auf den Auftrag des Bundesrates hat der Steuerungsausschuss Vote électronique (SA VE) am 29. November 2019 die Unterarbeitsgruppe Neuausrichtung und Wiederaufnahme der Versuche (UAGNW) eingesetzt. Die UAGNW erhielt den Auftrag, Massnahmen für die Neuausrichtung und die Wiederaufnahme der Versuche auszuarbeiten. Sie soll weiter eine Etappierung der Massnahmen vorschlagen, damit eine Wiederaufnahme der Versuche mit dem vollständig verifizierbaren Post-System im Rahmen der ersten Etappe der Neuausrichtung möglich wird.

Die UAGNW setzte sich aus dem Projektteam Vote électronique der BK (Leitung und Sekretariat) sowie Vertreterinnen und Vertretern der Kantone Bern, Fribourg, Basel-Stadt, St. Gallen, Graubünden, Aargau, Thurgau und Neuenburg zusammen. Die Arbeiten der UAGNW haben im Zeitraum von Dezember 2019 bis Oktober 2020 stattgefunden. Die Post als verbleibende Systemanbieterin war jeweils an den Sitzungen der UAGNW vertreten.¹¹ Der vorliegende Bericht umfasst die Ergebnisse der Arbeiten der UAGNW. Der SA VE hat den Bericht an seiner Sitzung vom 30. November 2020 verabschiedet.

¹¹ Die Post als Systemanbieterin ist gegenüber den Kantonen verantwortlich für Entwicklung und Betrieb ihres E-Voting-Systems. Die Post wurde zum Dialog eingeladen, damit sie ihre Expertise in der praktischen Umsetzung der Sicherheitsanforderungen einbringen konnte. Sie konnte nicht über die Massnahmen zur Neuausrichtung mitbestimmen.

2. Dialog mit der Wissenschaft

2.1 Einbezug von Expertinnen und Experten

Zur Erarbeitung der Grundlagen für die Neuausrichtung hat die BK unter Mitwirkung der weiteren Mitglieder der UAGNW einen Dialog mit Expertinnen und Experten aus der Wissenschaft und einigen Expertinnen und Experten aus der Industrie geführt. Die von der BK mandatierten verwaltungsexternen Expertinnen und Experten umfassten Vertreterinnen und Vertreter aus Informatik, Kryptografie sowie Politikwissenschaften.¹² Sie haben die UAGNW bei der Erörterung des Handlungsbedarfs und von Fragestellungen rund um mögliche Massnahmen für die Neuausrichtung unterstützt. Der Dialog mit der Wissenschaft wurde aus Mitteln von E-Government Schweiz finanziert.

Vertreterinnen und Vertreter weiterer Kantone¹³ und Bundesstellen¹⁴ wurden laufend über den Dialog mit der Wissenschaft informiert und erhielten einen Zugang zur Diskussionsplattform.

2.2 Vorgehen und Ausgestaltung des Dialogs

Für den Dialog mit den externen Expertinnen und Experten hat die BK unter Einbezug der weiteren Mitglieder der UAGNW folgende Themenbereiche definiert, zu denen verschiedene Fragestellungen diskutiert wurden:

1. Risiken und Sicherheitsmassnahmen heute und morgen
2. Unabhängige Überprüfungen
3. Zusammenarbeit Wissenschaft und Einbezug Öffentlichkeit
4. Transparenz und Vertrauensbildung
5. Risikobeurteilung und Massnahmenplan
6. Krisenmanagement

Zu Beginn des Dialogs wurde den Expertinnen und Experten im Februar 2020 ein umfassender Fragebogen mit rund 60 Fragen zugestellt. Aufgrund der Massnahmen zur Eindämmung des Coronavirus wurden die ursprünglich geplanten Workshops mit einem moderierten schriftlichen Dialog auf einer Internetplattform ersetzt. Die Diskussionen auf der Plattform fanden zwischen Mai und Juli 2020 statt.

Der Fragebogen umfasste alle sechs Themenbereiche. Die Expertinnen und Experten erhielten die Möglichkeit, allgemeine Überlegungen zum Thema «vertrauenswürdige E-Voting» zu äussern, konkrete Fragestellungen im Zusammenhang mit möglichen Massnahmen zu beantworten sowie weitere Massnahmen vorzuschlagen. Das Ziel des Fragebogens bestand in einer breiten Übersicht, die es erlaubte, Konsens sowie Diskussions- und Klärungsbedarf zu erkennen und strukturiert anzugehen.

Gestützt auf die Auswertung der Antworten auf den Fragebogen wurden die folgenden Diskussionsblöcke für die Internetplattform definiert:

Themenbereiche	Diskussionsblöcke
1	Block 1: Wirksamkeit der Kryptografie
1	Block 2: Diversität zur Förderung von Sicherheit und Vertrauen
1	Block 3: Druckerei (Verteilte Parametergenerierung)
1	Block 4: Public Bulletin Board
2	Block 5: Mandatierte Überprüfung
4	Block 6: Entwicklung und Offenlegung
4	Block 7: Public Intrusion Test / Bug Bounty

¹² Vgl. Liste der mandatierten Expertinnen und Experten vom Juni 2020 unter www.bk.admin.ch > Politische Rechte > E-Voting.

¹³ Kantone Zürich, Luzern, Glarus, Tessin und Genf.

¹⁴ Nationales Zentrum für Cybersicherheit (NCSC), Führungsunterstützungsbasis (FUB), Büro des Sondergesandten für Cyber-Aussen- und -Sicherheitspolitik des EDA und OIC MELANI des Nachrichtendienstes des Bundes (NDB).

5	Block 8: Risikomanagement
5	Block 9: Risikominimierende Audits und Plausibilisierung zur Limitierung von Risiken
6	Block 10: «Forensic Readiness»
alle	Block 11: Gesamtbild («Big Picture»)
3	Block 12: Zukünftiger Dialog

Zu jedem Diskussionsblock wurden Thesen, Lösungsvorschläge und offene Fragen für die schriftliche Diskussion mit und unter den Expertinnen und Experten aufbereitet. Die Teilnehmenden diskutierten verschiedene Themen parallel, konnten Stellungnahmen auf die Antworten anderer Teilnehmenden verfassen oder Fragen aneinander richten. Die Beiträge waren jeweils für alle Teilnehmenden sichtbar. Ziel war das Festhalten von Konsens, die Klärung von offenen Fragen, das Validieren von Schlussfolgerungen und gegebenenfalls das Festhalten von abweichenden Haltungen.

Insgesamt wurden auf der Plattform über 700 Stellungnahmen erfasst. Darunter befanden sich sowohl kurze als auch ausführliche Antworten. Parallel zur Diskussion auf der Plattform wurden einzelne Expertinnen und Experten mit der Behandlung von weiteren Fragestellungen rund um mögliche Massnahmen mandatiert. Zum Abschluss des Dialogs hat die BK unter Einbezug weiterer Mitglieder der UAGNW eine Zusammenfassung erstellt. Die entsprechenden Dokumente sind auf der Webseite der BK publiziert.¹⁵

Der Dialog mit den Expertinnen und Experten wurde im Auftrag der BK von Christian Folini, Senior Security Consultant bei der netnea AG, moderiert.

2.3 Zusammenfassung der Ergebnisse des Dialogs

2.3.1 Allgemeine Einschätzung

Die Expertinnen und Experten sehen Handlungsbedarf bei der Sicherheit, der Transparenz sowie der unabhängigen Prüfung. Gleichzeitig vertreten die Expertinnen und Experten die Ansicht, dass während der letzten 15 Jahre wertvolle Ergebnisse erzielt wurden. Sie empfehlen, Fragen der Sicherheit auch bei den übrigen Stimmkanälen zu analysieren. Fragen der Vertrauensbildung sind weiter zu vertiefen.

Die Expertinnen und Experten unterstreichen die Wichtigkeit, Fachpersonen – namentlich aus der Wissenschaft – bei der Konzeption, der Entwicklung und der Prüfung von E-Voting Systemen laufend einzubeziehen. Die Beauftragung eines wissenschaftlichen Komitees wurde verschiedentlich angeregt.

2.3.2 Bereitstellung eines sicheren Systems

Behörden sollen weiterhin die Sicherheit vorgeben

Es soll nach Ansicht der Expertinnen und Experten die Aufgabe der Behörden bleiben, Risiken zu beurteilen und bei Bedarf Massnahmen vorzusehen. Ein wissenschaftliches Komitee könnte dabei eine Funktion übernehmen.

Standardisierung der kryptografischen Bausteine

Die bereits heute geforderten Sicherheitsbeweise im Bereich der Kryptografie sind wichtig; sie sollen laufend dem aktuellen Stand der Wissenschaft angepasst werden. Zudem raten die Expertinnen und Experten den Behörden, auf eine Standardisierung der kryptografischen Bausteine hinzuwirken.

Qualität und Überprüfbarkeit des Quellcodes gewährleisten

Es muss darauf geachtet werden, dass die Systemdokumentation und der Quellcode in einer Form vorliegen, die eine effiziente Überprüfung der Konformität mit den rechtlichen Anforderungen zulässt. Die

¹⁵ www.bk.admin.ch > Politische Rechte > E-Voting.

Expertinnen und Experten haben als mögliche Grundlage für die Entwicklungsprozesse verschiedene Standards genannt. Simplizität soll bei der Systemkonzeption als Grundprinzip gelten.

Mehr Diversität als Grundvoraussetzung für Vertrauenswürdigkeit

Diversität unter den Komponenten, die für die Verifizierbarkeit wichtig sind (sog. Kontrollkomponenten und Verifier), bildet für die Expertinnen und Experten eine Grundvoraussetzung für die Vertrauenswürdigkeit eines Systems: Fehler in einzelnen Komponenten sollen dank anderen, korrekt funktionierenden Komponenten keine negative Auswirkung auf die Verifizierbarkeit haben (exponentieller Sicherheitsgewinn). Zu den Elementen für eine Diversifizierung gehört die Software. Verbesserungspotenzial sehen die Expertinnen und Experten auch bei der Generierung der Systemparameter (beispielsweise der Prüfcodes für die individuelle Verifizierbarkeit), die verifizierbar und verteilt durchgeführt werden sollte. Für den Druck der Stimmrechtsausweise haben sie Lösungen für einen verteilten Druckprozess skizziert. Die Expertinnen und Experten anerkennen die Kosten und Erhöhung der Komplexität beim Betrieb, die durch die Einführung von mehr Diversität entsteht, unterstreichen jedoch den Mehrwert.

Public Bulletin Board für noch mehr Verifizierbarkeit

Als komplementärer Ansatz, um die Verifizierbarkeit auszubauen und unabhängiger zu gestalten, wurde der Einsatz eines sogenannten öffentlichen Anschlagbretts (Public Bulletin Board) diskutiert, das aus der wissenschaftlichen Literatur zu E-Voting bekannt ist. Die Expertinnen und Experten betrachten ein solches, öffentliches Anschlagbrett als geeignetes Instrument für die Vertrauensbildung, sehen das Vertrauen aber auch gefährdet, wenn bei der Konzeption oder der Umsetzung Fehler gemacht werden. Die Bedürfnisse der Stimmenden, namentlich bei der Kommunikation, der visuellen Darstellung oder der Benutzerfreundlichkeit, müssen frühzeitig untersucht und berücksichtigt werden.

2.3.3 Mandatierte und öffentliche Prüfung

Mandatierte Überprüfung

Der Zertifizierung der Systeme wird keine entscheidende Bedeutung beigemessen. Dennoch könnte im Rahmen der Prüfung des Betriebs eine Zertifizierung sinnvoll sein (Zertifizierung nach ISO27001). Statt auf Zertifizierungen sollen die Behörden auf unabhängige Prüfungen durch Personen mit den nötigen Kompetenzen setzen. Kryptografinnen und Kryptografen sollen auch bei der Prüfung des Quellcodes und des Betriebs beigezogen werden. Die Überprüfung muss einem ganzheitlichen Konzept folgen, um Lücken zu verhindern. Die Überprüfung soll durch den Bund oder ein unabhängiges Komitee in Auftrag gegeben werden.

Öffentliche Überprüfung

Die Expertinnen und Experten messen der öffentlichen Überprüfung eine grosse Wichtigkeit zu. Sie würden es daher begrüßen, wenn der 2019 durchgeführte PIT durch ein ständig laufendes Bug-Bounty-Programm mit finanzieller Entschädigung ersetzt würde. Das Bug-Bounty-Programm soll sich nicht auf erfolgreiche Angriffe auf die Infrastruktur des Anbieters beschränken, sondern auch Fehler in der Dokumentation des Systems sowie im Quellcode zum Gegenstand haben. Die Festlegung der Zielsetzung und Modalitäten sowie die Oberaufsicht über das Bug-Bounty-Programm werden beim Bund oder einem unabhängigen Komitee gesehen.

Zusätzlich zum Bug-Bounty-Programm könnten auch weitere Massnahmen für die Beteiligung der Öffentlichkeit geprüft werden, wie beispielsweise Hackathons. Auch der Einbezug von Personen ohne einen technischen Hintergrund könnte sich als sinnvoll erweisen, beispielsweise im Rahmen eines Citizen-Science-Projekts, das sich der Benutzerfreundlichkeit oder der Kommunikation widmet.

Transparenz und Offenlegung des Quellcodes

Transparenz bildet die Voraussetzung für eine wirksame öffentliche Überprüfung. Bei der Offenlegung des Quellcodes sollte nach Ansicht der Expertinnen und Experten auf eine Geheimhaltungserklärung unbedingt verzichtet werden.

Neben dem Quellcode sollen alle Unterlagen offengelegt werden, die nötig sind, um zu verstehen, wie das System funktioniert und betrieben wird. Zudem soll es möglich sein, das System auf eigenen Rechnern zu testen. Mit Blick auf den Fall, dass Anpassungen am Quellcode nicht unmittelbar offengelegt werden, raten die Expertinnen und Experten, eine erste Iteration an Prüfungen vorzunehmen, um unnötige Fehler und den damit verbundenen Vertrauensverlust zu vermeiden.

Mängel sollen offengelegt und Hinweise aus der Öffentlichkeit beantwortet werden. Die detaillierten Bestimmungen dazu soll der Bund festlegen. Die Mehrheit der Expertinnen und Experten rät zudem, Prüfberichte zu publizieren. Manche geben aber zu bedenken, dass Prüfberichte, die qualitativ mangelhaft sind, zu einem Vertrauensverlust führen können.

Die Expertinnen und Experten halten es für möglich, dass eine Offenlegung auch ohne Open-Source-Lizenz¹⁶ eine zielführende öffentliche Prüfung ermöglicht. Allerdings erachten sie eine Offenlegung unter einer Open-Source-Lizenz als erfolgsversprechender.

Umgang mit Nichtkonformitäten

Idealerweise findet die Überprüfung so weit im Vorfeld statt, dass Nichtkonformitäten so früh entdeckt werden, dass sie für den Einsatz behoben werden können. Für den Umgang mit Nichtkonformitäten, die spät entdeckt werden, sollen Entscheidungsprozesse festgelegt werden.

Nicht bei jeder Nichtkonformität muss der Einsatz von E-Voting gestoppt werden. Die Expertinnen und Experten halten es für nachvollziehbar, dass geringe Risiken akzeptiert werden. Die Schwierigkeit besteht darin, das Risiko richtig einzuschätzen. Vergleiche mit bereits akzeptierten Risiken können helfen. Ebenso zu berücksichtigen sind der faktische Verlust des Stimmrechts von Teilen des Auslandschweizer Elektorats sowie die Tatsache, dass der Verzicht auf E-Voting eine verstärkte Nutzung der ebenfalls risikobehafteten brieflichen Stimmabgabe zur Folge hat. Je stärker eine Nichtkonformität das System betrifft und je weniger sie sich auf die umgebenden Prozesse beschränkt, desto eher muss sie behoben werden. Fehler im kryptografischen Protokoll oder dessen Umsetzung im Quellcode sollen grundsätzlich nicht akzeptiert werden.

2.4 Einschätzungen zum Dialog mit der Wissenschaft

Der Einbezug von Expertinnen und Experten aus verschiedenen Fachgebieten hat zu einer breiten Diskussion des Handlungsbedarfs und möglicher Lösungen geführt und bot der UAGNW eine gute Grundlage für ihre Arbeit. Die Rückmeldungen der beteiligten Expertinnen und Experten zum Dialog sind positiv; sie haben den Einbezug begrüsst. Ausserdem befürworten sie eine Weiterführung im Rahmen eines ständigen Austausches zwischen den Behörden und der Wissenschaft. Der durchgeführte Dialog mit der Wissenschaft hat insbesondere technische Fragestellungen ins Zentrum gestellt, in Zukunft sollten sozialwissenschaftliche Themenbereiche stärker akzentuiert werden. Die Expertinnen und Experten äusseren zudem die Ansicht, dass bei der Sicherheitsdiskussion neben E-Voting auch die übrigen Stimmkanäle einzubeziehen seien. Eine ganzheitliche Sicht auf mögliche Angriffe würde der Verbesserung der Sicherheit bei Wahlen und Abstimmungen insgesamt dienen.

Der Bund und die Kantone teilen die Meinung, dass auch in Zukunft verstärkt mit Expertinnen und Experten aus Industrie und Wissenschaft zusammengearbeitet werden soll. Die UAGNW sieht dazu Massnahmen vor, um den Einbezug in verschiedenen Bereichen zu fördern.

¹⁶ Open-Source-Lizenzen erlauben die Verwendung der Software für beliebige Zwecke.

3. Beschreibung der Massnahmen

In der Folge werden die Massnahmen für die Neuausrichtung und Wiederaufnahme der Versuche erläutert und beurteilt und es wird ein Bezug zum Dialog mit der Wissenschaft hergestellt (s. Kap. 2.3 sowie die Zusammenfassung der Ergebnisse des Dialogs).¹⁷ Die Übersicht zu den Massnahmen befindet sich im Massnahmenkatalog im Anhang. Die Inputs der Expertinnen und Experten werden bei der Umsetzung der Massnahmen berücksichtigt.

A. Weiterentwicklung der Systeme

Nr.	Massnahme	Zeitpunkt Umsetzung	Zuständigkeit
A.1	Präzisierung der Kriterien für die Qualität des Quellcodes und der Dokumentation	Wiedereinsatz	Anforderungen: BK Umsetzung: Kantone, Systemanbieter
<p><u>Zielsetzung und Beschreibung der Massnahme</u></p> <p>Die Qualität des Quellcodes und der Dokumentation ist ein zentrales Element für die Sicherheit von E-Voting. In den heute geltenden Rechtsgrundlagen werden die entsprechenden Anforderungen gestellt. Diese umfassen jedoch eher allgemeine Umschreibungen, wie etwa die Aufbereitung und Dokumentation nach besten Praktiken (Art. 7b VELeS) und die Umsetzung bestimmter Punkte der Common Criteria, die nach dem Schutzprofil des Deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) ausgewählt wurden. In diesem Bereich besteht Handlungsbedarf. Die BK wird deshalb die bestehenden Qualitätskriterien präzisieren, die der Quellcode und seine Dokumentation erfüllen müssen. Mit klaren Kriterien soll eine hohe Qualität der E-Voting-Systeme sichergestellt werden. Ausserdem sollen die Prüfungen aller Akteure sowie der Öffentlichkeit erleichtert werden.</p> <p>Die BK wird sich bei der Präzisierung der Qualitätskriterien an bestehenden Normen orientieren (z.B. ISO Systems and software Quality Requirements and Evaluation) und die Rechtsgrundlagen entsprechend anpassen. Beim Wiedereinsatz der Versuche sind diese Kriterien einzuhalten. Zudem soll sich der Qualitätssicherungsprozess bei der Softwareentwicklung ebenfalls auf diese Kriterien abstützen.</p> <p><u>Dialog mit der Wissenschaft</u></p> <p>Der Quellcode und die Dokumentation müssen eine hohe Qualität aufweisen und in einer Form vorliegen, die eine wirksame Überprüfung der Konformität mit den rechtlichen Anforderungen und dem Sicherheitsmodell zulässt. Zudem soll bei der Systemkonzeption Simplizität als Grundprinzip gelten. Die Qualität des Quellcodes und der Dokumentation ist ein Querschnittsthema, für detailliertere Einschätzungen der Expertinnen und Experten wird auf die Ausführungen zu weiteren Massnahmen verwiesen (z.B. unabhängige Überprüfungen, Qualitätssicherung im Entwicklungsprozess, Offenlegung des Quellcodes).</p> <p><u>Auswirkungen der Massnahme¹⁸ und Gesamtbeurteilung des SA VE</u></p> <p>Eine hohe Qualität des Quellcodes und der Dokumentation wurde bei E-Voting immer gefordert. Die entsprechenden Qualitätsanforderungen werden nun präzisiert. Damit wird einerseits gegenüber den Systemanbietern Transparenz über das geforderte Anforderungsniveau geschaffen und andererseits hilft dies zu gewährleisten, dass die Software in der erwarteten Qualität entwickelt wird. Zudem soll damit die Überprüfbarkeit von Quellcode und Dokumentation verbessert werden. Diese Massnahme steht im Zusammenhang mit der Qualitätssicherung im Entwicklungsprozess (Massnahme A.2), dem Build und Deployment (Massnahme A.3), den unabhängigen Überprüfungen (Massnahmen B.1 und B.2) und der Offenlegung des Quellcodes (Massnahme C.2).</p> <p>Die Sicherstellung einer hohen Qualität des Quellcodes und der Dokumentation führt grundsätzlich zu hohen Kosten. Da es sich bei dieser Massnahme um eine Präzisierung der Qualitätskriterien handelt, ist nicht mit zusätzlichen Kosten für Bund und Kantone zu rechnen.</p>			

¹⁷ Die vollständigen Dokumente sind auf der Webseite der BK publiziert: www.bk.admin.ch > Politische Rechte > E-Voting.

¹⁸ Bei den finanziellen Auswirkungen werden jeweils Schätzungen von zusätzlich anfallenden Kosten (externen Kosten oder zusätzlichen Ressourcen) von Bund und Kantonen angegeben. Skala: Tief (<50'000 CHF) / mittel (50'000-500'000 CHF) / hoch (500'000-1 Mio. CHF) / sehr hoch (> 1 Mio. CHF).

Nr.	Massnahme	Zeitpunkt Umsetzung	Zuständigkeit
A.2	Stärkung der Qualitätssicherung im Entwicklungsprozess von E-Voting-Systemen	Wiedereinsatz	Anforderungen: BK Umsetzung: Kantone, Systemanbieter

Zielsetzung und Beschreibung der Massnahme

Die Qualität von E-Voting-Systemen muss während des gesamten Entwicklungsprozesses sichergestellt werden. Um die Qualitätssicherung zu stärken, werden die Anforderungen der BK präzisiert. Damit sollen folgende Ziele erreicht werden:

- Anpassungen im System müssen nachvollzogen und überprüft werden können.
- Die Nachvollziehbarkeit zwischen den einzelnen Elementen der Dokumentation (Protokoll, Spezifikation, Architektur, etc.) und dem Quellcode muss laufend und in beide Richtungen sichergestellt werden können.
- Die Ergebnisse von Prüfprozessen fliessen in die Entwicklungsarbeiten ein.
- Die Konformität mit den rechtlichen Anforderungen wird während des gesamten Lebenszyklus sichergestellt und aufrechterhalten.

