Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK
Sektion Politische Rechte

Vote électronique

Massnahmenkatalog von Bund und Kantonen

Verabschiedet vom Steuerungsausschuss Vote électronique (SA VE): 20. Februar 2023

Inhalt

1. Ausgangslage

Im Rahmen der Neuausrichtung des Versuchsbetriebs mit E-Voting haben Bund und Kantone einen Schlussbericht mit einem umfassenden Massnahmenkatalog verabschiedet.[1] Mit der Neuausrichtung des Versuchsbetriebs soll den Kantonen die Wiederaufnahme der Versuche und ein stabiler Versuchsbetrieb mit E-Voting-Systemen der neusten Generation ermöglicht werden. Die erste Etappe der Neuausrichtung umfasste zahlreiche Massnahmen, die insbesondere mit der Revision der Rechtsgrundlagen vom Juli 2022 umgesetzt wurden. Die Revision der Rechtsgrundlagen beinhaltete eine Teilrevision der Verordnung über die politische Rechte (VPR; SR 161.11) und eine Totalrevision der Verordnung der Bundeskanzlei (BK) über die elektronische Stimmabgabe (VEleS; SR 161.116).[2]

Mit der Revision wurde die Sicherheit der E-Voting-Systeme gestärkt, indem die Sicherheits- und Qualitätsanforderungen an die Systeme, deren Einsatz und deren Entwicklung präzisiert und erhöht wurden. Neu werden nur noch vollständig verifizierbare und von unabhängigen Expertinnen und Experten im Auftrag des Bundes überprüfte Systeme zugelassen. Sie dürfen für maximal 30 % des kantonalen und 10 % des schweizweiten Elektorats eingesetzt werden. Im Kern des neu ausgerichteten Versuchsbetriebs steht die kontinuierliche Verbesserung von E-Voting-Systemen sowie deren Betriebsmodalitäten. Die Sicherheit soll laufend weiterentwickelt und gestärkt werden. In diesen kontinuierlichen Verbesserungsprozess sollen auch die Erkenntnisse aus dem praktischen Einsatz einfliessen. Dieses Prinzip wird auch im Bewilligungsverfahren berücksichtigt. Gestützt auf Artikel 16 Absatz 2 VEleS kann die BK auch E-Voting-Systeme zulassen, wenn die Kantone Ausnahmen von der Erfüllung der Anforderungen geltend machen. Solche Ausnahmen sind von den Kantonen zu begründen, allfällige alternative Massnahmen zu beschreiben und die allfällige Behebung der Nichtkonformität anzukündigen. Bei bestehendem Handlungsbedarf kann das E-Voting-System nur eingesetzt werden, wenn die Risiken beim Einsatz des E-Voting-Systems trotzdem hinreichend gering sind.

Die Schweizerische Post hat den Quellcode und die Dokumentation ihres neuen Systems mit vollständiger Verifizierbarkeit ab 2021 veröffentlicht. Das System und sein Betrieb wurden seither in verschiedenen Schritten durch unabhängige Expertinnen und Experten und die Öffentlichkeit – im Rahmen eines Bug-Bounty-Programms und eines öffentlichen Intrusionstests – überprüft und durch die Post grundlegend verbessert. Dieses System soll in den Kantonen Basel-Stadt, St.Gallen und Thurgau für die Wiederaufnahme des in der VPR vorgesehenen Versuchsbetriebs eingesetzt werden.

Insbesondere in der unabhängigen Überprüfung im Auftrag der BK wurde weiterer Handlungsbedarf identifiziert. Dieser umfasst einige Punkte, die als Nichtkonformität bezeichnet werden, sowie Punkte, in denen weitere Verbesserungen für eine effektivere Erfüllung der Anforderungen notwendig sind. Um dem bekannten Handlungsbedarf zu begegnen und notwendige Weiterentwicklungen im Bereich von E-Voting anzugehen und aufzuzeigen, führen Bund und Kantone den vorliegenden gemeinsamen Massnahmenkatalog (vgl. Massnahme A.8 in Kapitel 2.2). Der Massnahmenkatalog wird regelmässig überprüft, angepasst und publiziert. Die Umsetzung der Massnahmen wird soweit möglich zeitlich terminiert. Die Kosten, die mit der Umsetzung der Massnahmen anfallen, werden im Rahmen der gemeinsamen Finanzplanung von Bund und Kantonen analysiert und abgebildet. Zudem soll die Umsetzung der Massnahmen mit Mitteln der Digitalen Verwaltung Schweiz unterstützt werden.

[1] Vgl. Schlussbericht des Steuerungsausschusses Vote électronique (SA VE) vom 30. November 2020 zur Neuausrichtung und Wiederaufnahme der Versuche; abrufbar unter www.bk.admin.ch > Politische Rechte > E-Voting > Berichte und Studien.

[2] Medienmitteilung des Bundesrates vom 25. Mai 2022; abrufbar unter www.bk.admin.ch > Politische Rechte > E-Voting > Medienmitteilungen.

2. Massnahmenkatalog

2.1 Pendente Massnahmen

Die folgende Tabelle umfasst den Stand der pendenten Massnahmen gemäss Beschluss des SA VE vom 20. Februar 2023. Angepasste Informationen werden kursiv dargestellt.

Nr.	Massnahme	Beschreibung	Zeitpunkt Umsetzung	Zuständigkeit	Stand Umsetzung
A.	**Weiterentwicklung der Systeme**				
A.4	Einsatz von herstellerunabhängigen Komponenten (Verifier / Kontrollkomponenten)	Vgl. Beschreibung im Massnahmenkatalog des Schlussberichts des SA VE vom 30.11.2020.	Studie und Antrag Online-Kontrollkomponenten an SA VE: *2024* Umsetzung unter Vorbehalt: *2028*	Studie Online-Kontrollkomponenten: Kantone unter Einbezug BK	Geplant
A.5	Abschwächung der Vertrauensannahmen beim Druckprozess und in die Software, die kryptografische Parameter generiert	Vgl. Beschreibung im Massnahmenkatalog des Schlussberichts des SA VE vom 30.11.2020.	Vertiefung und Anpassung kryptografisches Protokoll, Festlegung Zeitplan für Umsetzung: *2023 / 2024* Antrag an SA VE: *2025* Umsetzung unter Vorbehalt: *2025 / 2026*	Klärung offene Fragen für Anforderungen: BK Umsetzung: Kantone, *Systemanbieter*	Geplant
A.6	Vertiefung der Grundlagen für einen zusätzlichen Verifizierungsmechanismus, dessen Wirksamkeit nicht auf den heute geltenden Vertrauensannahmen basiert	Vgl. Beschreibung im Massnahmenkatalog des Schlussberichts des SA VE vom 30.11.2020.	Studie: *2025* Antrag an SA VE: *2025*	Studie: BK unter Einbezug der Kantone	Geplant
A.9	Fertigstellung der Systemspezifikation im Bereich der Authentifizierung der Stimmberechtigten	Spezifikationen dienen als Anleitung für die Systementwicklung. Sie bilden zudem Grundlagen für Analysen über die Konformität des Systems mit den rechtlichen Anforderungen. Das System darf nicht unterspezifiziert sein (Ziff. 2.13.2 Anhang VEleS). Im E-Voting-System der Post[3] werden die Stimmberechtigten vor der Stimmabgabe nach Ziff. 2.8 Anhang VEleS authentifiziert, jedoch ist diese Authentifizierung nicht vollständig spezifiziert. Die Spezifikation	2. Quartal 2023 (Einsatz ab NRW 2023)	Kantone, Systemanbieter	Neu

[3] Der in diesem Massnahmenkatalog ausgewiesene Handlungsbedarf bezieht sich auf die Version des Post-Systems, die im Juni 2023 zum ersten Mal eingesetzt werden soll.

Nr.	Massnahme	Beschreibung	Zeitpunkt Umsetzung	Zuständigkeit	Stand Umsetzung
		im Bereich Authentifizierung der Stimmberechtigten wird mit der vorliegenden Massnahme fertiggestellt und in den Konformitätsbeweisen nach Ziff. 2.14 Anhang VEleS soweit sinnvoll berücksichtigt. Die spezifizierten Teile des Systems, die durchgeführten Überprüfungen des Systems sowie Erläuterungen der Post führen im konkreten Fall zum Schluss, dass die mit der unvollständigen Spezifikation verbundenen Risiken als hinreichend gering gelten dürfen. Vgl. Anhang für ergänzende Informationen zu dieser Massnahme.			
A.10	Reduktion der Abhängigkeiten von externer Software im System der Post	Die Integration externer Software in das E-Voting-System kann sinnvoll sein, namentlich auch für die Sicherheit. Dies ist insbesondere dann der Fall, wenn die Software weltweit breit zum Einsatz kommt und dabei laufend geprüft und verbessert wird. Je mehr die Software überprüft wird, desto geringer ist die Wahrscheinlichkeit, dass es Angreifern gelingen könnte, unbemerkt schädlichen Code ins System einzuschleusen. Die Post hat bereits einen Prozess implementiert, um die Risiken, die mit der Verwendung externer Software in Verbindung stehen, zu minimieren. Mit der vorliegenden Massnahme wird die Post die Abhängigkeit von externer Software weiter reduzieren, namentlich von externen Software-Bibliotheken auf dem Java-Script-Client. Externe Bibliotheken werden nur dann verwendet, wenn triftige Gründe dafürsprechen.	Laufend; Java-Script Client: 2. Quartal 2023 (Einsatz ab NRW 2023)	Kantone, Systemanbieter	Neu
A.11	Offenlegung des Quellcodes der Software zur Erzeugung der PDF-Dateien für den Druck der Stimmrechtsausweise	Die Offenlegung von Software wird in Art. 11 VEleS gefordert. Sie trägt dazu bei, allfällige Fehler oder Schwachstellen zu entdecken. In Erfüllung von Art. 11 VEleS haben die Kantone die Software, die die Rohdaten für den Druck der Stimmrechtsausweise erzeugt, bereits offengelegt. In den Rohdaten sind die Codes für die Stimmabgabe und die Prüfung durch die Stimmenden im Sinne der individuellen Verifizierbarkeit nach Ziff. 2.5 Anhang VEleS enthalten. Für die Konversion der Rohdaten zu druckfertigen PDFs verwenden die Kantone BS und TG die Software «Voting Card Printing Service (VCPS)» der Post. Diese Software ist nicht offengelegt. Die Software für die Erzeugung der PDF-Dateien für den Druck der Stimmrechtsausweise soll künftig offengelegt werden. Der Funktionsumfang, die betrieblichen Vorkehrungen sowie durchgeführte Überprüfungen des Quellcodes führen zum Schluss, dass mit dem vorläufigen Verzicht auf die Offenlegung ein hinreichend geringes Risiko einhergeht. Vgl. Anhang für ergänzende Informationen zu dieser Massnahme.	2024	Kantone, Systemanbieter	Neu

