Verordnung der BK über die elektronische Stimmabgabe (VEleS)

vom …

Die Schweizerische Bundeskanzlei (BK),
gestützt auf die Artikel 27*e* Absatz 1[bis], 27*g* Absatz 2, 27*i* Absatz 3 und 27*l* Absätze 3 und 4 der Verordnung vom 24. Mai 1978[1] über die politischen Rechte (VPR),
verordnet:

Art. 1 Gegenstand

Diese Verordnung regelt die Voraussetzungen für die Erteilung der Zulassung der elektronischen Stimmabgabe.

Art. 2 Begriffe

[1] Die folgenden Ausdrücke bedeuten:

a. *System*: Gesamtheit der Software und der Infrastrukturen, die für die Durchführung von elektronischen Urnengängen verwendet werden;

b. *Online-System*: Teil des Systems, der zur Stimmrechtsprüfung, zur Abgabe der verschlüsselten Stimme und zur Aufbewahrung der verschlüsselten Stimme verwendet wird;

c. *vertrauenswürdiger Systemteil*: Teil des Systems, der die Kontrollkomponenten umfasst und der für die Definition des kryptografischen Protokolls als vertrauenswürdig angesehen werden darf;

d. *Kontrollkomponenten*: unabhängige Komponenten des Systems, die unterschiedlich ausgestaltet sind, von unterschiedlichen Personen betrieben werden und durch besondere Massnahmen gesichert sind;

e. *Systembetreiber*: Behörde oder Privatunternehmen, die auf Weisung des Kantons bei einem Urnengang das Online-System betreiben und dieses warten;

1 SR **161.11**

f. *Betrieb*: alle technischen, administrativen, rechtlichen und Führungstätigkeiten eines Kantons, eines Systembetreibers oder einer Druckerei, die für die Durchführung von elektronischen Urnengängen festgelegt wurden, einschliesslich der Wartung;

g. *Betriebsstellen*: die für den Betrieb zuständigen Organisationen oder Organisationseinheiten, wie eine Staatskanzlei, ein Systembetreiber oder eine Druckerei;

h. *Prüferinnen und Prüfer*: Personen, die im Auftrag des Kantons den korrekten Ablauf des Urnengangs prüfen;

i. *Infrastruktur*: Hardware, Software von Drittkomponenten nach Artikel 11 Absatz 2 Buchstabe a, Netzwerkelemente, Räumlichkeiten, Services und Betriebsmittel jeglicher Art bei allen Betriebsstellen, die zum sicheren Betrieb der elektronischen Stimmabgabe erforderlich sind;

j. *Software*: gesamte Implementierung des kryptografischen Protokolls für die vollständige Verifizierbarkeit, die durch die Softwareentwicklerin oder den Softwareentwickler für die elektronische Stimmabgabe vorgenommen wurde;

k. *kryptografisches Protokoll*: Protokoll mit kryptografischen Sicherheitsfunktionen zur Erreichung der Anforderungen im Anhang Ziffer 2; das kryptografische Protokoll ist in der Modellebene angesiedelt und enthält somit keine direkten Anweisungen für die Implementierung, sondern abstrakte Sicherheitsfunktionen;

l. *Benutzerplattform*: multifunktionales, programmierbares Gerät, das mit dem Internet verbunden ist und zur Stimmabgabe verwendet wird, wie ein handelsüblicher Computer, ein Smartphone oder ein Tablet;

m. *Stimme, wie sie die stimmende Person in die Benutzerplattform eingegeben hat*: Stimme, wie sie die stimmende Person auf der Benutzerplattform erfasst hat und die seither nicht manipuliert wurde; sie entspricht immer dem Willen der stimmenden Person, ausser dieser unterläuft bei der Eingabe ein Irrtum;

n. *registrierte Stimme*: Stimme, bei der der vertrauenswürdige Systemteil von der endgültigen Stimmabgabe Kenntnis genommen hat;