Die BK präzisiert für die Wiederaufnahme der Versuche die entsprechenden Anforderungen in den Rechtsgrundlagen.

Dialog mit der Wissenschaft

Die Expertinnen und Experten haben als mögliche Grundlage für die Entwicklungsprozesse verschiedene Standards genannt. Viele Expertinnen und Experten stellen die Nachvollziehbarkeit des Entwicklungsprozesses ins Zentrum. Ausserdem wurde die Wichtigkeit der Transparenz, des Einbezugs von unabhängigen Expertinnen und Experten sowie der korrekten Bereitstellung des Systems aus dem Quellcode hervorgehoben (vgl. dazu die Massnahmen A.1, A.3 und C.2). Die bereits heute geforderten Sicherheitsbeweise im Bereich der Kryptografie sind wichtig, sie sollen laufend dem aktuellen Stand der Wissenschaft angepasst werden. Zudem raten die Expertinnen und Experten den Behörden, auf eine Standardisierung der kryptografischen Bausteine hinzuwirken.

Auswirkungen der Massnahme und Gesamtbeurteilung des SA VE

Die Stärkung der Qualitätssicherung im Entwicklungsprozess wird als wichtig erachtet. Mit der Präzisierung der bestehenden Anforderungen wird sichergestellt, dass der Qualität des Systems im gesamten Entwicklungsprozess eine hohe Wichtigkeit beigemessen wird. Damit soll eine hohe Sicherheit des Systems gewährleistet und Überprüfungen durch die Behörden und unabhängige Expertinnen und Experten erleichtert werden. Diese Massnahme sollte keine direkten finanziellen Auswirkungen auf Bund und Kantone haben.

Nr.	Massnahme	Zeitpunkt Umsetzung	Zuständigkeit
A.3	Anwendung einer bewährten und nachvollziehbaren Build- und Deployment-Methode	Wiedereinsatz	Anforderungen: BK Umsetzung: Kantone, Systemanbieter

Zielsetzung und Beschreibung der Massnahme

Es ist eine korrekte Bereitstellung des Systems aus dem Quellcode bis zu seiner Installation in der Produktion (Build- und Deployment) sicherzustellen. Dazu ist vom Systemanbieter eine bewährte und nachvollziehbare Build- und Deployment-Methode einzusetzen. Die entsprechenden Anforderungen an das Build und Deployment werden überarbeitet, um die folgenden Zielsetzungen zu erreichen:

- Die Build- und Deployment-Methode erlaubt es, sicherzustellen, dass die eingesetzte Software mit der publizierten, geprüften und zugelassenen Version übereinstimmt.
- Zusätzlich zu dieser Nachvollziehbarkeit soll die Build- und Deployment-Methode Manipulationen der Systembestandteile so weit als möglich verhindern.

- Es muss verhindert werden, dass mit den eingesetzten Entwicklungsinstrumenten und Bibliotheken für die Software relevante Schwachstellen eingeführt werden, die das System angreifbar machen würden. Für den Umgang mit Nicht-Konformitäten wird ein Prozess erarbeitet (s. Massnahme B.3).

Die BK passt die Rechtsgrundlagen an, um entsprechende Anforderungen an die Systemanbieter zu stellen. Für die Wiederaufnahme der Versuche sind die neuen Anforderungen zu erfüllen.

Dialog mit der Wissenschaft

Die Expertinnen und Experten haben die Wichtigkeit des Einsatzes einer wirksamen und überprüfbaren Build- und Deployment-Methode bestätigt. Diese Methode muss für die Bereitstellung von sicheren Systemen geeignet sein sowie die Nachvollziehbarkeit und Überprüfung der eingesetzten Software erlauben. Es wurden Hinweise für beste Praktiken im Bereich des Build und Deployments eingebracht.

Auswirkungen der Massnahme und Gesamtbeurteilung des SA VE

Mit dieser Massnahme in Zusammenhang mit den Massnahmen A.1 und A.2 soll die Qualität, Nachvollziehbarkeit und Überprüfbarkeit des Systems im ganzen Prozess verbessert werden. Die Umsetzung dieser Massnahme hat keine finanziellen Auswirkungen auf den Bund; die finanziellen Auswirkungen auf die Kantone werden als tief eingeschätzt.

Nr.	Massnahme	Zeitpunkt Umsetzung	Zuständigkeit
A.4	Einsatz von herstellerunabhängigen Komponenten (Verifier / Kontrollkomponenten)	Studie und Antrag Online-Kontrollkomponenten an SA VE: bis 2 Jahre nach Wiedereinsatz Umsetzung unter Vorbehalt: rund 5 Jahre nach Wiedereinsatz	Studie Online-Kontrollkomponenten: Kantone unter Einbezug BK

Zielsetzung und Beschreibung der Massnahme

Die Verifizierbarkeit kann gestärkt werden, indem bei der Software einzelner Komponenten mehr Diversität und Unabhängigkeit geschaffen wird. Folgende Komponenten könnten mit einer Software betrieben werden, die nicht vom Hersteller des übrigen Systems zur Verfügung gestellt wird:

- Kontrollkomponenten für die Generierung der Prüfcodes und zur Aufbewahrung der Stimmen bis zur Auszählung (auch «Online-Kontrollkomponenten»).
- Kontrollkomponenten für das Mischen der Stimmen.
- Verifier zur Prüfung, dass alle von den Online-Kontrollkomponenten aufgezeichneten Stimmen korrekt gemischt, entschlüsselt und gezählt wurden.

Der SA VE beabsichtigt, herstellerunabhängige Online-Kontrollkomponenten in einem Zeithorizont von rund fünf Jahren nach dem Wiedereinsatz einzusetzen. Diese Absichtserklärung erfolgt vorbehaltlich der Sicherstellung der Finanzierung. Zur Lastenteilung braucht es eine kritische Masse an aktiven Kantonen. Insbesondere müssen sich eine genügende Anzahl Kantone bereit erklären, die von den Kantonen zu tragenden Kosten zu finanzieren. Ebenso gilt der Vorbehalt, dass keine heute unbekanntem erheblichen Gründe später gegen eine Umsetzung sprechen.

Priorität hat dabei die Erarbeitung der Grundlagen im Bereich der Online-Kontrollkomponenten. In einem ersten Schritt wird eine Studie mit Blick auf die mögliche Ausgestaltung und Zuständigkeiten bei der Auftragsvergabe, bei der Wartung, beim Betrieb sowie zur Behandlung allfälliger technischer Fragestellungen durchgeführt. Dabei sind insbesondere die Auswirkungen auf die betrieblichen Abläufe bei den Kantonen und die Kosten der Umsetzung aufzuzeigen. Zusätzlich soll in der Studie eine mögliche, konkrete Planung für die Umsetzung aufgezeigt werden (nach einer ersten Einschätzung der Kantone ist mit einem Zeithorizont von mindestens drei bis fünf Jahren für die Umsetzung zu rechnen). Die Studie soll Grundlage für den Umsetzungsentscheid sein. Die Kantone übernehmen die Federführung für die Erarbeitung der Studie.

Nach Abschluss der Studie unterbreiten die BK und die Kantone dem SA VE einen Antrag für das weitere Vorgehen.

Dialog mit der Wissenschaft

Diversität unter den Komponenten, die für die Verifizierbarkeit wichtig sind (sog. Kontrollkomponenten und Verifier), bildet für die Expertinnen und Experten eine Grundvoraussetzung für die Vertrauenswürdigkeit von E-Voting-Systemen: Fehler in einzelnen Komponenten sollen dank anderen, korrekt funktionierenden Komponenten keine negative Auswirkung auf die Verifizierbarkeit haben (exponentieller Sicherheitsgewinn). Die Expertinnen und Experten sprechen sich in diesem Sinne für den Einsatz herstellerunabhängiger Software auf den wichtigen Komponenten (sog. «Kontrollkomponenten» und «Verifier») aus. Sie anerkennen, dass die Einführung von mehr Diversität mit hohen Kosten und einer Erhöhung der Komplexität beim Betrieb verbunden ist, unterstreichen jedoch den Mehrwert.

Auswirkungen der Massnahme und Gesamtbeurteilung des SA VE

Diversität unter den für die Verifizierbarkeit wichtigen Komponenten ist eine Grundvoraussetzung für die Vertrauenswürdigkeit eines E-Voting-Systems. Mittelfristig wird deshalb der Einsatz von unabhängigen Online-Kontrollkomponenten angestrebt.

Die Erarbeitung der Studie hat tiefe bis mittlere finanzielle Auswirkungen auf die Kantone, beim Bund fallen keine Kosten an. Die konkrete Ausgestaltung und Umsetzungsmöglichkeiten von unabhängigen Kontrollkomponenten sowie die damit verbundenen Kosten sind im Rahmen der Studie zu vertiefen. Gestützt auf heutige Annahmen zur Ausgestaltung würden gemäss einer ersten Schätzung der Post die folgenden Kosten für die Umsetzung unabhängiger Kontrollkomponenten (Betrieb durch Post) anfallen:

- Einmalige Kosten: 1.8-2.2 Mio. CHF
- Wiederkehrende Kosten (im Durchschnitt): 600'000-800'000 CHF / Jahr

Für die Umsetzung eines unabhängigen Verifiers hat die Berner Fachhochschule (BFH) folgende Kosten geschätzt:

- Einmalige Kosten: 900'000-1 Mio. CHF
- Wiederkehrende Kosten (im Durchschnitt): 200'000 CHF / Jahr

Gemäss der heutigen Aufteilung der Zuständigkeiten müssten die Kantone diese Kosten tragen. Sie weisen jedoch darauf hin, dass die Kosten für die Umsetzung die Ressourcen der Kantone überschreiten würden. Eine Mitfinanzierung durch den Bund ist zu prüfen.

Nr.		Zeitpunkt Umsetzung	Zuständigkeit
A.5	Abschwächung der Vertrauensannahmen beim Druckprozess und in die Software, die kryptografische Parameter generiert	Vertiefung / Anpassung Protokoll: 1 Jahr nach Wiedereinsatz Antrag an SA VE: bis 2 Jahre nach Wiedereinsatz Umsetzung unter Vorbehalt: rund 4 Jahre nach Wiedereinsatz	Klärung offene Fragen für Anforderungen: BK Umsetzung: Kantone

Zielsetzung und Beschreibung der Massnahme

Die Verifizierbarkeit bei E-Voting ist nur dann wirksam, wenn in der Vorbereitungsphase die relevanten kryptografischen Parameter korrekt generiert werden und vertrauliche Werte (z.B. Prüfcodes) nicht in falsche Hände geraten. Die heutigen Rechtsgrundlagen erlauben, dass die vertraulichen Werte der Stimmberechtigten von einer einzigen Druckmaschine gedruckt werden. Organisatorische Sicherheitsmassnahmen müssen demnach so weit greifen, dass diese Werte geheim bleiben. Wie weit sich die korrekte Wahl der Parameter ebenfalls auf organisatorische Massnahmen abstützen darf, wird nicht spezifiziert. Es besteht daher Handlungsbedarf, um die Wirksamkeit der Verifizierbarkeit zu stärken.

Die zulässigen Vertrauensannahmen beim Druckprozess und in die Software, die kryptografische Parameter generiert, sollen abgeschwächt werden. Mit herstellerunabhängiger Software soll festgestellt werden können, dass kryptografische Parameter und insbesondere die Prüfcodes zufällig erzeugt wurden. Zur Erreichung der gewünschten Entropie müssen für die Erzeugung privater Werte mindestens vier

Kontrollkomponenten zum Einsatz kommen. Stichprobeweise sollen zufällig ausgewählte Stimmrechtsausweise dahingehend geprüft werden, ob die Werte korrekt im Sinne der überprüften Werte gedruckt wurden.

Der SA VE beabsichtigt, die Parametergenerierung sowie den Druckprozess in einem Zeithorizont von rund vier Jahren nach dem Wiedereinsatz anzupassen. Diese Absichtserklärung erfolgt vorbehaltlich der Sicherstellung der Finanzierung. Zur Lastenteilung braucht es eine kritische Masse an aktiven Kantonen. Insbesondere müssen sich eine genügende Anzahl Kantone bereit erklären, die von den Kantonen zu tragenden Kosten zu finanzieren. Ebenso gilt der Vorbehalt, dass keine heute unbekanntem erheblichen Gründe später gegen eine Umsetzung sprechen.

In einer ersten Etappe werden die BK und die Kantone das Lösungskonzept vertiefen; die Kantone werden das kryptografische Protokoll anpassen lassen. In Zusammenarbeit mit der Post definieren sie die Prozesse der Kantone. Eine erste Einschätzung zum Zeithorizont ergab, dass eine Umsetzung (inkl. Anpassung kryptografisches Protokoll) sicher drei Jahre dauern dürfte. Die Planung der Umsetzung soll im Rahmen der ersten Etappe weiter vertieft werden.

Nach Abschluss der Vertiefungsarbeiten unterbreiten die BK und die Kantone dem SA VE einen detaillierten Antrag zur Umsetzung.

Dialog mit der Wissenschaft

Die Expertinnen und Experten sind sich einig, dass die korrekte Parametergenerierung (bspw. der Prüfcodes für die individuelle Verifizierbarkeit) verifizierbar und wo nötig verteilt (gestützt auf mehrere Zufallswerte) erfolgen muss. In diesem Bereich sehen sie Verbesserungspotenzial. Für den Druck der Stimmrechtsausweise haben sie Lösungen für einen verteilten Druckprozess skizziert. Sie legen nahe, dass der Druck der Werte nicht mit der gleichen Druckmaschine erfolgen soll, sondern auf mehrere verteilt wird. Die Expertinnen und Experten anerkennen die Kosten und Erhöhung der Komplexität beim Betrieb, die durch die Einführung von mehr Diversität entsteht, unterstreichen jedoch den Mehrwert.

Auswirkungen der Massnahme und Gesamtbeurteilung des SA VE

Im Dialog mit der Wissenschaft hat die BK in Zusammenarbeit mit den Kantonen den Expertinnen und Experten eine Skizze für eine mögliche Regelung in diesem Bereich unterbreitet. Diese bringt einen Gewinn in der Sicherheit, sieht aus Kostengründen aber weiterhin den Einsatz einer einzigen Druckmaschine vor. Die Post und die Berner Fachhochschule (BFH) haben für ihre jeweiligen Systeme eine erste Studie für die Umsetzbarkeit der skizzierten Anforderungen erarbeitet und diese einigen Experten unterbreitet. Die Ergebnisse zeigen, dass die Anforderungen umsetzbar zu sein scheinen. Die Post hat berechnet, dass die notwendige Anpassung des kryptografischen Protokolls rund ein Jahr dauern würde. Die Grundlagen zur Abschwächung der Vertrauensannahmen werden in einer ersten Etappe vertieft.

Die Abschwächung der Vertrauensannahmen ist für die Vertrauenswürdigkeit von E-Voting wichtig. Deren Umsetzung wird mittelfristig angestrebt.

Die Vertiefung hat tiefe finanzielle Auswirkungen auf den Bund. Die Anpassung des kryptografischen Protokolls wird hingegen mit hohen Kosten verbunden sein. Gemäss einer ersten Schätzung der Post werden folgende Kosten anfallen:

- Einmalige Kosten Anpassung kryptografisches Protokoll: 850'000 bis 1 Mio. CHF

Die Finanzierung dieser Arbeiten ist noch zu klären. Die konkrete Ausgestaltung und die mit der Umsetzung verbundenen Kosten sind im Rahmen der Studie zu vertiefen. Gestützt auf heutige Annahmen zur Ausgestaltung würden gemäss einer ersten Schätzung der Post die folgenden Kosten für die Umsetzung anfallen:

- Einmalige Kosten für die weitere Umsetzung: 700'000-900'000 CHF
- Wiederkehrende Kosten für Support, Wartung und Betrieb (im Durchschnitt): 100'000 CHF / Jahr

Gemäss der heutigen Aufteilung der Zuständigkeiten müssten die Kantone diese Kosten tragen. Sie weisen jedoch darauf hin, dass die Kosten für die erste Etappe und die anschliessende Umsetzung die Ressourcen der Kantone überschreiten würden. Eine Mitfinanzierung durch den Bund ist zu prüfen.

Nr.	Massnahme	Zeitpunkt Umsetzung	Zuständigkeit
A.6	Vertiefung der Grundlagen für einen zusätzlichen Verifizierungsmechanismus, dessen Wirksamkeit nicht auf den heute geltenden Vertrauensannahmen basiert	Studie: 1 Jahr nach Wiedereinsatz Antrag an SA VE: bis 2 Jahre nach Wiedereinsatz	Studie: BK unter Einbezug der Kantone

Zielsetzung und Beschreibung der Massnahme

Um die Diversität zu erhöhen, werden die Möglichkeiten eines zusätzlichen Mechanismus für die Verifizierbarkeit vertieft. Dabei soll geprüft werden, ob und wie den Stimmberechtigten ein zusätzliches Instrument zu den vom Hersteller zur Verfügung gestellten Instrumenten für die Verifizierbarkeit angeboten werden kann. Ein solcher Mechanismus könnte beispielsweise in Form eines öffentlichen Anschlagbretts (sog. «Public Bulletin Board») eingeführt werden. Mit einem Public Bulletin Board könnten die Stimmdaten unter Wahrung des Stimmgeheimnisses veröffentlicht werden und die Stimmberechtigten könnten mithilfe eines Zweitgeräts (z.B. eines Mobiltelefons) feststellen, ob ihre Stimme korrekt bei einer oder mehreren vom Hersteller unabhängigen Instanzen angekommen ist. Damit würde die Wirksamkeit der individuellen Verifizierbarkeit nicht von der Vertrauenswürdigkeit der Druckerei oder der Kontrollkomponenten abhängen. Im Rahmen der Überprüfung im Sinne der universellen Verifizierbarkeit könnten die Kantone feststellen, ob alle bei den unabhängigen Instanzen eingegangenen Stimmen bei der Auszählung mitberücksichtigt wurden.

In einem ersten Schritt wird eine Studie erarbeitet, um den Nutzen eines zusätzlichen Mechanismus sowie die Form einer allfälligen Umsetzung zu vertiefen. Die Studie soll Fragen rund um die technische Umsetzung und, unter Einbezug von Stimmberechtigten, zur Vertrauensbildung und Akzeptanz behandeln. Die BK übernimmt die Federführung für die Erarbeitung der Studie.

Nach Abschluss der Vertiefungsarbeiten unterbreiten die BK und die Kantone dem SA VE einen Antrag, ob und wie ein Public Bulletin Board umgesetzt werden soll. Mit Blick auf eine allfällige Umsetzung ist die Finanzierung sicherzustellen.

Dialog mit der Wissenschaft

Als zusätzliche Möglichkeit für die Verifizierung der Stimmen wurde die Veröffentlichung der verschlüsselten Stimmen auf einem sogenannten «Public Bulletin Board» behandelt. Diese Massnahme als Ergänzung zu den Prüfcodes ist aus der wissenschaftlichen Literatur bekannt. Die Expertinnen und Experten betrachten den Einsatz eines öffentlichen Anschlagbretts als geeignetes Instrument für die Vertrauensbildung, sehen das Vertrauen aber auch gefährdet, wenn bei der Konzeption oder der Umsetzung Fehler gemacht werden oder wenn die Bedürfnisse der Stimmenden, namentlich bei der Kommunikation, der visuellen Darstellung oder der Benutzerfreundlichkeit, nicht berücksichtigt werden. Dahingehend wurden Citizen-Science-Projekte als Massnahme zur Begleitung von allfälligen Versuchen genannt. Fragen zum Umgang mit Meldungen der Stimmenden über negativ ausgefallene Prüfungen sowie Sicherheitsaspekte müssten mit Blick auf die Ausarbeitung einer konkreten Lösung weiter vertieft werden.

Auswirkungen der Massnahme und Gesamtbeurteilung des SA VE

Im Rahmen des Dialogs mit der Wissenschaft haben einige Expertinnen und Experten im Rahmen einer Studie die Thematik aus kryptografischer Perspektive vertieft und mögliche Ansätze aufgezeigt. Eine weitere Vertiefung dieser Arbeiten ist notwendig, bevor über eine allfällige Umsetzung eines solchen zusätzlichen Mechanismus für die Verifizierbarkeit entschieden werden kann. Diverse Aspekte in Bezug auf die mögliche Ausgestaltung und auf die Chancen und Risiken einer solchen Lösung sind zum heutigen Zeitpunkt noch offen. Bei der Studie sollen insbesondere Fragen zur Benutzerfreundlichkeit und zur Kommunikation gegenüber den Stimmberechtigten vertieft werden. Die Erarbeitung der Studie führt beim Bund zu Kosten in mittlerer Höhe; bei den Kantonen fallen keine zusätzlichen Kosten an.

Die Ausgestaltung und die mit der Umsetzung verbundenen Kosten sind im Rahmen der Studie zu vertiefen. Gestützt auf Annahmen zur Ausgestaltung würden gemäss einer ersten Schätzung die folgenden Kosten für die Umsetzung anfallen:

- Einmalige Kosten: 600'000 CHF
- Wiederkehrende Kosten (im Durchschnitt): 200'000 CHF / Jahr

Die Zuständigkeit für die Umsetzung und damit für die Finanzierung ist im Rahmen der Studie zu klären. Die Kantone weisen darauf hin, dass die Kosten für die Umsetzung die Ressourcen der Kantone überschreiten würden. Eine Finanzierung durch den Bund ist zu prüfen.

Nr.	Massnahme	Zeitpunkt Umsetzung	Zuständigkeit
A.7	Verbesserung der Grundlagen zur Erkennung (Monitoring) und Untersuchung (IT-Forensik) von Vorfällen	Definition Anforderungen und Verbesserungsprozess: Wiedereinsatz	Anforderungen: BK Verbesserungsprozess: Systemanbieter, Kantone

Zielsetzung und Beschreibung der Massnahme

E-Voting-Systeme müssen eine wirksame Erkennung und Untersuchung von Vorfällen – wie beispielsweise vermutete Manipulationen von Stimmen oder Angriffe auf das System – ermöglichen. Das gesamte System muss so konzipiert und entwickelt werden, dass das Auftreten von Vorfällen antizipiert und entsprechende Instrumente zur Untersuchung dieser Vorfälle eingesetzt werden (sog. «forensic readiness»). Die gesammelten und gespeicherten Informationen müssen in der Untersuchung von Vorfällen und rechtlichen Verfahren als digitales Beweismaterial genutzt werden können. In den heute geltenden bundesrechtlichen Anforderungen sind gewisse Grundsätze für die Entdeckung und Meldung von Sicherheitsereignissen und -schwächen sowie für deren Handhabung und Verbesserung geregelt (Ziff. 3.2 Anhang der VEleS).

Für die Wiederaufnahme der Versuche werden die bestehenden Anforderungen an die Sammlung von Belegen wie folgt präzisiert: Für die Erkennung und Untersuchung von Vorfällen sind konsistente Protokolle über alle Elemente des Systems anzufertigen. Diese Protokolle müssen so erfasst, übertragen und gespeichert werden, dass sie nicht manipuliert werden können. Der Inhalt und Umfang der Protokolle ist so zu definieren, dass eine wirksame Untersuchung von Vorfällen durchgeführt werden kann. Dabei ist das Stimmgeheimnis zu gewährleisten.