Nr.	Massnahme	Beschreibung	Zeitpunkt Umsetzung	Zuständigkeit	Stand Umsetzung
A.12	Die symbolischen Beweise über die Konformität des kryptografischen Protokolls werden weiterentwickelt	Gestützt auf symbolische Modelle werden Sicherheitsbeweise computergestützt erbracht. Solche Sicherheitsbeweise werden in Ziff. 2.14.1 Anhang VEIeS als Beleg gefordert, dass ein kryptografisches Protokoll die Anforderungen an die Verifizierbarkeit, das Stimmgeheimnis sowie die Authentifizierung erfüllt. Die Post hat ein symbolisches Modell erstellt und nutzt zur Erbringung des Beweises das Programm ProVerif. Damit ProVerif innert nützlicher Frist ein Ergebnis hervorbringen kann, ist es gebräuchlich, in symbolischen Modellen die tatsächlichen Systemeigenschaften in vereinfachter Form zu erfassen, was naturgemäss in Konflikt mit dem Aussagegehalt eines Beweises steht. Die durchgeführten Überprüfungen des Post-Systems führen zum Schluss, dass die vorliegenden Modelle von guter Qualität sind und die Beweise als Beleg über die Konformität des kryptografischen Protokolls einen substantiellen Gehalt aufweisen. Im Sinne der kontinuierlichen Verbesserung während des Versuchsbetriebs soll in einem nächsten Schritt der Gehalt der Beweise soweit sinnvoll und möglich weiter vergrössert werden. Die Modelle werden mit dem Ziel, dass sie die Systemeigenschaften möglichst realitätstreu wiedergeben, wie folgt ergänzt: - Die Authentifizierung wird soweit sinnvoll gestützt auf die Spezifikation modelliert und in den symbolischen Beweisen mitberücksichtigt (vgl. auch Massnahme A.9). - Weitere Ergänzungen werden geprüft und anschliessend entweder umgesetzt oder ein Verzicht materiell begründet (vgl. Empfehlungen 4.1 und 4.2.1 im Prüfbericht der University of Surrey vom 17.10.2022[4]). Ausserdem werden soweit sinnvoll zusätzliche Belege erbracht, dass die Modelle geeignet sind, um Nichtkonformitäten aufzudecken (vgl. Empfehlung 4.2.3 im Prüfbericht der University of Surrey vom 17.10.2022).	Authentifizierung: 2. Quartal 2023 (Einsatz ab NRW 2023) Übrige Punkte: 2025	Kantone, Systemanbieter	Neu
A.13	Verzicht auf das SGSP[5]-Problem als Sicherheitsannahme	Kryptografische Sicherheitsbeweise werden in Ziff. 2.14.1 Anhang VEleS als Beleg gefordert, dass ein kryptografisches Protokoll die Anforderungen an die Verifizierbarkeit, das Stimmgeheimnis sowie die Authentifizierung erfüllt. In der Beweisführung werden kryptografische	2025 / 2026 (gemeinsam mit Massnahme A.5)	Kantone, Systemanbieter	Neu

[4] Abrufbar unter www.bk.admin.ch > Politische Rechte > E-Voting > Überprüfung von Systemen.

[5] Subgroup Generated by Small Primes.

Nr.	Massnahme	Beschreibung	Zeitpunkt Umsetzung	Zuständigkeit	Stand Umsetzung
		Protokolle in Beziehung mit elementaren kryptografischen Problemstellungen gebracht. Wenn der Beweis korrekt geführt wird, nämlich wenn die Beziehungen korrekt erstellt werden, und wenn die Sicherheitsannahmen gelten, nämlich, dass die elementaren kryptografischen Problemstellungen «schwer zu lösen» und damit de facto unlösbar sind, darf ein Protokoll im Sinne der VEleS als sicher gelten. Ziff. 2.14.3 Anhang VEleS legt fest, dass die kryptografischen Sicherheitsbeweise unter allgemein akzeptierten Sicherheitsannahmen geführt werden dürfen. Im kryptografischen Protokoll der Post wird eine Konstruktion verwendet, die im kryptografischen Sicherheitsbeweis mit dem sogenannten SGSP-Problem in Beziehung gebracht wird. Es handelt sich dabei um eine elementare kryptografische Problemstellung, die mit dem als Sicherheitsannahme allgemein akzeptierten DDH[6]-Problem verwandt ist. Trotz der Verwandtschaft mit dem DDH-Problem gilt das SGSP-Problem als wenig erforscht. Die Post passt ihr kryptografisches Protokoll so an, dass dessen Konformität nicht von der faktischen Unlösbarkeit des SGSP-Problems abhängt. Vgl. Anhang für ergänzende Informationen zu dieser Massnahme.			
A.14	Verzicht auf den Geltungsbereich der Stimmberechtigung als zwingendes Kriterium für die Bildung von Zählkreisen	Aufgrund der technischen Ausgestaltung des Systems der Post können Stimmen von Stimmberechtigten mit unterschiedlicher Stimmberechtigung nicht untereinander gemischt und ausgezählt werden. So muss zu Bundesvorlagen die Ergebnisermittlung für Stimmen von Auslandschweizer Stimmberechtigten zwingend in einem separaten Zählkreis erfolgen, sofern sie für kantonale oder kommunale Vorlagen desselben Urnengangs nicht stimmberechtigt sind. Je mehr Stimmen untereinander gemischt und gezählt werden, desto grösser ist der Schutz des Stimmgeheimnisses. Die bundesrechtlichen Anforderungen schreiben den Kantonen keine minimale Grösse für die Zählkreise vor, dies gilt auch für die elektronische Stimmabgabe. Demnach entspricht die von der Post gewählte Lösung den bundesrechtlichen Anforderungen. Allerdings ist mit Blick auf Kantone, in denen die Stimmen der Auslandschweizer Stimmberechtigten dezentral verarbeitet werden, mehr Flexibilität bei der Bildung von Zählkreisen wünschenswert. Insbesondere sollen Gründe der technischen Ausgestaltung keine Schranken bilden.	2025 / 2026 (gemeinsam mit Massnahme A.5)	Kantone, Systemanbieter	Neu

[6] Decisional Diffie-Hellman.

Nr.	Massnahme	Beschreibung	Zeitpunkt Umsetzung	Zuständigkeit	Stand Umsetzung
		Für Vorlagen auf Bundesebene sollen die Kantone künftig die Option erhalten, die Stimmen der Auslandschweizer Stimmberechtigten gemeinsam mit den Stimmen der übrigen Stimmberechtigten derselben Gemeinde zu mischen und auszuzählen. Die Post passt ihr System dementsprechend an.			
A.15	Die Implementierung der Crypto-Primitives richtet sich verstärkt nach den Design-Prinzipien der objektorientierten Programmierung	Eine konsequente Anwendung von Design-Prinzipien bei der Implementierung erleichtert die Wartbarkeit und wirkt Fehlern entgegen. Bei den Crypto-Primitives im System der Post handelt es sich um eine Sammlung von Algorithmen, die grundlegende kryptografische Operationen ausführen. Die Implementierung richtet sich nach den Grundsätzen der objektorientierten Programmierung. Sie ist unter einer Open-Source-Lizenz offengelegt. Die durchgeführten Überprüfungen des Post-Systems führen zum Schluss, dass in einigen Bereichen das Potential besteht, noch stärker von den Design-Prinzipien der objektorientierten Programmierung zu profitieren. Verbesserungspotential besteht namentlich in der Benennung von Klassen und Interfaces, der konsequenten Anwendung semantischer Kriterien bei der Bildung von Hierarchien (Vererbung von Klassen, Implementierung von Interfaces) sowie der Definition geeigneter Methoden auf hoher Abstraktionsstufe und deren effizienten Verwendung. In den folgenden Bereichen sollen Anpassungen vorgenommen werden (vgl. auch Ziff. 3.2.1 im Prüfbericht der Berner Fachhochschule BFH vom 23.02.2023[7]): - Implementierung algebraischer Gruppen - Implementierung von Tupeln, Vektoren und Matrizen - Interface «Hashable» als Grundlage für die Berechnung kryptografischer Hashes Sofern die Zielsetzungen hinter den Bemerkungen im Prüfbericht auf andere Weise erreicht werden, kann von den Empfehlungen abgewichen werden.	2025	Kantone, Systemanbieter	Neu

[7] Abrufbar unter www.bk.admin.ch > Politische Rechte > E-Voting > Überprüfung von Systemen.

