Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK

Sektion Politische Rechte

Teilrevision der Verordnung über die politischen Rechte und Totalrevision der Verordnung der BK über die elektronische Stimmabgabe (Neuausrichtung des Versuchsbetriebs)

Erläuternder Bericht zur Vernehmlassung

---

28. April 2021

Inhalt

1. Ausgangslage ... 3

2. Neuausrichtung des Versuchsbetriebs ... 4

2.1 Aufträge des Bundesrates ... 4

2.2 Dialog mit der Wissenschaft ... 4

2.3 Stossrichtungen der Neuausrichtung ... 5

3. Übersicht zur vorliegenden Vernehmlassungsvorlage ... 7

4. Auswirkungen auf Bund, Kantone und weitere Akteure ... 8

5. Erläuterungen zu den einzelnen Bestimmungen ... 9

5.1 Verordnung über die politischen Rechte (VPR) ... 9

5.1.1 Anpassungen in Abschnitt 6a: Versuche mit elektronischer Stimmabgabe ... 9

5.1.2 Anpassungen im 3. Abschnitt und Anhang 3a ... 12

5.2 Verordnung der BK über die elektronische Stimmabgabe (VEleS) ... 13

5.2.1 Hauptteil ... 13

5.2.2 Anhang mit den technischen und administrativen Anforderungen an die elektronische Stimmabgabe ... 21

1. Ausgangslage

Die elektronische Stimmabgabe in der Schweiz befindet sich seit 2004 in einer Versuchsphase und ist Teil der E-Government-Strategie Schweiz von Bund und Kantonen. Die rechtlichen Grundlagen für die Versuche bilden Artikel 8*a* des Bundesgesetzes vom 17. Dezember 1976 über die politischen Rechte (BPR; SR 161.1), die Artikel 27*a*-27*q* 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.

Die Schweizerische Post hat 2019 den Quellcode ihres künftigen Systems mit vollständiger Verifizierbarkeit offengelegt und einen öffentlichen Intrusionstest durchgeführt.[1] Nachdem in ihrem bisher eingesetzten sowie in ihrem künftigen System verschiedene Mängel entdeckt wurden, hat die Post im Juli 2019 kommuniziert, dass das bisherige System mit individueller Verifizierbarkeit nicht mehr eingesetzt wird und sie sich auf die Weiterentwicklung des vollständig verifizierbaren Systems konzentriere. Die Post hat im Januar 2021 in einem ersten Schritt das kryptografische Protokoll ihres vollständig verifizierbaren Systems publiziert, dessen Ausgestaltung auf die Erfüllung der Anforderungen des Bundes an die vollständige Verifizierbarkeit ausgerichtet ist.

Der Kanton Genf hat ein eigenes System entwickelt und betrieben, das von mehreren Kantonen eingesetzt wurde. Im November 2018 hat der Kanton Genf darüber informiert, sein System 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. Im Juni 2019 hat der Kanton Genf kommuniziert, dass er den Betrieb seines bisherigen Systems per sofort einstellt.[2] Der Kanton Genf hat den Quellcode seines noch nicht fertig entwickelten Systems mit vollständiger Verifizierbarkeit 2019 unter Open Source Lizenz publiziert. Die Berner Fachhochschule hat die sicherheitskritischen Elemente des Genfer Systems fertiggestellt und im Herbst 2020 unter Open Source Lizenz zur Verfügung gestellt. Die Ausgestaltung dieses Systems ist ebenfalls auf die Erfüllung der Anforderungen des Bundes an die vollständige Verifizierbarkeit ausgerichtet.

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. 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.

[1] Medienmitteilung der BK vom 29. März 2019; abrufbar unter www.bk.admin.ch > Politische Rechte > E-Voting > Medienmitteilungen.

[2] Medienmitteilungen des Kantons Genf vom 28. November 2018 und 19. Juni 2019; abrufbar unter www.ge.ch/document/point-presse-du-conseil-etat-du-28-novembre-2018#extrait-12897 und www.ge.ch/document/point-presse-du-conseil-etat-du-19-juin-2019.

2. Neuausrichtung des Versuchsbetriebs

2.1 Aufträge des Bundesrates

Gestützt auf die Ergebnisse der Vernehmlassung zur Überführung von E-Voting in den ordentlichen Betrieb hat der Bundesrat am 26. Juni 2019 beschlossen, vorerst auf die Teilrevision des BPR zu verzichten. Mit diesem Entscheid hat er auch den Entwicklungen zu den beiden damals verfügbaren Systemen Rechnung getragen. Gleichzeitig hat er die BK beauftragt, gemeinsam mit den Kantonen eine Neuausrichtung des Versuchsbetriebs von E-Voting zu konzipieren.[3] Der Bundesrat hat dabei folgende Ziele für die Neuausrichtung des Versuchsbetriebs vorgegeben:

1. Weiterentwicklung der Systeme
2. Wirksame Kontrolle und Aufsicht
3. Stärkung der Transparenz und des Vertrauens
4. Stärkere Vernetzung mit der Wissenschaft

Der Steuerungsausschuss Vote électronique (SA VE) hat zur Konzipierung der Neuausrichtung die Unterarbeitsgruppe «Neuausrichtung und Wiederaufnahme der Versuche»[4] eingesetzt und sie mit der Ausarbeitung von Massnahmen für die Neuausrichtung sowie deren Etappierung mit Blick auf die Wiederaufnahme der Versuche beauftragt.

An seiner Sitzung vom 18. Dezember 2020 hat der Bundesrat den Schlussbericht des SA VE vom 30. November 2020 zur Neuausrichtung und Wiederaufnahme der Versuche zur Kenntnis genommen. Er hat die BK beauftragt, die für die Neuausrichtung erforderlichen Massnahmen in Zusammenarbeit mit den Kantonen schrittweise umzusetzen und bis Mitte 2021 eine Vernehmlassungsvorlage mit den notwendigen Anpassungen der Verordnung über die politischen Rechte (VPR) und der Verordnung der BK über die elektronische Stimmabgabe (VEleS) vorzulegen.

Ziel des Bundesrates ist, dass die Kantone wieder begrenzte Versuche mit der elektronischen Stimmabgabe durchführen können. Präzisere Sicherheitsvorgaben, erhöhte Transparenzvorschriften, die engere Zusammenarbeit mit unabhängigen Fachpersonen sowie eine wirksame Überprüfung im Auftrag des Bundes sollen die Sicherheit der elektronischen Stimmabgabe gewährleisten.[5]

2.2 Dialog mit der Wissenschaft

Zur Erarbeitung der Neuausrichtung haben Bund und Kantone mit 23 in- und ausländischen Expertinnen und Experten aus Informatik, Kryptografie und Politikwissenschaften einen breit angelegten Dialog über E-Voting in der Schweiz geführt. Die umfassenden Auswertungen des Dialogs sind publiziert.[6]

Die Expertinnen und Experten sehen Handlungsbedarf bei der Sicherheit, der Transparenz sowie der unabhängigen Überprüfung der Systeme. 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 Verifizierbarkeit und die Diversität unter den Komponenten, die für die Verifizierbarkeit wichtig sind (sog. Kontrollkomponenten und Verifier), bilden für die Expertinnen und Experten eine Grundvoraussetzung für die Vertrauenswürdigkeit eines Systems. Die bereits heute geforderten Sicherheitsbeweise im Bereich der Kryptografie sind wichtig; sie sollen laufend dem aktuellen Stand der Wissenschaft angepasst

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

[4] Die Unterarbeitsgruppe «Neuausrichtung und Wiederaufnahme der Versuche» setzte sich unter der Leitung der BK aus Vertreterinnen und Vertretern der Kantone BE, FR, BS, SG, GR, AG, TG und NE zusammen. Die Post als verbleibende Systemanbieterin war jeweils an den Sitzungen der Unterarbeitsgruppe vertreten.

[5] Medienmitteilung des Bundesrates vom 21. Dezember 2020; abrufbar unter www.bk.admin.ch > Politische Rechte > E-Voting > Medienmitteilungen.

[6] Medienmitteilungen der BK vom 23. Juni 2020 und vom 19. November 2020; abrufbar unter www.bk.admin.ch > Politische Rechte > E-Voting > Medienmitteilungen.

werden. Ferner raten die Expertinnen und Experten den Behörden, auf eine Standardisierung der kryptografischen Bausteine hinzuwirken.

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

Statt wie bisher auf eine Zertifizierung der Systeme zu setzen, sollen die Behörden einen kontinuierlichen Verbesserungsprozess ermöglichen. Die unabhängigen Überprüfungen sollen durch den Bund oder ein unabhängiges Komitee in Auftrag gegeben werden. Durch den Einbezug von unabhängigen Expertinnen und Experten und die Schaffung geeigneter Rahmenbedingungen soll eine wirksame und ständige (öffentliche) Prüfung erreicht werden. Einer öffentlichen Überprüfung wird eine hohe Wichtigkeit beigemessen und Transparenz bildet die Voraussetzung für deren Wirksamkeit. Statt eines öffentlichen Intrusionstests (PIT), wie er 2019 durchgeführt wurde, empfehlen die Expertinnen und Experten Hackathons oder ein ständig laufendes Bug-Bounty-Programm, bei dem finanziell entschädigt wird, wer einen Fehler findet.

Insgesamt hat der Dialog mit Expertinnen und Experten aus verschiedenen Fachgebieten zu einer breiten Diskussion des Handlungsbedarfs und möglicher Lösungen geführt. Die Expertinnen und Experten befürworten eine Weiterführung im Rahmen eines ständigen Austausches zwischen den Behörden und der Wissenschaft, in Zukunft sollten sozialwissenschaftliche Themenbereiche stärker akzentuiert werden. Konkret empfehlen die Expertinnen und Experten, Fragen der Vertrauensbildung weiter zu vertiefen und äusserten 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.

2.3 Stossrichtungen der Neuausrichtung

Im Anschluss an den Dialog mit der Wissenschaft haben Bund und Kantone einen Schlussbericht mit einem umfassenden Massnahmenkatalog erarbeitet. Die Ergebnisse aus dem Dialog flossen bei der Ausarbeitung der Massnahmen ein. Der SA VE hat seinen Schlussbericht zur Neuausrichtung des Versuchsbetriebs und Wiederaufnahme der Versuche am 30. November 2020 verabschiedet.[7]

Mit der Umsetzung zahlreicher Massnahmen soll dem eruierten Handlungsbedarf in den vier durch den Bundesrat vorgegebenen Zielen begegnet werden. Die Umsetzung der Massnahmen soll schrittweise erfolgen. Eine erste Etappe sieht die Umsetzung von Massnahmen für die Wiederaufnahme der Versuche vor. Damit soll die Wiederaufnahme der Versuche in kleinem Umfang möglich sein, während laufend an der Umsetzung der mittel- bis langfristigen Zielsetzungen gearbeitet wird.

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 den Systemanbietern verloren gehen. Sie erlaubt ausserdem allen beteiligten Akteuren, unerlässliche 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. Weitere Massnahmen sind für die Folgejahre vorgesehen. Die Umsetzung der mittel- bis längerfristigen Massnahmen soll nach ersten Schätzungen innert fünf Jahren nach der Wiederaufnahme der Versuche erfolgen.

Die Stossrichtungen der Neuausrichtung und die zeitliche Etappierung der Umsetzung lassen sich wie folgt zusammenfassen:

[7] Der Schlussbericht und die vollständigen Dokumente zum Dialog mit der Wissenschaft sind auf der Webseite der BK publiziert: www.bk.admin.ch > Politische Rechte > E-Voting.

Stossrichtungen	Etappierung der Umsetzung	Abbildung Vernehmlassungsvorlage 2021
1. Weiterentwicklung der Systeme		
Sicherstellung der Qualität des Systems durch präzisere Vorgaben der Qualitätskriterien und nachvollziehbare Entwicklungs- und Bereitstellungsprozesse	Wiederaufnahme der Versuche; kontinuierlicher Verbesserungsprozess	Präzisierung der Anforderungen
Sicherstellung der «forensic readiness» der eingesetzten Systeme durch eine wirksame Erkennung und Untersuchung von Vorfällen	Wiederaufnahme der Versuche; kontinuierlicher Verbesserungsprozess	Präzisierung der Anforderungen
Schaffung eines gemeinsamen, öffentlichen Planungsinstruments von Bund und Kantonen zur laufenden Umsetzung sicherheitsrelevanter Massnahmen	Wiederaufnahme der Versuche; laufende Überprüfung	--
Stärkung der Verifizierbarkeit durch mehr Diversität und Unabhängigkeit einzelner Komponenten	Mittelfristig; Vertiefungen bis 2 Jahre nach Wiederaufnahme der Versuche	--
2. Wirksame Kontrolle und Aufsicht		
Sicherstellung der Wirksamkeit der unabhängigen Überprüfungen des Systems	Wiederaufnahme der Versuche	Anpassung der Verantwortlichkeiten und Präzisierung der Anforderungen
Schaffung eines geregelten Vorgehensprozesses zum Umgang mit erwiesenen und vermuteten Nicht-Konformitäten	Wiederaufnahme der Versuche	--
Verbesserungen im Bereich der Risikobeurteilungen und des Krisenmanagements	Wiederaufnahme der Versuche; kontinuierlicher Verbesserungsprozess	Präzisierung der Anforderungen (Risikobeurteilung)
Weiterentwicklung der Plausibilisierung	Laufend, erste Etappe bis 2022	--
Anpassungen und Überprüfung der Abläufe im Bewilligungsverfahren, sowie der Prozesse, Rollen und Aufgaben	Wiederaufnahme der Versuche und langfristige Überprüfung	Anpassung an die neuen Verantwortlichkeiten
3. Stärkung der Transparenz und des Vertrauens		
Limitierung des Elektorats im Versuchsbetrieb	Wiederaufnahme der Versuche	Anpassung
Mehr Transparenz und Erleichterung des Zugangs zu Systeminformationen, Prüfberichten und Ergebnissen	Laufend	Präzisierung der Anforderungen
Vermehrter Aufbau und Einbezug einer Community von Fachpersonen und der Öffentlichkeit (Politik, Fachkreise, Interessensverbände und breite Öffentlichkeit) für eine ständige öffentliche Überprüfung	Laufend	Präzisierung der Anforderungen
4. Stärkere Vernetzung mit der Wissenschaft		
Kontinuierliche Begleitung durch die Wissenschaft und Einbezug unabhängiger Expertinnen und Experten	Querschnittsthema, Umsetzung laufend	Anpassung
Aufbau eines wissenschaftlichen Ausschusses zur Unterstützung und Beratung von Bund und Kantonen	Mittelfristig	--

3. Übersicht zur vorliegenden Vernehmlassungsvorlage

Mit der vorliegenden Vernehmlassungsvorlage wird eine Teilrevision der VPR und eine Totalrevision der VEleS und ihres Anhangs unterbreitet. Diese Anpassungen stehen in Erfüllung der ersten Etappe der Umsetzung der Massnahmen zur Neuausrichtung des Versuchsbetriebs.

Die wichtigsten Eckpunkte der Vernehmlassungsvorlage:

- **Weiterführung des Versuchsbetriebs:**
  E-Voting soll sich weiterhin in einem Versuchsbetrieb befinden. Bisher sahen die bundesrechtlichen Vorgaben bei der Limitierung des Elektorats drei Abstufungen vor, abhängig vom Entwicklungsstand der Systeme. In der nächsten Phase des Versuchsbetriebs soll die Limitierung auch für den Einsatz von vollständig verifizierbaren Systemen einheitlich auf höchstens 30 Prozent des kantonalen und höchstens 10 Prozent des nationalen Elektorats festgelegt werden. Die Höhe der Limiten wird unter Berücksichtigung der Entwicklungen im Bereich von E-Voting regelmässig überprüft. Die Auslandschweizer Stimmberechtigten werden bei der Berechnung der Limite wie bis anhin nicht mitgezählt (Art. 27*f* Abs. 3 VPR). Neu sollen auch Stimmberechtigte mit einer Behinderung, die ihre Stimme nicht autonom unter Wahrung des Stimmgeheimnisses abgeben können, von den Limiten ausgenommen werden.