o. *Teilstimme*:
   1. bei Abstimmungen: Stimme für eine Vorlage, einen Gegenvorschlag oder eine Stichfrage;
   2. bei Wahlen: die Wahl einer Liste oder einer kandidierenden Person;

p. *systemkonform abgegebene Stimme*: Stimme:
   1. die einer vorgesehenen Art entspricht, einen Stimm- oder Wahlzettel auszufüllen,
   2. die eine Absenderin oder ein Absender endgültig abgegeben hat,
   3. deren verwendeten clientseitigen Authentisierungsmerkmale beziehungsweise deren daraus resultierenden Authentisierungsnachrichten den serverseitigen Authentisierungsmerkmalen entsprechen, die in der

Vorbereitungsphase des Urnengangs festgelegt und einer stimmberechtigten Person zugewiesen wurden, und

4. wenn der vertrauenswürdige Systemteil des Online-Systems zuvor keine Stimme registriert hat, die unter Verwendung derselben Authentisierungsmerkmale abgegeben wurde;

q. c*lientseitiges Authentisierungsmerkmal*: für die einzelnen Stimmberechtigten individuell bereitgestellte Information, die sie – allenfalls zusammen mit weiteren clientseitigen Authentisierungsmerkmalen – brauchen, um eine Stimme abgeben zu können, wie einen PIN;

r. *serverseitiges Authentisierungsmerkmal*: Information, die es – allenfalls zusammen mit weiteren serverseitigen Authentisierungsmerkmalen – braucht, um mithilfe von Authentisierungsnachrichten die Absenderin oder den Absender einer Stimme als stimmberechtigte Person zu authentisieren;

s. *Authentisierungsnachrichten*: Informationen, die eine Benutzerplattform nach Eingabe des clientseitigen Authentisierungsmerkmals an das Online-System übermittelt, damit dieses die Absenderin oder den Absender einer Stimme als stimmberechtigte Person authentisiert.

[2] Im Übrigen gelten die Begriffe im Anhang Ziffer 1.

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

Die Zulassung der elektronischen Stimmabgabe erfolgt pro Urnengang; sie wird erteilt, wenn folgende Voraussetzungen erfüllt sind:

a. Das System ist so ausgestaltet und wird so betrieben, dass eine verifizierbare, sichere und vertrauenswürdige Stimmabgabe gewährleistet ist.

b. Das System ist für die Stimmberechtigten einfach zu handhaben; die besonderen Bedürfnisse möglichst aller Stimmberechtigten sind berücksichtigt.

c. Das System und die betrieblichen Abläufe sind so ausgestaltet und dokumentiert, dass die technischen und organisatorischen Abläufe im Detail überprüft und nachvollzogen werden können.

d. Der Öffentlichkeit werden adressatengerechte Informationen zur Funktionsweise des Systems und zu den betrieblichen Abläufen zugänglich gemacht und Anreize zur Mitwirkung von fachkundigen Personen aus der Öffentlichkeit sind vorhanden.

Art. 4 Risikobeurteilung

[1] Der Kanton führt eine Risikobeurteilung durch, mit der er nachweist und begründet, dass die Sicherheitsrisiken in seinem Verantwortungsbereich hinreichend gering sind. Dabei sind auch das Vertrauen und die Akzeptanz der Öffentlichkeit in die elektronische Stimmabgabe zu berücksichtigen.

[2] Er prüft, ob er Risiken im Aufgabenbereich seiner Dienstleister selber beurteilen kann und inwiefern separate Risikobeurteilungen durch diese nötig sind. Gegebe-

nenfalls fordert er diese separaten Risikobeurteilungen ein.

[3] Die Risikobeurteilungen beziehen sich auf folgende Sicherheitsziele:

a. Korrektheit des Ergebnisses;

b. Wahrung des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse;

c. Erreichbarkeit und Funktionsfähigkeit des Stimmkanals;

d. Schutz der persönlichen Informationen über die Stimmberechtigten;

e. Schutz der für die Stimmberechtigten bestimmten Informationen vor Manipulationen;

f. keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten.