Nr.	Massnahme	Beschreibung	Zeitpunkt Umsetzung	Zuständigkeit	Stand Umsetzung
A.16	Die Post prüft Möglichkeiten zur Reduktion der Komplexität des Systems und setzt geeignete Vereinfachungen um	Grundsätzlich begünstigen Konstruktionen, die sich durch Einfachheit auszeichnen, die frühzeitige Erkennung und Behebung von Fehlern. Gleichzeitig weisen sichere E-Voting-Systeme naturgemäss einen substantiellen Umfang auf. Die Systeme sollten so umfangreich wie nötig und so einfach wie möglich ausgestaltet werden. Das System der Post ist nicht grundsätzlich unnötig kompliziert aufgebaut. Dennoch wird die Post Möglichkeiten zur weiteren Vereinfachung des Systems prüfen, sofern deren Umsetzung ohne Einbusse bei den implementierten Sicherheitseigenschaften möglich ist und die Umsetzung sinnvoll ist, vgl. auch Ziff. 1.4 «Potential for Simplifications» im Prüfbericht der BFH vom 23.02.2023[8]. Insbesondere setzt sie in folgenden Bereichen Vereinfachungen um: - Der Vorgang der Authentifizierung der Stimmberechtigten erfolgt mit einem Austausch von Nachrichten, der mehrere Runden umfasst. Dabei kommen Zertifikate zum Einsatz, die zwar den bundesrechtlichen Anforderungen an Zertifikate nicht genügen, deren Verwendung gleichzeitig aber auch keine Rolle für die Konformität des Systems spielt. Auf Nachrichten und Zertifikate, für die kein substantieller Mehrwert dokumentiert ist, soll verzichtet werden. Entsprechende Vereinfachungen erfolgen im Zug der Erstellung der Spezifikation der Authentifizierung (vgl. auch Massnahme A.9). - Nebst der abgegebenen Stimme werden als Bestandteil des Stimmdatensatzes Elemente mitgeschickt, die für die Generierung der Prüfcodes durch das Online-System nötig sind. Diese Elemente werden in verschlüsselter Form verschickt, obwohl dies nicht nötig wäre (vgl. auch Ziff. 5.1.4 der Swiss Post Voting System – System Specification Version 1.2.0[9]). Auf unnötige Verschlüsselungen soll verzichtet werden.	Vereinfachung Authentifizierung: 2. Quartal 2023 (Einsatz ab NRW 2023) Verzicht auf unnötige Verschlüsselungen im Stimmdatensatz sowie weitere Vereinfachungen bei Bedarf: 2025 / 2026 (gemeinsam mit Massnahme A.5)	Kantone, Systemanbieter	Neu
A.17	Bund, Kantone und die Systemanbieterin Post harmonisieren ihre Terminologie	Bund, Kantone und die Post verwenden teilweise unterschiedliche Begriffe für das Gleiche (Konzepte, Objekte etc.). Gleichzeitig weisen die Unterlagen der Akteure starke materielle Bezüge untereinander auf. Die Verwendung unterschiedlicher Begriffe kann die Nachvollziehbarkeit der Unterlagen insgesamt erschweren.	Raster und Plan: 2024	BK unter Einbezug Kantone, Systemanbieter	Neu

[8] Abrufbar unter www.bk.admin.ch > Politische Rechte > E-Voting > Überprüfung von Systemen.

[9] Abrufbar unter https://gitlab.com/swisspost-evoting > E-Voting > E-Voting documentation > System.

Nr.	Massnahme	Beschreibung	Zeitpunkt Umsetzung	Zuständigkeit	Stand Umsetzung
		Bund, Kantone und die Post erstellen ein Raster, das die durch die jeweiligen Akteure verwendeten Begriffe aufeinander abbildet. Sie prüfen die Möglichkeit, das Raster der Öffentlichkeit als Hilfestellung für die Lektüre der offengelegten Unterlagen zur Verfügung zu stellen. Gestützt auf das Raster entscheiden Bund, Kantone und die Post über mögliche Vereinheitlichungen und erstellen einen Plan für die Umsetzung. Das Ziel besteht darin, in den Unterlagen, die mit Blick auf den Einsatz von Release 2.0 des Systems der Post erstellt oder angepasst werden, eine möglichst einheitliche Terminologie zu verwenden.			
A.18	Die Kantone dokumentieren die Bezüge zwischen ihren betrieblichen Anleitungen und dem kryptografischen Protokoll sowie den Anforderungen der VEleS	Das kryptografische Protokoll legt gestützt auf das Vertrauensmodell in Ziff. 2 Anhang VEleS die durchzuführenden Operationen für alle Systemteilnehmenden fest. Für die Durchführung einiger Operationen sind betriebliche Handlungsschritte nötig, die durch Menschen erbracht werden, beispielsweise das Setzen von Passwörtern (vgl. Ziff. 4.2.2 Swiss Post Voting System – System Specification Version 1.2.0[10]). Ausserdem stellt die VEleS in Ziff. 3 des Anhangs zusätzliche Anforderungen an den Betrieb der Komponenten, deren korrekte Funktionsweise zur Erfüllung der Sicherheitsziele entscheidend ist (der sog. «vertrauenswürdigen Komponenten»). Beispielsweise fordert die VEleS die Sicherstellung von genügend Entropie für die Wahl von Zufallswerten (Ziff. 3.2 Anhang VEleS). Die Kantone legen mit dieser Massnahme einen Schwerpunkt auf die Dokumentation der Bezüge zwischen ihren betrieblichen Anleitungen und dem kryptografischen Protokoll sowie den Anforderungen der VEleS. Damit wird ein Beitrag dazu geleistet, dass die wichtigen Handlungsschritte nachhaltig korrekt umgesetzt werden, namentlich bei einer Anpassung am kryptografischen Protokoll oder der VEleS.	2025	Kantone mit Unterstützung Systemanbieter und BK	Neu
A.19	Bund und Kantone untersuchen die Nutzung der Prüfelemente durch die Stimmenden und definieren bei Bedarf Massnahmen zur Förderung deren Nutzung	Die VEleS fordert für die Stimmberechtigten verschiedene Prüfmöglichkeiten, um Angriffe zu erkennen und auf sie zu reagieren: - Prüfung, ob die Stimme korrekt registriert wurde (Ziff. 2.5 Anhang VEleS); - Prüfung, ob im Namen der stimmberechtigten Person eine Stimme missbräuchlich abgegeben wurde (Ziff. 2.5 Anhang VEleS); - Prüfung, ob auf der Benutzerplattform die korrekte Software mit den korrekten Verschlüsselungsparametern ausgeführt wird (Ziff. 2.7.3 Anhang VEleS);	Untersuchung und bei Bedarf Definition von Massnahmen: 2025	BK unter Einbezug der Kantone und Systemanbieter	Neu

[10] Abrufbar unter https://gitlab.com/swisspost-evoting > E-Voting > E-Voting documentation > System.

Nr.	Massnahme	Beschreibung	Zeitpunkt Umsetzung	Zuständigkeit	Stand Umsetzung
		- Prüfung der Authentizität der zur Stimmabgabe benutzten Internetseite (Ziff. 8.10 Anhang VEleS). Zudem enthält Ziff. 8 Anhang VEleS Mindestanforderungen an Informationen und Anleitungen zuhanden der Stimmberechtigten. Die Prüfmöglichkeiten entfalten ihre Wirkung nur dann, wenn Stimmberechtigte sie nutzen. Den am Betrieb beteiligten Stellen dienen Meldungen über negativ ausgefallene Prüfungen seitens der Stimmberechtigten als Indizien für mögliche systematische Angriffe. Auch für sie besteht ein Interesse, dass Stimmberechtigte in ausreichendem Umfang von den Prüfmöglichkeiten Gebrauch machen. Der Versuchsbetrieb soll den Rahmen bilden, um die Nutzung der Prüfmöglichkeiten durch die Stimmberechtigten zu untersuchen und gegebenenfalls Verbesserungen an deren Ausgestaltung sowie der Kommunikation vorzunehmen. Die BK und die Kantone untersuchen die Nutzung der Prüfelemente durch die Stimmenden und definieren bei Bedarf Massnahmen zur Förderung deren Nutzung.			
A.20	Bei der öffentlichen Überprüfung können Urnengänge ausgehend von den eCH-Dateien aufgesetzt werden	Ausgehend vom offengelegten Quellcode können Personen das System der Post in der eigenen Infrastruktur aufsetzen und Urnengänge mit vorgegebenen Testdateien simulieren. Im Rahmen des Bug-Bounty-Programms der Post wird die Meldung relevanter Mängel entgolten. Um interessierten Personen mehr Flexibilität beim Simulieren von Urnengängen zu gewährleisten, prüft die Post Massnahmen, wie beispielsweise die Durchführung von Urnengängen ausgehend von den eCH-Dateien, die die fachlichen Parameter (Abstimmungsvorlagen, Listen und Kandidierende, Stimmberechtigte) enthalten.	Erste Verbesserungen: 2. Quartal 2023 (Einsatz ab NRW 2023) Weitere Verbesserungen: 2024	Kantone, Systemanbieter	Neu
A.21	Implementierung des spezifizierten sogenannten «Dispute Resolvers»	Die Post hat zur Behebung möglicher Inkonsistenzen unter den Kontrollkomponenten in Bezug auf die Frage, welche Stimmen zu zählen sind, den sogenannten «Dispute Resolver» spezifiziert (vgl. auch Erläuterungen im Anhang zu Massnahme A.24). Diesen gilt es nun zu implementieren, damit die Kantone oder die Post ihn bei Bedarf unmittelbar einsetzen können. Die Wahrscheinlichkeit von Inkonsistenzen darf als gering gelten. Im Vorfeld der Implementierung des «Dispute Resolvers» hätten Inkonsistenzen vor der Umsetzung der vorliegenden Massnahme zur Folge, dass die nötige Funktionalität unter Berücksichtigung der nötigen	2024	Kantone, Systemanbieter	Neu