In einem zweiten Schritt wird ein kontinuierlicher Verbesserungsprozess bei der Erkennung und Untersuchung von Vorfällen definiert und ab der Wiederaufnahme umgesetzt. Dabei sind insbesondere die folgenden Aspekte zu berücksichtigen:

- Es findet ein offener Austausch zwischen Bund, Kantonen und Systemanbieter statt.
- Es werden regelmässige Analysen der Zweckmässigkeit der Monitoring- und Untersuchungsgrundlagen durchgeführt. Die in der Krisenvereinbarung definierten Szenarien werden bei diesen Analysen berücksichtigt. Der Einbezug von Fachpersonen aus der IT-Forensik in diese Analysen ermöglicht eine effizientere Verbesserung.
- Bei der Verbesserung der Instrumente und Prozesse werden die aus der Analyse resultierenden Elemente berücksichtigt.

Dialog mit der Wissenschaft

Aus Sicht der Expertinnen und Experten ist es wichtig, dass das System so aufgebaut wird, dass die Entdeckung und Untersuchung von Vorfällen möglich ist. Es ist darauf zu achten, dass die notwendigen Informationen im ganzen Prozess nachvollziehbar angelegt werden. Dabei darf das Stimmgeheimnis nicht verletzt werden. Es sind geeignete Instrumente zur Sammlung der Informationen einzusetzen und regelmässige Simulationen einer Untersuchung durchzuführen, um zu überprüfen, ob die richtigen Informationen gesammelt werden und diese nachvollziehbar abgerufen werden können.

Auswirkungen der Massnahme und Gesamtbeurteilung des SA VE

Mit dieser Massnahme soll ein offener Austausch zwischen Bund, Kantonen und Systemanbieter zur kontinuierlichen Verbesserung des Monitorings und der IT-Forensik erreicht werden. Die Rechtsgrundlagen sind so zu präzisieren, dass klare Anforderungen an die notwendigen Elemente gestellt werden, die für eine sachgerechte Entdeckung und Untersuchung von Vorfällen notwendig sind. Damit wird die «forensic readiness» des Systems verbessert und das Vertrauen in den elektronischen Stimmkanal gestärkt.

Die Umsetzung dieser Massnahme hat keine finanziellen Auswirkungen auf den Bund. Da es sich um eine Präzisierung der Anforderungen handelt, rechnen die Kantone nicht mit zusätzlichen Kosten. Aus dem Verbesserungsprozess, der im Rahmen der Massnahme aufgegleist werden soll, könnten aber Kosten in noch unbestimmter Höhe resultieren.

Nr.	Massnahme	Zeitpunkt Umsetzung	Zuständigkeit
A.8	Schaffung eines gemeinsamen Massnahmenplans von Bund und Kantonen	Wiedereinsatz	BK, Kantone
<p><u>Zielsetzung und Beschreibung der Massnahme</u></p> <p>Bund und Kantone führen zukünftig einen gemeinsamen Massnahmenplan. Der Massnahmenplan bildet die Entscheidungen zur Neuausrichtung des Versuchsbetriebs ab und zeigt auf, welche Massnahmen bereits für den Wiedereinsatz umgesetzt werden und mit welchen Massnahmen E-Voting mittel- bis längerfristig weiterentwickelt werden soll. Wo immer möglich, sind Zeithorizonte für die Umsetzung der Massnahmen bzw. der geplanten ersten Etappen anzugeben. Verabschiedet und publiziert wird der Massnahmenplan in Form einer Absichtserklärung durch den SA VE. Die Publikation erfolgt spätestens bei der Wiederaufnahme der Versuche. Der Massnahmenplan wird regelmässig überprüft und damit die Gewährleistung der Sicherheit unter Berücksichtigung neuester Entwicklungen sichergestellt.</p> <p><u>Dialog mit der Wissenschaft</u></p> <p>Die Expertinnen und Experten sind sich einig, dass Handlungsbedarf besteht und geeignete Massnahmen umgesetzt werden müssen. Einige dieser Massnahmen sind aufwändig und brauchen für die Umsetzung Zeit.</p> <p><u>Auswirkungen der Massnahme und Gesamtbeurteilung des SA VE</u></p> <p>Ein publizierter Massnahmenplan ist ein zielführendes Instrument, um der Öffentlichkeit und allen beteiligten Akteuren die geplanten Entwicklungen und Arbeiten aufzuzeigen. Das Führen eines Massnahmenplans hat keine direkten finanziellen Auswirkungen auf Bund und Kantone. Die Kosten der umzusetzenden Massnahmen sind bei den jeweiligen Massnahmen aufzuzeigen.</p>			

B. Wirksame Kontrolle und Aufsicht

Nr.	Massnahme	Zeitpunkt Umsetzung	Zuständigkeit												
B.1	Anpassung der Zuständigkeiten bei den Konformitätsprüfungen des Systems und der zugrundeliegenden Prozesse	Wiedereinsatz	BK												
<p><u>Zielsetzung und Beschreibung der Massnahme</u></p> <p>Die Erfahrungen von 2019 haben gezeigt, dass die bisherigen Anforderungen im Bereich der Überprüfungen des Systems und der Prozesse nicht gegriffen haben. Bei der Offenlegung des Quellcodes und einer nachträglichen unabhängigen Überprüfung wurden erhebliche Sicherheitsmängel entdeckt, die durch die vorangehenden Prüfungen und Zertifizierungen nicht festgestellt wurden. Um die Wirksamkeit und Glaubwürdigkeit der Prüfungen sicherzustellen, werden die Zuständigkeiten mit der vorliegenden Massnahme sowie die Ausgestaltung der Prüfungen der Systeme mit der Massnahme B.2 angepasst.</p> <p>Bei der Anpassung der Zuständigkeiten spielt die Unabhängigkeit zwischen der Prüfstelle und der geprüften Stelle eine wichtige Rolle. Deshalb wird die Aufgabenteilung zwischen Bund und Kantonen so angepasst, dass der Bund mehr Verantwortung und eine direktere Rolle bei der Prüfung der Systeme übernimmt. Die Zuständigkeiten sollen wie folgt angepasst werden:</p> <table border="1"> <thead> <tr> <th>Prüfungen gemäss Anhang VEleS</th> <th>Zuständigkeiten bisher</th> <th>Zuständigkeiten in Zukunft</th> </tr> </thead> <tbody> <tr> <td>5.1 Prüfung des kryptografischen Protokolls</td> <td>Zuständigkeit: Kanton Auftraggeber: Systemanbieter Auftragnehmer: akkreditierte Stelle</td> <td>Zuständigkeit: BK Auftraggeber: BK Auftragnehmer: Experten Kryptografie</td> </tr> <tr> <td>5.2 Prüfung der Funktionalität</td> <td>Zuständigkeit: Kanton Auftraggeber: Systemanbieter Auftragnehmer: akkreditierte Stelle</td> <td>Zuständigkeit: BK Auftraggeber: BK Auftragnehmer: Experten Kryptografie und Experten Entwicklung</td> </tr> <tr> <td>5.3 Prüfung der Infrastruktur und des Betriebs</td> <td>Zuständigkeit: Kanton Auftraggeber: Systemanbieter Auftragnehmer: akkreditierte Stelle</td> <td><i>Infrastruktur des Systemanbieters für die Zertifizierung nach ISO 27001</i> Zuständigkeit: Kanton Auftraggeber: Systemanbieter</td> </tr> </tbody> </table>				Prüfungen gemäss Anhang VEleS	Zuständigkeiten bisher	Zuständigkeiten in Zukunft	5.1 Prüfung des kryptografischen Protokolls	Zuständigkeit: Kanton Auftraggeber: Systemanbieter Auftragnehmer: akkreditierte Stelle	Zuständigkeit: BK Auftraggeber: BK Auftragnehmer: Experten Kryptografie	5.2 Prüfung der Funktionalität	Zuständigkeit: Kanton Auftraggeber: Systemanbieter Auftragnehmer: akkreditierte Stelle	Zuständigkeit: BK Auftraggeber: BK Auftragnehmer: Experten Kryptografie und Experten Entwicklung	5.3 Prüfung der Infrastruktur und des Betriebs	Zuständigkeit: Kanton Auftraggeber: Systemanbieter Auftragnehmer: akkreditierte Stelle	<i>Infrastruktur des Systemanbieters für die Zertifizierung nach ISO 27001</i> Zuständigkeit: Kanton Auftraggeber: Systemanbieter
Prüfungen gemäss Anhang VEleS	Zuständigkeiten bisher	Zuständigkeiten in Zukunft													
5.1 Prüfung des kryptografischen Protokolls	Zuständigkeit: Kanton Auftraggeber: Systemanbieter Auftragnehmer: akkreditierte Stelle	Zuständigkeit: BK Auftraggeber: BK Auftragnehmer: Experten Kryptografie													
5.2 Prüfung der Funktionalität	Zuständigkeit: Kanton Auftraggeber: Systemanbieter Auftragnehmer: akkreditierte Stelle	Zuständigkeit: BK Auftraggeber: BK Auftragnehmer: Experten Kryptografie und Experten Entwicklung													
5.3 Prüfung der Infrastruktur und des Betriebs	Zuständigkeit: Kanton Auftraggeber: Systemanbieter Auftragnehmer: akkreditierte Stelle	<i>Infrastruktur des Systemanbieters für die Zertifizierung nach ISO 27001</i> Zuständigkeit: Kanton Auftraggeber: Systemanbieter													

		Auftragnehmer: akkreditierte Stelle nach ISO 27001 <i>Infrastruktur Systemanbieter und Kanton für die Anforderungen nach VEleS</i> Zuständigkeit: BK Auftraggeber: BK Auftragnehmer: Experten Kryptografie und Experten Betrieb
5.4 Prüfung der Kontrollkomponenten	Zuständigkeit: Kanton Auftraggeber: Systemanbieter Auftragnehmer: akkreditierte Stelle	Zuständigkeit: BK Auftraggeber: BK Auftragnehmer: Experten Kryptografie und Experten Entwicklung
5.5 Prüfung des Schutzes gegen Versuche in die Infrastruktur einzudringen	Zuständigkeit: Kanton Auftraggeber: Systemanbieter Auftragnehmer: akkreditierte Stelle	Zuständigkeit: BK Auftraggeber: BK Auftragnehmer: Sicherheitsexperten
5.6 Prüfung einer Druckerei	Zuständigkeit: Kanton Auftraggeber: Kanton Auftragnehmer: akkreditierte Stelle	Zuständigkeit: BK Auftraggeber: BK Auftragnehmer: Experten Kryptografie und Experten Betrieb

Der Systemanbieter wird damit weiterhin für Prüfungen in Bezug auf den Betrieb des Systems in seinen Rechenzentren zuständig sein (Zertifizierung ISO 27001 gemäss Ziff. 5.3 Anhang der VEleS). Auf eine weitergehende Zertifizierung durch Stellen, die von der Schweizerischen Akkreditierungsstelle (SAS) akkreditiert sind, wird in Zukunft verzichtet. Der Bund ist für die Prüfungen der Erfüllung der Anforderungen in Bezug auf das System und die zugrundeliegenden Prozesse zuständig. Für die Überprüfungen sind unabhängige Expertinnen und Experten zu mandatieren.

Die BK passt für die Wiederaufnahme die VEleS und den Anhang an.

Dialog mit der Wissenschaft

Die Expertinnen und Experten haben hervorgehoben, dass unabhängige Überprüfungen durch ein unabhängiges Komitee oder den Bund in Auftrag gegeben werden sollen. Eine Zertifizierung könnte lediglich im Rahmen der Prüfung des Betriebs sinnvoll sein (Zertifizierung nach ISO 27001). Die Behörden sollen auf unabhängige Prüfungen durch Personen mit den nötigen Kompetenzen setzen. Geeignete Kompetenzen im Bereich der Überprüfung sind wesentlich wertvoller als eine Zertifizierung von E-Voting-Systemen. Kryptografinnen und Kryptografen sollen auch bei der Prüfung des Quellcodes und des Betriebs beigezogen werden. Die Überprüfung muss einem ganzheitlichen Konzept folgen, um Lücken zu verhindern. Darüber hinaus wird insbesondere die Bedeutung der öffentlichen Überprüfung unterstrichen (public scrutiny).

Auswirkungen der Massnahme und Gesamtbeurteilung des SA VE

Die Wirksamkeit der Prüfungen kann gewährleistet werden, indem der Bund in Zukunft den Hauptteil der Überprüfungen in Auftrag gibt. Dies wird zusammen mit der Erstellung des Prüfkonzepts (Massnahme B.2) als wichtig und zielführend erachtet.

Die Finanzierung der Überprüfungen übernimmt die jeweils zuständige Stelle. Somit hat die Anpassung der Zuständigkeiten hohe finanzielle Auswirkungen auf den Bund. Die Kantone bleiben für die Prüfung der Infrastruktur des Systemanbieters zuständig (Zertifizierung nach ISO 27001). Dadurch entfallen die bisherigen Kosten für eine Zertifizierung durch eine von der SAS akkreditierte Stelle. Die Kantone gehen davon aus, dass sich dadurch bei den Kantonen keine unmittelbaren Kosteneinsparungen ergeben (die Verschiebung der Zuständigkeit bedingt eine umfassendere Vorbereitung des Systemanbieters, der personelle Aufwand für die Durchführung der Prüfung bleibt unverändert).

Die Anpassung der Zuständigkeiten wirkt sich auf die Abläufe zwischen Bund, Kantonen und Systemanbieter sowie auf das Bewilligungsverfahren aus (s. Massnahme B.9). Die BK wird den Kantonen die Prüfberichte laufend zustellen und ihnen ihre ersten Einschätzungen zu den Prüfergebnissen mitteilen. Damit sollen den Kantonen die erforderlichen Informationen für die Beurteilung der Gesuchstellung an den Bund zur Verfügung gestellt werden. Die BK wird in diesem Sinne sicherstellen, dass die Kantone in die Prüfungen involviert sind und sie tauscht sich regelmässig mit den Kantonen aus.

Nr.	Massnahme	Zeitpunkt Umsetzung	Zuständigkeit
B.2	Erarbeitung eines Prüfkonzepts für die Beurteilung der Konformität des Systems und der zugrundeliegenden Prozesse	Wiedereinsatz	BK in Zusammenarbeit mit Kantonen und Systemanbieter

Zielsetzung und Beschreibung der Massnahme

Die Zuständigkeiten bei den Überprüfungen des Systems und der Prozesse werden mit der Massnahme B.1 angepasst. Um diese neuen Zuständigkeiten abzubilden, eine lückenlose Überprüfung sicherzustellen und insgesamt eine höhere Wirksamkeit der Prüfungen zu erreichen, wird ein neues Prüfkonzept erarbeitet. Das Prüfkonzept wird so ausgestaltet, dass eine umfassende Überprüfung der Sicherheitsanforderungen gewährleistet wird.

Das Prüfkonzept soll u.a. die folgenden Aspekte vorsehen:

- Klare Definition der Prüftiefe der verschiedenen Bereiche: Der Geltungsbereich der einzelnen Prüfbereiche und die Gültigkeitsdauer der Prüfungen werden definiert.
- Durchlässigkeit zwischen den verschiedenen Prüfbereichen: Mit der Durchlässigkeit zwischen den Prüfbereichen wird eine konsistente und lückenlose Überprüfung sichergestellt.
- Für die Prüfungen werden qualifizierte und unabhängige Expertinnen und Experten mandatiert.
- Die Prüfberichte werden publiziert (vgl. dazu Massnahme C.4).

Grundsätzlich sollen Überprüfungen des Systems frühzeitig stattfinden, damit vor dem Einsatz des Systems genügend Zeit zur Behebung von Nicht-Konformitäten und zur erneuten Prüfung zur Verfügung steht (zum Umgang mit Nicht-Konformitäten vgl. Massnahme B.3).

Das Prüfkonzept wird durch die BK erarbeitet. Die Prüfungen vor der Wiederaufnahme der Versuche werden gestützt auf das neue Prüfkonzept durchgeführt. Die BK kann bei der Erarbeitung des Prüfkonzepts externe Expertinnen und Experten beiziehen.

Dialog mit der Wissenschaft

Vgl. dazu die Ausführungen unter der Massnahme B.1.

Auswirkungen der Massnahme und Gesamtbeurteilung des SA VE

Vgl. dazu die Ausführungen unter der Massnahme B.1. Für die Erarbeitung eines Prüfkonzepts sind die finanziellen Auswirkungen auf den Bund tief. Allenfalls fallen Kosten für den Einbezug externer Expertinnen und Experten an. Auf die Kantone hat diese Massnahme keine finanziellen Auswirkungen.

Nr.	Massnahme	Zeitpunkt Umsetzung	Zuständigkeit
B.3	Erarbeitung und Umsetzung eines Prozesses zum Umgang mit Nicht-Konformitäten	Wiedereinsatz	BK in Zusammenarbeit mit Kantonen und Systemanbieter

Zielsetzung und Beschreibung der Massnahme

Nicht-Konformitäten, wie etwa Mängel im System und den zugrundeliegenden Prozessen, können jederzeit entdeckt werden. Werden Nicht-Konformitäten kurz vor oder während des Einsatzes von E-Voting entdeckt oder vermutet, ist ein geregelter Vorgehensprozess von grosser Wichtigkeit. Nicht jede Nicht-Konformität muss dazu führen, dass das System nicht eingesetzt werden kann. Nicht-Konformitäten müssen hinsichtlich ihrer Auswirkungen auf die Risiken beurteilt werden und es ist zu prüfen, ob das mit einer Nicht-Konformität verbundene Risiko mit anderen Massnahmen minimiert werden kann. Mit der Erarbeitung eines Prozesses zum Umgang mit Nicht-Konformitäten soll sichergestellt werden, dass Unklarheiten im Auftretensfall so weit als möglich vermieden und ein Einsatz von E-Voting sichergestellt werden kann, bei dem die Anforderungen der VELeS erfüllt werden.

Die BK erarbeitet bis zur Wiederaufnahme der Versuche und in Zusammenarbeit mit den Kantonen und dem Systemanbieter einen Prozess zum Umgang mit erwiesenen und vermuteten Nicht-Konformitäten und definiert dabei die folgenden Aspekte:

- Definition von Nicht-Konformitäten: Es wird festgelegt, welche Art von Nicht-Konformität den Prozess auslöst.

- Festlegen von Kriterien: Es werden Kriterien festgelegt, die im Umgang mit Nicht-Konformitäten angewendet werden. Die Nicht-Konformitäten sind hinsichtlich ihrer Auswirkungen auf die Risiken zu beurteilen. Dabei sind auch die Risiken zu berücksichtigen, die sich aus einem Zurückziehen des Systems ergeben. Grundsätzlich kann das E-Voting-System eher zum Einsatz kommen, wenn sich Nicht-Konformitäten nicht auf das System, sondern auf die umliegenden Prozesse beziehen. Wird eine Nicht-Konformität für einen Einsatz akzeptiert, soll die Behebung der Nicht-Konformität vorgesehen werden und allenfalls im Massnahmenplan von Bund und Kantonen aufgenommen werden (vgl. Massnahme A.8).
- Regelung der Akteure und deren Rollen: Die Rollen und die Zusammenarbeit zwischen Bund, Kantonen, Systemanbieter und allenfalls weiterer Akteure sind zu definieren. Im Umgang mit Nicht-Konformitäten sind unabhängige Expertinnen und Experten einzubeziehen.

Dialog mit der Wissenschaft

Die Expertinnen und Experten haben die Wichtigkeit eines klar geregelten Prozesses zum Umgang mit Nicht-Konformitäten hervorgehoben. Sie sind sich einig, dass der Einsatz von E-Voting nicht bei jeder Nicht-Konformität gestoppt werden muss. Geringe Risiken können akzeptiert werden. Dazu müssen die Risiken jedoch richtig eingeschätzt werden, was in manchen Fällen schwer möglich ist. Alternativ könnte die Schwere der Nichtkonformität als Entscheidungskriterium verwendet werden. Vergleiche mit bereits akzeptierten Risiken können dabei hilfreich sein. Ebenso zu berücksichtigen sind der faktische Verlust des Stimmrechts von Teilen des Auslandschweizer Elektorats sowie die Tatsache, dass der Verzicht auf E-Voting eine verstärkte Nutzung der ebenfalls risikobehafteten brieflichen Stimmabgabe zur Folge hat. Je stärker eine Nicht-Konformität das System betrifft und je weniger sie sich auf die umgebenden Prozesse beschränkt, desto eher muss sie behoben werden. Fehler im kryptografischen Protokoll oder dessen Umsetzung im Quellcode sollen grundsätzlich nicht akzeptiert werden.

Auswirkungen der Massnahme und Gesamtbeurteilung des SA VE

Die Regelung des Umgangs mit Nicht-Konformitäten wird als wichtige Massnahme erachtet. Alle beteiligten Akteure profitieren von einem klar definierten Entscheidungsprozess, der die wichtigsten Kriterien für den Umgang mit Nicht-Konformitäten umfasst. Die Umsetzung dieser Massnahme hat keine finanziellen Auswirkungen auf die Kantone. Beim Bund fallen allenfalls tiefe Kosten für den Einbezug externer Expertinnen und Experten an.

Nr.	Massnahme	Zeitpunkt Umsetzung	Zuständigkeit
B.4	Erneuerung und Verbesserung des Leitfadens für die Risikobeurteilungen	Wiedereinsatz	BK in Zusammenarbeit mit Kantonen und Systemanbieter

Zielsetzung und Beschreibung der Massnahme

Die bestehenden Grundlagen und Vorgaben für die Risikobeurteilungen werden erneuert und verbessert. Die Risikobeurteilungen der BK, der Kantone und des Systemanbieters (vgl. dazu Massnahme B.5) sollen gestützt auf einen Leitfaden vorgenommen werden. Der Leitfaden wird das grundlegende Konzept für die Risikobeurteilungen beinhalten und die Zuständigkeiten regeln. Die Wahl der Methode zur Beurteilung der Risiken soll weiterhin den zuständigen Akteuren obliegen. Der Leitfaden wird insbesondere die folgenden Aspekte umfassen:

- Katalog der Informationsressourcen (information assets)
- Katalog von Bedrohungen (basierend auf der Liste der Bedrohungen in Ziff. 3.1 Anhang der VELeS)
- Katalog der Massnahmen zur Risikominimierung
- Zuständigkeiten in Bezug auf den Schutz der information assets

Im Leitfaden sollen u.a. die Länge der Schlüssel zur Verschlüsselung, die mehrfache Abgabe von Stimmen über verschiedene Stimmkanäle, der Stimmenkauf, «long term privacy» und die Abhängigkeit von einem einzigen Anbieter berücksichtigt werden.

Der Leitfaden wird von der BK in Zusammenarbeit mit den Kantonen, den Systemanbietern sowie IT-Sicherheitsexpertinnen und -experten erarbeitet. Er wird vor der Wiederaufnahme der Versuche publiziert, um die Transparenz und Vertrauensbildung zu stärken. Zudem erhält die Öffentlichkeit so die Möglichkeit, Feedback zu geben. Der Leitfaden ist periodisch zu überprüfen und gegebenenfalls anzupassen.