[4] Jedes Risiko wird mit Bezug auf die folgenden Eigenschaften anhand der Dokumentation zum System und zu dessen Betrieb identifiziert und klar beschrieben:

a. Sicherheitsziele;

b. allfällige mit den Sicherheitszielen verbundenen Datensätze;

c. Bedrohungen;

d. Schwachstellen.

Art. 5 Anforderungen an die vollständige Verifizierbarkeit

[1] Es ist sichergestellt, dass jede Manipulation, die zu einer Verfälschung des Ergebnisses führt, unter Wahrung des Stimmgeheimnisses erkannt werden kann (vollständige Verifizierbarkeit). Dies ist gegeben, wenn die Anforderungen an die individuelle und an die universelle Verifizierbarkeit erfüllt sind.

[2] Anforderungen an die individuelle Verifizierbarkeit:

a. Die stimmende Person hat die Möglichkeit zu erkennen, ob ihre Stimme auf der Benutzerplattform oder auf dem Übertragungsweg manipuliert oder abgefangen worden ist.

b. Dazu erhält die stimmende Person einen Beweis, dass der vertrauenswürdige Systemteil (Art. 8) die Stimme so, wie sie die stimmende Person in die Benutzerplattform eingegeben hat, als systemkonform abgegeben registriert hat; der Beweis bestätigt für jede Teilstimme die korrekte Registrierung.

c. Eine stimmberechtigte Person, die ihre Stimme nicht elektronisch abgegeben hat, kann nach der Schliessung des elektronischen Stimmkanals innert der gesetzlichen Beschwerdefristen einen Beweis anfordern, dass der vertrauenswürdige Systemteil keine Stimme registriert hat, die unter Verwendung ihres clientseitigen Authentisierungsmerkmals abgegeben wurde.

[3] Anforderungen an die universelle Verifizierbarkeit:

a. Zur universellen Verifizierung erhalten die Prüferinnen und Prüfer einen Beweis der korrekten Ergebnisermittlung; der Beweis bestätigt, dass das ermittelte Ergebnis folgende Stimmen berücksichtigt:

1. alle systemkonform abgegebenen Stimmen, die durch den vertrauenswürdigen Systemteil registriert wurden,
2. ausschliesslich systemkonform abgegebene Stimmen,
3. alle Teilstimmen gemäss des im Rahmen der individuellen Verifizierung generierten Beweises.

b. Die Prüferinnen und Prüfer werten den Beweis in einem beobachtbaren Prozess aus; dazu müssen sie technische Hilfsmittel verwenden, die vom Rest des Systems unabhängig und isoliert sind.

Art. 6 Stichhaltigkeit der Beweise

Für die Stichhaltigkeit der Beweise nach Artikel 5 massgebend ist ausschliesslich die Vertrauenswürdigkeit:

a. des vertrauenswürdigen Systemteils für Beweise nach Artikel 5 Absätze 2 und 3;

b. des Verfahrens bei der Generierung und beim Druck des Stimmmaterials für Beweise nach Artikel 5 Absatz 2;

c. des technischen Hilfsmittels, das von den Prüferinnen und Prüfern zur Überprüfung eingesetzt wird für Beweise nach Artikel 5 Absatz 3.

Art. 7 Wahrung des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse

Für die Wahrung des Stimmgeheimnisses und den Ausschluss vorzeitiger Teilergebnisse innerhalb der Infrastruktur massgebend ist die Vertrauenswürdigkeit des vertrauenswürdigen Systemteils sowie des Verfahrens bei der Generierung und beim Druck des Stimmmaterials.

Art. 8 Anforderungen an den vertrauenswürdigen Systemteil

[1] Der vertrauenswürdige Systemteil umfasst eine oder mehrere Gruppen von Kontrollkomponenten.