Nr.	Massnahme	Beschreibung	Zeitpunkt Umsetzung	Zuständigkeit	Stand Umsetzung
		Transparenz und Nachvollziehbarkeit bei Bedarf kurzfristig implementiert werden müsste. Dies könnte zur Folge haben, dass bis zur Auflösung der Inkonsistenz Tage verstreichen. Das mit der vorläufig unterbliebenen Implementierung des «Dispute Resolvers» verbundene Risiko darf als hinreichend gering gelten.			
A.22	Anpassung der Aufgaben der Prüferinnen und Prüfer, damit sie keine betrieblichen Aufgaben wahrnehmen	Im Rahmen der Konfigurationsphase eines Urnengangs werden beim Kanton die kryptografischen Parameter für den Urnengang gesetzt. Es handelt sich dabei um eine betriebliche Aufgabe und gehört damit nicht in den eigentlichen Zuständigkeitsbereich der Prüferinnen und Prüfer. Die Operationen, die dazu nötig sind, nehmen viel Zeit in Anspruch. Mit dem Ziel, die Prozesse zu optimieren, haben Kantone und Post einen der besonders zeitaufwändigen Schritte in die Zuständigkeit der Prüferinnen und Prüfer nach Art. 2 Abs. 1 Bst. h VEleS gelegt. Für diese Arbeiten verwenden die Prüferinnen und Prüfer den ihnen zugewiesenen Laptop. So kann dieser Schritt parallel zu anderen Arbeiten erfolgen. Da der Laptop, den die Prüferinnen und Prüfer verwenden, durch die zuständige Stelle beim Kanton aufbewahrt und unter denselben Modalitäten betrieben wird wie der Laptop, der eigentlich für diesen Schritt vorgesehen wäre, ist die Lösung aus sicherheitstechnischer Sicht als gleichwertig zu bewerten. Mit der vorliegenden Massnahme soll sichergestellt werden, dass Prüferinnen und Prüfer keine betrieblichen Aufgaben wahrnehmen. Insbesondere soll bei der Ausarbeitung der Massnahme A.5 darauf geachtet werden, dass die Durchführung betrieblicher Aufgaben nicht oder nicht allein von der korrekten Funktionsweise des Laptops der Prüferinnen und Prüfer abhängt. Vgl. Anhang für ergänzende Informationen zu dieser Massnahme.	2025 / 2026 (gemeinsam mit Massnahme A.5)	Kantone, Systemanbieter	Neu
A.23	Weiterentwicklung des Entwicklungsprozesses insbesondere Secure Development Lifecycle	Der Prüfbericht von SCRT vom 02.11.2022 zum Entwicklungsprozess der Post[11] enthält Vorschläge für Verbesserungen im Bereich der Sicherheitsvorkehrungen bei der Software-Entwicklung. Die Post hat bereits damit begonnen, diese Vorschläge im Rahmen des kontinuierlichen Verbesserungsprozesses umzusetzen. Mit dieser Massnahme wird festgelegt, dass die Empfehlungen aus den Prüfberichten adressiert werden und der jeweils aktuelle Stand der Sicherheitsvorkehrungen der BK für die wiederkehrenden Überprüfungen unterbreitet wird. Die Ergebnisse werden 2024 für ein erstes Review bereitgestellt.	Laufend; Umsetzung und Bereitstellung für ein erstes Review: 2024	Kantone, Systemanbieter	Neu

[11] Abrufbar unter www.bk.admin.ch > Politische Rechte > E-Voting > Überprüfung von Systemen.

Nr.	Massnahme	Beschreibung	Zeitpunkt Umsetzung	Zuständigkeit	Stand Umsetzung
A.24	Weitere Verbesserung der Schlüssigkeit der kryptografischen Konformitätsbeweise und Vergrösserung ihres Aussagegehalts	Kryptografische Sicherheitsbeweise werden in Ziff. 2.14.1 Anhang VEleS als Beleg gefordert, dass ein kryptografisches Protokoll die Anforderungen an die Verifizierbarkeit, das Stimmgeheimnis sowie die Authentifizierung erfüllt. In der Beweisführung werden kryptografische Protokolle in Beziehung mit elementaren kryptografischen Problemstellungen gebracht. Wenn der Beweis korrekt geführt wird, nämlich wenn die Beziehungen korrekt erstellt werden, und wenn die Sicherheitsannahmen gelten, nämlich, dass die elementaren kryptografischen Problemstellungen «schwer zu lösen» und damit de facto unlösbar sind, darf ein Protokoll im Sinne der VEleS als sicher gelten. Der Prüfbericht von Haines, Pereira und Teague vom 13.02.2023[12] zeigt auf, dass die Schlüssigkeit der Beweise und damit die Argumentation, weshalb das kryptografische Protokoll mit den elementaren Problemstellungen korrekt in Verbindung gebracht wurde, weiter verbessert werden muss. Um die Schlüssigkeit der Beweise zu verbessern, müssen in einigen Fällen die vorgebrachten Argumente vertieft werden. In einzelnen Fällen müssen fehlerhafte oder irreführende Argumente, die bereits in hinreichender Tiefe vorliegen, korrigiert werden. Der Aussagegehalt der Beweise muss nicht als grundsätzlich zu gering gelten. Allerdings würde der Aussagegehalt der Beweise erhöht werden, wenn weitere Systemelemente, die derzeit aus den Sicherheitsbeweisen ausgeblendet sind, mitberücksichtigt werden. Die Beweise sollen solche Systemelemente künftig soweit sinnvoll mitberücksichtigen. Vgl. Anhang für ergänzende Informationen zu dieser Massnahme.	2024	Kantone, Systemanbieter	Neu
A.25	Weitere Verbesserung der Qualität der Spezifikation und der Software	Die Einhaltung von Qualitätskriterien in der Spezifikation und der Software trägt entscheidend dazu bei, dass Fehlern oder Schwachstellen zuvorgekommen wird oder sie zumindest frühzeitig erkannt und behoben werden. Die VEleS stellt mit Blick auf die Qualität verschiedene Anforderungen, wie beispielsweise zur Nachvollziehbarkeit, Vollständigkeit, Kohärenz, Einheitlichkeit sowie zur Verständlichkeit (vgl. Ziff. 25 Anhang VEleS). Der Post ist es gelungen, die Qualität der Spezifikation und des Quellcodes ihres Systems substantiell zu erhöhen. Dennoch besteht Verbesserungsbedarf. Beispiele für Punkte, die verbessert werden sollen,	Verbesserungen: laufend Beschreibung geplanter noch ausstehender Verbesserungen: laufend und spätestens bis 1. Quartal 2024	Kantone, Systemanbieter	Neu

[12] Abrufbar unter www.bk.admin.ch > Politische Rechte > E-Voting > Überprüfung von Systemen.

Nr.	Massnahme	Beschreibung	Zeitpunkt Umsetzung	Zuständigkeit	Stand Umsetzung
		finden sich in den Prüfberichten.[13] Teilweise werden sie hier im Anhang genannt. Im Sinne des kontinuierlichen Verbesserungsprozesses werden Verbesserungen laufend vorgenommen. Die vorliegende Massnahme soll darüber hinaus dazu beitragen, dass der derzeit bekannte Verbesserungsbedarf (Stand Februar 2023) im Bereich der Qualität bis 2025 adressiert und soweit behoben wird. Im Rahmen dieser Arbeiten soll die Post der BK und den Kantonen jeweils eine materielle Beschreibung der geplanten Verbesserungen zur Verfügung stellen, damit diese vor deren Umsetzung diskutiert und bei Bedarf angepasst sowie allfällige Unklarheiten und Differenzen, allenfalls unter Einbezug externer Expertinnen und Experten, geklärt werden können. Die visierte Beschreibung soll auch in die unabhängige Überprüfung der BK nach Art. 10 Abs. 1 VEleS einfliessen. Die mit dem Verbesserungsbedarf im Bereich der Qualität verbundenen Risiken dürfen als hinreichend gering gelten. Vgl. Anhang für ergänzende Informationen zu dieser Massnahme.	Behebung des derzeit bekannten Verbesserungsbedarfs: 2025		
B.	**Wirksame Kontrolle und Aufsicht**				
B.6	Erneuerung des Krisenmanagements mit Durchführung von Krisenübungen	Vgl. Beschreibung im Massnahmenkatalog des Schlussberichts des SA VE vom 30.11.2020.	Wiedereinsatz	BK (Federführung), Kantone und Systemanbieter	In Bearbeitung
B.8	Weiterentwicklung der Plausibilisierung der E-Voting-Ergebnisse	Vgl. Beschreibung im Massnahmenkatalog des Schlussberichts des SA VE vom 30.11.2020.	Wiedereinsatz: Erster Austausch Prüfung standardisierte Methode: *bis 2023*	Kantone	In Bearbeitung (erster Austausch ist 2022 erfolgt)
B.10	Langfristige Überprüfung der Prozesse, Rollen und Aufgaben	Vgl. Beschreibung im Massnahmenkatalog des Schlussberichts des SA VE vom 30.11.2020.	Langfristig	AG Zukunft VE	In Bearbeitung
B.11	Kontinuierliche Verbesserung der Risikodokumentation der Kantone	Die Risikobeurteilungen 2022 der Kantone widerspiegeln die Situation nach der Umsetzung der Anforderungen der VEleS. Sie wurden nach dem Leitfaden der BK für Risikobeurteilungen erstellt. Die Risikodokumentation soll kontinuierlich verbessert und dabei ein Schwerpunkt auf die Nachvollziehbarkeit gelegt werden, indem die Überlegungen, die zu einer Beurteilung führen, vermehrt dokumentiert werden. Gestützt	Laufend; Umsetzung erste Verbesserungen: 2024	Kantone	Neu

[13] Abrufbar unter www.bk.admin.ch > Politische Rechte > E-Voting > Überprüfung von Systemen.

Nr.	Massnahme	Beschreibung	Zeitpunkt Umsetzung	Zuständigkeit	Stand Umsetzung
		auf die Zusammenarbeit mit den Kantonen und die bestehende Dokumentation kommt die BK zum Schluss, dass die Kantone ihre Risiken systematisch und ausreichend beurteilt haben. Mit der vorliegenden Massnahme soll lediglich die Dokumentation verbessert werden, um das Risikomanagement der Kantone nachvollziehbarer zu machen.			
B.12	Verbesserung der Zugänglichkeit und Nachvollziehbarkeit der Risikodokumentation der Post	Zur Zugänglichkeit: Im Rahmen der Zulassungsgesuche an die BK müssen die Kantone ihre Risikobeurteilungen und ggf. die ihrer Dienstleister (wie etwa des Systembetreibers) einreichen (Art. 15 Abs. 1 Bst. a VEleS). Sie müssen nachweisen und begründen, dass die Sicherheitsrisiken hinreichend gering sind (Art. 4 Abs. 1 und 2 VEleS). Die Risikobeurteilung der Post erfolgt nach ihren internen Weisungen, die mehrere Ebenen umfassen: Konzern, IT und E-Voting. Die Dokumentation kann aufgrund der Klassifizierung des Inhalts nur vor Ort bei der Post eingesehen werden. Dieser Zugang ist für die Bewilligungsbehörde aufwendig und ermöglicht keine Flexibilität. Die Post und die Kantone prüfen Möglichkeiten, wie der BK eine Form des Zugangs ermöglicht werden kann, die den Bedürfnissen und Einschränkungen aller Beteiligten entspricht. Der Zugang muss die Nachvollziehbarkeit der verschiedenen Risikobeurteilungen gewährleisten. Zur Nachvollziehbarkeit: Nach der Konsultation der Bedrohungs- und Risikodokumentation der Post kommt die BK zum Schluss, dass die implementierten Prozesse geeignet sind, damit die Risikoeigner die Verantwortung für die Identifizierung, Bewertung und Dokumentation der Risiken wahrnehmen. Diese Prozesse gewährleisten zwar, dass die Risiken unter Kontrolle sind. Jedoch besteht in der Dokumentation, die der BK unterbreitet wurde, Verbesserungspotential. Sie wird angepasst und ergänzt, um der BK einen konsolidierten Überblick über alle Risiken und Bedrohungen (entwicklungs- oder betriebsbezogen, technischer oder organisatorischer Natur) in ausreichender Detailtiefe zu bieten.	Bestimmung der Form und des Zeitplans für die Verbesserung der Zugänglichkeit sowie der Nachvollziehbarkeit: 3. Quartal 2023	Kantone, Systemanbieter	Neu
B.13	Verbesserung der Möglichkeiten zur unabhängigen Untersuchung von Vorfällen	Die Informationen, die den Kantonen für die Untersuchung von Vorfällen zur Verfügung stehen, sind von der Systemanbieterin Post abhängig (Berichte mit ausgewählten Statistiken; Untersuchungsberichte auf Bestellung). Diese Abhängigkeit könnte zu Problemen führen, wenn ein Fehlverhalten, das in den Verantwortungsbereich der Post fällt, untersucht werden soll. Die Kantone prüfen, in welchem Umfang ein direkterer Zugang zu den für solche Untersuchungen relevanten Infor-	Erste Lagebeurteilung: 2024, anschliessend Definition der Massnahmen	Kantone, Systemanbieter	Neu