- **Stärkung der Sicherheit:**
  In Zukunft soll der Bund nur noch vollständig verifizierbare Systeme zulassen. Dies ist eine wichtige Massnahme zur Gewährleistung der Sicherheit von E-Voting: Die vollständige Verifizierbarkeit erlaubt es, Manipulationen an den elektronisch abgegebenen Stimmen festzustellen. Die Sicherheit der E-Voting-Systeme soll durch präzisere Sicherheits- und Qualitätsvorgaben für die Systeme sowie deren Entwicklung weiter gestärkt werden.

- **Aufteilung der Zuständigkeiten zwischen Bund und Kantonen:**
  Jeder Kanton entscheidet weiterhin selber, ob er E-Voting-Versuche durchführen möchte. Auch die Beschaffung der Systeme bleibt Sache der Kantone und sie können wie bisher ein eigenes System betreiben, das System eines anderen Kantons verwenden oder ein privates Unternehmen beiziehen (Art. 27*k*^{bis} Abs. 1 Bst. b VPR). Der Bund setzt weiterhin den regulatorischen Rahmen und ist für die Bewilligungen zuständig.

- **Unabhängige Überprüfungen:**
  Statt der bisher geforderten Zertifizierung der Systeme und des Betriebs soll neu eine unabhängige Überprüfung im Auftrag des Bundes eine wirksame Prüfung der Sicherheit und damit der Bewilligungsvoraussetzungen gewährleisten sowie für die Zukunft Verbesserungspotential erörtern. Die vorliegende Vernehmlassungsvorlage sieht deshalb vor, dass der Hauptteil der Überprüfungen künftig nicht mehr im Auftrag der Kantone bzw. des Systembetreibers, sondern im Auftrag der BK erfolgen soll.

- **Transparenz, Einbezug der Öffentlichkeit und Zusammenarbeit mit der Wissenschaft:**
  Erhöhte Transparenzvorschriften und ein verstärkter Einbezug von unabhängigen Fachpersonen in die Konzeption, Entwicklung und Prüfung von E-Voting-Systemen sollen dazu beitragen, einen Prozess der kontinuierlichen Verbesserung zu etablieren. Die Öffentlichkeit soll Zugang zu allen Informationen zu System, Betrieb sowie Prüfberichten haben und die Mitwirkung soll gefördert werden. Damit wird das Fundament für eine laufende öffentliche Überprüfung gelegt, wobei auch der Wissenschaft eine wichtige Rolle zukommt. In diesem Rahmen sollen die bestehenden Anforderungen an die Offenlegung des Quellcodes von E-Voting-Systemen präzisiert und die Durchführung eines Bug-Bounty-Programms zur Pflicht werden. Bestandteil eines solchen Programms ist die finanzielle Entschädigung von wertvollen Hinweisen aus der Öffentlichkeit.

4. Auswirkungen auf Bund, Kantone und weitere Akteure

Die Sicherheit ist für die elektronische Stimmabgabe zentral. Dies bleibt für Behörden und Systemanbieter nicht ohne Kostenfolge. Die Finanzierung der Kosten erfolgt gemäss der Aufgabenteilung zwischen Bund und Kantonen im Bereich der politischen Rechte, womit der Hauptteil der Kosten weiterhin bei den Kantonen anfallen wird.

Die Umsetzung der ersten Etappe von Massnahmen im Zeitraum von 2021-2022 verursacht bei den Kantonen gemäss deren Schätzungen zusätzliche Kosten von rund 1.2-1.5 Millionen Schweizer Franken. Die jährlichen Betriebskosten werden sich voraussichtlich um rund 50’000-70'000 Schweizer Franken erhöhen. Für die Umsetzung der mittel- bis längerfristigen Massnahmen werden zusätzliche Kosten von 3.4-4.1 Millionen Schweizer Franken geschätzt. Diese Massnahmen bringen eine Erhöhung der jährlichen Betriebskosten von rund 0.9-1.1 Millionen Schweizer Franken mit sich. Es handelt sich bei den genannten Schätzungen um die Gesamtkosten für alle Kantone.

Der Bund schätzt die in der ersten Etappe einmalig anfallenden Mehrkosten auf rund 1.25 Millionen Schweizer Franken. Diese Kosten fallen im Zeitraum 2021-2022 an und umfassen insbesondere die unabhängigen Überprüfungen von E-Voting-Systemen, die künftig im Auftrag der BK erfolgen sollen. Mittel- bis längerfristig ist mit wiederkehrenden Kosten zu rechnen. Beim Bund führt die Neuausrichtung zu keinem Bedarf nach zusätzlichen personellen Ressourcen.

Die Kosten sind voraussichtlich über längere Zeit von wenigen Kantonen zu tragen. Soll die Einführung von E-Voting langfristig sichergestellt werden, muss sich der Bund im Versuchsbetrieb vermehrt an den Kosten der Kantone beteiligen. Für die Mitfinanzierung von kantonalen E-Voting-Projekten stehen zwei bestehende Instrumente zur Verfügung. Kantonale Projektkosten können über den Umsetzungsplan von E-Government Schweiz resp. der Digitalen Verwaltung Schweiz sowie teilweise gestützt auf das Auslandschweizergesetz (Art. 21 ASG; SR 195.1) und die Auslandschweizerverordnung (Art. 15 V-ASG; SR 195.11) mitfinanziert werden.

Die Massnahmen zur Neuausrichtung wirken sich weiter auf die Schweizerische Post aus, welche derzeit einzige Systemanbieterin ist. Allfällige Kosten, die bei der Post anfallen und die über die oben genannten Kostenschätzungen bei Bund und Kantonen hinausgehen, sind dem Bund nicht bekannt.

5. Erläuterungen zu den einzelnen Bestimmungen

5.1 Verordnung über die politischen Rechte (VPR)

In der VPR umfasst die vorliegende Vernehmlassungsvorlage insbesondere die Anpassungen zur Umsetzung der Neuausrichtung des Versuchsbetriebs der elektronischen Stimmabgabe (Anpassungen in Abschnitt 6*a*, vgl. Kapitel 5.1.1). Zusätzlich enthält die Vernehmlassungsvorlage einige Aktualisierungen des 3. Abschnitts und des Anhangs 3a der VPR (vgl. Kapitel 5.1.2).

5.1.1 Anpassungen in Abschnitt 6*a*: Versuche mit elektronischer Stimmabgabe

Art. 27b Bst. b

Um das Verhältnis zwischen dem Grundbewilligungs- und dem Zulassungsverfahren zu verdeutlichen, wird Buchstabe b mit dem Verweis auf die Erfüllung der Voraussetzungen für die Zulassung ersetzt. Diese Anpassung entspricht der bisherigen Handhabung und hat keine praktischen Auswirkungen.

Art. 27c Abs. 2

Mit der Anpassung von Artikel 27*b* Buchstabe b E-VPR kann diese Bestimmung aufgehoben werden.

Art. 27d Bst. c

In der Grundbewilligung hält der Bundesrat nicht nur fest, für welches Gebiet, sondern auch für welchen Anteil des Elektorats die elektronische Stimmabgabe bewilligt wird. Die Angabe der Anzahl Stimmberechtigter, welche zur elektronischen Stimmabgabe zugelassen werden sollen, benötigt der Bundesrat zur Kontrolle der Einhaltung der Limite gemäss Artikel 27*f* Absatz 1 E-VPR.

Art. 27e Abs. 1-2

Abs. 1 und 1bis: Die Absätze umfassen den bisherigen Absatz 1 mit der Ergänzung, dass die BK die Anforderungen an das System und dessen Betrieb festlegt. Dieser Delegationsinhalt war bisher in Artikel 27*f* VPR enthalten und wird nun hier geregelt.

Abs. 2: Redaktionelle Überarbeitung.

Art. 27f Limiten

Abs. 1: Die bisher vorgesehene Abstufung der Limiten war an die Umsetzung von Sicherheitsanforderungen geknüpft. Für vollständig verifizierbare Systeme hätte der Bundesrat einen unlimitierten Einsatz bewilligen können. Im bisherigen Versuchsbetrieb hat noch kein Kanton die Voraussetzungen erfüllt, um mehr als 30 Prozent des kantonalen Elektorats zuzulassen. Auch die Limite von 10 Prozent des schweizweiten Elektorats wurde bisher nie erreicht.[8] Neu soll die Limitierung auch beim Einsatz von vollständig verifizierbaren Systemen einheitlich auf 30 Prozent des kantonalen und 10 Prozent des nationalen Elektorats festgelegt werden. Mit dieser Limitierung des Elektorats auf der bisher tiefsten Kategorie wird der Versuchscharakter der elektronischen Stimmabgabe unterstrichen.

Die Einhaltung der kantonalen Limite obliegt wie bisher den Kantonen. Es steht den Kantonen frei, wie sie die Einhaltung der Limite für Inlandschweizer Stimmberechtigte sicherstellen. In der Praxis wurde dies bisher beispielsweise mit einem Anmeldeverfahren oder dem Einsatz in Pilotgemeinden umgesetzt. Für die Einhaltung der Limite in Bezug auf den schweizweiten Einsatz ist der Bund zuständig.

Abs. 2: Die Limitierung in Absatz 1 soll für die nächste Phase des Versuchsbetriebs gelten. Den Kantonen soll ermöglicht werden, Erfahrungen mit der Anwendung von vollständig verifizierbaren Systemen zu sammeln, während die Versuche weiterhin begrenzt bleiben. Mit einer regelmässigen Überprüfung der

[8] Am höchsten war das zugelassene Elektorat der Inlandschweizer Stimmberechtigten am Urnengang vom 10. Februar 2019, als knapp 2.5 Prozent zur elektronischen Stimmabgabe zugelassen waren.

Höhe der Limiten kann den Entwicklungen rund um E-Voting Rechnung getragen werden. Bei der Prüfung ist der aktuelle und geplante Einsatz der elektronischen Stimmabgabe in den Kantonen, das politische Umfeld, die Stabilität des Versuchsbetriebs und das Vertrauen der Bevölkerung zu berücksichtigen. Erachtet die BK unter Berücksichtigung dieser Aspekte eine Anpassung der Limiten als angezeigt, stellt sie dem Bundesrat einen entsprechenden Antrag auf Anpassung von Absatz 1.

Abs. 3: Ursprünglicher Absatz 2 mit folgender Anpassung: Neben den Auslandschweizer Stimmberechtigten zählen auch Stimmberechtigte mit einer Behinderung, die ihre Stimme nicht autonom unter Wahrung des Stimmgeheimnisses abgeben können, zu den besonderen Zielgruppen der elektronischen Stimmabgabe. Mit der Ergänzung von Absatz 3 können beide Zielgruppen bei der Berechnung der Limiten ausgenommen werden. Damit haben die Kantone die Möglichkeit, die elektronische Stimmabgabe diesen Zielgruppen anzubieten, ohne dass die Limitierung des Elektorats einen Hinderungsgrund darstellen würde.

Art. 27i Abs. 1 und 2

Die bisherige Formulierung in Artikel 27*i* Absätzen 1 und 2 bezog sich auf die Möglichkeit, entweder nur einen Teil oder das gesamte Elektorat zur elektronischen Stimmabgabe zuzulassen. Da gemäss Artikel 27*f* Absatz 1 E-VPR in der nächsten Versuchsphase die Möglichkeit einer Zulassung des gesamten Elektorats wegfällt, ist die Formulierung anzupassen.

Abs. 1: Die Plausibilisierung der Ergebnisse von Urnengängen mit dem elektronischen Stimmkanal soll Hinweise auf versehentliche Fehler bei der Ergebnisermittlung und auf mögliche Manipulationen der Ergebnisse geben. Wie bisher können die Kantone für die Plausibilisierung verschiedene Methoden anwenden. So können beispielsweise von Kontrolleuren protokolliert abgegebene Stimmen überprüft, die Ergebnisse mit der brieflichen und persönlichen Stimmabgabe an der Urne verglichen oder die ausgezählten elektronischen Stimmen mit den Protokolldateien (Log-Dateien) des Abstimmungs- oder Wahlservers abgeglichen werden. Statistische Methoden sollen – sofern verfügbar und soweit die Datenbasis es zulässt – in den Versuchen zum Einsatz kommen.

Abs. 2: Die Verifizierbarkeit der elektronischen Stimmabgabe ist die zentrale Massnahme zur Gewährleistung der Sicherheit von E-Voting, da sie die Feststellung von Manipulationen an den elektronisch abgegebenen Stimmen erlaubt. Die Verifizierbarkeit sieht vor, dass überprüft werden können muss, ob:

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

Neben der Plausibilisierung nach Absatz 1 sollen in der Schweiz künftig nur noch E-Voting-Systeme zugelassen werden, wenn sie die vollständige Verifizierbarkeit aufweisen, auch wenn nur ein Teil des Elektorats zur elektronischen Stimmabgabe zugelassen wird. Die bestehende Bestimmung wurde zusätzlich sprachlich leicht überarbeitet.

Art. 27k^{bis} Abs. 2

Die Bestimmung kann aufgehoben werden, da die BK im Gegensatz zur früheren Praxis nicht mehr in die vertraglichen Beziehungen involviert ist. Die vertragliche Beziehung zwischen Kantonen und allfälligen privaten Unternehmen ergibt sich aus Absatz 1.

Art. 27l Evaluation der Systeme und der Betriebsmodalitäten

Abs. 1: Übernimmt die bisherige Bestimmung in Absatz 2 und regelt die Auslöser für eine Evaluation.

Abs. 2: Der Prüfgegenstand der Evaluation entspricht der bisherigen Regelung. Die prüfende Stelle muss von der geprüften Stelle unabhängig sein.

Abs. 3 und 4: Die BK regelt in ihrer Verordnung die zu prüfenden Inhalte, die Voraussetzungen, welche die mandatierten Stellen erfüllen müssen, sowie die Zuständigkeiten bei der Mandatierung. Seit der Revision der Rechtsgrundlagen von 2013 wurde die Evaluation von E-Voting-Systemen in den meisten Fällen durch akkreditierte, externe Stellen gefordert. Die Verantwortung lag bei den Kantonen, die geforderte Zertifizierung entweder selbst oder durch den Systembetreiber in Auftrag zu geben und die Nachweise im Bewilligungsverfahren zu erbringen. Im Rahmen der Arbeiten zur Neuausrichtung des Versuchsbetriebs hat sich gezeigt, dass eine Beauftragung der Überprüfungen durch den Bund wünschenswert ist. Künftig soll die Aufgabenteilung zwischen Bund und Kantonen so ausgestaltet werden, dass der Bund mehr Verantwortung und eine direktere Rolle bei der Prüfung der Systeme übernimmt.

Art. 27m Einbezug und Information der Öffentlichkeit

Abs. 1: Zum Einbezug der Öffentlichkeit und von Fachkreisen setzen die BK und die Kantone Massnahmen um, die beispielsweise die Veranstaltung von wissenschaftlichen Tagungen und Konferenzen, die Organisation von Ideenwettbewerben und Hackathons, Betreiben von Informationsplattformen oder die Durchführung von Citizen-Science-Projekten umfassen können. Insbesondere für die Mitwirkung von Fachpersonen aus der Öffentlichkeit sind Anreize zu setzen, wie etwa mit der Durchführung eines Bug-Bounty-Programms durch die Kantone.