Dialog mit der Wissenschaft

Im Dialog mit der Wissenschaft wurde die Erarbeitung eines Leitfadens als Grundlage für die Risikobeurteilungen diskutiert. Aus Sicht der Expertinnen und Experten muss ein solcher Leitfaden vom Bund (in Zusammenarbeit mit den Kantonen, Systemanbietern und allenfalls externen Fachpersonen) erarbeitet werden, um eine einheitliche Basis für die Risikobeurteilungen und eine umfassende Risikoabdeckung zu bieten. Die Wahl der Methode für die Risikobeurteilung soll weiterhin den zuständigen Stellen überlassen werden. Der Leitfaden soll Bedrohungen nennen, risikominimierende Massnahmen vorschlagen und die Zuständigkeiten definieren. Der Leitfaden ist zu publizieren, um Rückmeldungen von externen Fachpersonen zu ermöglichen.

Auswirkungen der Massnahme und Gesamtbeurteilung des SA VE

Mit dem Leitfaden kann eine wirksame und einheitliche Grundlage für die Ausgestaltung der Risikobeurteilungen erarbeitet werden, an der sich alle Akteure zur Beurteilung der Risiken orientieren können. Dies erleichtert die Prozesse. Die Massnahme hat auf den Bund tiefe finanzielle Auswirkungen. Für die Kantone hat die Massnahme keine unmittelbaren finanziellen Auswirkungen. Der Leitfaden muss vor der Umsetzung der Massnahme B.5 vorliegen.

Nr.	Massnahme	Zeitpunkt Umsetzung	Zuständigkeit
B.5	Erarbeitung und Umsetzung eines neuen Vorgehens für die Risikobeurteilungen für vollständig verifizierbare Systeme	Wiedereinsatz	BK, Kantone, Systemanbieter

Zielsetzung und Beschreibung der Massnahme

Die bisher vorgesehenen Risikobeurteilungen werden neu strukturiert. Zukünftig sollen nicht nur die Kantone, sondern jeder Akteur (BK, Kantone, Systemanbieter) für seinen Zuständigkeitsbereich eine eigene Risikobeurteilung erstellen. Die Zuständigkeiten und das Vorgehen richten sich nach dem Leitfaden unter Massnahme B.4. Die Risikobeurteilungen sollen die jeweils aktuelle Situation widerspiegeln und neuste Entwicklungen und Erkenntnisse fortlaufend in die Beurteilung einfließen. Die Risikobeurteilungen werden mindestens jährlich sowie bei wesentlichen Änderungen des Systems überarbeitet. Ausserdem ist vor jedem Urnengang zu prüfen, ob sich spezifische Risiken stellen oder bestehende Risiken erhöht sind. Können risikominimierende Massnahmen nicht unmittelbar umgesetzt werden, sind sie in den Massnahmenplan (Massnahme A.8) aufzunehmen. Unabhängige Fachpersonen werden für die Beurteilung der Risiken beigezogen.

Die BK passt die VELeS an. Für die Wiederaufnahme der Versuche müssen Risikobeurteilungen von allen Akteuren vorliegen.

Dialog mit der Wissenschaft

Die Expertinnen und Experten befürworten, dass jeder Akteur (BK, Kantone, Systemanbieter) für seinen Zuständigkeitsbereich eine Risikobeurteilung erstellt. Sie sind sich einig, dass die Risiken regelmässig mit einer systematischen und umfassenden Methode bewertet werden sollten. Die Überprüfung der Risikobeurteilungen sollte mindestens jährlich und aufgrund wesentlicher Änderungen des Systems vorgenommen werden. Eine gezielte Überprüfung im Hinblick auf einen Urnengang (alle drei Monate) ist erwünscht. Allerdings sind alle drei Monate etwas anspruchsvoll und es könnte sinnvoll sein, nach einigen Jahren zu einem längeren Intervall zurückzukehren. Die Wahl der angewandten Methodik spielt eine untergeordnete Rolle. Die Risiken, die aus der Abhängigkeit von Drittlieferanten und -herstellern entstehen (sog. «supply chain risks»), wurden von der Hälfte der Expertinnen und Experten als besonders schwierig zu bewältigen eingestuft. Eine Mehrheit ist der Meinung, dass ein Expertenausschuss zur Unterstützung des Risikomanagementprozesses nützlich sein könnte. Die Expertinnen und Experten haben verschiedene Vor- und Nachteile einer Publikation der Risikobeurteilungen diskutiert. Sie empfehlen, die detaillierte Risikobeurteilung nicht sofort zu publizieren. Es könnte aber nützlich sein, Grafiken, statistische Daten sowie Informationen über die Governance zu veröffentlichen und die Regeln für eine mögliche spätere Veröffentlichung der detaillierten Risikobeurteilung transparent zu machen.

Auswirkungen der Massnahme und Gesamtbeurteilung des SA VE

Ein wirksames Risikomanagement kann sichergestellt werden, indem jeder Akteur diejenigen Risiken beurteilt und adressiert, die in seinem Verantwortungsbereich liegen. Mit dem Leitfaden nach Massnahme B.4 wird die Aufteilung der Zuständigkeiten und eine gemeinsame Basis für die Beurteilung der Risiken geregelt. Es ist wichtig, dass ein kontinuierlicher Austausch und Absprache zwischen den verschiedenen Akteuren stattfindet, damit gegenseitig von Erfahrungen profitiert werden kann (wie z.B.

Erfahrungen des Kantons Fribourg mit der Anwendung von Octave Allegro, einer Methode zur Beurteilung der Risiken). Bund und Kantone können bei der Identifizierung und der Beurteilung der Risiken von der Beratung externer Fachpersonen profitieren.

Die Umsetzung dieser Massnahme kann bei Bund und Kantonen punktuell zu einem Mehraufwand führen, der jedoch mit den bestehenden Ressourcen bewältigt werden kann. Allenfalls fallen tiefe Kosten für die Mandatierung externer Fachpersonen an.

Nr.	Massnahme	Zeitpunkt Umsetzung	Zuständigkeit
B.6	Erneuerung des Krisenmanagements mit Durchführung von Krisenübungen	Wiedereinsatz	BK (Federführung), Kantone und Systemanbieter

Zielsetzung und Beschreibung der Massnahme

Ein wirksames und funktionierendes Krisenmanagement ist ein wichtiger Aspekt bei der Umsetzung eines vertrauenswürdigen und sicheren E-Voting-Systems. Bisher legten Bund und Kantone in einer Krisenvereinbarung fest, wie die Information, Zusammenarbeit und Kommunikation bei einem Vorfall mit der elektronischen Stimmabgabe erfolgen soll. Diese Praxis wird erneuert, um Entwicklungen im Bereich von E-Voting Rechnung zu tragen und um die Wirksamkeit des Krisenmanagements zu verbessern. Dazu ist eine neue Krisenvereinbarung auszuarbeiten. Diese soll in Form einer Rahmenvereinbarung die folgenden Eigenschaften aufweisen:

- Trilaterale Vereinbarung: Die Krisenvereinbarung wird zwischen der BK, den Anwenderkantonen und dem Systemanbieter abgeschlossen.
- Prozesse, Rollen und Aufgaben: Die Prozesse im Krisenmanagement und die Rollen und Aufgaben der beteiligten Akteure werden festgelegt.
- Kommunikation: Die Krisenvereinbarung enthält einen Kommunikationsprozess zwischen den beteiligten Akteuren (interne Kommunikation) sowie einen Prozess zur Koordination der Kommunikation gegen aussen (externe Kommunikation). Für die Kommunikation zwischen den beteiligten Akteuren wird eine geeignete Kommunikationsplattform zur Verfügung gestellt.
- Übungen: Das Krisenmanagement wird in festzulegenden zeitlichen Abständen geübt, um die Prozesse und die Zusammenarbeit im Krisenmanagement zu verbessern.
- In der Krisenvereinbarung sind die Krisenszenarien an die neuen Risikobeurteilungen für vollständig verifizierbare Systeme anzupassen. Bestehende Strukturen bei Bund, Kantonen und Systemanbietern werden bei der Ausgestaltung des Krisenmanagements so weit als möglich beibehalten.

Für die Wiederaufnahme der Versuche sind die neuen Krisenvereinbarungen auszuarbeiten und zu unterzeichnen. Die ersten praktischen Übungen können auch nach dem Wiedereinsatz stattfinden.

Dialog mit der Wissenschaft

Die Expertinnen und Experten haben betont, dass beim Krisenmanagement klar definierte Prozesse sowie Handlungs- und Kommunikationspläne zentral sind. Sie haben ausserdem vorgeschlagen, dass im Krisenmanagement neben der zuständigen Stelle beim Bund, den betroffenen Kantonen und dem Systemanbieter auch weitere Bundesstellen (GovCERT / MELANI), Fachpersonen aus dem Bereich Kommunikation und unabhängige (technische) Expertinnen und Experten einbezogen werden.

Auswirkungen der Massnahme und Gesamtbeurteilung des SA VE

Diese Massnahme ist notwendig, um das bestehende Krisenmanagement an die aktuelle Ausgangslage anzupassen und um einen kontinuierlichen Verbesserungsprozess zu ermöglichen. Die Umsetzung dieser Massnahme hat geringe finanzielle Auswirkungen auf den Bund. Den Kantonen entstehen für Umsetzung und Implementierung des Krisenmanagements und für die Übungen keine zusätzlichen externen Kosten.

Nr.	Massnahme	Zeitpunkt Umsetzung	Zuständigkeit
B.7	Integration von E-Voting als Teil der kritischen Infrastruktur des Bundes	Wiedereinsatz	BK (Federführung), Kantone und Systemanbieter

Zielsetzung und Beschreibung der Massnahme

Die kritischen Infrastrukturen im Sinne der Nationalen Strategie zum Schutz kritischer Infrastrukturen erhalten eine erhöhte Unterstützung der Melde- und Analysestelle Informationssicherung (MELANI) und dem nationalen Computer Emergency Response Team (GovCERT). Diese Unterstützung wäre bei der Analyse von Bedrohungen und der Untersuchung von Vorfällen im Bereich von E-Voting wertvoll. Mit dieser Massnahme soll die Zusammenarbeit zwischen der BK, den Kantonen, dem Systemanbieter und GovCERT / MELANI im Bereich E-Voting festgelegt werden, um einen priorisierten Zugang für den Umgang mit Vorfällen zu gewährleisten. Diese Zusammenarbeit soll auch im Krisenmanagement berücksichtigt werden.

Dialog mit der Wissenschaft

Das Thema von E-Voting als Teil der kritischen Infrastruktur wurde im Dialog mit der Wissenschaft nicht explizit diskutiert. Expertinnen und Experten haben die Zusammenarbeit mit GovCERT / MELANI als Vorteil genannt.

Auswirkungen der Massnahme und Gesamtbeurteilung des SA VE

Diese Massnahmen hat keine finanziellen Auswirkungen auf Bund und Kantone.

Nr.	Massnahme	Zeitpunkt Umsetzung	Zuständigkeit
B.8	Weiterentwicklung der Plausibilisierung der E-Voting-Ergebnisse	Wiedereinsatz: Erster Austausch Prüfung standardisierte Methode: 2022	Kantone

Zielsetzung und Beschreibung der Massnahme

Das geltende Recht sieht die Plausibilisierung der Ergebnisse von Urnengängen mit dem elektronischen Stimmkanal vor (Art. 27i Abs. 1 VPR). Die Plausibilisierung soll Hinweise auf versehentliche Fehler bei der Ergebnisermittlung und auf mögliche Manipulationen der Ergebnisse geben. Dazu sollen statistische Methoden, soweit die Datenbasis dies erlaubt, eingesetzt werden können (Ziff. 3.2.8 Anhang der VEleS). Die Kantone plausibilisieren die E-Voting-Ergebnisse unterschiedlich. Es soll ein vermehrter Austausch unter den Kantonen und mit der BK stattfinden, damit Erfahrungen und Lösungsansätze im Sinne von «best practice» diskutiert werden können. Ausserdem wird geprüft, ob und in welcher Form eine standardisierte statistische Methode ausgearbeitet werden kann. Mit der Einführung eines standardisierten Verfahrens bestünde ein weiteres Instrument, um Hinweise auf allfällige Fehlfunktionen oder Manipulationen zu erhalten. Die Methode muss auf die spezifischen Gegebenheiten jedes einzelnen Kantons anwendbar sein. Für die Nachvollziehbarkeit der Plausibilisierung sollen die E-Voting-Ergebnisse von eidgenössischen Urnengängen publiziert werden (s. Massnahme C.5). Es ist ausserdem zu prüfen, welche Informationen in Bezug auf die Plausibilisierungsarbeiten der Kantone in Zukunft publiziert werden können. Damit soll der Öffentlichkeit die Möglichkeit gegeben werden, die Plausibilisierung der E-Voting-Ergebnisse durch die Behörden zu beurteilen.

Ein erster Austausch unter den Kantonen und mit der BK zur bisherigen Praxis soll im Hinblick auf die Wiederaufnahme stattfinden. Die Abklärungen zu einer standardisierten Methode und die Prüfung, welche Informationen in Bezug auf die Plausibilisierungsarbeiten der Kantone künftig publiziert werden sollen, sollen bis 2022 umgesetzt werden.

Dialog mit der Wissenschaft

Im Dialog mit der Wissenschaft wurde das Thema einer standardisierten statistischen Methode zur Plausibilisierung diskutiert. Heute existiert noch keine solche Methode, die Expertinnen und Experten denken jedoch, dass eine solche Methode entwickelt werden könnte. Aus Sicht der Expertinnen und Experten können mit statistischen Methoden zwar keine Manipulationen festgestellt werden, die Plausibilisierung kann jedoch Hinweise auf Unregelmässigkeiten liefern. Gestützt auf diese Hinweise können Untersuchungen zu möglichen Manipulationen durchgeführt werden. Das Ausbleiben von Hinweisen ist jedoch keine Garantie für die Absenz von Manipulationen.

Auswirkungen der Massnahme und Gesamtbeurteilung des SA VE

Es besteht Handlungsbedarf, um die bereits heute vorgeschriebene Plausibilisierung in den Kantonen weiterzuentwickeln. Bei der Umsetzung dieser Massnahme sind die Auswirkungen auf die anderen Stimmkanäle sowie die in verschiedenen Kantonen bereits laufenden Bestrebungen, die Plausibilisierung der Abstimmungs- und Wahlergebnisse generell zu verbessern, zu berücksichtigen.

Diese Massnahme hat keine finanziellen Auswirkungen auf den Bund. Bei den Kantonen sind die finanziellen Auswirkungen abhängig davon, ob und welche Plausibilisierungsmethoden entwickelt werden, sie dürften jedoch eher tief sein.

Nr.	Massnahme	Zeitpunkt Umsetzung	Zuständigkeit
B.9	Anpassungen des Bewilligungsverfahrens	Wiedereinsatz	BK unter Einbezug der Kantone

Zielsetzung und Beschreibung der Massnahme

Die Umsetzung verschiedener Massnahmen für die Wiederaufnahme der Versuche macht eine Anpassung der Abläufe im Bewilligungsverfahren notwendig. Dazu gehören insbesondere die Massnahmen zur Neuregelung der Zuständigkeiten bei den unabhängigen Überprüfungen (Massnahme B.1) sowie die Anpassung der Anforderungen im Bereich der Transparenzmassnahmen (Massnahmen C.2 und C.3). Ausserdem sind der Einbezug unabhängiger Expertinnen und Experten im Bewilligungsverfahren und das kontinuierliche Risikomanagement zu berücksichtigen. Am bisherigen Rahmen des Bewilligungsverfahrens gemäss VPR (Grundbewilligung durch den Bundesrat, Zulassung durch die BK) wird für die Wiederaufnahme der Versuche festgehalten.

Zur Umsetzung dieser Massnahme wird die BK die Abläufe im Bewilligungsverfahren anpassen. Dazu überarbeitet sie ihre Anforderungskataloge für das Bewilligungsverfahren. Ausserdem prüft die BK, inwiefern der Grundbewilligungsentscheid des Bundesrates in einen systembezogenen und einen kantonsspezifischen Teil aufgeteilt werden kann.

Dialog mit der Wissenschaft

Die Ausgestaltung des Bewilligungsverfahrens wurde im Dialog mit der Wissenschaft nicht explizit thematisiert. Grundsätzlich wird mit Blick auf die Beurteilung von E-Voting-Systemen dem Einbezug kompetenter und unabhängiger Personen und Fachstellen eine hohe Bedeutung beigemessen.

Auswirkungen der Massnahme und Gesamtbeurteilung des SA VE

Die Anpassung des Bewilligungsverfahrens ist notwendig, um insbesondere der neu konzipierten unabhängigen Überprüfung Rechnung zu tragen. Es ist unabdingbar, dass sich die BK und die betroffenen Kantone frühzeitig abstimmen, um die Abläufe zu koordinieren. Wie unter Massnahme B.1 ausgeführt, wird die BK sicherstellen, dass die Kantone in die Prüfungen involviert sind. Sie wird sich regelmässig mit den Kantonen austauschen. Mit einer Aufteilung des Grundbewilligungsentscheids in einen systembezogenen und einen kantonsspezifischen Teil, soll eine gewisse Planungssicherheit für Kantone geschaffen werden, die eine Grundbewilligung für ein bereits zugelassenes System beantragen. Setzen sie dieselbe Version des Systems wie andere Kantone ein, haben sie die Gewissheit, dass der allgemeine Systemteil die Anforderungen des Bundes erfüllt.

Die Umsetzung dieser Massnahme hat keine finanziellen Konsequenzen für Bund und Kantone.

Nr.	Massnahme	Zeitpunkt Umsetzung	Zuständigkeit
B.10	Langfristige Überprüfung der Prozesse, Rollen und Aufgaben	Langfristig	AG Zukunft VE

Zielsetzung und Beschreibung der Massnahme

Die Zuständigkeiten, Rollen und Aufgaben von Bund, Kantonen und Systemanbietern haben einen direkten Einfluss auf die (sicherheitsrelevante) Ausgestaltung der E-Voting Systeme. Sie sollen langfristig überprüft und in einer Strategie festgehalten werden. In diesem Rahmen können grundlegendere Anpassungen der Zuständigkeiten, Rollen und Aufgaben diskutiert werden. Bund und Kantone können Massnahmen erarbeiten, die der veränderten Ausgangslage bezüglich der Anzahl der Systemanbieter, der Gouvernanz und dem Finanzierungsbedarf der elektronischen Stimmabgabe Rechnung tragen. Die heutige Verteilung von Aufgaben, Kompetenzen und Verantwortung entspricht der föderalistischen Auf-

gabenteilung im Bereich der politischen Rechte. Die Prozesse, Rollen und Aufgaben müssen so weiterentwickelt und ausgestaltet werden, damit die Sicherheit laufend und zielgerichtet gewährleistet und gestärkt werden kann. Dabei sind die bei Bund und Kantonen vorhandenen technischen Kompetenzen und personellen Ressourcen sowie die Abhängigkeit vom Systemanbieter zu berücksichtigen.

Die Definition der zu behandelnden Fragestellungen und die Umsetzung der Massnahme soll der Arbeitsgruppe Zukunft Vote électronique obliegen, die von der Schweizerischen Staatsschreiberkonferenz zur Behandlung langfristiger Fragestellungen vorgeschlagen worden ist. Die AG Zukunft soll prüfen, ob und für welche Aufgaben im Bereich der politischen Rechte zentralisiertere Strukturen für E-Voting künftig einen Mehrwert bringen könnten. Diese Arbeiten sollen in die übergeordnete E-Government-Strategie und -Struktur eingebettet werden und über E-Voting hinaus alle Aspekte der E-Democracy umfassen. Ein Mandatsentwurf für die AG Zukunft VE wurde von den Kantonen erarbeitet, die Schweizerische Staatsschreiberkonferenz entscheidet über das weitere Vorgehen.

Dialog mit der Wissenschaft

Die Überprüfung der Prozesse, Rollen und Aufgaben wurde im Dialog mit der Wissenschaft nicht als eigenständiges Thema, sondern im Kontext einzelner Massnahmen (wie z.B. unabhängige Überprüfungen) diskutiert.

Auswirkungen der Massnahme und Gesamtbeurteilung des SA VE

Die Umsetzung dieser Massnahme hat keine finanziellen Auswirkungen auf Bund und Kantone.

C. Stärkung der Transparenz und des Vertrauens

Nr.	Massnahme	Zeitpunkt Umsetzung	Zuständigkeit
C.1	Begrenzung des zulässigen Elektorats für vollständig verifizierbare Systeme	Wiedereinsatz	BK

Zielsetzung und Beschreibung der Massnahme

Gemäss dem Entscheid des Bundesrates vom 26. Juni 2019 wird vorläufig auf eine Überführung in den ordentlichen Betrieb verzichtet und der Versuchsbetrieb wird weitergeführt. Dabei sollen in Zukunft nur noch vollständig verifizierbare Systeme eingesetzt werden. Um den Versuchsbetrieb zu unterstreichen, wird mit dieser Massnahme die bisher angewendete Limitierung des zulässigen Elektorats beibehalten, auch wenn vollständig verifizierbare Systeme zum Einsatz kommen.

Die BK passt die Rechtsgrundlagen so an, dass im Versuchsbetrieb das zulässige Elektorat beim Einsatz von vollständig verifizierbaren Systemen limitiert wird. Die Limiten sollen 30 Prozent des kantonalen und 10 Prozent des nationalen Elektorats betragen. Die Einhaltung der kantonalen Limiten obliegt wie im bisherigen Versuchsbetrieb den Kantonen (Anmeldeverfahren, Einsatz in Pilotgemeinden oder nur für Auslandschweizer Stimmberechtigte). Auslandschweizer Stimmberechtigte werden bei der Berechnung der Limiten weiterhin nicht eingerechnet. Diese Limitierung soll für die nächste Phase des Versuchsbetriebs gelten, damit Erfahrungen mit vollständig verifizierbaren Systemen gesammelt werden können und das Vertrauen mit einer schrittweisen Einführung der elektronischen Stimmabgabe gestärkt werden kann.

Dialog mit der Wissenschaft

Im Dialog wurden in Bezug auf die Limitierung des Elektorats verschiedene Positionen vertreten. Eine Mehrheit der Expertinnen und Experten unterstützt die Limitierung im Versuchsbetriebs als risikominimierende Massnahme. Zur Frage, ob die Limitierung des Elektorats darüber hinaus zur Stärkung des Vertrauens beiträgt, teilen sich die Meinungen in zwei etwa gleich starke Gruppen auf: Die eine Gruppe ist der Meinung, dass der Einsatz in geringem Umfang langfristig zur Förderung von Akzeptanz und Vertrauen beiträgt. Die zweite Gruppe vertritt die Position, dass eine Limitierung des Elektorats das Vertrauen nicht beeinflusst oder das Vertrauen möglicherweise gar senkt, wenn die Limitierung signalisiert, dass das System als nicht vertrauenswürdig angesehen wird. Die Limitierung soll auf jeden Fall nur eine vorübergehende Massnahme darstellen.