Nr.	Massnahme	Beschreibung	Zeitpunkt Umsetzung	Zuständigkeit	Stand Umsetzung
		mationen notwendig und möglich ist. Sie bauen während der Versuchsphase und gestützt auf Bedürfnisse, die während den Urnengängen identifiziert werden, Kompetenzen zur Untersuchung von Vorfällen auf. Angesichts der Bedingungen der Versuchsphase (insbesondere die Limitierung des zugelassenen Elektorats) ist diese Abhängigkeit bis zur Umsetzung der Verbesserungsmassnahmen vertretbar. Die Versuchsphase dient auch dem Aufbau solcher Kompetenzen.			
B.14	Revision der Rechtsgrundlagen zur Ausräumung von Unklarheiten	Die 2022 revidierten Rechtsgrundlagen des Bundes sind mit Blick auf die Wiederaufnahme der Versuche 2023 erstmals zur Anwendung gelangt. Verschiedene Fragen haben sich in der Anwendung der Rechtsgrundlagen erstmals gestellt. Dabei wurde ersichtlich, dass die Nachvollziehbarkeit in einzelnen Punkten verbessert werden könnte, indem der Wortlaut der VEleS angepasst oder die Erläuterungen ergänzt oder präzisiert werden. So hat beispielsweise eine Inkonsistenz in den Rechtsgrundlagen dazu geführt, dass in einem Prüfbericht die teilweise Nichterfüllung einer Anforderung geltend gemacht werden musste, obwohl die gewählte Lösung der Kantone aus sicherheitstechnischer Sicht zu bevorzugen ist (vgl. Ziff. 8, Punkt 15.4 im Prüfbericht von SCRT vom 17.02.2023 zu Infrastruktur und Betrieb bei den Kantonen[14]). Der Versuchsbetrieb soll den Rahmen bieten, auch mit Blick auf die Rechtsgrundlagen Lehren zu ziehen und Anpassungen vorzunehmen, die der Nachvollziehbarkeit dienen. Eine solche Überarbeitung soll vorgenommen werden, sobald eine erneute Revision der Rechtsgrundlagen im Rahmen der nächsten Etappen der Neuausrichtung des Versuchsbetriebs ansteht.	Bei nächster Revision der Rechtsgrundlagen	BK	Neu

C.	Stärkung der Transparenz und des Vertrauens				
C.6	Vermehrter Einbezug der Öffentlichkeit	Vgl. Beschreibung im Massnahmenkatalog des Schlussberichts des SA VE vom 30.11.2020.	Konzept: *2023*	BK unter Einbezug Kantone und Systemanbieter	In Bearbeitung
C.7	Bereitstellung zusätzlicher Unterlagen, die zur Meinungsbildung über die Vertrauenswürdigkeit und die Sicherheit beitragen	Sowohl für Stimmberechtigte ohne fachliche Kenntnisse als auch für Fachleute stellen sich elementare Fragen in Bezug auf die Vertrauenswürdigkeit und die Sicherheit der elektronischen Stimmabgabe. Trans-	Workshops BK: 2023 Bereitstellung Unterlagen: laufend und bei Bedarf	BK und Kantone	Neu

[14] Abrufbar unter www.bk.admin.ch > Politische Rechte > E-Voting > Überprüfung von Systemen.

Nr.	Massnahme	Beschreibung	Zeitpunkt Umsetzung	Zuständigkeit	Stand Umsetzung
		parenz bildet eine entscheidende Voraussetzung, damit sich interessierte Personen eine fundierte Meinung bilden können und sich eine fruchtbare, faktenbezogene öffentliche Debatte einstellen kann. Bund, Kantone und die Post haben in ihren jeweiligen Zuständigkeitsbereichen Unterlagen offengelegt und auch aktiv Unterlagen mit Erklärungen zur elektronischen Stimmabgabe an die Adresse der Stimmberechtigten aufbereitet. Gestützt auf die bereits erbrachten Leistungen soll der bevorstehende Versuchsbetrieb Aufschluss geben, welche Fragen für die Stimmberechtigten im Zentrum stehen und welche Bedürfnisse und Erwartungen an die Inhalte der Kommunikation seitens der Behörden und ihrer Dienstleister bestehen. Erhebung des Bedarfs: - Die BK führt in Absprache mit den Kantonen Workshops mit unabhängigen Personen aus der Öffentlichkeit durch. - Die BK und die Kantone werten in Zusammenarbeit mit deren Dienstleistern Rückmeldungen aus, die im Verlauf des Versuchsbetriebs an sie gelangen. Die BK und die Kantone stellen der Öffentlichkeit bei Bedarf weitere Unterlagen zu ihren jeweiligen Verantwortungsbereichen bereit.			

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	Vgl. Beschreibung im Massnahmenkatalog des Schlussberichts des SA VE vom 30.11.2020.	Konzept: *2023*	BK unter Einbezug Kantone	In Bearbeitung
D.2	Einbezug unabhängiger Expertinnen und Experten	Vgl. Beschreibung im Massnahmenkatalog des Schlussberichts des SA VE vom 30.11.2020.	Im Rahmen der einzelnen Massnahmen	BK unter Einbezug Kantone	Laufend
D.3	Erstellung eines Konzepts für den Aufbau eines wissenschaftlichen Ausschusses	Vgl. Beschreibung im Massnahmenkatalog des Schlussberichts des SA VE vom 30.11.2020.	Konzept: *2023*	BK unter Einbezug Kantone	In Bearbeitung

2.2 Erledigte Massnahmen

Nr.	Massnahme	Beschreibung	Zeitpunkt Umsetzung	Zuständigkeit	Stand Umsetzung
A.	**Weiterentwicklung der Systeme**				
A.1	Präzisierung der Kriterien für die Qualität des Quellcodes und der Dokumentation	Vgl. Beschreibung im Massnahmenkatalog des Schlussberichts des SA VE vom 30.11.2020.	Wiedereinsatz	Anforderungen: BK Umsetzung: Kantone, Systemanbieter	Erledigt (vgl. Ziff. 24 und 25 Anhang VEleS; Umsetzung ist durch Kantone und Systemanbieter erfolgt)
A.2	Stärkung der Qualitätssicherung im Entwicklungsprozess von E-Voting-Systemen	Vgl. Beschreibung im Massnahmenkatalog des Schlussberichts des SA VE vom 30.11.2020.	Wiedereinsatz	Anforderungen: BK Umsetzung: Kantone, Systemanbieter	Erledigt (vgl. Ziff. 17 und 24 Anhang VEleS; Umsetzung ist durch Kantone und Systemanbieter erfolgt)
A.3	Anwendung einer bewährten und nachvollziehbaren Build- und Deployment-Methode	Vgl. Beschreibung im Massnahmenkatalog des Schlussberichts des SA VE vom 30.11.2020.	Wiedereinsatz	Anforderungen: BK Umsetzung: Kantone, Systemanbieter	Erledigt (vgl. Ziff. 24.3 Anhang VEleS; Umsetzung ist durch Kantone und Systemanbieter erfolgt)
A.7	Verbesserung der Grundlagen zur Erkennung (Monitoring) und Untersuchung (IT-Forensik) von Vorfällen	Vgl. Beschreibung im Massnahmenkatalog des Schlussberichts des SA VE vom 30.11.2020.	Definition Anforderungen und Verbesserungsprozess: Wiedereinsatz	Anforderungen: BK Verbesserungsprozess: Systemanbieter, Kantone	Erledigt (vgl. Ziff. 14 Anhang VEleS; Umsetzung des Verbesserungsprozesses erfolgt laufend durch Kantone und Systemanbieter)
A.8	Schaffung eines gemeinsamen Massnahmenplans von Bund und Kantonen	Vgl. Beschreibung im Massnahmenkatalog des Schlussberichts des SA VE vom 30.11.2020.	Wiedereinsatz	BK / Kantone	Erledigt (vgl. vorliegender Massnahmenkatalog, der regelmässig überprüft, angepasst und publiziert wird)
B.	**Wirksame Kontrolle und Aufsicht**				
B.1	Anpassung der Zuständigkeiten bei den Konformitätsprüfungen des Systems und der zugrundeliegenden Prozesse	Vgl. Beschreibung im Massnahmenkatalog des Schlussberichts des SA VE vom 30.11.2020.	Wiedereinsatz	BK	Erledigt (vgl. Art. 27/ VPR und Art. 10 VEleS i.V.m. Ziff. 26 Anhang VEleS)
B.2	Erarbeitung eines Prüfkonzepts für die Beurteilung der Konformität des Systems und der zugrundeliegenden Prozesse	Vgl. Beschreibung im Massnahmenkatalog des Schlussberichts des SA VE vom 30.11.2020.	Wiedereinsatz	BK in Zusammenarbeit mit Kantonen und Systemanbieter	Erledigt (vgl. Audit Concept für unabhängige Überprüfungen unter www.bk.admin.ch > Politische Rechte > E-Voting > Überprüfung von Systemen)
B.3	Erarbeitung und Umsetzung eines Prozesses zum Umgang mit Nicht-Konformitäten	Vgl. Beschreibung im Massnahmenkatalog des Schlussberichts des SA VE vom 30.11.2020.	Wiedereinsatz	BK in Zusammenarbeit mit Kantonen und Systemanbieter	Erledigt (Prozess zum Umgang mit Nichtkonformitäten wurde von der BK in Zusammenarbeit mit den Kantonen und dem Systemanbieter definiert)