Abs. 2: Die Veröffentlichung von Informationen über System und Betrieb der elektronischen Stimmabgabe dient der Nachvollziehbarkeit der Abläufe. Als Adressaten sind sowohl Fachpersonen als auch Personen ohne Fachkenntnisse zu berücksichtigen. Zentrale Massnahme bildet hier die Offenlegung des Quellcodes und der dazugehörigen Dokumentation. Bereits heute verlangen die Artikel 7*a* und 7*b* VEleS von den Kantonen, den Quellcode der Software eines vollständig verifizierbaren Systems für die elektronische Stimmabgabe offenzulegen und hinreichend zu dokumentieren. Aus dem Quellcode lässt sich ersehen, wie die Stimmen vom System registriert und verarbeitet werden sollen. Der Grundsatz der Transparenz ist wichtig und soll nun auf Stufe der VPR verankert werden. Die veröffentlichten Informationen dienen fachkundigen Kreisen dazu, sich einzubringen. Dies soll sich förderlich auf die Sicherheit und die Qualität der Systeme sowie das Vertrauen auswirken. Die Veröffentlichung von Informationen zum System, d.h. namentlich des Quellcodes, und des Betriebs trägt zu einer sachlichen und faktenbasierten Debatte bei. Durch die Verfügbarkeit von Informationen wird der Abhängigkeit von einzelnen Personen und Organisationen entgegengewirkt. Die BK wird die Präzisierung weiterhin in ihrer Verordnung vornehmen.

Abs. 3: Entspricht dem bisherigen Absatz 1 und wurde sprachlich leicht überarbeitet. Wie bisher sollen die Kantone die Stimmberechtigten informieren. Dazu gehören typischerweise Informationen auf dem Stimm- und Wahlmaterial, die den konkreten Ablauf zur elektronischen Stimmabgabe sowie das Vorgehen bei Unregelmässigkeiten oder Problemen erläutert. Zusätzlich wird es als wichtig erachtet, den Stimmberechtigten das Grundkonzept der Verifizierbarkeit näher zu bringen. Denn der Vorgang der Verifizierbarkeit ermöglicht es erst dann Unregelmässigkeiten festzustellen, wenn er durch die Stimmberechtigten auch genutzt wird. Die vollständige Verifizierbarkeit kann nur dann vertrauensfördernd wirken, wenn ihr Nutzen im Kern verstanden wird.

Abs. 4: Entspricht im Grundsatz dem bisherigen Absatz 2. Die Bestimmung wurde präzisiert, indem verdeutlicht wird, dass sich die Möglichkeit der Beobachtung auf Vorgänge bei der Abwicklung eines Urnengangs bezieht (z.B. Prozess der Auszählung, Ver- und Entschlüsselung der Urne). Diese Bestimmung dient weiterhin der Transparenz gegenüber den Stimmberechtigten. Die Bestimmung fordert wie bisher nicht, dass die Kantone eine ständige Vertretung der Stimmberechtigten, zum Beispiel in der Form von Wahlkommissionen, schaffen müssen. Grundsätzlich genügt es, wenn Verfahren und Vorgänge beispielsweise durch ein Wahlbüro bestehend aus Stimmberechtigten, das die zuständige Behörde eingesetzt hat, mitverfolgt werden können. Ausserdem sind nicht *alle* Schritte zugänglich zu machen bzw. *alle* Dokumente zu veröffentlichen. Sprechen gewichtige Gründe gegen einen Zugang bzw. eine Veröffentlichung, kann dies nach wie vor abgelehnt werden. Hier können die Ausnahmebestimmungen der anwendbaren Öffentlichkeitsgesetzgebung herangezogen werden. Der Verweis auf das Öffentlichkeitsgesetz vom 17. Dezember 2004 wird nicht mehr als nötig erachtet und kann gestrichen werden. Im Vordergrund steht die zeitgerechte Abwicklung eines Urnengangs; dies darf aufgrund dieser Bestimmung zu keiner Zeit gefährdet werden.

Abs. 5: Die Kantone sollen neu verpflichtet werden, die Ergebnisse für den elektronischen Stimmkanal zu veröffentlichen. Die Publikation dient primär der Transparenz.

Zu publizieren sind die folgenden Ergebnisse:

- bei Abstimmungen: die Anzahl der elektronisch abgegebenen Ja-, Nein- und Leer-Stimmen.
- bei Wahlen: die Anzahl der elektronisch abgegebenen Stimmen pro Kandidatin oder Kandidat (Kandidatenstimmen) und pro Liste (Listenstimmen).

Grundsätzlich sind die Daten so detailliert wie möglich zu publizieren. Bei Abstimmungen ist eine Publikation mit Angaben pro Gemeinde und bei Wahlen mit Angaben pro Wahlkreis anzustreben. Das Stimmgeheimnis darf durch die Publikation nicht gefährdet werden. Das Stimmgeheimnis wird durch die Publikation gefährdet, wenn beispielsweise nur Auslandschweizer Stimmberechtigte zur elektronischen Stimmabgabe zugelassen sind und in einer Gemeinde nur eine im Ausland lebende Person stimmberechtigt ist. Wird das Stimmgeheimnis durch die Publikation gefährdet, soll in der Regel nicht vom Publikationsgrundsatz abgewichen, sondern alternative Möglichkeiten geprüft werden. Beispielsweise ist zu prüfen, ob und wie eine Publikation mit angepasstem Detaillierungsgrad, wie etwa der Zusammenfassung der Ergebnisse mehrerer Gemeinden, stattfinden kann.

Die Publikation muss nicht im Amtsblatt stattfinden, die Offenlegung auf der Webseite des Kantons genügt. Die Informationen müssen leicht zugänglich und weiterverwertbar sein.

Art. 27o Beizug unabhängiger Fachpersonen und wissenschaftliche Begleitung

Abs. 1: Die Behörden sollen sich bei ihren Arbeiten vermehrt von unabhängigen Fachpersonen begleiten lassen, wo dies einen Mehrwert bietet, beispielsweise indem es den Erkenntnisgewinn zu Fragen der Sicherheit des elektronischen Stimmkanals fördert. Die Fachpersonen sollten vom Systembetreiber und nach Möglichkeit auch von der Behörde unabhängig sein. Der Beizug kann die Mandatierung von Fachpersonen mit konkreten Dienstleistungen oder Beratungen wie beispielsweise die Überprüfung des Systems, die Unterstützung und Beratung bei der Erstellung einer Risikobeurteilung oder die Mitarbeit beim Betrieb – wie beispielsweise bei der Auswertung von Verifizierungsergebnissen und bei allfälligen Folgeuntersuchungen – umfassen.

Abs. 2: Zusätzlich soll die BK die Versuche mit der elektronischen Stimmabgabe wissenschaftlich begleiten lassen. Diese Bestimmung umfasst Forschungsarbeiten durch die Wissenschaft, die – in Abgrenzung zu Absatz 1 – nicht direkt den Arbeiten der Behörden zudienen müssen, die unmittelbar für die Durchführung von Urnengängen nötig sind. Dadurch soll die Entstehung einer Grundlage gefördert werden, die der Auswertung dient und für Verbesserungen am Versuchsbetrieb wegweisend sein kann.

Abs. 3: Entspricht im Wesentlichen dem bisherigen Absatz 2.

5.1.2 Anpassungen im 3. Abschnitt und Anhang 3a

Art. 8a Abs. 1

Die Bestimmung wird redaktionell angepasst. Seit dem 1. November 2015 müssen die Kantone mit Verhältniswahl einen Montag im August des Wahljahres als Wahlanmeldeschluss bestimmen (AS **2015** 543). In Kantonen mit Mehrheitswahl, die eine Wahlanmeldung kennen, wäre ein Wahlanmeldeschluss Anfang September unter Umständen allerdings künftig auch denkbar.

Art. 8d Abs. 3

In der Praxis werden für diese Meldungen keine Telefax mehr verwendet. Die Bestimmung kann daher bereinigt werden.

Anhang 3a und Anhang 3a Rückseite

Diverse Anpassungen infolge der Änderung des BPR vom 26. September 2014 (AS **2015** 543).

5.2 Verordnung der BK über die elektronische Stimmabgabe (VEleS)

5.2.1 Hauptteil

Art. 1 Gegenstand

Die Begriffe werden neu im Hauptteil der VEleS geregelt (vgl. Art. 2 E-VEleS).

Art. 2 Begriffe

Abs.1: Übernimmt im Wesentlichen die Begriffsbestimmungen aus dem bisherigen Anhang zur VEleS, soweit relevant für den Hauptteil.

Erläuterungen zu einzelnen Begriffen:

Bst. a: Zum System gehören auch Komponenten mit speziellen Funktionen, die für die Verifizierbarkeit der elektronischen Stimmabgabe wichtig sind. Dabei handelt es sich um Kontrollkomponenten, Setup-Komponenten, Druckkomponenten und die technischen Hilfsmittel der Prüferinnen und Prüfer.

Bst. b: Nicht zum Online-System gehören Systembestandteile, die zur Vorbereitung und zur Auszählung verwendet werden (wie etwa die Druckerei und die Setup-Komponente).

Bst. c: Mit dem vertrauenswürdigen Systemteil soll sichergestellt werden, dass Fehlfunktionen oder Angriffe auch dann erkannt werden können, wenn nur eine Kontrollkomponente korrekt funktioniert. Darüber hinaus ermöglichen die Kontrollkomponenten eine Verteilung der Informationen, die nötig sind, um die Stimmen zu entschlüsseln. Damit müsste ein Angreifer in alle Kontrollkomponenten einbrechen, um Stimmen lesen zu können. Die Details ergehen aus den Bestimmungen in Anhang Ziffer 2.

Bst. d: Die Anforderungen an die unabhängige Ausgestaltung und den unabhängigen Betrieb befinden sich in Anhang Ziffer 3.

Bst. h: Der Einsatz von Prüferinnen und Prüfern dient der Transparenz. Die Stimmberechtigten sollen davon ausgehen können, dass Prüferinnen und Prüfer im Zweifelsfall auf Unregelmässigkeiten aufmerksam machen würden. Der Einsatz von Prüferinnen und Prüfern im Sinne einer Vertretung der Stimmberechtigten erfüllt Artikel 27*m* Absatz 4 E-VPR (vgl. dazu auch die entsprechenden Erläuterungen). Die konkrete Organisation und Ausgestaltung des Einsatzes von Prüferinnen und Prüfern richtet sich nach kantonalem Recht.

Bst. i: Die Benutzerplattform gehört nicht zur Infrastruktur.

Bst. j: Betrifft insbesondere die Implementierung der folgenden Elemente:

- Generierung der kryptografischen Geheimelemente
- Stimmrechtsprüfung (Prüfung anhand des serverseitigen Authentisierungsmerkmals, ob es sich beim Absender um eine stimmberechtigte Person handelt; dies kann anonym erfolgen)
- Gültigkeitsprüfung
- Registrierung der eingehenden Stimmen
- kryptografisches Mischen der registrierten Stimmen
- Entschlüsselung der Stimmen
- Erstellung der Beweise, die unter Einsatz der Kontrollkomponenten aus der Gewährleistung der individuellen und der universellen Verifizierbarkeit resultieren

Bst. n: In diesem Kontext bezieht sich der vertrauenswürdige Systemteil auf eine Gruppe von Kontrollkomponenten, die zum Online-System gehört.

Bst. p Ziff. 1: Freitextfelder bei Majorzwahlen gelten immer als systemkonform ausgefüllt.

Bst. q: Aufgrund eines clientseitigen Authentisierungsmerkmals erstellt das verwendete technische Hilfsmittel eine Authentisierungsnachricht (beispielsweise die Signatur der Stimme), die an die Infrastruktur geschickt wird; mithilfe der Authentisierungsnachricht und des serverseitigen Authentisierungsmerkmals (beispielsweise ein öffentlicher Schlüssel zur Überprüfung der Signatur) authentisiert die Infrastruktur den

Absender oder die Absenderin einer Stimme als stimmberechtigte Person. Clientseitige Authentisierungsmerkmale sollen schwer zu erraten sein.

Bst. s: Es soll in der Praxis unmöglich sein, eine gültige Authentisierungsnachricht ohne Kenntnis eines clientseitigen Authentisierungsmerkmals zu generieren.

Art. 3 Grundvoraussetzungen für die Zulassung der elektronischen Stimmabgabe pro Urnengang

Einleitungssatz, Bst. a und c: Die Bestimmungen wurden redaktionell überarbeitet. Ausserdem wurde Buchstabe a mit der Verifizierbarkeit ergänzt, die gemäss Artikel 27*i* Absatz 2 E-VPR neu für den Einsatz aller E-Voting-Systeme gefordert wird.

Bst. a: Betrifft insbesondere die Erfüllung der Anforderungen in den Artikeln 4-9 E-VEleS.

Bst. c: Betrifft insbesondere die Erfüllung der Anforderungen in den Artikeln 10-12 E-VEleS.

Bst. d: Ergänzung der bestehenden Bestimmung mit einer neuen Voraussetzung zum öffentlichen Zugang zu Informationen und zum Einbezug der Öffentlichkeit (insbes. nach Art. 27*m* E-VPR und Art. 13 E-VEleS). Diese Ergänzung verdeutlicht die Wichtigkeit der Transparenz und des Einbezugs der Öffentlichkeit bei E-Voting. Die adressatengerechte Aufbereitung der Informationen ergibt sich aus den jeweiligen Zielgruppen, wie namentlich der breiten Öffentlichkeit oder Fachkreisen.

Art. 4 Risikobeurteilung

Abs. 1: Um eine Zulassung zu erhalten, müssen die Kantone wie bisher Beurteilungen für die Risiken in ihrem Verantwortungsbereich erstellen. Sämtliche Risiken, die sich für die Erfüllung der Sicherheitsziele ergeben, müssen über eine Risikobeurteilung bestimmt werden. Ferner müssen auch Risiken beurteilt werden, die das Umfeld der elektronischen Stimmabgabe in Administration und Öffentlichkeit betreffen.

Bei den Risikobeurteilungen sind auch das Vertrauen und die Akzeptanz der Öffentlichkeit in die elektronische Stimmabgabe zu berücksichtigen. Dabei handelt es sich um ein übergreifendes Ziel und muss als Querschnittsthema in Bezug auf alle Sicherheitsziele und Risiken einfliessen. Anwendungsbeispiele:

- Beispiel 1: Um Zweifeln an der Korrektheit der Ergebnisse möglichst zuvorzukommen, wird der Prozess, der definiert, wie vorgegangen wird, wenn die Prüfung des Ergebnisses auf Korrektheit negativ ausfällt, im Detail aufgezeigt und vermittelt.
- Beispiel 2: Um dem Risiko eines materiell unbegründeten Vertrauensverlusts entgegenzuwirken, der aus der Entdeckung eines unerheblichen Mangels im System resultieren könnte, werden für die Beurteilung und die Kommunikation unabhängige Expertinnen und Experten beigezogen.

Die Beurteilung muss gemäss einer Methodik erfolgen, die die Einhaltung folgender Tätigkeiten vorsieht: Risiken identifizieren, Risiken analysieren und Risiken bewerten. Die Details der verwendeten Methodik sowie die vom Kanton vorgegebenen Risikoakzeptanzkriterien müssen dokumentiert werden. Die Risikobeurteilungen sind mindestens jährlich sowie bei wesentlichen Änderungen des Systems zu überarbeiten. Ausserdem ist vor jedem Urnengang zu prüfen, ob sich neue Risiken stellen oder bestehende Risiken erhöht sind.