Auswirkungen der Massnahme und Gesamtbeurteilung des SA VE

Diese Massnahme ist ein wirksames Instrument, weil damit betont wird, dass es sich um einen Versuchsbetrieb handelt und die Einführung von E-Voting schrittweise erfolgt. Mit der Weiterführung der bisherigen Praxis eines limitierten Einsatzes soll das Vertrauen in E-Voting gestärkt werden. Die Limiten

von 30 Prozent des kantonalen und 10 Prozent des nationalen Elektorats sollen für die erste Phase der Wiederaufnahme der Versuche gelten. Eine Anhebung oder gegebenenfalls Aufhebung der Limitierung wird geprüft, wenn sich die vollständig verifizierbaren Systeme dereinst in einem stabilen Versuchsbetrieb bewährt haben.

Für den Bund hat die Umsetzung dieser Massnahme keine finanziellen Auswirkungen. Er wird im Rahmen der Bewilligungsverfahren mit den gesuchstellenden Kantonen die Einhaltung des nationalen Elektorats sicherstellen. Die Kantone müssen Massnahmen zur Einhaltung der kantonalen Limiten umsetzen. Dies kann je nach Wahl des Instruments zu Kosten im mittleren Bereich führen (bspw. Einführung eines Anmeldeverfahrens). Mit Mehrkosten müssten Kantone rechnen, die bisher einen flächendeckenden Einsatz geplant und noch keine Massnahmen zur Limitierung des Elektorats umgesetzt haben.

Die Limitierung des Elektorats könnte dazu führen, dass gewisse Kantone von einer Einführung von E-Voting abgehalten werden. Dies kann eintreffen, wenn beispielsweise die nationale Limite bereits erreicht wird oder wenn ein Kanton E-Voting nur anbieten möchte, wenn das gesamte Elektorat zugelassen wird. In der Praxis ist in den nächsten Jahren nicht damit zu rechnen, dass die vorgeschlagenen Limiten solche Einschränkungen zur Folge haben werden. Sobald Einschränkungen bemerkbar sind, ist die Massnahme zu überprüfen.

Nr.	Massnahme	Zeitpunkt Umsetzung	Zuständigkeit
C.2	Präzisierung der Anforderungen an die Offenlegung des Quellcodes	Wiedereinsatz	Anforderungen: BK Offenlegung: Kantone, Systemanbieter

Zielsetzung und Beschreibung der Massnahme

Die Erfahrungen mit der Offenlegung des Quellcodes des Post-Systems haben gezeigt, dass in diesem Bereich Handlungsbedarf besteht. Die Anforderungen an die zu publizierenden Unterlagen werden so präzisiert, dass insbesondere folgende Aspekte berücksichtigt werden:

- Der Quellcode und die Dokumentation der Software sowie die Dateien mit relevanten Inputparametern sind offenzulegen.
- Hilfestellungen und ergänzende Dokumentationen sind zu publizieren, so dass fachkundige Personen das System in der eigenen Infrastruktur effizient kompilieren, in Betrieb nehmen und analysieren können.
- Dokumentationen zu Infrastruktur, Drittsoftware und Betriebsprozessen sind so weit als möglich zu publizieren. Zumindest die wesentlichen Elemente sind zusammenfassend zu beschreiben.
- Die Darstellung der offengelegten Unterlagen entspricht der gängigen Praxis.

Die Anforderungen in Bezug auf die Nutzungsbedingungen werden wie folgt ausgestaltet:

- Der Zugang zum Quellcode wird unentgeltlich und anonym gewährt. Es wird darauf verzichtet, Personen, die auf die offengelegten Informationen zugreifen möchten, zur Preisgabe ihrer Identität aufzufordern.
- Der Quellcode darf für ideelle und namentlich wissenschaftliche Zwecke genutzt werden. Dazu gehört der Austausch bei der Fehlersuche sowie das Recht zu publizieren. Dieses Recht wird vom Eigner explizit eingeräumt.
- Wer die Nutzungsbedingungen einhält, wird rechtlich nicht verfolgt. Ein Verstoss gegen die Nutzungsbedingungen wird nur verfolgt, wenn der Quellcode oder Teile davon kommerziell verwendet oder produktiv eingesetzt werden. In den Nutzungsbedingungen wird auf diese Haftungsbeschränkung hingewiesen.
- Es reicht, in den Lizenzbestimmungen auf die Nutzungsbedingungen hinzuweisen. Auf Willenserklärungen der Nutzenden ist, wenn möglich, zu verzichten.

Die BK überarbeitet ihre Anforderungen bis zur Wiederaufnahme der Versuche. Der SA VE spricht sich dafür aus, dass künftige Systeme und Systembestandteile unter einer Open-Source-Lizenz (OSL) publiziert werden. Ausserdem wird mit der Post als heutige Systemanbieterin geprüft, ob bereits entwickelte Komponenten des Quellcodes ihres vollständig verifizierbaren Systems zusätzlich unter eine OSL gestellt werden können.

Dialog mit der Wissenschaft

Die Expertinnen und Experten betonen, dass Transparenz als Basis einer wirksamen öffentlichen Überprüfung von hoher Wichtigkeit ist. Die Offenlegung des Quellcodes und seiner Dokumentation mit möglichst tiefen Zugangshürden ist dabei ein wichtiges Instrument. Es wurden verschiedene Möglichkeiten zur Verbesserung der bestehenden Bestimmungen zur Offenlegung des Quellcodes diskutiert. Auf Geheimhaltungserklärungen soll unbedingt verzichtet werden.

Die Expertinnen und Experten erachten eine Offenlegung des Quellcodes unter einer OSL als erfolgsversprechender als eine Publikation unter proprietärer Lizenz. Mit einer OSL können die Ziele von Transparenz, öffentlicher Überprüfung, Vertrauen der Öffentlichkeit und Aufbau einer Community von Fachpersonen wirksamer erreicht werden. Eine Offenlegung unter einer proprietären Lizenz kann auch zur Erreichung dieser Ziele führen, jedoch nicht in demselben Ausmass. Die Expertinnen und Experten empfehlen eine Open-Source-Publikation auch deshalb, weil damit v.a. die kryptografischen Elemente in anderen Anwendungen eingesetzt und weiterentwickelt werden können. Von einer solchen Weiterverwendung könnten die Entwicklung und die Sicherheit von E-Voting-Systemen profitieren.

Viele der Expertinnen und Experten plädieren dafür, den Quellcode und die Dokumentation frühzeitig offenzulegen. Dabei könnte auch eine Vorabversion offengelegt werden, bevor die finale Version, die produktiv eingesetzt werden soll, publiziert wird. Gleichzeitig wurde darauf hingewiesen, dass die offengelegte Dokumentation von guter Qualität sein müsste und dass Anpassungen ersichtlich sein sollen. Aus Sicht der Expertinnen und Experten sollen zusätzlich zum Quellcode alle Unterlagen offengelegt werden, die nötig sind, um zu verstehen, wie das System funktioniert und betrieben wird. Zudem soll es möglich sein, das System auf eigenen Rechnern zu testen.

Auswirkungen der Massnahme und Gesamtbeurteilung des SA VE

Die Offenlegung des Quellcodes zur öffentlichen Überprüfung ist wichtig und der Aufbau einer entsprechenden Community von Fachpersonen soll gefördert werden. Bei der Offenlegung des Quellcodes besteht Handlungsbedarf. Für die Wiederaufnahme der Versuche werden die Anforderungen an die zu publizierenden Unterlagen und die Nutzungsbedingungen wie in der Massnahme beschrieben präzisiert und angepasst.

Unabhängig von der Offenlegung des Quellcodes und den Modalitäten der Offenlegung stellt sich die Frage, ob der Quellcode eines E-Voting-Systems unter einer Open-Source-Lizenz (OSL) publiziert werden soll. Vereinfacht gesagt ermöglicht eine solche Lizenz Dritten, den Quellcode zu verwenden, zu ändern und für eigene Zwecke (auch produktiv) einzusetzen und zu nutzen. Der SA VE spricht sich dafür aus, dass künftige Systeme und Komponenten unter einer OSL publiziert werden sollen. Eine Veröffentlichung des Quellcodes des Systems der Post unter OSL ist aber keine Voraussetzung für den Einsatz des Systems der Post. Mit der Post als heutige Systemanbieterin wird jedoch geprüft, ob bereits entwickelte Komponenten des Quellcodes ihres vollständig verifizierbaren Systems zusätzlich unter eine OSL gestellt werden können.

Die Offenlegung des Quellcodes ist grundsätzlich mit hohen Kosten verbunden, die Umsetzung dieser Massnahme dürfte jedoch unmittelbar keine zusätzlichen direkten finanziellen Auswirkungen auf Bund und Kantone haben.

Nr.	Massnahme	Zeitpunkt Umsetzung	Zuständigkeit
C.3	Führen eines Bug-Bounty-Programms	Wiedereinsatz	Anforderungen: BK Durchführung: Kantone, Systemanbieter

Zielsetzung und Beschreibung der Massnahme

Zum Einbezug unabhängiger Fachkreise im Sinne einer öffentlichen Überprüfung wird zum offengelegten Quellcode und der Dokumentation von E-Voting-Systemen ein Bug-Bounty-Programm geführt. Dieses soll u.a. folgende Anforderungen erfüllen:

- Der Systemanbieter führt ein Bug-Bounty-Programm, das grundsätzlich ununterbrochen läuft. Das Programm soll frühzeitig vor der Einreichung eines definitiven Gesuchs auf Grundbewilligung des Bundesrates gestartet werden (rund drei Monate).
- Die Meldung von Mängeln ist in Abhängigkeit von deren Schwere finanziell zu entschädigen. Die Höhe der Entschädigungen soll sich am PIT 2019 orientieren.

- Teilnehmende können den Quellcode in der eigenen Infrastruktur anhand des laufenden Systems analysieren. Für den Anspruch auf eine Entschädigung reicht es, Mängel anhand des Quellcodes aufzuzeigen, ein erfolgreicher Angriff muss nicht stattfinden.
- Das Bug-Bounty-Programm umfasst drei Bereiche:
 - Suche von Fehlern in der offengelegten Dokumentation oder dem offengelegten Quellcode (statischer Test)
 - Suche nach Fehlern durch Analyse des lauffähigen Systems in der eigenen Infrastruktur (dynamischer Test)
 - Angriffe auf die Infrastruktur des Anbieters (Internet-Test). Die Zielsetzung dieses Tests besteht ausschliesslich im Eindringen in die Infrastruktur. Denial-of-Service- (DoS) und Social-Engineering-Angriffe können vom Bug-Bounty-Programm ausgeschlossen werden. Angriffe auf die Infrastruktur dürfen in begründeten Fällen verboten werden (z.B. während eines Urnengangs).

Zuständigkeiten und Umgang mit Meldungen:

- Der Systemanbieter ist für das Bug-Bounty-Programm zuständig. Er ermöglicht die Durchführung, nimmt Meldungen entgegen und kategorisiert diese. Er begründet seine Entscheidungen gegenüber den betroffenen Teilnehmenden und publiziert sämtliche bestätigten Befunde. Ausserdem trifft der Systemanbieter Massnahmen zur Behebung der Mängel.
- Die BK legt die grundlegenden Rahmenbedingungen für das Bug-Bounty-Programm fest.
- Bund und Kantone erhalten uneingeschränkten Zugriff auf die Meldungen und Antworten des Systemanbieters. Im Rahmen der Bewilligungsverfahren ist eine Zusammenfassung der Meldungen und der Massnahmen, die aufgrund der Meldungen getroffen werden, einzureichen.

Die Nutzungsbedingungen sind wie folgt auszugestalten:

- Eine Teilnahme ist anonym möglich. Auf die Preisgabe der Identität darf nur für die Auszahlung einer Entschädigung im Rahmen eines Bug-Bounty-Programms bestanden werden.
- Publikationen zu Mängeln oder vermuteten Mängeln durch die Teilnehmenden sind erlaubt. Dafür kann die Einhaltung einer Frist gefordert werden (s. unten).
- Im Sinne einer «responsible disclosure» können die Teilnehmenden zur Einhaltung folgende Regeln aufgefordert werden:
 - Mängel werden umgehend gemeldet.
 - Mit der öffentlichen Bekanntgabe eines Mangels wird zugewartet; eine durch BK, Kantone und Systemanbieter festzulegende Sperrfrist darf dabei nicht überschritten werden.
 - Mit Informationen zu vermuteten Mängeln wird verantwortungsvoll umgegangen. Sich abzeichnende Entdeckungen von Sicherheitslücken werden nicht unnötig gestreut. Informationen dazu werden nur mit Personen geteilt und diskutiert, die zur Behandlung der Fragestellung vermuthungsweise fähig und gewillt sind und die ebenfalls verantwortungsvoll damit umgehen.
 - Verstösse gegen die «responsible disclosure» sollen nicht geahndet werden. In den Nutzungsbedingungen wird auf diese Haftungsbeschränkung hingewiesen.
- Für den Internet-Test: Eine Einwilligung des Systemanbieters in den Test schützt die Teilnehmenden vor Strafverfolgung, sofern die Angriffe vom Test nicht ausgeschlossen sind.

Bis zur Wiederaufnahme der Versuche passt die BK in Absprache mit den Kantonen die Rechtsgrundlagen an, um ein Bug-Bounty-Programm vorzusehen. In einem Anforderungskatalog legt sie in Absprache mit den Kantonen und dem Systemanbieter die grundlegenden Rahmenbedingungen des Bug-Bounty-Programms fest. Eine Eskalationsmöglichkeit für Teilnehmende, die mit der Entscheidung des Systemanbieters nicht einverstanden sind, ist ebenfalls zu prüfen.

Für die Wiederaufnahme der Versuche soll der Internet-Test auf dem produktiven System durchgeführt werden. Anschliessend kann basierend auf den Erfahrungen über das weitere Vorgehen entschieden werden. Dabei stehen die Varianten offen, dass der Internet-Test wiederkehrend auf dem produktiven System oder als laufender Test auf einem Zwillingssystem durchgeführt wird.

Dialog mit der Wissenschaft

Die Expertinnen und Experten messen der öffentlichen Überprüfung eine grosse Wichtigkeit zu. Mängel sollen offengelegt und Hinweise aus der Öffentlichkeit beantwortet werden. Sie empfehlen ein ständig

laufendes Bug-Bounty-Programm mit finanzieller Entschädigung. Das Bug-Bounty-Programm soll sich nicht auf erfolgreiche Angriffe auf die Infrastruktur des Anbieters beschränken, sondern auch Fehler in der Dokumentation des Systems sowie im Quellcode zum Gegenstand haben. Angriffe auf die Backend-Infrastruktur des Systemanbieters, physisches Eindringen sowie DoS- und Social-Engineering-Angriffe sollen nicht in den Anwendungsbereich des Bug-Bounty-Programms fallen, sondern beispielsweise im Rahmen von mandatierten Penetrationstests getestet werden. Die Festlegung der Zielsetzung und Modalitäten sowie die Oberaufsicht werden beim Bund oder einem unabhängigen Komitee gesehen.

Auswirkungen der Massnahme und Gesamtbeurteilung des SA VE

Ein Programm zur Fehlersuche kann bei der kontinuierlichen Verbesserung des Systems helfen. Mit dem Bug-Bounty-Programm wird die öffentliche Überprüfung verstärkt. Dies kann zum Aufbau einer Community von Fachpersonen sowie zur Stärkung des Vertrauens der Öffentlichkeit beitragen. Die BK gibt die Rahmenbedingungen für das Bug-Bounty-Programm vor. Die Definition der Einzelheiten wie etwa die Kategorisierung der Mängel und die Höhe der finanziellen Entschädigungen wird bis auf weiteres den Systemanbietern überlassen. Dies soll in Absprache mit dem NCSC, der BK und den Kantonen erfolgen. Dabei ist darauf zu achten, dass eine wirksame und glaubwürdige Entschädigung und Behandlung von gemeldeten Mängeln erfolgt.

Kostenschätzungen für die Varianten des weiteren Vorgehens beim Internet-Test (ohne finanzielle Entschädigungen):

- Bug-Bounty-Programm mit ständiger Fehlersuche (statischer und dynamischer Test) und einem wiederkehrenden Internet-Test:
 - Einmalige Kosten: 230'000-290'000 CHF
 - Wiederkehrende Kosten (im Durchschnitt): 55'000-70'000 CHF / Jahr
- Bug-Bounty-Programm mit ständiger Fehlersuche (statischer und dynamischer Test) und einem laufenden Internet-Test:
 - Einmalige Kosten: 255'000-360'000 CHF
 - Wiederkehrende Kosten (im Durchschnitt): 550'000-650'000 CHF / Jahr

Nach Ansicht der BK sind die Kosten primär von den Kantonen zu tragen. Eine Mitfinanzierung des Bundes für das Führen des Programms ist ebenso zu prüfen wie eine Beteiligung von weiteren Bundesstellen.

Nr.	Massnahme	Zeitpunkt Umsetzung	Zuständigkeit
C.4	Publikation bewilligungsrelevanter Prüfberichte	Wiedereinsatz	BK, Kantone, Systemanbieter

Zielsetzung und Beschreibung der Massnahme

Bund, Kantone und Systemanbieter schaffen gegenüber der Öffentlichkeit Transparenz in Bezug auf bewilligungsrelevante Prüfergebnisse. Dies soll eine Überprüfung durch Fachkreise ermöglichen und die Vertrauensbildung und den Aufbau einer Community von Fachpersonen unterstützen. Mit dieser Massnahme werden die folgenden Aspekte geregelt:

- Berichte, Belege und Zertifikate, die im Rahmen der Prüfungen gemäss Ziffer 5 des Anhangs der VELeS erstellt werden, sind zu publizieren. Zuständig für die Publikation ist der jeweilige Auftraggeber des Prüfberichts.
- Die publizierten Prüfberichte müssen nachvollziehbar sein. Wird in den Prüfberichten auf weitere Unterlagen verwiesen, sind diese in der Regel offenzulegen. Können zusätzliche Unterlagen nicht veröffentlicht werden, soll die Nachvollziehbarkeit der Prüfberichte mit einer zusammenfassenden Beschreibung der relevanten Aspekte aus den nicht publizierten Unterlagen gewährleistet werden.
- Von der Publikation der Prüfberichte oder weiterer Unterlagen kann in begründeten Fällen abgesehen werden. Solche Ausnahmen sind beispielsweise möglich, wenn durch die Publikation ein Risiko erhöht würde oder der Publikation Gründe des Datenschutzes oder interner Sicherheitsrichtlinien entgegenstehen.
- Repliken, welche die geprüfte Organisation in Bezug auf die publizierten Prüfberichte erstellt, sollen auch publiziert werden.

Die BK passt die Rechtsgrundlagen bis zur Wiederaufnahme der Versuche an.

Dialog mit der Wissenschaft

Die Expertinnen und Experten sind sich einig, dass Transparenz die Voraussetzung für eine wirksame öffentliche Überprüfung ist. Die Mehrheit der Expertinnen und Experten empfiehlt, Prüfberichte zu publizieren. Dabei ist jedoch auf eine hohe Qualität und Nachvollziehbarkeit der Prüfberichte zu achten, ansonsten könnte die Publikation zu einem Vertrauensverlust führen.

Auswirkungen der Massnahme und Gesamtbeurteilung des SA VE

Es wird als wichtig erachtet, dass in Bezug auf bewilligungsrelevante Prüfberichte mehr Transparenz geschaffen wird. Zielpublikum der Publikationen sind primär Fachkreise und mittelbar die breite Öffentlichkeit. Es ist wichtig, die vorgesehene Publikation der Prüfberichte im ganzen Prozess der Mandatierung von Expertinnen und Experten zu berücksichtigen. Die Publikation ist bereits zum Zeitpunkt der Mandatsvergabe mit den Mandatsträgern zu thematisieren. Die Umsetzung dieser Massnahme hat allenfalls tiefe finanzielle Auswirkungen auf die auftraggebende Stelle. Dies ist primär der Bund.

Nr.	Massnahme	Zeitpunkt Umsetzung	Zuständigkeit
C.5	Publizieren der Ergebnisse von eidgenössischen Urnengängen für E-Voting	Wiedereinsatz	Anforderungen: BK Publikation: Kantone

Zielsetzung und Beschreibung der Massnahme

Gegenüber der Öffentlichkeit wird Transparenz in Bezug auf E-Voting-Ergebnisse geschaffen. Die Kantone sollen deshalb die Ergebnisse von eidgenössischen Wahlen und Abstimmungen für den elektronischen Stimmkanal publizieren. Dies soll der Bevölkerung erlauben, die Ergebnisse von E-Voting mit dem Gesamtergebnis zu vergleichen und eine Plausibilisierung vorzunehmen. Damit kann das Vertrauen in E-Voting gestärkt werden. Ausserdem werden mit einer Publikation der E-Voting-Ergebnisse Daten und Informationen bereitgestellt, die eine interessante Grundlage für Forschungszwecke bieten können.

Die BK passt die VELeS an und sieht grundsätzlich eine Publikation der E-Voting-Ergebnisse bis auf Gemeindeebene vor. Dabei sind Ausnahmen vorzusehen, damit das Stimmgeheimnis in jedem Fall gewährleistet werden.

Dialog mit der Wissenschaft

Die Mehrheit der Expertinnen und Experten hat sich dafür ausgesprochen, dass die E-Voting-Ergebnisse publiziert werden. Hauptgründe dafür sind Transparenz und Vertrauen. Zusätzlich wurde auch genannt, dass die Publikation der Ergebnisse mittelbar zur Entdeckung von Mängeln im System führen kann. Das Stimmgeheimnis und der Datenschutz müssen bei einer Publikation gewährleistet werden.

Auswirkungen der Massnahme und Gesamtbeurteilung des SA VE

E-Voting-Ergebnisse sollen publiziert werden. In Bezug auf den Detaillierungsgrad der Publikation geben die Kantone zu bedenken, dass eine Publikation auf Gemeindeebene problematisch sein kann. In den Rechtsgrundlagen sind Ausnahmen vorzusehen, so dass mit der Publikation das Stimmgeheimnis nicht verletzt wird.

Die Umsetzung dieser Massnahme hat keine finanziellen Auswirkungen auf den Bund; die finanziellen Auswirkungen auf die Kantone werden als gering eingestuft.

Nr.	Massnahme	Zeitpunkt Umsetzung	Zuständigkeit
C.6	Vermehrter Einbezug der Öffentlichkeit	Konzept: Wiedereinsatz	BK unter Einbezug Kantone und Systemanbieter

Zielsetzung und Beschreibung der Massnahme

Bei E-Voting soll die Öffentlichkeit vermehrt einbezogen werden. Mit verschiedenen im Rahmen der Neuausrichtung vorgeschlagenen Massnahmen wird die Transparenz und der Aufbau einer Community von Fachpersonen gefördert. Zusätzlich zu diesen Massnahmen werden Bund, Kantone und Systemanbieter ein Konzept zum weiteren, vermehrten Einbezug der Öffentlichkeit erstellen. In diesem Konzept sind Vorhaben zur aktiven Kommunikation vorzusehen. Die laufende Umsetzung von Veranstaltungen

und Informationsmassnahmen ist sicherzustellen. Dabei soll neben Politik, Fachkreisen und Interessensverbänden auch ein Fokus auf die breite Öffentlichkeit gelegt werden. Dazu können u.a. folgende Aktivitäten vorgesehen werden:

- Durchführung und Beteiligung an Informations- und Diskussionsveranstaltungen (Konferenz für Politik, Parteien, Verbände und die Wissenschaft; E-VoteID-Konferenz in Bregenz).
- Ideenwettbewerbe (bspw. für Social-Engineering-Attacks) und Hackathons.
- Betreiben einer Informationsplattform.