Nr.	Massnahme	Beschreibung	Zeitpunkt Umsetzung	Zuständigkeit	Stand Umsetzung
B.4	Erneuerung und Verbesserung des Leitfadens für die Risikobeurteilungen	Vgl. Beschreibung im Massnahmenkatalog des Schlussberichts des SA VE vom 30.11.2020.	Wiedereinsatz	BK in Zusammenarbeit mit Kantonen und Systemanbieter	Erledigt (vgl. Leitfaden der BK unter www.bk.admin.ch > Politische Rechte > E-Voting > Bundesrechtliche Anforderungen)
B.5	Erarbeitung und Umsetzung eines neuen Vorgehens für die Risikobeurteilungen für vollständig verifizierbare Systeme	Vgl. Beschreibung im Massnahmenkatalog des Schlussberichts des SA VE vom 30.11.2020.	Wiedereinsatz	BK, Kantone, Systemanbieter	Erledigt (vgl. Art. 4 VEleS; Risikobeurteilungen aller Akteure liegen vor; die Risikobeurteilung der BK wird publiziert)
B.7	Integration von E-Voting als Teil der kritischen Infrastruktur des Bundes	Vgl. Beschreibung im Massnahmenkatalog des Schlussberichts des SA VE vom 30.11.2020.	Wiedereinsatz	BK (Federführung), Kantone und Systemanbieter	Erledigt
B.9	Anpassungen des Bewilligungsverfahrens	Vgl. Beschreibung im Massnahmenkatalog des Schlussberichts des SA VE vom 30.11.2020.	Wiedereinsatz	BK unter Einbezug der Kantone	Erledigt (vgl. Leitfaden der BK unter www.bk.admin.ch > Politische Rechte > E-Voting > Bundesrechtliche Anforderungen)
C.	**Stärkung der Transparenz und des Vertrauens**				
C.1	Begrenzung des zulässigen Elektorats für vollständig verifizierbare Systeme	Vgl. Beschreibung im Massnahmenkatalog des Schlussberichts des SA VE vom 30.11.2020.	Wiedereinsatz	BK	Erledigt (vgl. Art. 27*f* VPR)
C.2	Präzisierung der Anforderungen an die Offenlegung des Quellcodes	Vgl. Beschreibung im Massnahmenkatalog des Schlussberichts des SA VE vom 30.11.2020.	Wiedereinsatz	Anforderungen: BK Offenlegung: Kantone, Systemanbieter	Erledigt (vgl. Art. 27*f*^{bis} VPR und Art. 11 und 12 VEleS; Offenlegung durch Kantone und Systemanbieter ist erfolgt)
C.3	Führen eines Bug-Bounty-Programms	Vgl. Beschreibung im Massnahmenkatalog des Schlussberichts des SA VE vom 30.11.2020.	Wiedereinsatz	Anforderungen: BK Durchführung: Kantone, Systemanbieter	Erledigt (vgl. Art. 27*f*^{ter} VPR und Art. 13 VEleS; Durchführung durch Kantone und Systemanbieter ist erfolgt; vgl. Community-Programm | Evoting-Community (post.ch))
C.4	Publikation bewilligungsrelevanter Prüfberichte	Vgl. Beschreibung im Massnahmenkatalog des Schlussberichts des SA VE vom 30.11.2020.	Wiedereinsatz	BK, Kantone, Systemanbieter	Erledigt (vgl. Art. 10 Abs. 4 VEleS; Publikation durch BK, Kantone und Systemanbieter ist erfolgt)
C.5	Publizieren der Ergebnisse von eidgenössischen Urnengängen für E-Voting	Vgl. Beschreibung im Massnahmenkatalog des Schlussberichts des SA VE vom 30.11.2020.	Wiedereinsatz	Anforderungen: BK Publikation: Kantone	Erledigt (vgl. Art. 27*m* Abs. 3 VPR; Publikation erfolgt durch die Kantone nach der Durchführung der Urnengänge)

Anhang: Ergänzende Informationen zu einzelnen pendenten Massnahmen

Nr.	Massnahme
A.9	**Fertigstellung der Systemspezifikation im Bereich der Authentifizierung der Stimmberechtigten**

Die Authentifizierung der Stimmberechtigten ist in zwei Etappen gegliedert. Pro Etappe geben die Stimmberechtigten einen vertraulichen Code ein, den sie dem Stimmrechtsausweis entnehmen:

1. Nach der Eingabe des ersten vertraulichen Codes erfolgt die initiale Authentifizierung. Ist sie erfolgreich, schickt das Online-System einen vertraulichen Parameter für die Stimmabgabe an das Gerät der Stimmberechtigten. Ohne diesen Parameter kann die Benutzerplattform keine Stimme übermitteln, die vom Online-System akzeptiert wird (es erfolgt eine Authentifizierung anhand des Stimmdatensatzes).
2. Mit der Eingabe eines zweiten vertraulichen Codes bestätigen die Stimmenden, dass sie die korrekte Übermittlung der Stimme anhand der Prüfcodes für die individuelle Verifizierbarkeit mit positivem Ergebnis überprüft haben. Der eingegebene Code kann auch als Authentisierungsmerkmal verstanden werden, anhand dessen die stimmberechtigte Person authentifiziert wird (vgl. Erläuterungen vom 25. Mai 2022 zu Ziff. 2.12.8 Anhang VEleS[15]).

Im Post-System, das im Juni 2023 zum ersten Mal eingesetzt werden soll, ist die initiale Authentifizierung der ersten Etappe nicht spezifiziert.

Der vorliegenden System-Spezifikation kann entnommen werden, dass die Sicherheit des Systems in folgendem Sinne mit der Geheimhaltung des vertraulichen Parameters in Verbindung steht:

Angenommen, Angreifer hätten Zugriff auf den Parameter, so könnten sie dennoch keine Stimme abgeben. Es braucht dazu die Eingabe des zweiten vertraulichen Codes. Auch die Verifizierbarkeit nach Ziff. 2.5 und 2.6 Anhang VEleS wäre bei erfolgtem Zugriff auf den Parameter nicht in Frage gestellt. Beides lässt sich aus dem kryptografischen Konformitätsbeweis nach Ziff. 2.14.1 Anhang VEleS ableiten. Der Zugriff auf den Parameter könnte Vorteile bei Versuchen bringen, auf den Inhalt der verschlüsselt abgegebenen Stimmen zu schliessen. Zur Erfüllung von Ziff. 2.7 Anhang VEleS darf kein Zugriff möglich sein. Zwar müssten Angreifer, um von ihrer Kenntnis des vertraulichen Parameters zu profitieren, an zusätzliche Informationen gelangen, die im Online-System bei der Stimmabgabe erhoben werden. Allerdings darf infolge von Ziff. 2.7 Anhang VEleS der Zugriff auf die Gesamtheit der Daten, die im Online-System geführt wird, keine Schlüsse auf den Inhalt der abgegebenen Stimmen zulassen.

Zur Geheimhaltung des vertraulichen Parameters: Der in der ersten Etappe verschickte vertrauliche Parameter liegt dem Online-System nur in verschlüsselter Form vor. Dasselbe gilt für andere Werte des Online-Systems, die eine Entschlüsselung des vertraulichen Parameters ermöglichen würden. Die Entschlüsselung ist nur bei Kenntnis des ersten vertraulichen Codes möglich. Dementsprechend verschickt die Benutzerplattform diesen Code in einer abgeänderten Form, die keine Entschlüsselung zulässt. Damit könnten Angreifer, die in Besitz der verschlüsselten Werte des Online-Systems kommen, den vertraulichen Parameter dennoch nicht entschlüsseln. Diese Beobachtungen werden nicht durch eine Spezifikation, sondern allein durch Aussagen der Post sowie Beobachtungen am Quellcode gestützt. Die Fertigstellung und die Prüfung der Spezifikation werden es erlauben, eine strukturiertere Analyse des Quellcodes vorzunehmen, und so dazu beitragen, noch grössere Sicherheit in Bezug auf die Erfüllung der Anforderungen nach Ziff. 2.7 Anhang VEleS zu erlangen.

Nr.	Massnahme
A.11	**Offenlegung des Quellcodes der Software zur Erzeugung der PDF-Dateien für den Druck der Stimmrechtsausweise**

Für die Wirksamkeit des kryptografischen Protokolls, das in Erfüllung der Anforderungen an die individuelle Verifizierbarkeit, die Wahrung des Stimmgeheimnisses sowie die Authentifizierung steht, ist entscheidend, dass Codes für die Stimmrechtsausweise vertraulich bleiben und korrekt in die PDF-Dateien übernommen werden.

[15] Abrufbar unter www.bk.admin.ch > Politische Rechte > E-Voting > Bundesrechtliche Anforderungen.

Eine durchgeführte Sicherheitsprüfung sowie folgende Überlegungen führen zum Schluss, dass ein vorläufiger Verzicht auf die Offenlegung von VCPS mit hinreichend geringen Risiken verbunden ist:

- Die betroffenen Kantone sichern zu, im Betrieb per Stichprobe zu prüfen, dass die korrekten Codes ins PDF übernommen wurden.
- VCPS wird auf einem Laptop betrieben, für dessen Betrieb Ziff. 3 Anhang VEleS gilt und damit besonders geschützt ist. Insbesondere wird er ohne Netzwerkverbindung betrieben.
- Auf dem Laptop werden abgesehen von den Rohdaten für den Druck keine kritischen Daten nach Art. 2 Abs. 1 Bst. v VEleS geführt.