Die BK kann im Rahmen ihrer Beurteilung der Situation eine eigene Beurteilung der Risiken in ihrem Zuständigkeitsbereich erstellen. Das Vorliegen einer Risikobeurteilung der BK ist keine Zulassungsbedingung, die sich an die Kantone richtet; sie kann jedoch bei der Entscheidung über die Erteilung der Zulassung berücksichtigt werden. Sie wird den Kantonen zur Kenntnisnahme zugestellt, damit diese die Einschätzung der BK einbeziehen können. Die BK zieht die Risikobeurteilungen der Kantone für die eigene Risikobeurteilung bei.

Die BK stellt den Kantonen einen Leitfaden zur Verfügung, nach dem sich die Risikobeurteilungen richten müssen. Alle Risikobeurteilungen müssen die jeweils aktuelle Situation widerspiegeln und neuste Entwicklungen und Erkenntnisse sind fortlaufend in die Beurteilung einzubeziehen.

Abs. 2: Insbesondere beim Beizug eines externen Systems soll der Systembetreiber bzw. Systemhersteller neu eine eigene Risikobeurteilung erstellen. Für weitere Dienstleister mit sicherheitsrelevanten Dienst-

leistungen, wie zum Beispiel Druckereien, Anbieter von technischen Hilfsmitteln für Prüferinnen und Prüfer (Verifier) oder Kontrollkomponenten, muss der Kanton prüfen, ob die Risikobeurteilung allein durch den Kanton vorgenommen werden kann oder ob eine zusätzliche Risikobeurteilung durch den Dienstleister nötig ist. Die Dienstleister erstellen die Risikobeurteilungen zu Handen des Kantons. Dieser berücksichtigt sie für die eigene Risikobeurteilung und reicht sie dem Bund im Rahmen des Bewilligungsverfahrens ein.

Abs. 3: Sprachliche Überarbeitung des Einleitungssatzes und der Sicherheitsziele in Buchstaben a-e. Das bestehende Sicherheitsziel in Buchstabe f wird präzisiert, um den Zweck zu verdeutlichen. Unter dieses Sicherheitsziel fällt beispielsweise das Thema des Stimmenkaufs.

Abs. 4: Entspricht im Wesentlichen dem bisherigen Absatz 2. Die Begründung, dass die Risiken als hinreichend gering eingeschätzt werden, wurde in Absatz 1 aufgenommen.

Die ursprüngliche Bestimmung in Absatz 3 kann gestrichen werden, da die Unterlagen gemäss Artikel 11 E-VEleS umfassend offengelegt werden müssen und diese Bestimmung dadurch an Bedeutung verloren hat.

Art. 5 Anforderungen an die vollständige Verifizierbarkeit

Die vollständige Verifizierbarkeit erlaubt es, systematische Fehlfunktionen im Wahl- bzw. Abstimmungsablauf infolge von Softwarefehlern, menschlichen Fehlleistungen oder vorsätzlichen Manipulationsversuchen unter Wahrung des Stimmgeheimnisses zu erkennen. Dazu gehört zwingend, dass Stimmende einen Beweis erhalten, dass ihre Stimme das System unverändert erreicht hat und nicht – beispielsweise durch ein Schadprogramm auf dem verwendeten Computer – manipuliert wurde. Prüferinnen und Prüfer können unabhängig vom eingesetzten System feststellen, dass sämtliche Stimmen, deren korrekte Abgabe zuvor durch die Stimmenden überprüft werden konnte, auch korrekt – das heisst entsprechend dem Beweis, den die Stimmenden erhalten hatten – ausgezählt wurden. Die Umsetzung der Verifizierbarkeit muss sich auf anerkannte Methoden der Kryptografie abstützen.

Künftig werden nur noch vollständig verifizierbare Systeme zugelassen. Die Anforderungen der bisherigen Artikel 4 und 5 werden mit einigen Überarbeitungen in den Artikeln 5-8 E-VEleS aufgenommen.

Abs. 2: Die individuelle Verifizierbarkeit ermöglicht es den Stimmberechtigten, jegliche missbräuchliche Verwendung ihres Stimmrechts festzustellen. Dies soll möglich sein, auch wenn die Benutzerplattform und der Übertragungsweg nicht vertrauenswürdig sind. Konkret muss a priori von nicht entdeckbaren Viren oder anderen Eingriffen auf der Benutzerplattform oder dem Übertragungsweg ausgegangen werden.

Abs. 3: Die universelle Verifizierbarkeit ermöglicht es, Manipulationen in der Infrastruktur zu entdecken. Die Möglichkeit, universell zu verifizieren, muss im Gegensatz zur individuellen Verifizierbarkeit jedoch nicht zwingend den Stimmberechtigten angeboten werden. Stattdessen können Prüferinnen und Prüfer eingesetzt werden, die von der universellen Verifizierbarkeit Gebrauch machen. Der Prozess der Überprüfung muss beobachtbar sein. Das heisst, dass die Prüferinnen und Prüfer die Bedeutung und die Ergebnisse der einzelnen Handlungsschritte möglichst nachvollziehen können sollen. Dazu müssen sie die Möglichkeit haben, die korrekte Durchführung der Handlungsschritte sowie die Prüfergebnisse bezeugen zu können, beispielsweise indem sie sich an den Ort der Durchführung begeben.

Art. 6 Stichhaltigkeit der Beweise

Kein Beweis kann mit absoluter Sicherheit bestätigen, dass alle Stimmen im Sinne der Anforderungen in Artikel 5 Absätze 2 und 3 korrekt verarbeitet wurden. Beweise müssen demnach unter Berücksichtigung ihrer Stichhaltigkeit interpretiert werden. Artikel 6 regelt minimale Anforderungen an die Stichhaltigkeit, auf die sich Personen, die einen Beweis interpretieren, verlassen dürfen müssen. Eine hohe Stichhaltigkeit entspricht einer tiefen Fälschbarkeit. Präzisierungen sowie zusätzliche Anforderungen an die Stichhaltigkeit befinden sich im Anhang (Ziff. 2.9.1, 2.9.2 und 2.11).

Eine stimmberechtigte Person, die von der individuellen Verifizierbarkeit profitiert, soll sich auf der Grundlage einer brieflich zugestellten Verifizierungsreferenz darauf verlassen können, dass ihre Stimme mit

hoher Wahrscheinlichkeit ihren Bestimmungsort erreicht hat, sofern die Generierung und der Druck der Daten für die Verifizierungsreferenz richtig funktioniert hat und sofern eine von vier Kontrollkomponenten richtig funktioniert (vgl. Erläuterungen zu Anhang Ziff. 2). Wenn die stimmberechtigte Person nicht darauf vertraut, dass diese Voraussetzungen gegeben sind, dann hätte das Ergebnis der Beweisprüfung für diese Person folgerichtig keine oder nur eine beschränkte Bedeutung. Das bedeutet: Der Beweis wäre für diese Person «nicht genügend stichhaltig».

Die korrekte Funktionsweise der Benutzerplattform der stimmberechtigten Personen und der Übertragungsweg müssen für die Stichhaltigkeit des Beweises nach Artikel 5 Absatz 2 Buchstaben a und b nicht vorausgesetzt werden. Das heisst, dass der Beweis auch dann stichhaltig sein muss, wenn eine manipulierte Benutzerplattform oder ein Man-in-the-middle[9] die Stimme unbemerkt manipuliert – dank dem Beweis nach Artikel 5 Absatz 2 können die Stimmberechtigten die Manipulation eben doch bemerken.

Analog zur Stichhaltigkeit der Beweise nach Absatz 3: Der Beweis ist stichhaltig, wenn er den Prüferinnen und Prüfern dazu dient, Manipulationen unter den gegebenen Vertrauensannahmen erkennen zu können. Dadurch kann der Angreifer die Prüferinnen und Prüfer nicht irreführen, indem er mithilfe der nicht vertrauenswürdigen Systemkomponenten einen Beweis zur Rechtfertigung eines manipulierten Ergebnisses anfertigt. Solange die Prüferinnen und Prüfer darauf vertrauen, dass eine von vier Kontrollkomponenten und das von ihnen eingesetzte technische Hilfsmittel zur Prüfung der Beweise (typischerweise ein Laptop) korrekt funktionieren, dann sind die Beweise stichhaltig.

Art. 7 Wahrung des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse

Für die Wahrung des Stimmgeheimnisses und den Ausschluss vorzeitiger Teilergebnisse muss das System so ausgestaltet sein, dass für einen erfolgreichen Angriff nach der Stimmabgabe mindestens drei der vier Kontrollkomponenten unter Kontrolle gebracht werden müssten. Es gelten stärkere Anforderungen für das Online-System, falls dieses von einem privaten Systembetreiber betrieben wird. Präzisierungen befinden sich im Anhang (Ziff. 2.9.3).

Art. 8 Anforderungen an den vertrauenswürdigen Systemteil

Diese Anforderungen dienen dem Ziel, dass ein erfolgreicher unerlaubter Zugriff möglichst keinen Vorteil beim Versuch verschafft, unbemerkt auf eine weitere Kontrollkomponente zuzugreifen.

Art. 9 Zusätzliche Massnahmen zur Risikominimierung

Entspricht mit einigen sprachlichen Anpassungen dem bisherigen Artikel 6 VEIeS.

Art. 10 Anforderungen an die Überprüfung

Um die Wirksamkeit der Überprüfungen und die Unabhängigkeit zwischen der Prüfstelle und der geprüften Stelle zu stärken, wird die Aufgabenteilung zwischen Bund und Kantonen so angepasst, dass der Bund mehr Verantwortung und eine direktere Rolle bei der Überprüfung der Systeme übernimmt. So sollen die Überprüfungen künftig zum grössten Teil durch die BK in Auftrag gegeben werden (Abs. 1). In diesen Bereichen wird auf eine Zertifizierung durch Stellen, die von der Schweizerischen Akkreditierungsstelle (SAS) akkreditiert sind, verzichtet. Der Kanton sorgt weiterhin dafür, dass eine Prüfung in Bezug auf den Betrieb des Systems im Rechenzentrum des Systemanbieters stattfindet (Abs. 2). Die weiterführenden Anforderungen wie Gegenstand, Zuständigkeiten und Zeitpunkte der Prüfungen werden weiterhin im Anhang geregelt (Ziff. 26).

Abs. 1 Bst. b: Anpassung der Bezeichnung; neu: «Software des Systems». Diese Prüfung umfasst die bisherige Prüfung nach Anhang Ziffer 5.2 (Funktionalität) und Ziffer 5.4 (Kontrollkomponenten). Mit der

[9] Bezeichnet den Angreifer in einem Man-in-the-middle-Angriff. Es handelt sich dabei um eine Angriffsform, die in Rechnernetzen ihre Anwendung findet. Der Angreifer steht dabei entweder physikalisch oder – heute meist – logisch zwischen den beiden Kommunikationspartnern und hat dabei mit seinem System vollständige Kontrolle über den Datenverkehr zwischen zwei oder mehreren Netzwerkteilnehmern und kann die Informationen nach Belieben einsehen und sogar manipulieren.

neuen Formulierung wird die Software des gesamten Systems und der Kontrollkomponenten zusammengefasst geprüft.

Abs. 1 Bst. c: Die Anforderungen an die Druckereien werden neu unter der Bestimmung «Sicherheit von Infrastruktur und Betrieb» geprüft.

Abs. 2: Der Betrieb des Systems im Rechenzentrum des Systemanbieters ist nach ISO 27001 zu zertifizieren. Ein Kanton, der selbst kein System betreibt, kann sich für die kantonalen Prozesse nach ISO 27001 zertifizieren lassen, muss dies aber nicht.

Abs. 3: Die BK und die für die Prüfungen nach Absatz 1 mandatierten Stellen müssen Zugang zu den notwendigen Unterlagen beim Kanton und seinen Dienstleistern erhalten. Dazu gehören alle Unterlagen, die für die Prüfungen nach Absatz 1 notwendig sind und alle verfügbaren Berichte (inkl. Zertifizierungsberichte), Belege und Zertifikate (ISO 27001-Zertifikat gemäss Abs. 2 und allfällige kantonale Zertifizierungen).

Abs. 4: Bewilligungsrelevante Prüfergebnisse werden publiziert. Für die Publikation ist diejenige Stelle zuständig, die eine Prüfung in Auftrag gegeben hat. Sie publiziert Belege und Zertifikate, die im Rahmen der Prüfungen nach den Absätzen 1 und 2 erstellt wurden. Unter den Begriff der Belege sind auch Prüfberichte zu subsumieren. Die publizierten Prüfergebnisse müssen nachvollziehbar sein. Wird darin auf weitere Unterlagen verwiesen, sind diese in der Regel offenzulegen. Können zusätzliche Unterlagen nicht veröffentlicht werden, soll die Nachvollziehbarkeit der Prüfergebnisse mit einer zusammenfassenden Beschreibung der relevanten Aspekte aus den nicht publizierten Unterlagen gewährleistet werden. Erstellt die geprüfte Stelle eine Replik auf einen Prüfbericht, soll diese auch publiziert werden. Von einer Publikation kann in begründeten Fällen abgesehen werden. Die Ausnahmen orientieren sich grundsätzlich an der Öffentlichkeits- und Datenschutzgesetzgebung. Dabei ist jeweils zwischen dem öffentlichen Interesse an der Publikation und dem Interesse an der Vertraulichkeit abzuwägen. Zu den Interessen an Vertraulichkeit können etwa interne Richtlinien, Schutz von Geschäftsinterna oder Schutz von Daten Dritter gelten.

Art. 11 Offenlegung des Quellcodes und der Dokumentation zum System und dessen Betrieb

Die bisherigen Anforderungen an die Offenlegung des Quellcodes und der Dokumentation zum System und dessen Betrieb werden präzisiert. Absatz 1 enthält neu eine Liste der Unterlagen, die offengelegt werden müssen. Erläuterungen einiger Begrifflichkeiten:

Abs. 1 Bst. a: Die «relevanten Parameter» umfassen alle Informationen und Daten, die notwendig sind, um das System bei sich in Betrieb zu nehmen.

Abs. 1 Bst. b: Die Dokumentation der Software umfasst insbesondere das kryptografische Protokoll, die Spezifikation und das Design, Anleitungen, Testkonzepte, Berichte zu Mängeln und Korrekturen sowie Ergebnisse des Reviewprozesses.

Abs. 1 Bst. c: Umfasst Dokumente, welche die Inbetriebnahme des Systems zu dessen Untersuchung unterstützen (z.B. Anleitungen, FAQ, etc.).

Abs. 1 Bst. d: Umfasst die Unterlagen, die die Erfüllung der Anforderungen der VEleS dokumentieren. Dazu gehören auch Unterlagen, die wesentliche risikominimierende Massnahmen dokumentieren, auf die in der Risikobeurteilung verwiesen wird. Im Grundsatz gilt: Je stärker die Dokumentation den Betrieb, die Wartung oder die Sicherung einer sogenannten vertrauenswürdigen Komponente oder die Handhabung eines Datenträgers mit kritischen Daten betrifft, desto wichtiger ist die Offenlegung. Darüber hinaus gelten die Ausnahmebestimmungen der Öffentlichkeitsgesetzgebung.

Abs. 1 Bst. e: Wenn dem Systembetreiber ein Mangel im offengelegten Quellcode oder in der Dokumentation bekannt ist, soll er darüber informieren. Er beschreibt den Mangel und allfällige geplante Massnahmen zur Behebung des Mangels. Dies dient der Nachvollziehbarkeit, der Transparenz und der Zusammenarbeit mit der Öffentlichkeit.

Abs. 2 Bst. c: Die begründeten Ausnahmen orientieren sich grundsätzlich an der Öffentlichkeits- und Datenschutzgesetzgebung. Zusätzlich kann bei Dokumenten mit tiefer oder keiner Relevanz für die Sicherheit des Systems und des Betriebs in begründeten Fällen von einer Publikation abgesehen werden.