Eine erste Version dieses Konzepts wird bis zur Wiederaufnahme der Versuche erstellt. Die BK übernimmt die Federführung. Die vorgesehenen Aktivitäten sollen laufend umgesetzt werden. Wenn möglich, sind erste Aktivitäten bereits bis zur Wiederaufnahme umzusetzen. Beispielsweise hat der Kanton St. Gallen bereits eine allgemeine Informationsplattform initiiert, mit der sich interessierte Personen Hintergrundinformationen zum Thema E-Voting beschaffen können. Die Plattform befindet sich in der Entwicklung.

Dialog mit der Wissenschaft

Grundsätzlich erachten die Expertinnen und Experten Transparenz und Kommunikation gegenüber der Öffentlichkeit als wichtig. Dabei muss zwischen Fachkreisen und der breiten Öffentlichkeit unterschieden werden. Spezifisch technisch-orientierte Veranstaltungen wie Hackathons und Ideenwettbewerbe werden als geeignet angesehen, um Fachkreise für E-Voting zu interessieren und einzubeziehen. Für die breite Öffentlichkeit soll ein Ansatz gewählt werden, der das Verständnis und Vertrauen in E-Voting fördert. Als Beispiele wurden Citizen-Science-Projekte und Workshops zum Einbezug der breiten Öffentlichkeit genannt.

Auswirkungen der Massnahme und Gesamtbeurteilung des SA VE

Der Stärkung der Transparenz und der Kommunikation gegenüber der breiten Öffentlichkeit, der Politik und Interessensverbänden sowie dem Aufbau einer Community von Fachpersonen kommt eine hohe Bedeutung zu. Die Erarbeitung eines Konzepts hat tiefe finanzielle Auswirkungen auf den Bund; bei den Kantonen entstehen keine Kosten. Die Umsetzung der Vorhaben kann Kosten bei Bund und Kantonen auslösen.

D. Stärkere Vernetzung mit der Wissenschaft

Nr.	Massnahme	Zeitpunkt Umsetzung	Zuständigkeit
D.1	Erstellung eines Konzepts für die wissenschaftliche Begleitung der Versuche und den Dialog mit externen Expertinnen und Experten	Konzept: 2021	BK unter Einbezug Kantone

Zielsetzung und Beschreibung der Massnahme

Die Versuche von E-Voting sollen laufend wissenschaftlich untersucht und begleitet werden. Darüber hinaus werden Bund und Kantone einen ständigen Dialog mit der Wissenschaft und kompetenten Fachstellen führen. Sie unterbreiten Fragen, reagieren auf Hinweise, beteiligen sich aktiv an den Diskussionen und sorgen für die nötige Infrastruktur sowie die Ressourcen für den Austausch. Ausserdem vergeben Bund und Kantone wissenschaftliche Studien in Bereichen, bei denen eine Vertiefung notwendig ist.

Für die Ausgestaltung der wissenschaftlichen Begleitung und des Dialogs mit externen Expertinnen und Experten während der Jahre 2022-2025 sowie für die Finanzierung erstellen Bund und Kantone in Zusammenarbeit mit Vertreterinnen und Vertretern der Wissenschaft ein Konzept. Die BK übernimmt die Federführung für die Erarbeitung des Konzepts.

Dialog mit der Wissenschaft

Die Expertinnen und Experten betonen, dass ein ständiger Dialog und eine ständige Zusammenarbeit zwischen den Behörden und der Wissenschaft zur Weiterentwicklung von E-Voting zentral sind. Insbesondere werden der Einbezug unabhängiger Expertinnen und Experten bei der Konzeption und der Entwicklung des Systems, bei öffentlichen und mandatierten Prüfungen und bei der Beurteilung von Risiken sowie die Förderung von Forschung und der allgemeine Aufbau einer Community von Fachpersonen befürwortet. Beim Dialog mit der Wissenschaft sollen neben technischen Fragestellungen vermehrt auch sozialwissenschaftliche Themenbereiche behandelt werden. Um eine ganzheitliche Sicht

und damit eine Verbesserung der Sicherheit bei Wahlen und Abstimmungen insgesamt zu ermöglichen, sollen bei der Sicherheitsdiskussion neben E-Voting auch die übrigen Stimmkanäle einbezogen werden.

Auswirkungen der Massnahme und Gesamtbeurteilung des SA VE

Eine ständige wissenschaftliche Begleitung ist zentral, um die Sicherheit und eine wissenschaftlich fundierte Weiterentwicklung von E-Voting sicherzustellen. Bei der Erarbeitung des Konzepts sind die Zielsetzungen und Erwartungen an die wissenschaftliche Begleitung zu klären. Dabei sind insbesondere die Zuständigkeiten von Bund und Kantonen sowie die Finanzierung der Begleitung zu definieren. Die Ausarbeitung des Konzepts hat tiefe finanzielle Auswirkungen auf Bund und Kantone. Die Umsetzung des Konzepts wird, je nach Ausgestaltung des Einbezugs, finanzielle Auswirkungen haben.

Nr.	Massnahme	Zeitpunkt Umsetzung	Zuständigkeit
D.2	Einbezug unabhängiger Expertinnen und Experten	Im Rahmen der einzelnen Massnahmen	BK unter Einbezug Kantone

Zielsetzung und Beschreibung der Massnahme

Bund und Kantone sollen bei ihren Arbeiten unabhängige Fachpersonen und Fachstellen der einschlägigen Fachbereiche der Wissenschaft sowie weitere Organisationen beiziehen, soweit dies sinnvoll ist und einen Mehrwert bietet, insbesondere bei den im Rahmen der Neuausrichtung definierten Massnahmen:

- Definition und Vergabe der unabhängigen Prüfungen durch die BK
- Konzeption und Umsetzung der E-Voting-Dienstleistung und der mit ihr verbundenen Abläufe durch die Kantone und deren Partner
- Beurteilung der Zulassungsgesuche und insbesondere der Prüfergebnisse
- Prüfung der Sicherheitsanforderungen des Bundes
- Ausarbeitung von Konzepten für Verbesserungsmassnahmen und deren Terminierung im Massnahmenplan
- Erstellung von Grundlagen für die Risikobeurteilungen
- Beurteilung einzelner Risiken
- Ausarbeitung von Massnahmen, die der Zielsetzung zudienen, dass sich unabhängige Fachexpertinnen und -experten beteiligen
- Durchführung von Workshops / Seminaren
- Benutzerfreundlichkeit / Ergonomie
- Prüfung verteilter Druckprozess

Die Form des Einbezugs wird im Zusammenhang mit den jeweiligen Aufgabenbereichen diskutiert. Bei einzelnen Aufgaben ist auch der Einbezug kompetenter Bundesstellen zu prüfen.

Dialog mit der Wissenschaft

Vgl. die Ausführungen zu den einzelnen Massnahmen und zur Massnahme D.1.

Auswirkungen der Massnahme und Gesamtbeurteilung des SA VE

Vgl. die Ausführungen zu den einzelnen Massnahmen und zur Massnahme D.1. Diese Massnahme hat grundsätzlich keine finanziellen Auswirkungen auf Bund und Kantone. Die Auswirkungen werden im Rahmen der einzelnen Massnahmen ausgewiesen.

Nr.	Massnahme	Zeitpunkt Umsetzung	Zuständigkeit
D.3	Erstellung eines Konzepts für den Aufbau eines wissenschaftlichen Ausschusses	Konzept: 2022	BK unter Einbezug Kantone
<p><u>Zielsetzung und Beschreibung der Massnahme</u></p> <p>Zur Beratung von Bund und Kantonen wird ein wissenschaftlicher Ausschuss aufgebaut. Der Ausschuss soll Beratungsaufgaben mit Blick auf die Zusammenarbeit mit der Wissenschaft (im Sinne der Massnahmen D.1 und D.2) übernehmen und einzelne Aufgaben auch selber wahrnehmen können. Es ist zu prüfen, wie der Ausschuss in die bestehenden Prozesse zur Beurteilung der Systeme eingebunden werden kann. Ebenfalls zu prüfen ist eine Funktion bei der Unterstützung der Kantone. Die Aufgaben sowie die Besetzung des Ausschusses sind festzulegen. Dazu erstellen Bund und Kantone unter der Federführung der BK ein Konzept für die Jahre 2022-2025.</p> <p><u>Dialog mit der Wissenschaft</u></p> <p>In Ergänzung zu den Ausführungen unter der Massnahme D.1 befürworten die Expertinnen und Experten die Schaffung eines wissenschaftlichen Ausschusses, der mit der Beratung der Behörden beauftragt wird. Der Ausschuss könnte eine Aufsichtsfunktion, aber keine regulatorischen Aufgaben übernehmen. Neben einem wissenschaftlichen Ausschuss wurde auch die Idee eines Bürgerbeirats eingebracht, der etwa Aufgaben in den Bereichen Information der Öffentlichkeit, öffentliche Vertrauensbildung und Benutzerfreundlichkeit übernehmen könnte.</p> <p><u>Auswirkungen der Massnahme und Gesamtbeurteilung des SA VE</u></p> <p>Neben der allgemeinen wissenschaftlichen Begleitung der Versuche wird die Schaffung eines wissenschaftlichen Beirats befürwortet, der den Bund und die Kantone beratend unterstützt. Bei der Erarbeitung des Konzepts sind die Aufgaben des Beirats sowie die Frage einer allfälligen finanziellen Entschädigung und die Zuständigkeit für die Finanzierung zu klären. Die Ausarbeitung des Konzepts hat keine finanziellen Auswirkungen auf Bund und Kantone.</p>			

4. Gesamtbeurteilung und weiteres Vorgehen

4.1 Zusammenfassung der Stossrichtungen und Etappierung der Massnahmen

Mit der Umsetzung der vorliegenden Massnahmen soll dem eruierten Handlungsbedarf für die Wiederaufnahme der Versuche sowie mittel- bis langfristig begegnet werden. Für die Sicherstellung der Qualität und Sicherheit der Systeme, der Wirksamkeit der Kontrolle und Prozesse sowie die Stärkung des Vertrauens in den elektronischen Stimmkanal ist ein kontinuierlicher Verbesserungsprozess notwendig. Dabei sollen ein verstärkter Dialog mit der Wissenschaft geführt und vermehrt unabhängige Fachpersonen und die Öffentlichkeit einbezogen werden. Für die Wiederaufnahme der Versuche müssen verschiedene Massnahmen umgesetzt und die Rechtsgrundlagen angepasst werden. Damit soll eine erste Etappe von Verbesserungen umgesetzt werden, während laufend an der Umsetzung der mittel- bis langfristigen Zielsetzungen gearbeitet wird. Die Stossrichtungen des Massnahmenkatalogs lassen sich wie folgt zusammenfassen:

Weiterentwicklung der Systeme

- Sicherstellung der Qualität des Systems durch präzisere Vorgaben der Qualitätskriterien und nachvollziehbare Entwicklungs- und Bereitstellungsprozesse	Wiedereinsatz; kontinuierlicher Verbesserungsprozess
- Sicherstellung der «forensic readiness» der eingesetzten Systeme durch eine wirksame Erkennung und Untersuchung von Vorfällen	Wiedereinsatz; kontinuierlicher Verbesserungsprozess
- Schaffung eines gemeinsamen, öffentlichen Planungsinstruments von Bund und Kantonen zur laufenden Umsetzung sicherheitsrelevanter Massnahmen	Wiedereinsatz; laufende Überprüfung
- Stärkung der Verifizierbarkeit durch mehr Diversität und Unabhängigkeit einzelner Komponenten	Mittelfristig; Vertiefungen bis 2 Jahre nach Wiedereinsatz

Wirksame Kontrolle und Aufsicht

- Sicherstellung der Wirksamkeit der unabhängigen Überprüfungen des Systems	Wiedereinsatz
- Schaffung eines geregelten Vorgehensprozesses zum Umgang mit erwiesenen und vermuteten Nicht-Konformitäten	Wiedereinsatz
- Verbesserungen im Bereich der Risikobeurteilungen und des Krisenmanagements	Wiedereinsatz; kontinuierlicher Verbesserungsprozess
- Weiterentwicklung der Plausibilisierung	Laufend, erste Etappe bis 2022
- Anpassungen und Überprüfung der Abläufe im Bewilligungsverfahren, sowie der Prozesse, Rollen und Aufgaben	Wiedereinsatz und langfristige Überprüfung

Stärkung der Transparenz und des Vertrauens

- Limitierung des Elektorats im Versuchsbetrieb	Wiedereinsatz
- Mehr Transparenz und Erleichterung des Zugangs zu Systeminformationen, Prüfberichten und Ergebnissen	Laufend
- Vermehrter Aufbau und Einbezug einer Community von Fachpersonen und der Öffentlichkeit (Politik, Fachkreise, Interessensverbände und breite Öffentlichkeit) für eine ständige öffentliche Überprüfung	

Stärkere Vernetzung mit der Wissenschaft

- Kontinuierliche Begleitung durch die Wissenschaft und Einbezug unabhängiger Expertinnen und Experten	Querschnittsthema, Umsetzung laufend
- Aufbau eines wissenschaftlichen Ausschusses zur Unterstützung und Beratung von Bund und Kantonen	Mittelfristig

4.2 Auswirkungen auf Bund und Kantone

4.2.1 Massnahmen für den Wiedereinsatz und die erste Etappe nach dem Wiedereinsatz

Ein Teil der Massnahmen für die Wiederaufnahme der Versuche hat keine bis tiefe direkte Kostenfolgen für den Bund und die Kantone. Es ist davon auszugehen, dass diese Kosten von Bund und Kantonen gemäss ihren Zuständigkeiten finanziert werden können. Die Folgenden, ebenfalls für die Wiederaufnahme oder die erste Etappe nach der Wiederaufnahme vorgesehenen Massnahmen, haben jedoch höhere finanzielle Auswirkungen:

- Herstellerunabhängiger Verifier und Kontrollkomponenten (Massnahme A.4): Für die Umsetzung der ersten Etappe (Erarbeitung einer Studie zu unabhängigen Online-Kontrollkomponenten) fallen bei den Kantonen gemäss einer ersten Schätzung voraussichtlich tiefe bis mittlere Kosten an.
- Abschwächung Vertrauensannahmen im Druckprozess (Massnahme A.5): Gemäss einer ersten Kostenschätzung fallen in der ersten Etappe für die Anpassung des kryptografischen Protokolls hohe Kosten an.¹⁹ Diese müssten gemäss den heutigen Zuständigkeiten von den Kantonen getragen werden. Für die Kantone sind diese Kosten nicht alleine tragbar; eine Mitfinanzierung des Bundes ist zu prüfen.
- Public Bulletin Board (Massnahme A.6): Für die Umsetzung der ersten Etappe (Erarbeitung einer Studie) fallen beim Bund gemäss einer ersten Schätzung voraussichtlich mittlere Kosten an.
- Unabhängige Überprüfung der Systeme (Massnahme B.1): Diese Massnahme hat hohe finanzielle Auswirkungen auf den Bund, der künftig diese Überprüfungen – bis auf die ISO27001-Zertifizierung des Systemanbieters – verantwortet, in Auftrag gibt und damit auch die entstehenden Kosten trägt. Die Durchführung der unabhängigen Überprüfungen kann voraussichtlich vom Bund finanziert werden, vorausgesetzt die entsprechenden Mittel werden bewilligt.
- Führen eines Bug-Bounty-Programms (Massnahme C.3): Gemäss einer ersten Kostenschätzung der Post fallen für die Umsetzung je nach Ausgestaltung mittlere bis hohe Kosten an.²⁰ Zusätzlich entstehen Kosten für die finanzielle Entschädigung von Meldungen. Gemäss der Aufteilung der Zuständigkeit sind diese Kosten durch die Kantone zu tragen. Für die Kantone sind diese Kosten nicht alleine tragbar; eine Mitfinanzierung des Bundes ist zu prüfen.

4.2.2 Mittel- bis langfristige Entwicklungen

Die Massnahmen sind wichtig für die Sicherheit und Vertrauenswürdigkeit von E-Voting und damit zentral für die Zukunft der elektronischen Stimmabgabe. Die Finanzierung der mittel- bis langfristigen Entwicklungen ist nicht sichergestellt. Sie ist insbesondere bei den folgenden drei Massnahmen kritisch. Bei diesen Massnahmen sind in einem ersten Schritt Studien und Vertiefungen vorgesehen, bei denen mit tiefen bis mittleren Kosten zu rechnen ist. Eine anschliessende Umsetzung hingegen wäre mit hohen Kosten verbunden:

- Herstellerunabhängiger Verifier und Kontrollkomponenten (Massnahme A.4): Die Kosten für den Einsatz herstellerunabhängiger Online-Kontrollkomponenten sind sehr hoch und gemäss den heutigen Zuständigkeiten von den Kantonen zu tragen. Für die Kantone sind die geschätzten Kosten²¹ nicht tragbar. Eine Mitfinanzierung des Bundes ist zu prüfen.
- Abschwächung Vertrauensannahmen im Druckprozess (Massnahme A.5): Die Kosten für die Umsetzung sind hoch und gemäss den heutigen Zuständigkeiten von den Kantonen zu tragen. Für die Kantone sind die geschätzten Kosten²² nicht tragbar. Eine Mitfinanzierung des Bundes ist zu prüfen.

¹⁹ Einmalige Kosten von 850'000-1 Mio. CHF.

²⁰ Kostenschätzung für das Bug-Bounty-Programm mit wiederkehrendem Internet-Test: Einmalige Kosten von 230'000-290'000 CHF und wiederkehrende Kosten von 55'000-70'000 CHF / Jahr. Bug-Bounty-Programm mit laufendem Internet-Test: Einmalige Kosten von 255'000-360'000 CHF und wiederkehrende Kosten von 550'000-650'000 CHF / Jahr.

²¹ Kontrollkomponenten: Einmalige Kosten von 1.8-2.2 Mio. CHF und wiederkehrende Kosten von 600'000-800'000 CHF / Jahr. Verifier: Einmalige Kosten von 0.9-1 Mio. CHF und wiederkehrende Kosten von 200'000 CHF / Jahr.

²² Einmalige Kosten von 700'000-900'000 CHF und wiederkehrende Kosten von 100'000 CHF / Jahr.

- Public Bulletin Board (Massnahme A.6): Bei einer allfälligen Umsetzung würden gemäss einer ersten Schätzung hohe Kosten²³ anfallen. Die Zuständigkeit für die Finanzierung ist noch zu klären.

4.2.3 Langfristige Sicherstellung der Finanzierung

Möglichkeiten für die Finanzierung

Die Gewährleistung der Sicherheit von E-Voting ist mit hohen Kosten verbunden und zukünftig ist mit noch höheren Kosten zu rechnen. Die Finanzierung muss langfristig gesichert werden. Können die Kantone die Kosten für materiell wichtige Massnahmen nicht tragen, sind neue Finanzierungsmöglichkeiten zu prüfen.

Es sollen folgende Finanzierungsmöglichkeiten sondiert werden:

- Der Umsetzungsplan von E-Government Schweiz sieht für E-Voting bis 2023 jährliche Mittel von 250'000 CHF vor. Damit können einzelne Projekte und Studien finanziert werden, die Finanzierung der mittel- und langfristigen Entwicklungen würde diese Mittel jedoch übersteigen. Es ist zu prüfen, ob die für E-Voting vorgesehenen Mittel im Umsetzungsplan von E-Government Schweiz erhöht und ob einzelne Projekte über weitere Mittel von E-Government Schweiz finanziert werden können.
- Die Erschliessung neuer Finanzierungsquellen bei den Kantonen ist zu prüfen.
- Die Erschliessung neuer Finanzierungsquellen beim Bund ist zu prüfen.

Zusätzlich sollen bei der Umsetzung der Massnahmen bei allen beteiligten Akteuren so weit als möglich Synergien genutzt werden. Dazu soll die Zusammenarbeit mit bereits bestehenden Strukturen intensiviert werden. Beispielsweise ist zu prüfen, wie die bestehenden Ressourcen beim Nationalen Zentrum für Cybersicherheit (NCSC) und die Schnittstellen zu bestehenden Prozessen bei der BK, den Kantonen und der Post ausgeschöpft werden können.

Einschätzung der Kantone

Für die Kantone ist klar, dass nur sichere E-Voting-Systeme eingesetzt werden sollen. Grundsätzlich ist der Spielraum der Kantone in Bezug auf die Finanzierung von E-Voting beschränkt. In vielen Kantonen ist der politische Druck auf die für E-Voting vorgesehenen Ressourcen gestiegen und es dürfte sich weiter verstärken, falls noch längere Zeit kein produktiver Einsatz von E-Voting möglich ist. Die Beantragung zusätzlicher Mittel scheint aus Sicht der Kantone unrealistisch. Ausserdem werden in den nächsten Jahren nur sehr wenige Kantone E-Voting anbieten können. Die Finanzierung der im Rahmen der Neuausrichtung definierten Massnahmen kann nicht durch diese wenigen Kantone getragen werden.

Die bisherigen Kosten waren für die Kantone tragbar. Es ist jedoch davon auszugehen, dass die Post die Umsetzung neuer Anforderungen an die Kantone weiterverrechnen wird. Für die Kantone ist jeweils der Preis pro stimmberechtigte Person relevant. Somit können Mehrkosten der Post nur durch ein grösseres für E-Voting zugelassenes Elektorat und zusätzliche Kantone gedeckt werden.

Bei der Entscheidung zur Umsetzung von Massnahmen ist der beschränkte Spielraum der Kantone in Bezug auf die Finanzierung zu berücksichtigen. Die Finanzierungsfrage muss mitentscheidend sein, ob eine Massnahme umgesetzt wird. Für die Massnahmen, bei denen die Kantone die Finanzierung nicht tragen können, sind alternative Finanzierungslösungen zu suchen. Es ist zu klären, in welchem Umfang sich der Bund an der Finanzierung beteiligen kann.

Einschätzung der BK

Die Gewährleistung der Sicherheit ist zentral für den Einsatz eines vertrauenswürdigen elektronischen Stimmkanals. Dabei werden die Behörden und Systemanbieter vermehrt mit hohen Kosten konfrontiert werden. Aus Sicht der BK bringen jedoch genau diejenigen Massnahmen, die mit hohen Kosten verbunden sind, einen erheblichen Sicherheitsgewinn. Insbesondere die «public scrutiny», der Einbezug der Wissenschaft sowie die Stärkung der Sicherheit und Verifizierbarkeit gestützt auf wissenschaftliche

²³ Einmalige Kosten von 600'000 CHF und wiederkehrende Kosten von 200'000 CHF / Jahr.

Erkenntnisse bieten aus Sicht der BK einen hohen Mehrwert. Die Umsetzung dieser Massnahmen ist daher zentral für die Entwicklung von E-Voting. Diese Einschätzung entspricht auch dem Ergebnis des Dialogs mit der Wissenschaft. Da die Finanzierung dieser Massnahmen mit den heutigen Budgets von Bund und Kantonen nicht sichergestellt ist, müssen neue Lösungen für die Finanzierung gesucht werden. Aus Sicht der BK ist es wichtig, dass Bund und Kantone die Umsetzung dieser Massnahmen anstreben und sich bereits heute dafür aussprechen, die notwendige Finanzierung sicherzustellen.