Nr.	Massnahme
A.13	**Verzicht auf das SGSP-Problem als Sicherheitsannahme**

Die Schwierigkeit, das SGSP-Problem zu lösen, lässt sich nicht anhand des DDH-Problems abschliessend quantifizieren. Damit darf das SGSP-Problem lediglich als höchstens gleich schwer zu lösen gelten wie das DDH-Problem. Gleichzeitig ist kein Ansatz bekannt, der für das SGSP-Problem einen effizienteren (wenn auch unpraktikablen) Lösungsweg aufzeigt als für das DDH-Problem, geschweige denn auf einen praktikablen Lösungsweg hindeutet.

Die Konformität des kryptografischen Protokolls mit den Anforderungen an die Verifizierbarkeit nach Ziff. 2.5 und 2.6 sowie die Authentifizierung nach Ziff. 2.8 Anhang VEleS stützt sich nicht auf das SGSP-Problem. Angreifer, denen es gelingt, in das Online-System einzudringen, auf die nötigen Daten zuzugreifen und das SGSP-Problem zu lösen, wären in der Lage, auf den Inhalt der verschlüsselt abgegebenen Stimmen zu schliessen. Damit würde das kryptografische Protokoll gegen Ziff. 2.7 Anhang VEleS verstossen: Infolge Ziff. 2.7 Anhang VEleS darf die Gesamtheit der Daten, die im Online-System geführt wird, auch bei erfolgtem Zugriff keine Schlüsse auf den Inhalt der abgegebenen Stimmen zulassen.

Folgende Überlegung führt zum Schluss, dass ein vorläufiges Festhalten am SGSP-Problem als Sicherheitsannahme mit hinreichend geringen Risiken verbunden ist: Sollte eine praktikable Lösung des SGSP-Problems aus mathematischer Sicht überhaupt existieren, müsste mit grosser Wahrscheinlichkeit ein erheblicher Aufwand in die Suche und auch in die Anwendung der Lösung investiert werden. Hinzu käme der Aufwand, um an die für den Angriff nötigen Daten zu gelangen, die im Online-System aus den Stimmdatensätzen generiert werden. Gleichzeitig wäre der Nutzen, der aus dem Aufwand überhaupt entstehen könnte, beim eingeschränkten Elektorat bis zur Umsetzung der Massnahme, gering.

Nr.	Massnahme
A.22	**Anpassung der Aufgaben der Prüferinnen und Prüfer, damit sie keine betrieblichen Aufgaben wahrnehmen**

Die Prüferinnen und Prüfer sollen Fälle entdecken, wo Stimmen manipuliert, gelöscht oder zu Unrecht gezählt worden sind (vgl. Ziff. 2.6 Anhang VEleS). Dazu werten sie kryptografische Beweise aus, die sie zusammen mit dem Ergebnis des Urnengangs erhalten. Ihr Hilfsmittel ist der Verifier, eine unter Open-Source-Lizenz offengelegte Software. Die Prüfung führen sie auf einem dedizierten Laptop durch.

Im System der Post führen die Prüferinnen und Prüfer darüber hinaus während der Konfigurationsphase eine Prüfung durch, deren korrekte Durchführung ausschlaggebend für die Erfüllung der Anforderungen an die individuelle Verifizierbarkeit nach Ziff. 2.5, an den Schutz des Stimmgeheimnisses nach Ziff. 2.7 sowie an die Authentifizierung nach Ziff. 2.8 Anhang VEleS ist. Bei dieser Prüfung handelt es sich um eine betriebliche Aufgabe, die grundsätzlich in den direkten Verantwortungsbereich der mit E-Voting betrauten Stelle eines Kantons fällt. Als technisches Hilfsmittel steht dieser Stelle ein eigener Laptop (sog. Setup-Komponente) zur Verfügung.

Da mit dem Laptop der Prüferinnen und Prüfer keine Daten verarbeitet werden, deren Vertraulichkeit für die Erfüllung der oben genannten Anforderungen eine Bedingung darstellt, und da für den Betrieb der Setup-Komponente sowie des technischen Hilfsmittels der Prüferinnen und Prüfer dieselben Modalitäten gelten, darf die von den Kantonen und Post gewählte Lösung aus Sicht der Sicherheit als gleichwertig gelten. Auch dem erläuternden Bericht zur Totalrevision der VEleS von 2022[16] kann entnommen

[16] Abrufbar unter www.bk.admin.ch > Politische Rechte > E-Voting > Bundesrechtliche Anforderungen.

werden, dass Prüferinnen und Prüfer für Aufgaben zum Einsatz gebracht werden dürfen, für die ansonsten die Setup-Komponente vorgesehen wäre (vgl. Erläuterungen zu Ziff. 2.1 Anhang VEleS).

Betriebliche Aufgaben sollen auch langfristig unter Berücksichtigung der notwendigen Vorkehrungen ausgeführt werden. Gleichzeitig soll den Prüferinnen und Prüfern mehr Unabhängigkeit eingeräumt werden können, sofern dies gewünscht und durch das kantonale Recht ermöglicht wird. Betriebliche Aufgaben sollen deshalb direkt durch die für Urnengänge verantwortliche Stelle ausgeführt werden. Demgegenüber sollen die Prüferinnen und Prüfer allfällige betriebliche Fehlverhalten im Sinne ihrer Zuständigkeit aufdecken.

Nr.	Massnahme
A.24	**Weitere Verbesserung der Schlüssigkeit der kryptografischen Konformitätsbeweise und Vergrösserung ihres Aussagegehalts**

Die kryptografischen Sicherheitsbeweise dienen dazu, die Leserschaft – und allen voran auch die für die Führung des Beweises zuständigen Personen selbst – davon zu überzeugen, dass das kryptografische Protokoll die Anforderungen an die Verifizierbarkeit, das Stimmgeheimnis sowie die Authentifizierung erfüllt. Zwar muss aus einer Unschlüssigkeit im Beweis nicht *a priori* gefolgert werden, dass das kryptografische Protokoll eine Schwachstelle aufweist, geschweige denn eine Schwachstelle, die sich tatsächlich für einen Angriff verwenden lässt. Im Vorfeld der weiteren Analyse muss eine Unschlüssigkeit aber als potentieller Hinweis auf eine mögliche Schwachstelle gelten. Es ist deshalb wichtig, Unschlüssigkeiten zu untersuchen und sie auszuräumen, entweder indem allein der Beweis oder falls nötig auch das kryptografische Protokoll verbessert wird. Die Post hat die Beweisführung substantiell verbessert. Das Ziel der vorliegenden Massnahme besteht darin, die Arbeit weiterzuführen bis die Beweise als durchgehend schlüssig gelten dürfen.

Der Prüfbericht von Haines, Pereira und Teague und vom 13.02.2023[17] zeigt Beispiele mit fehlerhaften oder irreführenden Argumenten in den Beweisen auf (vgl. Ziff. 2.5.1 und 2.5.2 des Berichts). Es handelt sich dabei um Unschlüssigkeiten, die leicht behoben werden können, allein indem die Argumentation im Beweis angepasst wird. Hinter den Unschlüssigkeiten sind keine Schwachstellen im kryptografischen Protokoll verborgen und es muss nicht angepasst werden. Dennoch ist es wertvoll und wichtig, die Anpassungen am Beweis vorzunehmen. So müssen Personen, die den Beweis lesen, die zur Verfügung stehende Zeit nicht in Fragestellungen investieren, die andere bereits analysiert haben. Vielmehr können sie den Beweis gezielt auf neue Unschlüssigkeiten hin überprüfen und so dazu beitragen, dass allfälliger Verbesserungsbedarf am kryptografischen Protokoll zu einem frühen Zeitpunkt entdeckt und angegangen wird.

In Ziff. 2.5 wird im selben Prüfbericht festgehalten, dass die Argumentation in der Beweisführung an verschiedenen Stellen weiter ausgeführt werden müsste, damit sie nachvollzogen und allfällige Fehler oder Lücken in der Argumentation identifiziert werden können. Ohne die ausstehenden Ausführungen kann der Nutzen der Beweise in solchen Fällen stark eingeschränkt sein. Im Sinne der vorliegenden Massnahme soll die Argumentation an den betroffenen Stellen in den Beweisen weiter ausgeführt werden.

Die Beweise sollen zudem weitere Systemelemente mitberücksichtigen. In Sicherheitsbeweisen ist es gebräuchlich, Systemeigenschaften in vereinfachter Form darzustellen, was naturgemäss in Konflikt mit dem Aussagegehalt eines Beweises steht. Allerdings sind derzeit einzelne Funktionen, denen mit Blick auf die implementierten Sicherheitseigenschaften des kryptografischen Protokolls eine besondere Bedeutung zukommt, nicht mitberücksichtigt. Damit durch den Beweis auf strukturierte Art nachvollzogen werden kann, dass diese Funktionen den versprochenen Nutzen bringen und gleichzeitig keine Schwachstelle ins Protokoll einführen, sollen sie im Beweis mitberücksichtigt werden. Dies gilt insbesondere für folgende Systemelemente:

- Die Stimmen werden vor der Auszählung auf fünf verschiedenen sog. Kontrollkomponenten nach Art. 2 Abs. 1 Bst. d VEleS i.V.m. Ziff. 2 und 3 Anhang VEleS gemischt und entschlüsselt. Jede Kontrollkomponente verändert die Reihenfolge sowie die Verschlüsselung der Stimmen, ohne dabei die Stimmen zu verändern (es wird die Verschlüsselung verändert, nicht der Inhalt der Verschlüsselung). Nach dem Mischen führt jede Kontrollkomponente eine Teilentschlüsselung durch und gibt die gemischten und teilentschlüsselten Stimmen an die nächste Kontrollkomponente weiter. Die ersten vier der insgesamt fünf Kontrollkomponenten befinden sich bei der Post. Der private Schlüssel für die Teilentschlüsselung ist auf ihnen gespeichert. Mit Blick auf die Geheimhaltung

[17] Abrufbar unter www.bk.admin.ch > Politische Rechte > E-Voting > Überprüfung von Systemen.

der privaten Schlüssel gelten die Anforderungen in Ziff. 3 Anhang VEleS, dabei wird auch eine strenge Realisierung des Vieraugenprinzips gefordert. Die fünfte Kontrollkomponente ist in Form eines Laptops des Kantons realisiert, für den ebenfalls Ziff. 3 Anhang VEleS gilt. Allerdings ist der private Schlüssel für die fünfte Teilentschlüsselung und damit die definitive Entschlüsselung der Stimmen nicht auf diesem Laptop gespeichert. Stattdessen wird der private Schlüssel aus einem langen Passwort abgeleitet, das auf zwei Personengruppen beim Kanton aufgeteilt ist. Durch die Aufteilung des Passworts auf zwei Personengruppen wird verhindert, dass die fünfte Teilverschlüsselung de facto ihre Wirkung verliert, wenn eine einzelne Person das für die Entschlüsselung nötige Passwort weitergibt. Die Funktionen, die für die Berechnung des privaten Schlüssels aus den beiden Passwort-Teilen verwendet werden, sollen infolge ihrer Bedeutung für die Sicherheit neu in den Beweisen mitberücksichtigt werden. Insbesondere soll aufgezeigt werden, dass unter den Vertrauensannahmen für den Schutz des Stimmgeheimnisses nach Ziff. 2.7 Anhang VEleS einer der beiden Passwort-Teile allein nicht ausreicht, um die fünfte Teilentschlüsselung vorzunehmen.