Dazu gehören etwa Beschriebe von betrieblichen Prozessen ohne direkten Bezug zum System oder reine Präzisierungen, die für die Sicherheit nicht oder wenig entscheidend sind oder bei denen davon ausgegangen werden darf, dass sie korrekt umgesetzt werden. Dabei ist jeweils zwischen dem öffentlichen Interesse an der Publikation und dem Interesse an der Vertraulichkeit abzuwägen. Zu den Interessen an Vertraulichkeit können etwa interne Richtlinien, Schutz von Geschäftsinterna oder Schutz von Daten Dritter gelten.

Art. 12 Modalitäten der Offenlegung

Abs. 1: Die Unterlagen sollen über gängige Plattformen offengelegt werden. Die Organisation der Dateien soll unter Berücksichtigung des Umfangs und der Komplexität der gängigen Praxis entsprechen.

Abs. 2: Die offengelegten Unterlagen müssen anonym beziehbar sein und der Inhaber des Quellcodes darf interessierte Personen nicht zu einer Registrierung aufrufen, um die Unterlagen zu beziehen. Steht einer Person eine finanzielle Entschädigung nach Artikel 13 E-VEleS zu, darf der Inhaber für die zur Überweisung notwendigen Angaben bitten. Eine Offenlegung mindestens sechs Monate vor dem geplanten Einsatz des Systems wird als sinnvoll erachtet, um eine effektive Überprüfung durch die Öffentlichkeit zu ermöglichen.

Abs. 3: Der Austausch mit weiteren Personen und das Zitieren aus offengelegten Informationen muss insbesondere für die Arbeiten von Fachpersonen für die Fehlersuche ermöglicht werden.

Abs. 4: Im Sinne einer «responsible disclosure» kann der Inhaber die Teilnehmenden zur Einhaltung folgender Regeln auffordern:

- Mängel werden dem Inhaber umgehend gemeldet.
- Mit der öffentlichen Bekanntgabe eines Mangels wird zugewartet; eine bestimmte 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 vermutungsweise fähig und gewillt sind und die ebenfalls verantwortungsvoll damit umgehen.

Abs. 5: Der Inhaber darf Verstösse gegen die Nutzungsbedingungen nur in Ausnahmefällen ahnden. Er hat die teilnehmenden Personen in den Nutzungsbedingungen auf die Haftungsbeschränkung oder den Haftungsausschluss hinzuweisen. Auf eine Willenserklärung der Nutzenden ist zu verzichten.

Art. 13 Einbezug der Öffentlichkeit

Mit vorliegendem Artikel werden die Grundsätze eines Bug-Bounty-Programms geregelt, das eine Massnahme in Umsetzung von Artikel 27*m* Absatz 1 E-VPR darstellt. Die Kantone sollen nach Möglichkeit weitere Massnahmen ergreifen, um finanzielle und nicht-finanzielle Anreize zu setzen.

Abs. 1: Grundsätzlich sorgen die Kantone dafür, dass interessierte Personen aus der Öffentlichkeit Hinweise zur Verbesserung des Systems einreichen können (Bug-Bounty-Programm). Das Bug-Bounty-Programm soll frühzeitig vor der Einreichung eines definitiven Gesuchs auf Grundbewilligung des Bundesrates gestartet werden. Rund sechs Monate vor dem geplanten Einsatz werden als sinnvoll erachtet. Das Bug-Bounty-Programm sieht ein ständiges Programm zur Fehlersuche (Bst. a) sowie einen wiederkehrenden Internet-Test (Bst. b) vor.

Abs. 1 Bst. a: Suche von Fehlern in der offengelegten Dokumentation oder dem offengelegten Quellcode und Suche nach Fehlern durch Analyse des lauffähigen Systems in der eigenen Infrastruktur. Dieses Programm zur Fehlersuche läuft ununterbrochen.

Abs. 1 Bst. b: Die Zielsetzung dieses sogenannten Internet-Tests besteht ausschliesslich im Eindringen in die Infrastruktur. Denial-of-Service- (DoS) und Social-Engineering-Angriffe können vom Bug-Bounty-Programm ausgeschlossen werden. Der Internet-Test kann entweder als ständiges Programm oder als wiederkehrender Test mit beschränkter Laufzeit umgesetzt werden.

Die Teilnahme am Bug-Bounty-Programm richtet sich nach den Modalitäten in Artikel 12 E-VEleS.

Abs. 2: Die zu bezeichnende Stelle für die Abwicklung des Bug-Bounty-Programms kann der Systembetreiber oder eine externe Firma sein. Diese Stelle ermöglicht die Durchführung des Programms, nimmt Meldungen entgegen und übernimmt die Kommunikation mit der Person, die den Hinweis eingereicht hat. Sie ist über die Entscheide zum Umgang mit dem Hinweis und allfällige Massnahmen zu informieren.

Ausserdem sind die Informationen zu eingegangenen Hinweisen zu publizieren. Folgende Informationen werden publiziert: Information zum Inhalt des Hinweises, Angabe der Quelle des Hinweises (sofern die hinweisgebende Person oder Institution einverstanden ist), Einschätzung der für das Bug-Bounty-Programm zuständigen Stelle und Informationen zu allfälligen Massnahmen, die gestützt auf den Hinweis getroffen werden.

Abs. 3: Nicht nur Hinweise mit einem direkten, sondern auch mit einem mittelbaren Bezug zur Sicherheit sind zu entschädigen, sofern sie zur Verbesserung des Systems beitragen. Als Hinweise mit mittelbarem Bezug zur Sicherheit gelten beispielsweise Hinweise, mit denen die Qualität des Quellcodes erhöht wird. Denn die Qualität des Quellcodes ist unter anderem entscheidend für die Lesbarkeit und damit auch für die Wahrscheinlichkeit, dass Fehler gefunden werden können. Die Höhe der finanziellen Entschädigung muss aufgrund der Schwere des Mangels festgelegt werden. Die Höhe soll so gewählt werden, dass effektiv Anreize für eine Teilnahme von Fachpersonen aus der Öffentlichkeit entstehen.

Die Rechtsgrundlagen der BK legen lediglich die Rahmenbedingungen für das Bug-Bounty-Programm fest. Die detaillierte Ausgestaltung des Programms, z.B. die Festlegung von Kategorien zur Beurteilung der Schwere der Mängel sowie die Festlegung der Höhe der finanziellen Entschädigungen, obliegt den Kantonen bzw. dem Systembetreiber. Der Bund überprüft im Rahmen der Bewilligungsverfahren, inwiefern die Ziele des Bug-Bounty-Programms durch das von den Kantonen und der zuständigen Stelle nach Absatz 2 gewählte Vorgehen erreicht wurden.

Art. 14 Grundsätze der Verteilung von Aufgaben und Verantwortlichkeiten

Die Aufgaben und Verantwortlichkeiten wurden bisher im Anhang geregelt. Neu wird die Aufteilung der Aufgaben und Verantwortlichkeiten im Hauptteil der VEleS geregelt.

Abs. 1: Die wichtigen Aufgaben, die durch den Kanton auszuführen sind, ergeben sich aus den Bestimmungen im Anhang. Dazu gehören etwa die Ausgestaltung des Stimmmaterials und die Kommunikation mit den Stimmberechtigten zu Fragestellungen, die mit der Stimmabgabe im konkreten Fall in Verbindung stehen.

Abs. 2: Der Kanton kann die genannten Aufgaben an externe Organisationen delegieren. Dabei trägt er aber weiterhin die Gesamtverantwortung nach Absatz 1. So trägt er beispielsweise die Risiken, die im Zusammenhang mit der Durchführung einer Aufgabe stehen, auch bei einer Delegation vollumfänglich. Als Ausnahme zu Absatz 1 kann die Kommunikation zu Fragen der Funktionsweise des Systems delegiert werden, sofern diese Fragen sehr technischer Natur sind und vertieftes Expertenwissen voraussetzen.

Abs. 3: Die Betriebsstellen handeln auf Weisung des Kantons und übernehmen die Verantwortung für ihre Zuständigkeiten gegenüber dem Kanton.

Abs. 4: Die konkrete Organisation und Ausgestaltung des Einsatzes von Prüferinnen und Prüfern richtet sich nach kantonalem Recht.

Art. 15 Aufgaben der auf kantonaler Ebene verantwortlichen Stelle

Die Aufgaben der auf kantonaler Ebene verantwortlichen Stelle wurden bisher im Anhang geregelt. Neu werden die Aufgaben im Hauptteil der VEleS geregelt.

Bst. a: Die übergeordnete Informationssicherheitsrichtlinie definiert die Ziele, den Rahmen und die Verantwortlichkeiten für die Informationssicherheit. Sie stellt auch einen Katalog von Richtlinien für die Informationssicherheit auf unterer Ebene bereit und legt deren Verwaltung fest. Sie wird allen Mitarbeitenden kommuniziert und muss in geplanten Zeitintervallen überprüft und angepasst werden.

Bst. b: Die Informationsklassifizierungs- und Verarbeitungsrichtlinie definiert einen verbindlichen Sicherheitsrahmen für den gesamten Betrieb des Systems. Sie wird den betroffenen Mitarbeitenden kommuniziert und muss in geplanten Zeitintervallen überprüft und angepasst werden.

Bst. c: Die Risikomanagementrichtlinie definiert insbesondere den Geltungsbereich und die Grenzen für das Management von Informationssicherheitsrisiken, die Organisation des Risikomanagements, die Risikoakzeptanzkriterien und die Methode für die Durchführung der Risikobeurteilung. Sie muss in geplanten Zeitintervallen überprüft und angepasst werden.

Bst. d: Beispiele für Massnahmen: Durchführung der Risikobeurteilung, Überprüfung der Einhaltung von Informationssicherheitsrichtlinien, Überarbeitung von Informationssicherheitsrichtlinien, Bereitstellung von geeigneten Werkzeugen.

Bst. f: Als «kritische Handlungen und Operationen» gelten insbesondere die Vorbereitung des Urnengangs (Anhang Ziff. 5), das Öffnen und Schliessen des elektronischen Stimmkanals (Anhang Ziff. 9), die Auszählung der elektronischen Urne (Anhang Ziff. 11) und die Vernichtung der Daten nach der Erwahrung der Abstimmungs- und Wahlergebnisse (Anhang Ziff. 12.9).

Bst. g: Die konkrete Organisation und Ausgestaltung des Einsatzes von Prüferinnen und Prüfern richtet sich nach kantonalem Recht. Zur Instruktion der Prüferinnen und Prüfer gehört neben einer Ausbildung auch die Durchführung von Übungen.

Bst. h: Mit weiteren Indikatoren sind gemäss Anhang Ziffer 11.10 insbesondere auch die Zahl und die Art von Anomalien, die durch Stimmberechtigte beim Kanton gemeldet wurden, den Prüferinnen und Prüfern zu unterbreiten.

Art. 16 Belege zu den Gesuchen

Abs. 1: Mit der Anpassung von Artikel 27*b* Bst. b. E-VPR werden hier nur noch die Belege für das Gesuch um Zulassung geregelt. Die genauen Fristen und weitere Details werden durch die BK jeweils in einem separaten Dokument festgelegt. Die Liste der Belege wurde so angepasst, dass die neuen Bestimmungen der VEleS abgebildet werden. Ausserdem wurde die Liste in der bisherigen Ziffer 6 des Anhangs zur VEleS hier aufgenommen, damit nur noch eine Liste mit Belegen geführt wird.

Abs. 1 Bst. a: Anpassung an die neuen Zuständigkeiten bei der Überprüfung nach Artikel 10.

Abs. 1 Bst. b: Anpassung der bisherigen Bestimmung zu den Risikobeurteilungen gemäss Artikel 4 E-VEleS. Der Kanton verpflichtet sich, auf Veränderungen in der Einschätzung von Risiken umgehend hinzuweisen.

Abs. 1 Bst. c: Der Kanton reicht Belege ein, um zu bestätigen, dass die Unterlagen nach Artikel 11 E-VEleS offengelegt wurden. Dabei informiert er die BK über die Zeitpunkte, an denen die Unterlagen offengelegt wurden. Er reicht ausserdem Informationen zu den Hinweisen aus der Öffentlichkeit ein. Dazu gehört eine Auflistung der eingegangenen Hinweise, die jeweilige Beurteilung durch den Kanton oder die zuständige Stelle, die Höhe der ausgerichteten finanziellen Entschädigungen und eine Beschreibung der Massnahmen, die gestützt auf diese Hinweise getroffen wurden.

Abs. 1 Bst. d: Übernahme der bisherigen Ziffer 6.3 des Anhangs zur VEleS. Der Kanton reicht weitere Testprotokolle nach, falls ein Test erst kurz vor dem Urnengang durchgeführt wird. Bestehen Mängel im System, von denen der Kanton oder der Systembetreiber Kenntnis haben, ist die BK auf die Mängel, deren Auswirkungen und geplante Massnahmen hinzuweisen.

Abs. 2: Der Kanton kann über mehrere Urnengänge hinaus die Gültigkeit von Prüfergebnissen oder Belegen geltend machen. In diesem Fall begründet der Kanton, weshalb hinsichtlich des aktuellen Urnengangs keine Wiederholung der entsprechenden Prüfung notwendig ist. Dazu gibt er sämtliche vorgenommenen und geplanten Änderungen am System oder an den Betriebs- und Wartungsprozessen bis zum Zeitpunkt des Urnengangs an. Er zeigt dadurch auf, dass es sich um geringfügige Anpassungen handelt, die keinen negativen Einfluss auf die Risikobeurteilung haben. Der Begriff «gültig» ist im engeren Sinne der Gültigkeit (beispielsweise die Gültigkeit eines Zertifikats) sowie im weiteren Sinne zu verstehen (Unterlagen, die nicht angepasst wurden und nicht angepasst werden müssen, weil sich beispielsweise die Ausgestaltung des Systems, der Stand der wissenschaftlichen Erkenntnisse oder die Rechtsgrundlagen

nicht geändert haben). Bei Verweisen muss begründet und bestätigt werden, dass die Unterlagen weiterhin gültig sind.

Art. 17 Weitere Bestimmungen

Abs. 2: In Ausnahmefällen kann ein Kanton von der Umsetzung einzelner Anforderungen befreit werden. Diese Option ist an die drei Bedingungen unter Bst. a-c geknüpft. Insbesondere muss eine nachvollziehbare Begründung für den Ausnahmefall vorliegen. Beispiel für eine Ausnahme: bei Wahlen nach Majorzverfahren (Mehrheitswahlsystem) kann von der Anforderung der individuellen Verifizierbarkeit abgesehen werden, wenn die Stimme durch die Eingabe eines Namens in ein Freitextfeld abgegeben wird.

5.2.2 Anhang mit den technischen und administrativen Anforderungen an die elektronische Stimmabgabe

Allgemeine Bemerkungen

Der Verweis auf das Schutzprofil des Bundesamts für Sicherheit in der Informationstechnik (BSI Deutschland, bisherige Ziff. 3.15) wurde gestrichen, da es vom BSI nicht mehr gewartet wird und archiviert wurde. Die relevanten Anforderungen aus dem Schutzprofil wurden punktuell in bestehenden Anforderungen oder durch neue Anforderungen aufgenommen.

Erläuterungen zu ausgewählten Bestimmungen

Ziff. 1 Begriffsbestimmungen

Ziff. 1.5: Die stimmende Person vergleicht die Codes, die am Bildschirm angezeigt werden, mit den Codes in der Verifizierungsreferenz.

Ziff. 1.6: Daten, die es erlauben herauszufinden, ob die Stimmberechtigten eine Stimme abgegeben haben, fallen nicht unter den vorliegenden Geltungsbereich.