[2] Beweise sind auch dann stichhaltig (Art. 6) und das Stimmgeheimnis ist auch dann gewahrt (Art. 7), wenn pro Gruppe nur eine der Kontrollkomponenten korrekt funktioniert.

[3] Die Vertrauenswürdigkeit des vertrauenswürdigen Systemteils wird über die unterschiedliche Ausgestaltung der Kontrollkomponenten sowie die Unabhängigkeit von deren Betrieb und deren Überwachung sichergestellt.

Art. 9 Zusätzliche Massnahmen zur Risikominimierung

Sind die Risiken trotz der ergriffenen Massnahmen nicht hinreichend gering, so müssen zusätzliche Massnahmen zur Risikominimierung ergriffen werden. Dies gilt insbesondere auch dann, wenn sämtliche Anforderungen des Anhangs bereits umgesetzt sind.

Art. 10 Anforderungen an die Überprüfung

1 Unabhängige Stellen prüfen im Auftrag der Bundeskanzlei:

a. das kryptografische Protokoll (Anhang Ziff. 26.1);

b. die Software des Systems (Anhang Ziff. 26.2);

c. die Sicherheit von Infrastruktur und Betrieb (Anhang Ziff. 26.3);

d. den Schutz gegen Versuche, in die Infrastruktur einzudringen (Anhang Ziff. 26.4);

2 Der Kanton stellt sicher, dass der Systembetreiber über ein Informationssicherheitsmanagement-System (ISMS) verfügt und dieses von unabhängigen Stellen geprüft wird (Anhang Ziff. 26.5). Das ISMS umfasst mindestens die Prozesse und die Infrastruktur des Systembetreibers, die für die Erreichung der Sicherheitsziele relevant sind.

3 Der Kanton stellt sicher, dass die Bundeskanzlei und die von ihr beauftragten unabhängigen Stellen für die Durchführung der Prüfungen nach Absatz 1 Zugang zum System und den notwendigen Unterlagen erhalten.

4 Die nach den Absätzen 1 und 2 für die Prüfungen zuständigen Behörden publizieren die Belege und die Zertifikate. Zusätzlich sind weitere Unterlagen zu publizieren, sofern sie für die Nachvollziehbarkeit relevant sind. Von einer Publikation kann abgesehen werden, sofern eine begründete Ausnahme insbesondere gestützt auf das Öffentlichkeits- oder das Datenschutzrecht vorliegt.

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

1 Der Kanton sorgt dafür, dass folgende Unterlagen offengelegt werden:

a. der Quellcode der Software des Systems einschliesslich der Dateien mit relevanten Parametern;

b. die Dokumentation der Software;

c. Anleitungen und ergänzende Dokumentationen, die fachkundige Personen benötigen, um das System in der eigenen Infrastruktur kompilieren, in Betrieb nehmen und analysieren zu können;

d. die Dokumentation der Prozesse für den Betrieb, die Wartung und die Sicherung des Systems;

e. Informationen und Beschreibungen zu bekannten Mängeln.

2 Nicht offengelegt werden müssen:

a. der Quellcode von Drittkomponenten wie Betriebssystemen, Datenbanken, Web- und Applikationsservern, Rechteverwaltungssystemen, Firewalls oder Routern, sofern diese weit verbreitet sind und laufend aktualisiert werden;

b. der Quellcode von Behördenportalen, die mit dem System verbunden sind;

c. Dokumente, für die eine begründete Ausnahme von einer Publikation insbesondere gestützt auf das Öffentlichkeits- oder das Datenschutzrecht vorliegt.

Art. 12 Modalitäten der Offenlegung

[1] Die nach Artikel 11 offenzulegenden Unterlagen müssen so aufbereitet und dokumentiert werden, dass sich das Lesen und Analysieren möglichst einfach gestaltet.

[2] Um eine Überprüfung durch die Öffentlichkeit zu ermöglichen, sind die Unterlagen:

a. einfach, unentgeltlich und ohne Registrierung über das Internet beziehbar; und

b. rechtzeitig vor dem geplanten Einsatz verfügbar.