5. Schlussfolgerungen

Zur Erfüllung der Ziele, die der Bundesrat für die Neuausrichtung des Versuchsbetriebs definiert hat, hat der SA VE mit dem vorliegenden Schlussbericht einen Massnahmenkatalog verabschiedet. In diesem Massnahmenkatalog werden die kurz- sowie mittel- bis langfristigen Stossrichtungen der Arbeiten von Bund und Kantonen in den nächsten Jahren inklusive Zeithorizont der Umsetzung und Zuständigkeiten dargelegt. Im Vordergrund steht ein kontinuierlicher Verbesserungsprozess und nicht mehr ein durch die Zertifizierung verkörpertes Gütesiegel. Die Sicherheit, das Vertrauen und die Akzeptanz von E-Voting sollen laufend unter Einbezug von Expertinnen und Experten aus Wissenschaft und Industrie gestärkt werden. Bund und Kantone sollen die notwendigen Massnahmen laufend überprüfen und bei Bedarf anpassen.

In einer ersten Etappe werden Massnahmen für die Wiederaufnahme der Versuche umgesetzt und die Rechtsgrundlagen entsprechend angepasst. Parallel zur Wiederaufnahme der Versuche wird an der Umsetzung der mittel- bis langfristigen Massnahmen gearbeitet. Damit wird den Kantonen ermöglicht, die Versuche zeitnah wieder aufzunehmen. Mit der Weiterführung der Versuche in einzelnen Kantonen wird verhindert, dass die vorhandenen Ressourcen und Know-how sowie bereits getätigte Investitionen bei den Kantonen und bei der Post als Systemanbieterin verloren gehen. Es erlaubt ausserdem allen beteiligten Akteuren, wertvolle Erfahrungen mit dem Einsatz von vollständig verifizierbaren Systemen zu sammeln. Der Versuchscharakter wird mit verschiedenen Massnahmen wie etwa der Beibehaltung der Limitierung des Elektorats unterstrichen. Dabei wird weiterhin nach dem Prinzip «Sicherheit vor Tempo» gehandelt. In einer zweiten Etappe wird an der Umsetzung der mittel- bis langfristigen Massnahmen gearbeitet.

Die Gewährleistung der Sicherheit der eingesetzten Systeme hat oberste Priorität. Die Massnahmen zur Neuausrichtung sehen eine Präzisierung der Sicherheitsanforderungen, eine wirksamere Kontrolle und Aufsicht unter Einbezug der Wissenschaft sowie eine Verbesserung des Risikomanagements vor. Zusätzlich wollen Bund und Kantone das Vertrauen in die elektronische Stimmabgabe stärken, indem sie vermehrt Transparenz schaffen und eine verstärkte Zusammenarbeit mit der Öffentlichkeit und der Wissenschaft suchen. Die bestehende Community von Fachpersonen im Bereich E-Voting soll vergrössert werden. Der Wissenschaft wird dabei eine wichtige Rolle beigemessen. Bei der Erarbeitung der Grundlagen, der Begleitung der Versuche und insbesondere der Überprüfung der Systeme sollen vermehrt unabhängige Expertinnen und Experten einbezogen werden. Zusätzlich wird die Möglichkeit von öffentlichen Überprüfungen gestärkt. Die Informationen zum eingesetzten System (insbesondere Dokumentation und Quellcode) werden veröffentlicht und so die für eine Überprüfung notwendigen Unterlagen öffentlich zugänglich gemacht. Prüfberichte und die Ergebnisse des E-Voting-Stimmkanals werden veröffentlicht. Dadurch sollen sich Stimmberechtigte sowie Expertinnen und Experten ein eigenes Bild machen und jederzeit Rückmeldungen bei den Behörden einbringen können. Diese Rückmeldungen sollen der Weiterentwicklung und der laufenden Verbesserung von E-Voting dienen.

Um das Vertrauen in den elektronischen Stimmkanal zu fördern, kommt einer transparenten Kommunikation gegenüber der Öffentlichkeit eine wichtige Rolle zu. Bund und Kantone müssen die Öffentlichkeit über Sicherheitsthemen informieren. Dies ist bei technisch komplexen Themen wie E-Voting eine wichtige Aufgabe. Bund und Kantone wollen die Kommunikation und Information der Öffentlichkeit daher verstärken und entsprechende Massnahmen umsetzen.

Es ist zentral, dass die Ausgangslage für den Einsatz der elektronischen Stimmabgabe laufend und im Licht der aktuellen Entwicklungen beurteilt wird. Mit der Umsetzung diverser Massnahmen und der Anpassung der Rechtsgrundlagen soll die Weiterführung des Versuchsbetriebs von E-Voting ermöglicht werden. Laufende Weiterentwicklungen und kontinuierliche Verbesserungen sind wichtige Aspekte zur Gewährleistung der Sicherheit und der Vertrauenswürdigkeit von E-Voting. Um diese Weiterentwicklungen und kontinuierlichen Verbesserungen zu ermöglichen, muss die Finanzierung langfristig sichergestellt werden. Mit den heute vorgesehenen Mitteln bei Bund und Kantonen ist dies nicht möglich. Bund und Kantone sollen deshalb die Erschliessung neuer Finanzierungsmöglichkeiten prüfen.

Anhang: Massnahmenkatalog

Nr.	Massnahme	Beschreibung	Zeitpunkt Umsetzung	Zuständigkeit	Kostenschätzung ²⁴ <i>Tief (<50'000 CHF)</i> <i>Mittel (50'000 - 500'000 CHF)</i> <i>Hoch (500'000 - 1 Mio. CHF)</i> <i>Sehr hoch (> 1 Mio. CHF)</i>
A. Weiterentwicklung der Systeme					
A.1	Präzisierung der Kriterien für die Qualität des Quellcodes und der Dokumentation	Die bestehenden Qualitätskriterien, die der Quellcode und seine Dokumentation erfüllen müssen, werden präzisiert. Mit klaren Kriterien soll eine hohe Qualität der E-Voting-Systeme sichergestellt werden. Ausserdem sollen die Prüfungen aller Akteure sowie der Öffentlichkeit erleichtert werden. Der Qualitätssicherungsprozess bei der Softwareentwicklung soll sich ebenfalls auf diese Kriterien abstützen.	Wiedereinsatz	Anforderungen: BK Umsetzung: Kantone, Systemanbieter	Bund: keine Kantone: keine
A.2	Stärkung der Qualitätssicherung im Entwicklungsprozess von E-Voting-Systemen	Die Anforderungen im Bereich der Qualitätssicherung im Entwicklungsprozess von E-Voting-Systemen werden präzisiert. Damit sollen folgende Ziele erreicht werden: <ul style="list-style-type: none"> - Nachvollziehbarkeit und Kontrolle von Anpassungen - Laufende Nachvollziehbarkeit in beide Richtungen zwischen den einzelnen Elementen der Dokumentation (Protokoll, Spezifikation, Architektur, etc.) und dem Quellcode - Ergebnisse von Prüfprozessen in die Entwicklung einfliessen lassen - Konformität mit den rechtlichen Anforderungen während des gesamten Lebenszyklus sicherstellen und aufrechterhalten 	Wiedereinsatz	Anforderungen: BK Umsetzung: Kantone, Systemanbieter	Bund: keine Kantone: keine
A.3	Anwendung einer bewährten und nachvollziehbaren Build- und Deployment-Methode	Die Anforderungen an den Systemanbieter werden ergänzt, damit eine nachvollziehbare Methode zur Bereitstellung des Systems aus dem Quellcode bis zu seiner Installation in der Produktion (Build- und Deployment) angewendet wird. Damit sollen folgende Ziele erreicht werden: <ul style="list-style-type: none"> - Die Build- und Deployment-Methode erlaubt es, sicherzustellen, dass die eingesetzte Software mit der publizierten, geprüften und zugelassenen Version übereinstimmt. - Zusätzlich zu dieser Nachvollziehbarkeit soll die Build- und Deployment-Methode Manipulationen der Systembestandteile so weit als möglich verhindern. - Es muss verhindert werden, dass mit den eingesetzten Entwicklungsinstrumenten und Bibliotheken für die Software relevante 	Wiedereinsatz	Anforderungen: BK Umsetzung: Kantone, Systemanbieter	Bund: keine Kantone: tief

²⁴ Ausgewiesen werden Schätzungen von zusätzlich anfallenden Kosten (externe Kosten oder zusätzliche Ressourcen) von Bund und Kantonen. Beim Systemanbieter anfallende Kosten werden in den Kosten der Kantone ausgewiesen, sofern diese weiterverrechnet werden.

Nr.	Massnahme	Beschreibung	Zeitpunkt Umsetzung	Zuständigkeit	Kostenschätzung ²⁴ <i>Tief (<50'000 CHF)</i> <i>Mittel (50'000 - 500'000 CHF)</i> <i>Hoch (500'000 - 1 Mio. CHF)</i> <i>Sehr hoch (> 1 Mio. CHF)</i>
		Schwachstellen eingeführt werden, die das System angreifbar machen würden. Für den Umgang mit Nicht-Konformitäten wird ein Prozess erarbeitet (s. Massnahme B.3).			
A.4	Einsatz von herstellerunabhängigen Komponenten (Verifier / Kontrollkomponenten)	<p>Die BK und die Kantone vertiefen die Grundlagen im Bereich der herstellerunabhängigen Komponenten. Priorität hat die Erarbeitung der Grundlagen im Bereich der herstellerunabhängigen Kontrollkomponente, die bei der Erzeugung von Prüfcodes zum Einsatz kommt und die Stimmen bis zur Auszählung aufbewahrt (Online-Kontrollkomponente).</p> <p>Der SA VE beabsichtigt, herstellerunabhängige Online-Kontrollkomponenten in einem Zeithorizont von rund fünf Jahren nach dem Wiedereinsatz einzusetzen. Diese Absichtserklärung erfolgt vorbehaltlich der Sicherstellung der Finanzierung. Zur Lastenteilung braucht es eine kritische Masse an aktiven Kantonen. Insbesondere müssen sich eine genügende Anzahl Kantone bereit erklären, die von den Kantonen zu tragenden Kosten zu finanzieren. Ebenso gilt der Vorbehalt, dass keine heute unbekanntem erheblichen Gründe später gegen eine Umsetzung sprechen. In einem ersten Schritt wird eine Studie mit Blick auf die mögliche Ausgestaltung und Zuständigkeiten bei der Auftragsvergabe, bei der Wartung, beim Betrieb sowie zur Behandlung allfälliger technischer Fragestellungen durchgeführt. Dabei sind insbesondere die Auswirkungen auf die betrieblichen Abläufe bei den Kantonen und die Kosten der Umsetzung aufzuzeigen. Zusätzlich soll in der Studie eine mögliche, konkrete Planung für die Umsetzung aufgezeigt werden (nach einer ersten Einschätzung der Kantone ist mit einem Zeithorizont von mindestens drei bis fünf Jahren für die Umsetzung zu rechnen). Die Studie soll Grundlage für den Umsetzungsentscheid sein. Die Kantone übernehmen die Federführung für die Erarbeitung der Studie.</p> <p>Nach Abschluss der Studie unterbreiten die BK und die Kantone dem SA VE einen Antrag für das weitere Vorgehen.</p>	<p>Studie und Antrag Online-Kontrollkomponenten an SA VE: bis 2 Jahre nach Wiedereinsatz</p> <p>Umsetzung unter Vorbehalt: rund 5 Jahre nach Wiedereinsatz</p>	Studie Online-Kontrollkomponenten: Kantone unter Einbezug BK	<p><u>Studie Online-Kontrollkomponenten</u></p> <p>Bund: keine Kantone: tief bis mittel</p> <p><u>Schätzung für mögliche Umsetzung nach Studie</u></p> <p>Bund: Mitfinanzierung ist zu prüfen Kantone: sehr hoch</p> <p>Kontrollkomponenten:</p> <ul style="list-style-type: none"> - Einmalig: 1.8-2.2 Mio. CHF - Wiederkehrend: 600'000-800'000 CHF / Jahr <p>Verifier:</p> <ul style="list-style-type: none"> - Einmalig: 0.9-1 Mio. CHF - Wiederkehrend: 200'000 CHF / Jahr
A.5	Abschwächung der Vertrauensannahmen beim Druckprozess und in die Software, die kryptografische Parameter generiert	Die zulässigen Vertrauensannahmen beim Druckprozess und in die Software, die kryptografische Parameter generiert, sollen abgeschwächt werden. Mit herstellerunabhängiger Software soll festgestellt werden können, dass kryptografische Parameter und insbesondere die Prüfcodes zufällig erzeugt wurden. Zur Erreichung der gewünschten Entropie müssen für die Erzeugung privater Werte mindestens vier Kontrollkomponenten zum Einsatz kommen. Stichprobeweise sollen	Vertiefung und Anpassung kryptografisches Protokoll: 1 Jahr nach Wiedereinsatz	<p>Klärung offene Fragen für Anforderungen: BK</p> <p>Umsetzung: Kantone</p>	<p><u>Vertiefung und Anpassung kryptografisches Protokoll</u></p> <p>Bund: tief; Mitfinanzierung ist zu prüfen Kantone: hoch</p> <p>Anpassung kryptografisches Protokoll: 850'000 bis 1 Mio. CHF</p>

Nr.	Massnahme	Beschreibung	Zeitpunkt Umsetzung	Zuständigkeit	Kostenschätzung ²⁴ Tief (<50'000 CHF) Mittel (50'000 - 500'000 CHF) Hoch (500'000 - 1 Mio. CHF) Sehr hoch (> 1 Mio. CHF)
		<p>zufällig ausgewählte Stimmrechtsausweise dahingehend geprüft werden, ob die Werte korrekt im Sinn der überprüften Werte gedruckt wurden.</p> <p>Der SA VE beabsichtigt, die Parametergenerierung sowie den Druckprozess in einem Zeithorizont von rund vier Jahren nach dem Wiedereinsatz anzupassen. Diese Absichtserklärung erfolgt vorbehaltlich der Sicherstellung der Finanzierung. Zur Lastenteilung braucht es eine kritische Masse an aktiven Kantonen. Insbesondere müssen sich eine genügende Anzahl Kantone bereit erklären, die von den Kantonen zu tragenden Kosten zu finanzieren. Ebenso gilt der Vorbehalt, dass keine heute unbekanntem erheblichen Gründe später gegen eine Umsetzung sprechen.</p> <p>In einer ersten Etappe vertiefen die BK und die Kantone das Lösungskonzept; die Kantone werden das kryptografische Protokoll anpassen lassen. In Zusammenarbeit mit der Post definieren sie die Prozesse der Kantone. Eine erste Einschätzung zum Zeithorizont ergab, dass eine Umsetzung (inkl. Anpassung kryptografisches Protokoll) sicher drei Jahre dauern dürfte. Die Planung der Umsetzung soll im Rahmen der ersten Etappe weiter vertieft werden.</p> <p>Nach Abschluss der Vertiefungsarbeiten unterbreiten die BK und die Kantone dem SA VE einen detaillierten Antrag zur Umsetzung.</p>	<p>Antrag an SA VE: bis 2 Jahre nach Wiedereinsatz</p> <p>Umsetzung unter Vorbehalt: rund 4 Jahre nach Wiedereinsatz</p>		<p><u>Schätzung für mögliche Umsetzung nach Vertiefung</u></p> <p>Bund: Mitfinanzierung ist zu prüfen Kantone: hoch</p> <p>– Einmalig: 700'000-900'000 CHF – Wiederkehrend: 100'000 CHF / Jahr</p>
A.6	Vertiefung der Grundlagen für einen zusätzlichen Verifizierungsmechanismus, dessen Wirksamkeit nicht auf den heute geltenden Vertrauensannahmen basiert	<p>Die Möglichkeiten eines zusätzlichen Mechanismus für die Verifizierbarkeit werden vertieft. Dabei soll geprüft werden, ob und wie den Stimmberechtigten ein zusätzliches Instrument zu den vom Hersteller zur Verfügung gestellten Instrumenten für die Verifizierbarkeit angeboten werden kann. Ein solcher Mechanismus könnte beispielsweise in Form eines öffentlichen Anschlagbretts (sog. «Public Bulletin Board») eingeführt werden. Mit einem Public Bulletin Board könnten die Stimm-daten unter Wahrung des Stimmgeheimnisses veröffentlicht werden und die Stimmberechtigten könnten mithilfe eines Zweitgeräts (z.B. eines Mobiltelefons) feststellen, ob ihre Stimme korrekt bei einer oder mehreren vom Hersteller unabhängigen Instanzen angekommen ist. Damit würde die Wirksamkeit der individuellen Verifizierbarkeit nicht von der Vertrauenswürdigkeit der Druckerei oder der Kontrollkomponenten abhängen. Im Rahmen der Überprüfung im Sinne der universellen Verifizierbarkeit könnten die Kantone feststellen, ob alle bei den unabhängigen Instanzen eingegangenen Stimmen bei der Auszählung mitberücksichtigt wurden.</p>	<p>Studie: 1 Jahr nach Wiedereinsatz</p> <p>Antrag an SA VE: bis 2 Jahre nach Wiedereinsatz</p>	Studie: BK unter Einbezug der Kantone	<p><u>Studie</u></p> <p>Bund: mittel Kantone: keine</p> <p><u>Schätzung für mögliche Umsetzung nach Vertiefung</u></p> <p>Hoch. Die Zuständigkeit für die Finanzierung ist noch zu klären.</p> <p>– Einmalig: 600'000 CHF – Wiederkehrend: 200'000 CHF / Jahr</p>

Nr.	Massnahme	Beschreibung	Zeitpunkt Umsetzung	Zuständigkeit	Kostenschätzung ²⁴ Tief (<50'000 CHF) Mittel (50'000 - 500'000 CHF) Hoch (500'000 - 1 Mio. CHF) Sehr hoch (> 1 Mio. CHF)
		<p>In einem ersten Schritt wird eine Studie erarbeitet, um den Nutzen eines zusätzlichen Mechanismus sowie die Form einer allfälligen Umsetzung zu vertiefen. Die Studie soll Fragen rund um die technische Umsetzung und, unter Einbezug von Stimmberechtigten, zur Vertrauensbildung und Akzeptanz behandeln.</p> <p>Nach Abschluss der Vertiefungsarbeiten unterbreiten die BK und die Kantone dem SA VE einen Antrag, ob und wie ein Public Bulletin Board umgesetzt werden soll. Mit Blick auf eine allfällige Umsetzung ist die Finanzierung sicherzustellen.</p>			
A.7	Verbesserung der Grundlagen zur Erkennung (Monitoring) und Untersuchung (IT-Forensik) von Vorfällen	<p>E-Voting-Systeme müssen eine wirksame Erkennung und Untersuchung von Vorfällen – wie beispielsweise vermutete Manipulationen von Stimmen oder Angriffe auf das System – ermöglichen. Für die Wiederaufnahme der Versuche werden die bestehenden Anforderungen an die Sammlung von Belegen wie folgt präzisiert: Für die Erkennung und Untersuchung von Vorfällen sind konsistente Protokolle über alle Elemente des Systems anzufertigen. Diese Protokolle müssen so erfasst, übertragen und gespeichert werden, dass sie nicht manipuliert werden können. Der Inhalt und Umfang der Protokolle ist so zu definieren, dass eine wirksame Untersuchung von Vorfällen durchgeführt werden kann. Dabei ist das Stimmgeheimnis zu gewährleisten.</p> <p>In einem zweiten Schritt wird ein kontinuierlicher Verbesserungsprozess zur Erkennung und Untersuchung von Vorfällen definiert und ab der Wiederaufnahme umgesetzt. Dabei sollen insbesondere die folgenden Aspekte berücksichtigt werden:</p> <ul style="list-style-type: none"> – Offener Austausch zwischen Bund, Kantonen und Systemanbieter. – Regelmässige Analyse der Zweckmässigkeit der Monitoring- und Untersuchungsgrundlagen. Die in der Krisenvereinbarung definierten Szenarien werden bei diesen Analysen berücksichtigt. – Bei der Verbesserung der Instrumente und Prozesse werden die aus der Analyse resultierenden Elemente berücksichtigt. 	Definition Anforderungen und Verbesserungsprozess: Wiedereinsatz	Anforderungen: BK Verbesserungsprozess: Systemanbieter, Kantone	Bund: keine Kantone: keine; für die Umsetzung von Massnahmen aus dem kontinuierlichen Verbesserungsprozess werden Kosten in unbekannter Höhe anfallen
A.8	Schaffung eines gemeinsamen Massnahmenplans von Bund und Kantonen	Bund und Kantone führen zukünftig einen gemeinsamen Massnahmenplan. Der Massnahmenplan bildet die Entscheidungen zur Neuausrichtung des Versuchsbetriebs ab und zeigt auf, welche Massnahmen bereits für den Wiedereinsatz umgesetzt werden und mit welchen Massnahmen E-Voting mittel- bis längerfristig weiterentwickelt werden soll. Wo immer möglich, sind Zeithorizonte für die Umsetzung der Mas-	Wiedereinsatz	BK / Kantone	Bund: keine Kantone: keine

Nr.	Massnahme	Beschreibung	Zeitpunkt Umsetzung	Zuständigkeit	Kostenschätzung ²⁴ Tief (<50'000 CHF) Mittel (50'000 - 500'000 CHF) Hoch (500'000 - 1 Mio. CHF) Sehr hoch (> 1 Mio. CHF)
		nahmen bzw. der geplanten ersten Etappen anzugeben. Der Massnahmenplan wird als Absichtserklärung des SA VE verabschiedet und publiziert. Er wird regelmässig überprüft, um die Sicherheit unter Berücksichtigung neuester Entwicklungen sicherzustellen.			