Ziff. 2 Anforderungen an das kryptografische Protokoll für die vollständige Verifizierbarkeit (Art. 5)

Elektronische Stimmen reisen von der Abgabe bis zur Auszählung von den Benutzerplattformen durch das Internet und über zahlreiche Server des Systemanbieters zum Kanton. Die einzelnen Elemente der genutzten Infrastruktur sind zahlreich und lassen sich nur schwer kontrollieren. Kryptografische Protokolle erlauben es, die Zahl der Elemente, die ein Angreifer unter Kontrolle bringen müsste, um unbemerkt Stimmen zu verändern oder das Stimmgeheimnis zu brechen, auf ein Minimum zu reduzieren. Massnahmen zur Verhinderung, dass ein Angreifer ein Element unter seine Kontrolle bringen kann, können damit zielgerichtet auf jene beschränkte Zahl von Elementen fokussiert werden. Bei diesen Elementen handelt es sich demnach um besonders schützenswerte Elemente, die sich, im Idealfall, auch besonders gut und überzeugend schützen lassen.

Solche Elemente – sie befinden sich unter den in Ziffern 2.1 und 2.2 aufgeführten Systemteilnehmenden und Kommunikationskanälen – werden als «vertrauenswürdig» bezeichnet. Das mag auf den ersten Blick erstaunen: Warum wird ein Element, das besonders schützenswert ist, ausgerechnet als «vertrauenswürdig» bezeichnet? Der Ursprung liegt darin, dass kryptografische Protokolle sich nicht auf den Schutz jener Elemente richten. Die Bezeichnung als «vertrauenswürdig» signalisiert Autorinnen und Autoren sowie Leserinnen und Lesern des Dokuments, in dem das kryptografische Protokoll spezifiziert ist, dass sie sich keine Gedanken über mögliche Angriffe machen müssen, bei denen ein Angreifer diese Elemente unter Kontrolle bringt. Indem Systemteilnehmende vertrauenswürdig sind, weigern sie sich, mit einem Angreifer zusammenzuarbeiten. Das Protokoll muss so definiert sein, dass – solange sich die vertrauenswürdigen Systemteilnehmenden an das Protokoll halten – der Angreifer auch dann keinen Erfolg haben, wenn er die übrigen, nicht vertrauenswürdigen Systemteilnehmenden unter Kontrolle bringt. Die Verwendung des Begriffs stützt sich auf die Fachliteratur.

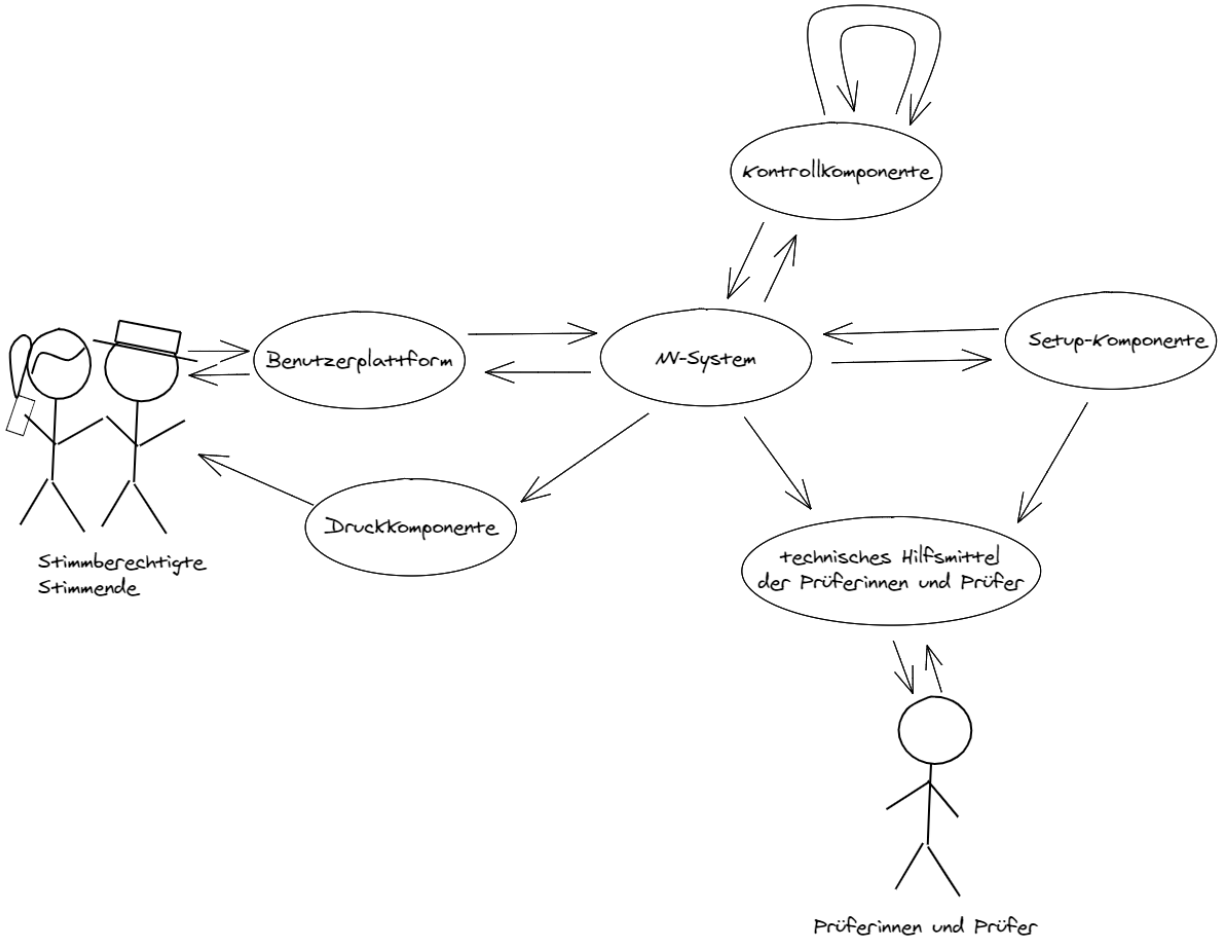
Das kryptografische Protokoll besteht aus abstrakten, in mathematischer Sprache abgefassten Anweisungen an alle Systemteilnehmenden, welche Berechnungen sie beim Erhalt welcher Nachrichten vornehmen, welche Daten sie abspeichern und welche Nachrichten sie über welche Kanäle verschicken müssen. Das Protokoll ist dann konform mit der VEleS, wenn der Angreifer nach Ziffer 2.3 trotz seiner Kontrolle über die nicht vertrauenswürdigen Systemteilnehmenden und Kommunikationskanäle nach Ziffern 2.1, 2.2 und 2.9 die Ziele in Ziffern 2.5-2.8 unter den Bedingungen in Ziffern 2.11 und 2.12 nicht erreichen kann. Dabei müssen nach Ziffer 2.13 sichere kryptografische Bausteine (beispielsweise Verschlüsselungsalgorithmen) eingesetzt werden und die Handlungsanweisungen an die Systemteilnehmenden müssen klar und dürfen nicht unterspezifiziert sein. Nach Ziffer 2.14 werden mathematische Beweise über die Konformität des Protokolls gefordert, wie dies in der wissenschaftlichen Praxis üblich ist.

Das kryptografische Protokoll ist die Grundlage für die Systementwicklung. Es kann nur dann seine Wirkung entfalten, wenn die Handlungsanweisungen der vertrauenswürdigen Elemente als Software korrekt umgesetzt werden und die Komponenten, auf denen die Software läuft, hinreichend geschützt sind. Die VEleS enthält entsprechende Anforderungen. Vgl. dazu auch die Erläuterungen zu Ziffern 2.3 und 2.4.

Ziff. 2.1:

- Stimmberechtigte / stimmende Person: Stimmberechtigte erhalten vom Kanton oder von der Druckerei vorgängig zum Urnengang ihre vertraulichen clientseitigen Authentisierungsmerkmale sowie die Verifizierungsreferenz brieflich zugestellt. Um eine Stimme abzuschicken, geben sie ihre clientseitigen Authentisierungsmerkmale und ihre Stimme in die Benutzerplattform ein. Um von der individuellen Verifizierbarkeit nach Artikel 5 i.V.m. Ziffer 2.5 Gebrauch zu machen, prüfen sie anhand der Verifizierungsreferenz die Beweise, die die Benutzerplattform ihnen anzeigt.
- Benutzerplattform: Die Benutzerplattform erstellt die Authentisierungsnachrichten und schickt sie zusammen mit der verschlüsselten Stimme und anderen Nachrichten, die für die Gewährleistung der Verifizierbarkeit nötig sind, an das NV-System. Dazu verwendet sie die Software inklusive öffentlicher Parameter, die sie vorgängig vom NV-System erhalten hat. Sie zeigt der stimmenden Person Nachrichten des NV-Systems an, wie beispielsweise die Beweise nach Ziffer 2.5.
- Nicht vertrauenswürdiges System (NV-System): Das NV-System dient als Knotenpunkt für die Kommunikation zwischen den übrigen Systemteilnehmenden. Es muss in Bezug auf alle Anforderungen an das kryptografische Protokoll als nicht vertrauenswürdig gelten (vgl. Ziff. 2.9).
- Setup-Komponente: Die Setup-Komponente wird in der Infrastruktur des Kantons betrieben (vgl. Ziff. 3.1). Mit Hilfe der Setup-Komponente bereitet der Kanton Daten für die Durchführung des Urnengangs auf. Dazu gehören insbesondere Daten, deren Zufälligkeit und Vertraulichkeit für die Erreichung der Anforderungen an das kryptografische Protokoll nach Ziffern 2.5, 2.7 und 2.8 massgeblich sind, wie beispielsweise die Verifizierungsreferenz der Stimmberechtigten. Auch dieser abstrakte Begriff kann mehrere technische Hilfsmittel wie Laptops und Datenträger umfassen.
- Eine oder mehrere Gruppen von Kontrollkomponenten: Die Kontrollkomponenten interagieren mit den übrigen Kontrollkomponenten ihrer Gruppe so, dass die Anforderungen an das kryptografische Protokoll nach Ziffern 2.5, 2.6 und 2.7 auch das erfüllt sein müssen, wenn nur eine von ihnen vertrauenswürdig ist und damit korrekt funktioniert.
- Druckkomponente: Sie druckt die Verifizierungsreferenz zuhanden der Stimmberechtigten. Der abstrakte Begriff umfasst die Verpackung und den Versand an die Stimmberechtigten. Darüber hinaus umfasst er alle technischen Hilfsmittel, die beim Druck verwendet werden. Der Begriff kann damit – nebst der Druckmaschine selbst – auch einen Laptop zur Entschlüsselung der Druckdaten sowie einen USB-Stick zur Aufbewahrung der verschlüsselten Daten umfassen.
- Prüferinnen und Prüfer: Die Prüferinnen und Prüfer erhalten nach der Auszählung vom NV-System einen Beweis nach Ziffer 2.6, der die korrekte Ergebnisermittlung bestätigt. Sie führen die Prüfung mindestens einmal mit einem technischen Hilfsmittel durch. Sie können auch während der Setup-Phase mit ihrem technischen Hilfsmittel allfällige Prüfaufgaben der Setup-Komponente übernehmen.
- Technisches Hilfsmittel der Prüferinnen und Prüfer: Die Prüferinnen und Prüfer benötigen zur Beurteilung des Beweises nach Ziffer 2.6 ein technisches Hilfsmittel.

Ziff. 2.2:



Ziff. 2.3: Für die Anforderungen an das kryptografische Protokoll wird nicht zwischen Angreifern mit unterschiedlichen Ressourcen oder Fachkenntnissen unterschieden: Ob ein Angreifer Systemteilnehmende via Drohung, Hacking oder Social Engineering unter Kontrolle bringt, ist für die Definition des kryptografischen Protokolls unerheblich. Vielmehr gehört es zur Voraussetzung, dass der Angreifer die nicht vertrauenswürdigen Systemteilnehmenden und Kommunikationskanäle unter seine Kontrolle gebracht hat. Das kryptografische Protokoll muss so definiert werden, dass der Angreifer trotz der erfolgreichen Angriffe auf solche Systemteilnehmende und Kommunikationskanäle keinen Schaden hervorrufen kann. Eine implizite Voraussetzung dazu bildet die Annahme, dass der Angreifer nicht fähig ist, die kryptografischen Bausteine und deren Implementierung im Quellcode zu brechen. Die Anforderungen in Ziffer 2.13 und 2.14 sowie Anforderungen zugunsten der Qualität bei der Softwareentwicklung nach Ziffern 24 und 25 sind auf dieses Ziel gerichtet.

Ziff. 2.4: Wenn der Angreifer alle Systemteilnehmenden kontrollieren könnte, wäre niemand mehr übrig, der sich dafür interessieren würde, ob Manipulationen stattgefunden haben. Es liegt in der Natur von Wahlen und Abstimmungen, dass ein grosser Anteil der Stimmberechtigten sich dafür interessiert, ob ihre Stimme richtig angekommen ist. Diese Stimmberechtigten können nicht vom Angreifer kontrolliert werden. Sie werden deshalb als vertrauenswürdig bezeichnet. Ähnlich dürfen einzelne Prüferinnen und Prüfer als vertrauenswürdig gelten. Auch sie kann der Angreifer nicht unter seine Kontrolle bringen. Da Stimmberechtigte sowie Prüferinnen und Prüfer mit technischen Hilfsmitteln arbeiten, müssen auch einige dieser technischen Hilfsmittel als vertrauenswürdig gelten dürfen – ansonsten könnte der Angreifer die vertrauenswürdigen Personen leicht in die Irre führen, indem er alle Hilfsmittel unter Kontrolle bringt, namentlich auch jene, die die Prüferinnen und Prüfer für ihre Arbeit verwenden. Indem lediglich technische Hilfsmittel, die sich in der Praxis besonders effektiv schützen lassen, als vertrauenswürdige Systemteilnehmende zugelassen werden, hat es ein Angreifer besonders schwer, unbemerkt Manipulationen vorzunehmen oder das Stimmgeheimnis zu brechen. Besonders effektiv schützen lassen sich technische

Hilfsmittel, die nicht mit einem Netzwerk verbunden sein müssen. Zudem lässt es sich vermeiden, einzelnen technischen Hilfsmitteln vertrauen zu müssen, indem ihre Funktion durch mehrere technische Hilfsmittel wahrgenommen werden. Um dadurch einen Mehrwert zu erhalten, muss das kryptografische Protokoll so definiert sein, dass der Angreifer keinen Schaden anrichten kann, solange er eines dieser Hilfsmittel nicht unter Kontrolle bringen kann. Dies lehnt sich an die Logik an, dass nicht alle Prüferinnen und Prüfer vertrauenswürdig sein müssen; es reicht, wenn ein Prüfer oder eine Prüferin auf einen entdeckten Mangel hinweist. Die entsprechende Aufteilung von Verantwortungen lässt sich in den Gruppen von Kontrollkomponenten erkennen: Ein Angreifer müsste alle Kontrollkomponenten unter seine Kontrolle bringen, um einen Schaden anrichten zu können. Dies ist aber besonders schwierig, wenn sich die Kontrollkomponenten punkto Software und Betriebsmodalitäten unterscheiden.

Die zulässigen Annahmen über die Vertrauenswürdigkeit der einzelnen Systemteilnehmenden und Kommunikationskanäle sind in Ziffer 2.9 aufgeführt.

Die Anforderungen an den Betrieb von vertrauenswürdigen Komponenten sind in Ziffer 3 wiedergegeben.

Eine Nachricht wird an dieser Stelle als authentisch bezeichnet, wenn der Nachrichtenempfänger darauf vertrauen darf, dass die Absenderin oder der Absender jenem Systemteilnehmenden entspricht, der durch die Definition des Kanals vorgegeben ist.