[3] Jede Person darf den Quellcode zu ideellen Zwecken untersuchen, verändern, kompilieren und ausführen sowie Studien dazu verfassen. Sie darf Studien und Erkenntnisse zu Mängeln publizieren. Sie darf sich insbesondere für die Fehlersuche mit weiteren Personen austauschen und dabei aus den offengelegten Informationen zitieren. Der Inhaber des Quellcodes kann dessen Nutzung zu anderen Zwecken erlauben.

[4] Der Inhaber kann für die Meldung von Mängeln (Art. 13 Abs. 1) spezifische Bestimmungen festlegen. Dabei kann er dazu auffordern, Mängel umgehend zu melden und für Publikationen zu vermuteten Mängeln eine bestimmte Frist einzuhalten.

[5] Stellt er Nutzungsbedingungen für den Quellcode und die Dokumentation auf, so darf er Verstösse dagegen nur dann verfolgen, wenn eine Person den Quellcode oder Teile davon kommerziell verwendet oder produktiv einsetzt. In den Nutzungsbedingungen wird auf diese Haftungsbeschränkung oder einen Haftungsausschluss hingewiesen.

Art. 13 Einbezug der Öffentlichkeit

[1] Der Kanton sorgt dafür, dass interessierte Personen aus der Öffentlichkeit Hinweise für die Verbesserung des Systems einreichen können, darunter:

a. Hinweise zu Mängeln in den offengelegten Unterlagen nach Artikel 11;

b. Hinweise auf der Grundlage von Versuchen zum Eindringen in das System im Rahmen von öffentlichen Tests.

[2] Er bezeichnet für die Organisation und die Abwicklung des Einbezugs interessierter Personen aus der Öffentlichkeit eine zuständige Stelle. Diese wertet die Hinweise aus und informiert die hinweisgebende Person über ihre Einschätzung und allfällige Massnahmen, die gestützt auf den Hinweis getroffen werden. Diese Informationen werden publiziert.

[3] Der Kanton sorgt dafür, dass Hinweise, die einen Bezug zur Sicherheit haben und die zu Verbesserungen des Systems beitragen, angemessen finanziell entgolten werden.

Art. 14 Grundsätze der Verteilung von Aufgaben und Verantwortlichkeiten

[1] Der Kanton trägt die Gesamtverantwortung für den korrekten Ablauf des Urnengangs mit der elektronischen Stimmabgabe. Wichtige Aufgaben sind durch den Kanton selbst auszuführen.

2 Der Kanton kann die Entwicklung der eingesetzten Software, Aufgaben des technischen Betriebs und die Kommunikation zu Fragen der Funktionsweise an externe Organisationen delegieren.

3 Bei einem Urnengang tragen die Betriebsstellen für die Bereitstellung und die Handhabung der technischen Aspekte der elektronischen Stimmabgabe die Verantwortung gegenüber dem Kanton.

4 Die nach kantonalem Recht zuständigen Prüferinnen und Prüfer übernehmen die Verantwortung für den Betrieb ihrer technischen Hilfsmittel.

Art. 15 Aufgaben der auf kantonaler Ebene verantwortlichen Stelle

Der Kanton bestimmt eine Stelle, die die Gesamtverantwortung trägt und insbesondere die folgenden Aufgaben wahrnimmt:

a. Festlegung einer übergeordneten Informationssicherheitsrichtlinie;

b. Festlegung einer Informationsklassifizierungs- und Verarbeitungsrichtlinie für die identifizierten Informationsbestände;

c. Festlegung einer Risikomanagementrichtlinie;

d. Definition und Umsetzung von Massnahmen zur Einhaltung der Richtlinien nach den Buchstaben a–c;

e. Beauftragung eines Systembetreibers und Festlegung der Anforderungen an dessen Überwachung und Überprüfung;

f. Festlegung von Fristen für die Durchführung von kritischen Handlungen und Operationen;

g. Überwachung und Überprüfung der Arbeiten des Systembetreibers;

h. Bestimmung und Instruktion der Prüferinnen oder Prüfer;

i. Beurteilung und Kommunikation der Korrektheit des Ergebnisses des Urnengangs gestützt auf die Beweise nach Artikel 5 und weitere Indikatoren.