- Vor dem Mischen und Teilentschlüsseln überprüft jede Kontrollkomponente, dass sämtliche vorangehenden Kontrollkomponenten die Stimmen korrekt verarbeitet haben. Dazu überprüfen sie erstens mathematische Beweise, die aufzeigen, dass die vorangehenden Kontrollkomponenten beim Mischen und Teilentschlüsseln keine Stimmen verändert haben. Zweitens überprüfen sie, dass die Liste der Stimmen, die die erste Kontrollkomponente gemischt und teilentschlüsselt hat, korrekt ist. Bei den vier oben genannten Kontrollkomponenten bei der Post handelt es sich um die gleichen Maschinen, die aus den übermittelten Stimmen die Prüfcodes in Erfüllung der individuellen Verifizierbarkeit nach Ziff. 2.5 Anhang VEleS generieren und die Stimmen bis zur Auszählung aufbewahren. Ihre Prüfung, ob die erste Kontrollkomponente die korrekten Stimmen gemischt und teilentschlüsselt hat, beinhaltet einen Abgleich mit der eigenen Liste der auszuzählenden Stimmen. Im Fall wo eine Kontrollkomponente eine Inkonsistenz zwischen der eigenen Liste und jener der ersten Kontrollkomponente anzeigt, muss eine Untersuchung stattfinden, die ergibt, wie die Liste auszuzählender Stimmen korrekterweise aussehen müsste. Als Instrument für diese Untersuchung ist ein sog. «Dispute Resolver» spezifiziert. Der kryptografische Sicherheitsbeweis soll neu die allfällige Verwendung des «Dispute Resolvers» berücksichtigen und insbesondere aufzeigen, dass unter den Vertrauensannahmen für die individuelle Verifizierbarkeit nach Ziff. 2.5 Anhang VEleS die korrekte Liste auszuzählender Stimmen gefunden werden kann.

Zusätzlich zu diesen beiden Punkten gibt es weitere Systemelemente, wo geprüft werden soll, ob eine Berücksichtigung in den kryptografischen Sicherheitsbeweisen angezeigt sein könnte oder zumindest eine informelle Begründung, weshalb das nicht der Fall ist (vgl. Ziff. 2.1.3 im Prüfbericht von Haines, Pereira und Teague vom 13.02.2023).

Derzeit bestehen keine konkreten Anhaltspunkte, dass hinter den Unschlüssigkeiten oder den in den Beweisen nicht berücksichtigten Systemelementen Schwachstellen im kryptografischen Protokoll verborgen sind. Die Verbesserungen der Beweise werden weiteren Aufschluss über allfällige Schwachstellen geben und welche Verbesserungen gegebenenfalls nötig sind. Das kryptografische Protokoll wurde auch unabhängig von der Prüfung der Beweise mit Blick auf die Konformität überprüft. Unter Berücksichtigung der Tatsache, dass das Elektorat bis zur Umsetzung der vorliegenden Massnahme eingeschränkt sein wird, darf das Risiko, das mit dem vorläufigen Handlungsbedarf an den kryptografischen Beweisen einhergeht, als hinreichend gering gelten.

Nr.	Massnahme
A.25	**Weitere Verbesserung der Qualität der Spezifikation und der Software**

In den untengenannten Punkten wird Verbesserungsbedarf identifiziert, der laufend und spätestens bis zur Umsetzung von Massnahme A.5 behoben werden soll. Die Liste stützt sich weitgehend auf die Ergebnisse der von der BK in Auftrag gegebenen unabhängigen Überprüfung.

Grundsätzlich sind alle hier oder in den Prüfberichten vorgebrachten Kritikpunkte, die die Qualität der Spezifikation und der Software betreffen, zu adressieren, ausser die Post legt dar, dass sie unberechtigt sind. In Fällen, wo die Post alternative Möglichkeiten für Verbesserungen vorschlägt, die der Zielsetzung hinter einem vorgebrachten Kritikpunkt in gleichem Umfang Rechnung tragen, können Verbesserungen im Sinne der Alternativen umgesetzt werden.

- Die Spezifikationsdokumente sollen klarer zum Ausdruck bringen, wie die durch die Protokollteilnehmer erzeugten und teilweise zwischen ihnen übergebenen Variablen im Verlauf des Protokolls

zu verwenden sind. Namentlich soll klarer ersichtlich sein, mit welchen Variablen die in Pseudocode spezifizierten Algorithmen aufgerufen werden. Zudem wäre es wertvoll, in der Spezifikation Grundsätze für die Prüfung der Gültigkeit der übergebenen Variablen stringenter zu formulieren. Aus den Grundsätzen sollte lückenlos und unmissverständlich hervorgehen, welche Variablen in welchen Fällen gegenüber welcher Grundlage und aus welchem Grund auf Gültigkeit überprüft werden müssen sowie welche Variablen in welchen Fällen verändert werden dürfen und welche nie. Abweichungen von den Grundsätzen sollen klar bezeichnet und begründet werden. Die Grundsätze sollen auch die Verwendung der Context-Variablen regeln, nämlich solche, die während eines Urnengangs unveränderlich sein und bleiben müssen (vgl. auch Ziff. 3.1.2 im Prüfbericht der BFH vom 23.02.2023[18]). Die Gültigkeitsprüfungen und andere Grundsätze, die sich aus der Spezifikation ableiten lassen, sollen im Quellcode in möglichst einheitlicher Form umgesetzt werden und leicht zu finden sein.

- Die Software ist an gewissen Stellen unterspezifiziert, so dass aus den Spezifikationsdokumenten nicht genügend klar hervorgeht, wie die Implementierung im Quellcode oder die betrieblichen Schritte auszugestalten sind. Beispielsweise besteht Klärungsbedarf in Bezug auf minimale Entropie bei der Wahl der Passwörter für die fünfte Teilentschlüsselung (vgl. Massnahme A.24). Das Vorgehen für die Weiterführung des Urnengangs, nachdem dank des «Dispute Resolvers» eine Inkonsistenz aufgelöst werden kann (vgl. Massnahme A.24), ist nicht hinreichend klar. Weitere Beispiele finden sich im Prüfbericht der BFH vom 23.02.2023 in Ziff. 2.4.1 («Election Use Cases»), Ziff. 3.4.1, Ziff. A.4.1 (3. Abschnitt), Ziff. A.4.2 und Ziff. B.4 sowie im Prüfbericht von Haines, Pereira und Teague vom 13.02.2023 in Ziff. 2.2.
- Weitere Erläuterungen zu bewusst gefällten Entscheidungen zur Ausgestaltung des Systems sowie zu allfälligen Risiken, die mit diesen Entscheidungen verbunden sind, können zu einem zielführenden Verbesserungsprozess beitragen und sollen zumindest dort angebracht werden, wo nicht auf gängige Standards, naheliegende Praktiken oder explizit vorgebrachte Empfehlungen zurückgegriffen wird. Vgl. dazu beispielsweise den Prüfbericht von Essex vom 21.11.2022 (Ziff. 5, «Clarify design choice of Bayer-Groth mixnet»), den Prüfbericht von Essex vom 13.02.2023 (Ziff. 2.2, Ziff. 2.3 und Ziff. 2.4), den Prüfbericht von Haines, Pereira und Teague vom 13.02.2023 (Ziff. 3.1) und den Prüfbericht der BFH vom 23.02.2023 (Ziff. 2.2.7, Ziff. 3.1.1, einzelne Punkte in Ziff. A.3.1, Ziff. A.3.2 im 1., 7. und 8. Abschnitt, Ziff. B.3.2 und Ziff. B.3.6). Die Erläuterungen sollen insbesondere auch in die materielle Beschreibung der geplanten Verbesserungen aufgenommen werden (vgl. Hauptteil dieses Dokuments zur vorliegenden Massnahme). Auf dieser Grundlage soll ein Dialog geführt werden können mit Blick auf die Frage, ob die Ausgestaltung des Systems in den einzelnen Punkten sinnvollerweise nicht doch im Sinne eines gängigen Standards, einer naheliegenden Praktik oder einer explizit vorgebrachten Empfehlung erfolgen müsste.
- Präzisierungen in der Notation, die Fehlern oder Missverständnissen entgegenwirken könnten, sollten umgesetzt werden, ebenso sollten auch kleine Fehler behoben werden, vgl. beispielsweise den Prüfbericht von Essex vom 21.11.2022 (Ziff. 5, «Implied modular reduction in subscript» und «Improper quotation marks») sowie den Prüfbericht der BFH vom 23.02.2023 (Ziff. 3.1.5, Ziff. 3.2.2 [«Algorithm 3.1», «Algorithm 3.8», «Algorithm 3.9» und «Algorithm 3.12»], Ziff. 3.2.3 [«Algorithm 4.11» und «Algorithm 4.13»] sowie weitere in Ziff. 3.2.5, Ziff. 3.2.7, Ziff. 3.2.8 und Ziff. 3.3.1).

[18] Abrufbar unter www.bk.admin.ch > Politische Rechte > E-Voting > Überprüfung von Systemen.