Ziff. 2.5: Die Beweise können ihre Wirksamkeit nur dann entfalten, wenn die Stimmenden die Beweise tatsächlich prüfen und sie sich im Zweifelsfall an die zuständige Behörde wenden. In welchem Umfang sie dies tun und welche Massnahmen dazu beitragen könnten, dass Stimmende die Beweise gemäss den Instruktionen prüfen, könnte Gegenstand der Forschung und der wissenschaftlichen Begleitung bilden. Einige Anforderungen der VEleS könnten dazu beitragen, dass sich die Beweise als wirksames Instrument erweisen: So soll die Aufteilung der Beweise in Teilbeweise nach Ziffern 2.12.5-2.12.10 es den Stimmenden erlauben, die Stimmabgabe vorzeitig abzubrechen und die Stimme brieflich oder persönlich abzugeben, wenn sie bei der Prüfung Schwierigkeiten haben. Im Gegensatz zu den vorgängigen Teilbeweisen muss die Prüfung des Teilbeweises, der die definitive Stimmabgabe bestätigt, besonders leicht durchzuführen sein. Die Anforderung in Ziffer 8.10 soll Social-Engineering-Angriffe erschweren, die zum Ziel haben, die Stimmenden von der korrekten Durchführung der Prüfung der Beweise abzuhalten. Darüber hinaus gelten mit Ziffer 8 weitere Anforderungen für die Information und Hilfestellungen an die Adresse der Stimmberechtigten. Social-Engineering-Angriffe müssen bei der Risikobeurteilung nach Ziffer 13 beurteilt werden.

Ein korrekter Beweis bestätigt den Stimmenden, dass mindestens die Kontrollkomponente, die nach Ziffer 2.9.1 als vertrauenswürdig gelten darf, die Stimme als systemkonform abgegeben registriert hat. Die Prüferinnen und Prüfer stellen durch die Prüfung des Beweises nach Ziffer 2.6 fest, dass die Stimme auch korrekt und damit im Sinne des Beweises nach Ziffer 2.5, der den Stimmenden angezeigt worden war, gezählt wurde. Als Bedingung für die erfolgreiche Prüfung des Beweises nach Ziffer 2.6 müssen alle Kontrollkomponenten dieselben Stimmen als systemkonform abgegeben registriert haben. Fälle, wo die Kontrollkomponenten diesbezüglich Inkonsistenzen aufweisen, müssen nach Ziffer 11.11 antizipiert und das Vorgehen vorgängig festgelegt werden.

Die Bestimmung schreibt nicht vor, wie Fälle zu interpretieren sind, wo ein Beweis falsch oder gar nicht angezeigt wird. Namentlich wäre es nicht unzulässig, wenn die Gruppe von Kontrollkomponenten eine Stimme als systemkonform registriert, obwohl sie nicht systemkonform abgegeben wurde. Allerdings folgt aus Ziffer 2.6, dass solche Stimmen später aussortiert werden müssen, damit die Prüferinnen und Prüfer feststellen können, dass der Angreifer keine nicht systemkonform abgegebenen Stimmen eingefügt hat. Darüber hinaus muss das NV-System (nicht zwingend die Gruppe von Kontrollkomponenten) nach Ziffer 10 solche Stimmen noch bei der Stimmabgabe entdecken und darf sie nicht als systemkonform abgegebene Stimmen behandeln.

Zu «…der Angreifer nicht im Namen der stimmberechtigten Person missbräuchlich eine Stimme abgegeben hat, die in der Folge als systemkonform abgegebene Stimme registriert und gezählt worden ist»: Ein solcher Beweis wäre während dem Urnengang nur bedingt nützlich, da der Angreifer weiterhin Zeit hätte, eine Stimme abzugeben. Deshalb reicht es, wenn Stimmberechtigte diesen Beweis nach dem Urnengang anfordern können. Aus Effizienzgründen reicht es, wenn die zuständige Stelle beim Kanton der stimmberechtigten Person bestätigt, dass keine Stimme in deren Namen abgegeben wurde. Für die Prüfung durch

die zuständige Stelle gelten die Vertrauensannahmen nach Ziffer 2.9.1, wobei das Hilfsmittel der Prüferinnen und Prüfer ebenfalls als vertrauenswürdig gelten darf. Ferner: Die Anforderung sprengt das Vertrauensmodell, insofern als der Angreifer überhaupt nicht auf die clientseitigen Authentisierungsmerkmale herankommen können darf. Mit Blick auf die vorliegende Anforderung muss die Annahme getroffen werden, dass der Angreifer Zugriff auf die clientseitigen Authentifizierungsmerkmale einzelner Stimmberechtigter hat.

Ziff. 2.6: Eine Stimme gilt nur dann als systemkonform abgegeben, wenn das dazu verwendete clientseitige Authentisierungsmerkmal einem serverseitigen Authentisierungsmerkmal entspricht, das in der Vorbereitungsphase des Urnengangs festgelegt und einem Stimmberechtigten «zugewiesen» wurde. Der Beweis muss daher die Bestätigung beinhalten, dass keine unzugewiesenen Authentisierungsmerkmale zum Abgeben von Stimmen erstellt wurden. Dazu müssen während der Vorbereitung des Urnengangs den Kontrollkomponenten oder den Prüferinnen und Prüfern entsprechende Daten als Vergleichsbasis übergeben worden sein. Die Prüferinnen und Prüfer müssen feststellen, dass die Anzahl der Authentisierungsmerkmale der (offiziellen) Anzahl der zugelassenen Stimmberechtigten entspricht. In diesem Fall dürfen die Authentisierungsmerkmale als einem Stimmberechtigten «zugewiesen» gelten. Dadurch ist zwar noch nicht sichergestellt, dass clientseitige Authentisierungsmerkmale vertrauenswürdiger Stimmberechtigter nicht missbräuchlich zur Abgabe einer systemkonformen Stimme verwendet wurden. Nach Ziffer 2.5 müssen die Stimmberechtigten dies allerdings feststellen können.

Ziff. 2.7.3: Es darf die Annahme gelten, dass die Manipulation an der serverseitigen Software keine Auswirkung auf die Vertrauenswürdigkeit der Benutzerplattform bei der Prüfung hat.

Die Möglichkeiten, die Benutzerplattformen vor Missbrauch zu schützen, sind viel schwächer als bei Komponenten in einer geschützten Umgebung. Allerdings ist es ein bewusster Entscheid, das Stimmgeheimnis und das Fehlen vorzeitiger Teilergebnisse nicht mittels dem kryptografischen Protokoll zu gewährleisten. Damit wird der Benutzerfreundlichkeit Rechnung getragen. Das Protokoll soll aber dort Schutz bieten, wo die Stimmen zentral aufbewahrt werden. Die Bezeichnung der Benutzerplattform als «vertrauenswürdig» signalisiert, dass bei der Entwicklung und der Analyse des kryptografischen Protokolls keine Angriffe auf die Benutzerplattform berücksichtigt werden müssen (vgl. einleitende Erläuterungen zu Ziffer 2).

Ziff. 2.9.3: Eine Implikation besteht darin, dass der Schlüssel, der zur Entschlüsselung der Stimmen nötig ist, auf vier verschiedene Kontrollkomponenten aufgeteilt werden muss. Mindestens eine dieser Kontrollkomponenten muss beim Kanton betrieben werden (explizit in Ziff. 3.1).

Ein signifikanter Anteil der Stimmberechtigten muss als nicht vertrauenswürdig zählen, damit das NV-System den Inhalt einer abgegebenen Stimme in Zusammenarbeit mit einem nicht vertrauenswürdigen Stimmberechtigten lernen kann. Dazu muss sichergestellt werden, dass dieser eine abgegebene verschlüsselte Stimme auch nicht nach äusserlichem Anpassen als seine eigene abgeben kann mit dem Ziel, durch den Beweis, den er im Rahmen der Prüfung des Beweises nach Ziffer 2.5 erhält, den Inhalt der Stimme zu lernen.

Ein Angreifer könnte versuchen, mithilfe der nicht vertrauenswürdigen Systemteilnehmenden vor der Auszählung Stimmen zu markieren und nachträglich anhand der entschlüsselten Stimmen das Stimmgeheimnis zu brechen. Die Prüferinnen und Prüfer könnten nach der Auszählung feststellen, dass die Stimmen nicht im Sinn ihrer Registrierung, sondern in markierter Form verarbeitet wurden. Zu diesem Zeitpunkt wäre das Stimmgeheimnis aber bereits gebrochen. Dies muss verhindert werden, indem vertrauenswürdige Komponenten vor der Auszählung sicherstellen, dass keine markierten Stimmen verarbeitet werden. Mit Blick auf diese Zielsetzung darf auch ein technisches Hilfsmittel der Prüferinnen und Prüfer als vertrauenswürdig gelten.

Zur Bezeichnung der Benutzerplattform als «vertrauenswürdig» siehe Erläuterung zu Ziffer 2.7 (zweiter Abschnitt).

Ziff. 2.11.1: Eine Implikation dieser Bestimmung besteht darin, dass ein Beweis mindestens 1000 verschiedene Werte annehmen können muss (bei einem numerischen Code beispielsweise alle Werte zwischen 000 und 999). Damit wäre die Wahrscheinlichkeit für den Angreifer, einen Beweis korrekt zu erraten, genau 0.1 Prozent. Indem er über die nicht vertrauenswürdigen Systemteilnehmenden und Kommunikationskanäle Informationen sammelt, könnte er sich einen Vorteil verschaffen, sodass er den Code nicht mehr ganz blind erraten müsste, wodurch die Wahrscheinlichkeit höher ausfallen würde. Mit Blick

auf solche Fälle muss ein Code a priori genügend Werte annehmen können, damit die Wahrscheinlichkeit 0.1 Prozent nicht überschreitet.

Ziff. 2.11.3: Als Beispiel wird angenommen, dass die Wahrscheinlichkeit für den Angreifer 1 Prozent beträgt. In diesem Fall müssen die Schritte bei der Auszählung soweit wiederholt werden können, dass die Wahrscheinlichkeit nach der Wiederholung tiefer als 1 Prozent liegt. Durch weitere Wiederholungen soll die Wahrscheinlichkeit so weit wie nötig reduziert werden können.

Ziff. 2.12.4: Mit dieser Erklärung wird die Stimme noch nicht definitiv abgegeben. Zunächst muss die stimmende Person die Möglichkeit haben, die korrekte Übermittlung anhand eines ersten Teilbeweises zu prüfen. Danach muss die stimmende Person die Möglichkeit haben, die Stimmabgabe abzubrechen und die Stimme über einen konventionellen Kanal abzugeben.

Ziff. 2.12.5: Es ist nicht zulässig, die Stimmenden aus rein psychologischen Gründen eine Prüfung vornehmen zu lassen, wenn das Ergebnis der Prüfung für die Beurteilung, ob die Stimme manipuliert wurde, keine Bedeutung hat.

Ziff. 2.12.8: Im Fall, dass zur Erfüllung von Ziffer 2.5 zwei Teilbeweise eingesetzt werden, ist der vorletzte Teilbeweis mit dem ersten Teilbeweis gleichbedeutend. Ferner lässt sich aus Ziffer 2.8 ableiten, dass die Stimmenden zusammen mit ihrer Willensbekundung nach Ziffer 2.12.8 ein Geheimelement eingeben müssen, das noch nicht in die Benutzerplattform eingegeben wurde. Das Geheimelement kann gleichzeitig als clientseitiges Authentisierungsmerkmal verstanden werden.

Ziff. 2.12.11: Setup-Komponenten und Druckkomponenten sind grundsätzlich für den Einsatz in der Vorbereitung des Urnengangs vorgesehen. Der Einsatz zu einem späteren Zeitpunkt beispielsweise wird an dieser Stelle nicht untersagt. Allerdings soll die Verarbeitung von Stimmen oder anderen Daten, die erst während dem Urnengang anfallen, nicht unter der Annahme erfolgen können, dass diese Komponenten vertrauenswürdig sind. Werden die Komponenten für die Verarbeitung solcher Daten verwendet, dann dürfen sie nicht als vertrauenswürdig gelten.

Ziff. 3 Anforderungen an vertrauenswürdige Komponenten nach Ziffer 2 und deren Betrieb

Hier werden Anforderungen an die Komponenten gestellt, die gemäss dem kryptografischen Protokoll bei der Erfüllung mindestens einer der Anforderungen nach Ziffern 2.5–2.8 als vertrauenswürdig angenommen werden. Es kann sich dabei um folgende Komponenten handeln:

- Setup-Komponenten
- Druckkomponenten
- Kontrollkomponenten
- Technische Hilfsmittel der Prüferinnen und Prüfer

Ziff. 3.1: Dazu gehört das Aufsetzen (Betriebssystem, Laufzeitumgebung, Software für die elektronische Stimmabgabe), die Prüfung der Korrektheit der Dateien mit der Software für die elektronische Stimmabgabe, das Aktualisieren, Konfigurieren und das Absichern. Vgl. auch Erläuterungen zu Ziffer 2.9.3.

Ziff. 3.4: Die konkrete Organisation und Ausgestaltung des Einsatzes von Prüferinnen und Prüfern richtet sich nach kantonalem Recht (vgl. dazu auch die Erläuterungen zu Art. 27*m* Abs. 4 E-VPR).

Ziff. 3.7: Damit ist nebst der Software für die elektronische Stimmabgabe auch die Software der Infrastruktur, wie beispielsweise Betriebssysteme, gemeint.

Ziff. 4 Stimmvorgang

Ziff. 4.10: Namentlich darf die Stichhaltigkeit der Beweise in diesem Fall von der Vertrauenswürdigkeit der Benutzerplattform abhängen. Dies erlaubt beispielsweise das Einscannen der Verifizierungsreferenz vorgängig zur Stimmabgabe. Diese Erleichterungen dürfen sich ausschliesslich an eine kleine Gruppe von Stimmberechtigten richten, die den Beweis ohne solche Erleichterungen nicht interpretieren können. Stimmberechtigte, für die dies nicht zutrifft, sollen grundsätzlich dazu animiert werden, Beweise gemäss der vorgesehenen Prozedur zu überprüfen.

Ziff. 4.11: Stimmende sind gehalten, der zuständigen kantonalen Behörde zu melden, falls Beweise falsch angezeigt werden oder sie sich diesbezüglich unsicher sind. Die briefliche oder persönliche Stimmabgabe bleibt eine Handlungsoption, sofern noch keine elektronische Stimme eingegangen ist. Um dies zu beurteilen, steht den Kantonen eine Funktion nach Ziffer 11.6 zur Verfügung.

Ziff. 4.12: Die Bestätigung der definitiven Stimmabgabe nach Ziffer 2.12.8 muss unter Verwendung eines Geheimelements erfolgen, das noch nicht in die Benutzerplattform eingegeben wurde. Es ist nicht ausgeschlossen, eine E-ID als Ersatz für dieses Geheimelement zu verwenden. Dies müsste gestützt auf eine Risikobeurteilung erfolgen. Allerdings kann eine E-ID die briefliche Zustellung der Verifizierungsreferenz nicht ersetzen. Eine briefliche Zustellung des Stimmmaterials wird vorläufig nötig bleiben.

Ferner gilt die Bestimmung, dass die Zulässigkeit des Einsatzes einer E-ID auf der Grundlage einer Risikobeurteilung geprüft werden muss auch dann, wenn diese vom Staat herausgegeben wird oder staatlich anerkannt ist.

Ziff. 7 Anforderungen an Druckereien

Die Anforderungen an Druckereien werden künftig nicht mehr in einem separaten Anforderungskatalog, sondern direkt im Anhang geregelt. Diese Bestimmungen gelten namentlich zusätzlich zu den Bestimmungen in Ziffer 3.