B. Wirksame Kontrolle und Aufsicht					
B.1	Anpassung der Zuständigkeiten bei den Konformitätsprüfungen des Systems und der zugrundeliegenden Prozessen	<p>Die Zuständigkeiten bei der Prüfung der Systeme werden überarbeitet. Damit wird die Wirksamkeit und Glaubwürdigkeit der Prüfung sichergestellt. Die Unabhängigkeit zwischen der Prüfstelle und der geprüften Stelle spielt hierbei eine wichtige Rolle.</p> <p>Die Aufgabenteilung zwischen Bund und Kantonen wird so angepasst, dass der Bund mehr Verantwortung und eine direktere Rolle bei der Prüfung der Systeme übernimmt:</p> <ul style="list-style-type: none"> - Der Bund ist neu für Prüfungen der Erfüllung der Anforderungen in Bezug auf das System und die zugrundeliegenden Prozesse zuständig (gemäss Ziff. 5.1, 5.2, 5.3 in Teilen, 5.4, 5.5 und 5.6 Anhang der VELeS) - Der Systemanbieter ist zukünftig nur noch für Prüfungen in Bezug auf den Betrieb des Systems in seinen Rechenzentren zuständig (Zertifikation ISO 27001 gemäss Ziff. 5.3 Anhang der VELeS) <p>Für die Überprüfungen sind unabhängige Expertinnen und Experten zu mandatieren.</p>	Wiedereinsatz	BK	Bund: hoch Kantone: keine (keine Kosteneinsparungen)
B.2	Erarbeitung eines Prüfkonzepts für die Beurteilung der Konformität des Systems und der zugrundeliegenden Prozesse	<p>Basierend auf den angepassten Zuständigkeiten bei der Überprüfung des Systems und der Prozesse gemäss Massnahme B.1 wird ein Prüfkonzept erstellt. Das Prüfkonzept wird so ausgestaltet, dass eine umfassende Prüfung der Sicherheitsanforderungen gewährleistet wird. Die Zuständigkeit liegt bei der BK. Die BK kann dazu externe Expertinnen und Experten beiziehen.</p> <p>Das Konzept soll u.a. die folgenden Aspekte vorsehen:</p> <ul style="list-style-type: none"> - Klare Definition der Prüftiefe der verschiedenen Bereiche in Bezug auf deren Geltungsbereich und Gültigkeitsdauer - Durchlässigkeit zwischen den verschiedenen Prüfbereichen, um eine konsistente und lückenlose Überprüfung sicherzustellen - Mandatierung von qualifizierten und unabhängigen Expertinnen und Experten - Publikation der Prüfberichte 	Wiedereinsatz	BK in Zusammenarbeit mit Kantonen und Systemanbieter	Bund: tief Kantone: keine

Nr.	Massnahme	Beschreibung	Zeitpunkt Umsetzung	Zuständigkeit	Kostenschätzung ²⁴ Tief (<50'000 CHF) Mittel (50'000 - 500'000 CHF) Hoch (500'000 - 1 Mio. CHF) Sehr hoch (> 1 Mio. CHF)
B.3	Erarbeitung und Umsetzung eines Prozesses zum Umgang mit Nicht-Konformitäten	<p>Die BK erarbeitet in Zusammenarbeit mit den Kantonen und dem Systemanbieter einen Prozess zum Umgang mit erwiesenen und vermuteten Nicht-Konformitäten. Ziel ist es, im Umgang mit Nicht-Konformitäten Unklarheiten so weit als möglich zu vermeiden und einen Einsatz von E-Voting sicherzustellen, bei dem die Anforderungen der VELeS erfüllt werden.</p> <p>In diesem Prozess werden folgende Aspekte definiert:</p> <ul style="list-style-type: none"> - Arten von Nicht-Konformitäten - Kriterien, die im Umgang mit Nicht-Konformitäten angewendet werden - Regelung der Akteure und deren Rollen 	Wiedereinsatz	BK in Zusammenarbeit mit Kantonen und Systemanbietern	Bund: tief Kantone: keine
B.4	Erneuerung und Verbesserung des Leitfadens für die Risikobeurteilungen	<p>Die BK erneuert in Zusammenarbeit mit den Kantonen, den Systemanbietern sowie IT-Sicherheitsexpertinnen und -experten den Leitfaden, der als Grundlage für die Risikobeurteilungen gemäss Massnahme B.5 dienen soll. Der Leitfaden umfasst insbesondere die folgenden Aspekte:</p> <ul style="list-style-type: none"> - Katalog der Informationsressourcen (information assets) - Katalog von Bedrohungen (basierend auf der Liste der Bedrohungen im Anhang der VELeS) - Katalog der Massnahmen zur Risikominimierung - Zuständigkeiten in Bezug auf den Schutz der information assets <p>Im Leitfaden sollen u.a. die Länge der Schlüssel zur Verschlüsselung, die mehrfache Abgabe von Stimmen über verschiedene Stimmkanäle, der Stimmenkauf, «long term privacy» und die Abhängigkeit von einem einzigen Anbieter berücksichtigt werden.</p> <p>Der Leitfaden wird publiziert, um die Transparenz und Vertrauensbildung zu stärken. Zudem erhält die Öffentlichkeit so die Möglichkeit, Feedback zu geben. Der Leitfaden ist periodisch zu überprüfen und gegebenenfalls anzupassen.</p>	Wiedereinsatz	BK in Zusammenarbeit mit Kantonen und Systemanbietern	Bund: tief Kantone: keine
B.5	Erarbeitung und Umsetzung eines neuen Vorgehens für die Risikobeurteilungen für vollständig verifizierbare Systeme	<p>Die Risikobeurteilung erfolgt neu von jedem Akteur (BK, Kantone, Systemanbieter) für seinen Zuständigkeitsbereich. Die Risikobeurteilungen richten sich nach dem Leitfaden unter Massnahme B.4. Sie werden mindestens jährlich sowie bei wesentlichen Änderungen des Systems und spezifisch vor jedem Urnengang überprüft und nötigenfalls angepasst. Können risikominimierende Massnahmen nicht unmittelbar umgesetzt werden, sind sie in den Massnahmenplan (Massnahme A.8)</p>	Wiedereinsatz	BK, Kantone, Systemanbieter	Bund: tief Kantone: tief

Nr.	Massnahme	Beschreibung	Zeitpunkt Umsetzung	Zuständigkeit	Kostenschätzung ²⁴ <i>Tief (<50'000 CHF)</i> <i>Mittel (50'000 - 500'000 CHF)</i> <i>Hoch (500'000 - 1 Mio. CHF)</i> <i>Sehr hoch (> 1 Mio. CHF)</i>
		aufzunehmen. Unabhängige Fachpersonen werden für die Beurteilung der Risiken beigezogen.			
B.6	Erneuerung des Krisenmanagements mit Durchführung von Krisenübungen	<p>Um Entwicklungen im Bereich E-Voting Rechnung zu tragen und die Wirksamkeit des Krisenmanagements zu verbessern, ist eine neue Krisenvereinbarung auszuarbeiten. Die neue Krisenvereinbarung soll in Form einer Rahmenvereinbarung die folgenden Eigenschaften aufweisen:</p> <ul style="list-style-type: none"> - Trilaterale Vereinbarung, Abschluss zwischen der BK, den Anwerdorkantonen und dem Systemanbieter - Festlegen der Prozesse im Krisenmanagement und der beteiligten Akteure - Festlegen des Kommunikationsprozesses zwischen den beteiligten Akteuren sowie der Prozesse zur Koordination der Kommunikation gegen aussen - Durchführung von Übungen zur Verbesserung des Krisenmanagements - Dabei sind die Krisenszenarien an die neuen Risikobeurteilungen für vollständig verifizierbare Systeme anzupassen. Bestehende Strukturen bei Bund, Kantonen und Systemanbietern werden bei der Ausgestaltung des Krisenmanagements so weit als möglich beibehalten. 	Wiedereinsatz	BK (Federführung), Kantone und Systemanbieter	Bund: tief Kantone: keine
B.7	Integration von E-Voting als Teil der kritischen Infrastruktur des Bundes	Die kritischen Infrastrukturen im Sinne der Nationalen Strategie zum Schutz kritischer Infrastrukturen erhalten eine erhöhte Unterstützung von MELANI und GovCERT. Diese Unterstützung wäre bei der Analyse von Bedrohungen und der Untersuchung von Vorfällen wertvoll. Mit dieser Massnahme soll die Zusammenarbeit zwischen der BK, den Kantonen, dem Systemanbieter und GovCERT / MELANI im Bereich E-Voting festgelegt werden, um einen priorisierten Zugang für den Umgang mit Vorfällen zu gewährleisten. Diese Zusammenarbeit soll auch im Krisenmanagement berücksichtigt werden.	Wiedereinsatz	BK (Federführung), Kantone und Systemanbieter	Bund: keine Kantone: keine
B.8	Weiterentwicklung der Plausibilisierung der E-Voting-Ergebnisse	Die Kantone plausibilisieren die Ergebnisse aus dem E-Voting-System unterschiedlich. Es soll ein vermehrter Austausch unter den Kantonen und mit der BK stattfinden, damit Erfahrungen und Lösungsansätze im Sinne von «best practice» diskutiert werden können. Ausserdem wird geprüft, ob und in welcher Form eine standardisierte statistische Methode ausgearbeitet werden kann. Mit der Einführung eines standardisierten Verfahrens bestünde ein weiteres Instrument, um Hinweise auf	Wiedereinsatz: Erster Austausch Prüfung standardisierte Methode: bis 2022	Kantone	Bund: keine Kantone: tief

Nr.	Massnahme	Beschreibung	Zeitpunkt Umsetzung	Zuständigkeit	Kostenschätzung ²⁴ <i>Tief (<50'000 CHF)</i> <i>Mittel (50'000 - 500'000 CHF)</i> <i>Hoch (500'000 - 1 Mio. CHF)</i> <i>Sehr hoch (> 1 Mio. CHF)</i>
		allfällige Fehlfunktionen oder Manipulationen zu erhalten. Die Methode muss auf die spezifischen Gegebenheiten jedes einzelnen Kantons anwendbar sein. Es ist ausserdem zu prüfen, welche Informationen in Bezug auf die Plausibilisierungsarbeiten in Zukunft publiziert werden können.			
B.9	Anpassungen des Bewilligungsverfahrens	Die Umsetzung verschiedener Massnahmen für die Wiederaufnahme der Versuche macht eine Anpassung der Abläufe im Bewilligungsverfahren notwendig. Dazu gehören insbesondere die Massnahmen zur Neuregelung der Zuständigkeiten bei den unabhängigen Überprüfungen (Massnahme B.1) sowie die Anpassung der Anforderungen im Bereich der Transparenzmassnahmen (Massnahmen C.2 und C.3). Ausserdem sind der Einbezug unabhängiger Expertinnen und Experten im Bewilligungsverfahren und das kontinuierliche Risikomanagement zu berücksichtigen. Die Anforderungskataloge der BK für das Bewilligungsverfahren werden überarbeitet. Ausserdem prüft die BK, inwiefern der Grundbewilligungsentscheid des Bundesrates in einen systembezogenen und einen kantonsspezifischen Teil aufgeteilt werden kann.	Wiedereinsatz	BK unter Einbezug der Kantone	Bund: keine Kantone: keine
B.10	Langfristige Überprüfung der Prozesse, Rollen und Aufgaben	Die Zuständigkeiten, Rollen und Aufgaben von Bund, Kantonen und Systemanbietern haben einen direkten Einfluss auf die (sicherheitsrelevante) Ausgestaltung der E-Voting Systeme. Diese werden überprüft und in einer langfristigen Strategie festgehalten. Bund und Kantone können Massnahmen erarbeiten, die der veränderten Ausgangslage bezüglich der Anzahl der Systemanbieter, der Gouvernanz und dem Finanzierungsbedarf der elektronischen Stimmabgabe Rechnung tragen.	Langfristig	AG Zukunft VE	Bund: keine Kantone: keine

C. Stärkung der Transparenz und des Vertrauens

C.1	Begrenzung des zulässigen Elektorats für vollständig verifizierbare Systeme	Im Versuchsbetrieb wird das zulässige Elektorat beim Einsatz von vollständig verifizierbaren Systemen limitiert. Die Limiten betragen 30 % des kantonalen und 10 % des nationalen Elektorats. Auslandschweizer Stimmberechtigte werden bei der Berechnung der Limiten nicht eingerechnet. Die Anhebung oder gegebenenfalls Aufhebung der Limiten wird geprüft, wenn sich die vollständig verifizierbaren Systeme dereinst in einem stabilen Versuchsbetrieb bewährt haben.	Wiedereinsatz	BK	Bund: keine Kantone: individuell, je nach Art der Steuerung des Elektorats (z.B. kann die Einführung eines Anmeldeverfahrens Kosten im mittleren Bereich mit sich bringen)
------------	---	--	---------------	----	---

Nr.	Massnahme	Beschreibung	Zeitpunkt Umsetzung	Zuständigkeit	Kostenschätzung ²⁴ Tief (<50'000 CHF) Mittel (50'000 - 500'000 CHF) Hoch (500'000 - 1 Mio. CHF) Sehr hoch (> 1 Mio. CHF)
C.2	Präzisierung der Anforderungen an die Offenlegung des Quellcodes	<p>Die bestehenden Anforderungen an die Offenlegung des Quellcodes werden präzisiert.</p> <p>Anforderungen an die Unterlagen:</p> <ul style="list-style-type: none"> - Quellcode und Dokumentation der Software sowie Dateien mit relevanten Inputparametern sind offenzulegen. - Hilfestellungen und ergänzende Dokumentationen sind zu publizieren, so dass fachkundige Personen das System in der eigenen Infrastruktur effizient kompilieren, in Betrieb nehmen und analysieren können. - Dokumentationen zur Infrastruktur, Drittsoftware und Betriebsprozesse sind so weit als möglich zu publizieren. - Die Darstellung der offengelegten Unterlagen entspricht der gängigen Praxis. <p>Anforderungen an die Nutzungsbedingungen:</p> <ul style="list-style-type: none"> - Der Zugang zum Quellcode wird unentgeltlich und anonym gewährt. - Der Quellcode darf für ideelle und namentlich wissenschaftliche Zwecke genutzt werden. Dazu gehört der Austausch bei der Fehlersuche sowie das Recht zu publizieren. Dieses Recht wird vom Eigner explizit eingeräumt. - Wer die Nutzungsbedingungen einhält, wird rechtlich nicht verfolgt. Ein Verstoß gegen die Nutzungsbedingungen wird nur verfolgt, wenn der Quellcode oder Teile davon kommerziell verwendet oder produktiv eingesetzt werden. In den Nutzungsbedingungen wird auf diese Haftungsbeschränkung hingewiesen. - Es reicht, in den Lizenzbestimmungen auf die Nutzungsbedingungen hinzuweisen, auf Willenserklärungen der Nutzenden ist, wenn möglich, zu verzichten. <p>Der SA VE spricht sich dafür aus, dass künftige Systeme und Systembestandteile unter einer Open-Source-Lizenz (OSL) publiziert werden. Ausserdem wird mit der Post als heutige Systemanbieterin geprüft, ob bereits entwickelte Komponenten des Quellcodes ihres vollständig verifizierbaren Systems zusätzlich unter eine OSL gestellt werden können.</p>	Wiedereinsatz	Anforderungen: BK Offenlegung: Kantone, Systemanbieter	Bund: keine Kantone: keine
C.3	Führen eines Bug-Bounty-Programms	Zum offengelegten Quellcode und der Dokumentation von E-Voting-Systemen wird ein Bug-Bounty-Programm geführt. Dieses soll u.a. folgende Anforderungen erfüllen:	Wiedereinsatz	Anforderungen: BK	Bund: Mitfinanzierung ist zu prüfen Kantone: hoch

Nr.	Massnahme	Beschreibung	Zeitpunkt Umsetzung	Zuständigkeit	Kostenschätzung ²⁴ <i>Tief (<50'000 CHF)</i> <i>Mittel (50'000 - 500'000 CHF)</i> <i>Hoch (500'000 - 1 Mio. CHF)</i> <i>Sehr hoch (> 1 Mio. CHF)</i>
		<ul style="list-style-type: none"> - Das Bug-Bounty-Programm läuft grundsätzlich ununterbrochen. - Die Meldung von Mängeln ist abhängig von deren Schwere finanziell zu entschädigen. Die Höhe der Entschädigung soll sich am PIT 2019 orientieren. - Das Bug-Bounty-Programm umfasst drei Bereiche: <ul style="list-style-type: none"> • Suche von Fehlern in der offengelegten Dokumentation oder dem offengelegten Quellcode (statischer Test) • Suche nach Fehlern durch Analyse des lauffähigen Systems in der eigenen Infrastruktur (dynamischer Test) • Angriffe auf die Infrastruktur des Anbieters (Internet-Test). Das Bug-Bounty-Programm muss Angriffe auf die Infrastruktur des Anbieters erlauben, DoS- und Social-Engineering-Angriffe können ausgeschlossen werden. Angriffe auf die Infrastruktur dürfen in begründeten Fällen verboten werden (z.B. während eines Urnengangs) - Zuständigkeiten und Umgang mit Meldungen: <ul style="list-style-type: none"> • Der Systemanbieter ist für das Bug-Bounty-Programm zuständig. Er ermöglicht die Durchführung, nimmt Meldungen entgegen und kategorisiert diese. Er begründet seine Entscheidungen gegenüber den betroffenen Teilnehmenden und publiziert sämtliche bestätigten Befunde. • Die BK legt die grundlegenden Rahmenbedingungen fest. • Bund und Kantone erhalten uneingeschränkten Zugriff auf die Meldungen und Antworten des Systemanbieters. Im Bewilligungsverfahren ist eine Zusammenfassung der Meldungen und der Massnahmen einzureichen, die aufgrund der Meldungen getroffen werden. - Nutzungsbedingungen: Anonyme Teilnahme und Publikationen zu Mängeln sind erlaubt, «responsible disclosure». Auf die Preisgabe der Identität darf nur für die Auszahlung einer Entschädigung im Rahmen eines Bug-Bounty-Programms bestanden werden. <p>Die BK legt die Anforderungen in Absprache mit den Kantonen fest und prüft eine allfällige finanzielle Beteiligung. Eine Eskalationsmöglichkeit für Teilnehmende, die mit der Entscheidung des Systemanbieters nicht einverstanden sind, ist ebenfalls zu prüfen.</p>		Durchführung: Kantone, Systemanbieter	<p>Umsetzung mit wiederkehrendem Internet-Test (Entschädigung nicht enthalten):</p> <ul style="list-style-type: none"> - Einmalig: 230'000-290'000 CHF - Wiederkehrend: 55'000-70'000 CHF / Jahr <p>Umsetzung mit laufendem Internet-Test (Entschädigungen nicht enthalten):</p> <ul style="list-style-type: none"> - Einmalig: 255'000-360'000 CHF - Wiederkehrend: 550'000-650'000 CHF / Jahr

Nr.	Massnahme	Beschreibung	Zeitpunkt Umsetzung	Zuständigkeit	Kostenschätzung ²⁴ <i>Tief (<50'000 CHF)</i> <i>Mittel (50'000 - 500'000 CHF)</i> <i>Hoch (500'000 - 1 Mio. CHF)</i> <i>Sehr hoch (> 1 Mio. CHF)</i>
		Für die Wiederaufnahme der Versuche soll der Internet-Test auf dem produktiven System durchgeführt werden. Anschliessend kann basierend auf den Erfahrungen über das weitere Vorgehen entschieden werden. Dabei stehen die Varianten offen, dass der Internet-Test wiederkehrend auf dem produktiven System oder als laufender Test auf einem Zwillingssystem durchgeführt wird			
C.4	Publikation bewilligungsrelevanter Prüfberichte	Bund, Kantone und Systemanbieter schaffen gegenüber der Öffentlichkeit Transparenz in Bezug auf bewilligungsrelevante Prüfergebnisse. Berichte, Belege und Zertifikate, die im Rahmen der Prüfungen gemäss Ziffer 5 des Anhangs der VELeS erstellt werden, sind zu publizieren. Die publizierten Prüfberichte müssen nachvollziehbar sein. Wird auf weitere Unterlagen verwiesen, sind diese offenzulegen. Von der Publikation kann in begründeten Fällen abgesehen werden (z.B. wenn die Publikation ein Risiko erhöht, aus Gründen des Datenschutzes, internen Sicherheitsrichtlinien, etc.). Repliken, welche die geprüfte Organisation in Bezug auf die publizierten Prüfberichte erstellt, sollen auch publiziert werden.	Wiedereinsatz	BK, Kantone, Systemanbieter	Bund: allenfalls tief Kantone: keine
C.5	Publizieren der Ergebnisse von eidgenössischen Urnengängen für E-Voting	Gegenüber der Öffentlichkeit wird Transparenz in Bezug auf E-Voting-Ergebnisse geschaffen. Die Kantone werden deshalb die Ergebnisse von eidgenössischen Wahlen und Abstimmungen für den elektronischen Stimmkanal publizieren. Dies soll der Bevölkerung erlauben, die Ergebnisse von E-Voting mit dem Gesamtergebnis zu vergleichen und eine Plausibilisierung vorzunehmen. Zur Wahrung des Stimmgeheimnisses sind Ausnahmen vorzusehen.	Wiedereinsatz	Anforderungen: BK Publikation: Kantone	Bund: keine Kantone: tief
C.6	Vermehrter Einbezug der Öffentlichkeit	Bund und Kantone erstellen in Absprache mit dem Systemanbieter ein Konzept, um einen vermehrten Einbezug der Öffentlichkeit sicherzustellen. Dabei soll neben Politik, Fachkreisen und Interessensverbänden auch ein Fokus auf die breite Öffentlichkeit gelegt werden. In diesem Konzept sind Vorhaben zur aktiven Kommunikation vorzusehen. Bis zum Wiedereinsatz ist die Umsetzung einzelner Aktivitäten zu prüfen.	Konzept: Wiedereinsatz	BK unter Einbezug Kantone und Systemanbieter	<u>Konzept</u> Bund: tief Kantone: keine <u>Umsetzung</u> je nach Aktivität; 2021 tiefe Kosten Bund

Nr.	Massnahme	Beschreibung	Zeitpunkt Umsetzung	Zuständigkeit	Kostenschätzung ²⁴ <i>Tief (<50'000 CHF)</i> <i>Mittel (50'000 - 500'000 CHF)</i> <i>Hoch (500'000 - 1 Mio. CHF)</i> <i>Sehr hoch (> 1 Mio. CHF)</i>
D. Stärkere Vernetzung mit der Wissenschaft					
D.1	Erstellung eines Konzepts für die wissenschaftliche Begleitung der Versuche und den Dialog mit externen Expertinnen und Experten	Die Versuche von E-Voting sollen laufend wissenschaftlich untersucht und begleitet werden. Darüber hinaus führen Bund und Kantone einen ständigen Dialog mit der Wissenschaft und kompetenten Fachstellen. Sie unterbreiten Fragen, reagieren auf Hinweise, beteiligen sich aktiv an den Diskussionen und sorgen für die nötige Infrastruktur sowie die Ressourcen für den Austausch. Ausserdem vergeben Bund und Kantone wissenschaftliche Studien in Bereichen, bei denen eine Vertiefung notwendig ist. Für die Ausgestaltung der wissenschaftlichen Begleitung und des Dialogs mit externen Expertinnen und Experten während der Jahre 2022-2025 sowie die Finanzierung erstellen Bund und Kantone in Zusammenarbeit mit Vertreterinnen und Vertretern der Wissenschaft ein Konzept.	Konzept: 2021	BK unter Einbezug Kantone	Bund: tief Kantone: tief
D.2	Einbezug unabhängiger Expertinnen und Experten	Bund und Kantone sollen bei ihren Arbeiten unabhängige Fachpersonen und Fachstellen der einschlägigen Fachbereiche der Wissenschaft sowie weitere Organisationen beiziehen, soweit dies sinnvoll ist und einen Mehrwert bietet, insbesondere bei den im Rahmen der Neuausrichtung definierten Massnahmen.	Im Rahmen der einzelnen Massnahmen	BK unter Einbezug Kantone	Schätzung im Rahmen der einzelnen Massnahmen
D.3	Erstellung eines Konzepts für den Aufbau eines wissenschaftlichen Ausschusses	Zur Beratung von Bund und Kantonen wird ein wissenschaftlicher Ausschuss aufgebaut. Der Ausschuss soll Beratungsaufgaben mit Blick auf die Zusammenarbeit mit der Wissenschaft (im Sinne der Massnahmen D.1 und D.2) übernehmen und einzelne Aufgaben auch selber wahrnehmen können. Dazu erstellen Bund und Kantone ein Konzept für die Jahre 2022-2025.	Konzept: 2022	BK unter Einbezug Kantone	<u>Ausarbeitung Konzept</u> Bund: keine Kantone: keine