Ziff. 7.4: Beispielsweise müssen der Datenträger und das Geheimelement zur Entschlüsselung getrennt voneinander an einem sicheren Ort (z.B. Tresor) aufbewahrt werden. Die Person, die das Geheimelement zur Entschlüsselung der Daten besitzt, darf den Tresor nicht unbemerkt öffnen können. Die Entschlüsselung und die Bearbeitung der Daten sowie der Druckvorgang erfolgen im Vieraugenprinzip. Es muss ausgeschlossen sein, dass die Daten unverschlüsselt auf einer Komponente vorliegen, ohne dass mindestens zwei Personen die Komponente überwachen.

Ist das Vieraugenprinzip bei der Bearbeitung kritischer Daten beispielweise infolge eines längeren Unterbruchs nicht nahtlos umsetzbar, müssen die Daten vernichtet werden.

Ziff. 7.6: Beim Vorliegen guter Gründe kann mit der Datenvernichtung zugewartet werden; spätestens bis die gesetzlichen Vorschriften bezüglich Aufbewahrung und Nachvollziehbarkeit erfüllt sind.

Ziff. 8 Informationen und Anleitungen

Ziff. 8.10: Die Stimmenden müssen das korrekte Vorgehen bei der Stimmabgabe kennen, um gegen Social-Engineering-Angriffe geschützt zu sein. Indem die Behörden die Instruktionen brieflich verschicken und sie mit dem Hinweis versehen, sich im Zweifelsfall an diese Instruktionen zu halten und sich bei Bedarf an die zuständige Stelle beim Kanton zu wenden, erschweren sie Social-Engineering-Angriffe. Die Wirksamkeit dieses Vorgehens sowie alternative Vorgehensweisen für Anleitung der Stimmberechtigten könnten Gegenstand der Forschung und der wissenschaftlichen Begleitung bilden.

Ziff. 10 Konformitätskontrolle und Ablage endgültig abgegebener Stimmen

Es dürfen nur systemkonform abgegebene Stimmen für die Auszählung abgelegt werden. Diese Funktionalität kann auch mittels einer nicht vertrauenswürdigen Komponente nach Ziffer 2 sichergestellt werden.

Ziff. 11 Auszählung der elektronischen Urne

Ziff. 11.1: Die Entschlüsselung nach Ziffer 11.2 muss am Abstimmungssonntag erfolgen. Vorgelagerte Entschlüsselungen, die beim Systemanbieter durchgeführt werden, dürfen bereits beginnen, sobald der elektronische Stimmkanal geschlossen wurde. Die Wirksamkeit der Verschlüsselung muss trotz den vorgelagerten Entschlüsselungen unverändert hoch bleiben.

Ziff. 11.2: Wird das System eines anderen Kantons verwendet, kann die Entschlüsselung und Auszählung auch beim systemanbietenden Kanton erfolgen.

Ziff. 11.6: Ob es sich bei einer brieflich oder persönlich abgegebenen Stimme um eine doppelte oder sogar mehrfache Stimmabgabe handelt, kann nicht entschieden werden, indem lediglich die elektronisch abgegebenen Stimmen als Vergleichsbasis beigezogen werden. Dennoch fällt die Funktionalität nach Ziffer 11.6 in den Geltungsbereich der VEleS. Es ist allerdings nicht nötig, die Funktionalität unter Bezugnahme auf Vertrauensannahmen nach Ziffer 2 zu spezifizieren.

Ziff. 12 Vertrauliche Daten

Ziff. 12.9: Insbesondere für Systemkomponenten, deren Vertrauenswürdigkeit für die Wahrung des Stimmgeheimnisses nach Ziffer 2.9.3 massgeblich ist, muss sichergestellt sein, dass die Daten unwiederbringlich gelöscht wurden.

Ziff. 13 Bedrohungen

Die Sicherheitsziele (vgl. Art. 4 Abs. 3) lassen sich nicht mit hundertprozentiger Gewissheit erreichen. In jedem Fall lassen sich Sicherheitsrisiken identifizieren. Auf der Basis einer methodischen Risikobeurteilung (Art. 4 Abs. 1) ist der Nachweis zu erbringen, dass sich jegliche Sicherheitsrisiken in einem ausreichend tiefen Rahmen bewegen.

Ein Risiko lässt sich über Bedrohungen und Schwachstellen des Systems identifizieren. Ein Risiko entsteht, wenn eine Schwachstelle des Systems durch eine Bedrohung ausgenutzt werden kann und dadurch die Erfüllung eines Sicherheitsziels potentiell in Frage gestellt wird. Zur Risikominimierung kommen Sicherheitsmassnahmen zum Einsatz. Sicherheitsmassnahmen müssen die Sicherheitsanforderungen auf den Ebenen Infrastruktur, Funktionalität und Betrieb soweit erfüllen, dass die identifizierten Risiken hinreichend minimiert werden.

Die Liste der Bedrohungen wurde entsprechend den neuen Erkenntnissen aus den letzten Jahren sowie an den Einsatz von vollständig verifizierbaren Systemen angepasst. Es wurde eine neue Definition und Benennung der Akteure bei Bedrohungen eingeführt, um die Szenarien zu verdeutlichen.

Ziff. 13.12: Das Protokoll verlangt, dass die Stimmenden die Beweise nach Ziffer 2.5 prüfen. Gemäss der Bestimmung muss das Risiko beurteilt werden, dass ein externer Angreifer die vom Kanton zur Verfügung gestellten Informationen verändert, um Stimmende dazu zu bringen, von den für die Prüfung zu befolgenden Schritten abzuweichen. Es geht hier nicht darum, falsche Informationen zu berücksichtigen, die in sozialen Netzwerken verbreitet werden könnten.

Ziff. 13.13, 13.14 und 13.15: Unter einem elektronischen Mittel wird hier ein Mittel verstanden, das den Zugriff auf wichtige Informationen ermöglicht, ohne dass der Angreifer physisch vor Ort sein muss. Es kann sich dabei beispielsweise um eine Malware handeln.

Unter einem physischen Mittel wird hier ein Mittel verstanden, das den Zugriff auf wichtige Informationen ermöglicht, indem sich der Angreifer persönlich vor Ort begibt.

Mit Social Engineering ist ein Vorgehen gemeint, durch das sich ein Angreifer Zugang zu wichtigen Informationen verschafft, indem er eine Person so in die Irre führt, dass sie die gewünschten Informationen direkt zur Verfügung stellt oder den Zugang auf physischem oder elektronischem Weg gewährt.

Ziff. 13.16, 13.17 und 13.18: Das kryptografische Protokoll definiert bestimmte Parameter, Algorithmen und Abläufe. Die hier genannten Bedrohungen würden eine Schwachstelle in einem oder mehreren dieser Elemente ausnutzen.

Ziff. 14 Feststellung und Meldung von Sicherheitsereignissen und -schwächen; Handhabung von Sicherheitsereignissen und -verbesserungen

E-Voting-Systeme müssen eine wirksame Erkennung und Untersuchung von Vorfällen – wie beispielsweise vermutete Manipulationen von Stimmen oder Angriffe auf das System – ermöglichen. Der Inhalt und Umfang der Protokolle müssen so definiert werden, um dies sicherzustellen. Dabei ist das Stimmgeheimnis zu gewährleisten.

Ausserdem muss ein kontinuierlicher Verbesserungsprozess bei der Erkennung und Untersuchung von Vorfällen definiert werden. 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.

Ziff. 14.2: Die Audit-, Identifizierungs- und Authentisierungsprozesse sind besonders sensibel und bedürfen einer besonderen Überwachung sowohl in dem vom Kanton betriebenen Teil des Systems als auch in dem vom Systemanbieter betriebenen Teil. Als Identifikation wird der Vorgang der Identifizierung einer Person bezeichnet, beispielsweise mit einem Benutzernamen oder einer Smartcard. Die Authentifizierung ist der Vorgang, bei dem das System die Zugriffsberechtigung sicherstellen kann. Dies geschieht beispielsweise durch die Verifizierung eines Passworts.

Ziff. 14.7: Das Ziel besteht darin festzustellen, dass Stimmen korrekt verarbeitet und gezählt werden. Dazu werden die Kontrollstimmen gemäss den selben Prozeduren verarbeitet wie die systemkonform abgegebenen Stimmen. Die Kontrollstimmen dürfen nicht als systemkonform abgegebene Stimmen im Endergebnis berücksichtigt werden.

Ziff. 14.10: Diese Bestimmung betrifft nicht zwingend nur das Online-System. Es können auch Komponenten bei der Vor- oder der Nachbereitung der Urnengänge betroffen sein.

Ziff. 15 Einsatz von kryptografischen Massnahmen und Schlüsselverwaltung

Ziff. 15.3: Die Verschlüsselung auf der Ebene der Software, deren Notwendigkeit aus Ziffer 2 hervorgeht, reicht zur Erfüllung dieser Anforderung nicht aus.

Ziff. 17 Tests des Systems

Ziff. 17.2: Als Schnittstellen werden die Elemente bezeichnet, die es der Software ermöglichen, Informationen mit der Umgebung auszutauschen. Dies können grafische Oberflächen, Befehlszeilen oder technische Schnittstellen (API) sein.

Ziff. 17.3: Bei dieser Anforderung werden zwei Ebenen der Softwarestruktur berücksichtigt:

- Ein Modul ist die unterste Ebene und stellt eine Gruppierung Klassen im Quellcode dar, die auf das gleiche, klar definierte Ziel hinarbeiten.
- Ein Teilsystem ist eine Sammlung von Modulen, die eine Systemfunktionalität abdeckt, beispielsweise die Verwaltung einer Abstimmung, die Erstellung einer Stimmrechtsausweises oder die Registrierung einer Stimmabgabe.

Ziff. 24 Entwicklung und Wartung von Informationssystemen

Die Qualität von E-Voting-Systemen muss während des gesamten Entwicklungsprozesses sichergestellt werden. Um die Qualitätssicherung zu stärken, wurden die Anforderungen mit folgenden Zielen präzisiert:

- 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.

Insbesondere werden die Anforderungen der Common Criteria Stufe EAL 4, die bisher für Kontrollkomponenten galten, auf das gesamte System ausgeweitet. Zusätzlich wurden sie mit Anforderungen aus Common Criteria über EAL 4 ergänzt, wenn dies einen wesentlichen Beitrag zu den Sicherheitszielen leistet und im Sinne der obengenannten Ziele ist.

Ziff. 24.1: Die hier berücksichtigten Entwicklungswerkzeuge sind die Werkzeuge, die für die Sicherheit der Softwareentwicklung wichtig sind. Dazu gehören IDEs, Build-Tools und Konfigurationsmanagement-Tools. Ebenso handelt es sich um Konfigurationsoptionen, die einen Einfluss auf die Sicherheit der Entwicklung haben können.

Wie in Ziffer 17.2 werden unter «Schnittstellen» die Elemente verstanden, die es der Software ermöglichen, Informationen mit der Umgebung auszutauschen. Dies können grafische Oberflächen, Befehlszeilen oder technische Schnittstellen (API) sein.

Eine Konfigurationsliste ist eine einheitliche Zusammenstellung von Konfigurationselementen, die den Zustand der Software und ihrer Dokumentation zu einem bestimmten Zeitpunkt darstellt. Idealerweise ermöglicht sie, eine vergangene Version der Software zu rekonstruieren.

Ziff. 24.3: Es muss eine korrekte Bereitstellung des Systems aus dem Quellcode bis zu seiner Installation in der Produktion (Build- und Deployment) sichergestellt werden. Dazu ist vom Systemanbieter eine bewährte und nachvollziehbare Build- und Deployment-Methode einzusetzen, mit der die folgenden Ziele erreicht werden:

- 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.

Dazu wurden neue Anforderungen eingeführt. Sie basieren auf den Richtlinien des US-Bundesstaates Colorado für die Verwendung elektronischer Wahlsysteme,[10] der von GitHub herausgegebenen Trusted-Build-Dokumentation[11] und der Reproducible-Builds-Dokumentation[12] des gleichnamigen Projekts.

Ziff. 24.4: Als Benutzende werden alle Personen verstanden, die mit der Software in irgendeiner Weise in Berührung kommen. Dazu können Mitarbeitende des Kantons, Stimmberechtigte, Testerinnen und Tester und letztlich alle gehören, die am System interessiert sind.

Damit der Entwickler Mängelberichte angemessen behandeln und in diesem Bereich effektiv kommunizieren kann, ist es wichtig, dass die Benutzenden wissen, wie sie Mängelberichte an den Entwickler übermitteln können und wie sie sich beim Entwickler registrieren können, um entsprechende Informationen zu erhalten.

Eine möglichst umfangreiche Sammlung von vermuteten Schwachstellen und deren systematische Behandlung soll zur Verbesserung der Systemsicherheit beitragen. Diese Anforderungen sind komplementär zur Offenlegung des Quellcodes (Art. 11-12 E-VEleS) und zum Bug-Bounty-Programm (Art. 13 E-VEleS).

Ziff. 25 Qualität Quellcode und Dokumentation

Die Qualität des Quellcodes und der Dokumentation ist ein zentrales Element für die Sicherheit von E-Voting. In den bisherigen Rechtsgrundlagen wurden entsprechende Anforderungen gestellt. Diese umfassten jedoch eher allgemeine Umschreibungen, wie etwa die Aufbereitung und Dokumentation nach

[10] Colorado Election Rules [8 CCR 1505-1] Rule 1. Definitions, 2020 und Colorado Voting Systems Trusted Build Procedures, 2020

[11] GitHub How to: Trusted builds, 2017

[12] https://reproducible-builds.org/

besten Praktiken und die Umsetzung bestimmter Punkte der Common Criteria. Die bisherigen Qualitätskriterien wurden daher präzisiert. Mit klaren Kriterien soll eine hohe Qualität der E-Voting-Systeme sichergestellt, was wiederum der Sicherheit zugutekommt, indem die Prüfungen aller Akteure sowie der Öffentlichkeit erleichtert werden. Um diese Qualitätskriterien zu definieren, wurde ein Qualitätsmodell für die E-Voting-Systeme erstellt. Dieses Modell basiert auf dem Standard ISO 25010 und auf dem Qualitätsmodell von McCall.[13] Die Kriterien wurden nach ihrem Beitrag zu den definierten Sicherheits- und Qualitätszielen ausgewählt.

Ziff. 26 Prüfkriterien für die Systeme und ihren Betrieb

Um die Wirksamkeit und Glaubwürdigkeit der Prüfungen sicherzustellen, wurden die Zuständigkeiten angepasst. Die Aufgabenteilung zwischen Bund und Kantonen wird so angepasst, dass der Bund mehr Verantwortung und eine direktere Rolle bei der Prüfung der Systeme übernimmt.

Der Bund ist neu für die Prüfungen der Erfüllung der Anforderungen in Bezug auf das System und die zugrundeliegenden Prozesse zuständig. Dadurch soll nicht zuletzt begünstigt werden, dass Erkenntnisse aus der Überprüfung zielgerichtet in den weiteren Verlauf des Versuchsbetriebs einfliessen. Für die Überprüfungen sind externe Expertinnen und Experten zu mandatieren.

Der Kanton bzw. der Systemanbieter ist weiterhin für Prüfungen in Bezug auf den Betrieb des Systems in seinen Rechenzentren zuständig (Zertifikation ISO 27001).

Auf eine weitergehende Zertifizierung durch Stellen, die von der Schweizerischen Akkreditierungsstelle (SAS) akkreditiert sind, wird verzichtet.

[13] FACTORS IN SOFTWARE QUALITY - Vol. 1: Concept and Definitions of Software Quality - Jim A. McCall, Paul K. Richards, Gene F. Walters (1977)