Art. 16 Belege zu den Gesuchen

1 Den Gesuchen nach Artikel 27*e* VPR sind beizulegen:

a. Zertifikate und deren Anhänge, die im Rahmen von Prüfungen nach Artikel 10 Absatz 2 erstellt wurden;

b. aktuelle Risikobeurteilungen nach Artikel 4 einschliesslich der Grundlagen, die für die Nachvollziehbarkeit notwendig sind;

c. Informationen zur Offenlegung der Unterlagen nach Artikel 11 und zu Hinweisen aus der Öffentlichkeit nach Artikel 13;

d. Protokolle von Tests, die der Kanton durchgeführt hat, und Hinweise auf bestehende Mängel im System.

2 Auf Unterlagen nach Absatz 1, die die Bundeskanzlei bereits erhalten hat und die noch gültig sind, kann verwiesen werden.

Art. 17 Weitere Bestimmungen

[1] Die detaillierten technischen und administrativen Anforderungen an die elektronische Stimmabgabe sind im Anhang geregelt.

[2] Ein Kanton kann in Ausnahmefällen von der Erfüllung einzelner Anforderungen befreit werden, sofern:

a. die nicht erfüllten Anforderungen im Gesuch bezeichnet sind;

b. eine nachvollziehbare Begründung für den Ausnahmefall vorliegt; und

c. der Kanton allfällige alternative Massnahmen beschreibt und mit Bezug auf die Risikobeurteilung begründet, weshalb er die Risiken als hinreichend gering einschätzt.

Art. 18 Aufhebung eines anderen Erlasses

Die Verordnung der BK vom 13. Dezember 2013[2] über die elektronische Stimmabgabe wird aufgehoben.

Art. 19 Inkrafttreten

Diese Verordnung tritt am … in Kraft.

… Schweizerische Bundeskanzlei:

Walter Thurnherr

2 AS **2013** 5371, **2018** 2279

Anhang
(Art. 2 Abs. 1 Bst. k und 2, 9, 10 Abs. 1 und 2 sowie 17 Abs. 1)

Technische und administrative Anforderungen an die elektronische Stimmabgabe

1. Begriffsbestimmungen

Zusätzlich zu Artikel 2 bedeuten die folgenden Ausdrücke:

1.1 *kritische Daten*: Daten, deren Integrität oder Vertraulichkeit für die Erfüllung der Anforderungen an das kryptografische Protokoll (Ziffer 2) massgeblich sind;

1.2. *kritischer Prozess*: Vorgang, bei dem kritische Daten bearbeitet werden;

1.3. *Wahrung des Stimmgeheimnisses*: Situation, wenn keiner Person oder Komponente folgende Daten vorliegen:

1.3.1 abgegebene Stimmen oder Daten, die auf den Inhalt abgegebener Stimmen schliessen lassen;

1.3.2 Daten, die es erlauben, die stimmende Person zu identifizieren (Daten über die Stimmberechtigten); und

1.3.3 Daten, die es erlauben, die Daten über die Stimmberechtigten den abgegebenen Stimmen zuzuordnen;

1.4 *Fehlen vorzeitiger Teilergebnisse*: Situation, wenn keiner Person oder Komponente die abgegebenen Stimmen vorliegen oder Daten, die auf die abgegebenen Stimmen schliessen lassen;

1.5 *Verifizierungsreferenz*: eine mit dem Stimmmaterial zugestellte Grundlage, damit die Stimmberechtigten nach Artikel 5 Absatz 2 in Verbindung mit Ziffer 2.5 des Anhangs prüfen können, ob ihre Stimme korrekt abgegeben wurde (z. B. eine Liste, auf der für jede Antwortmöglichkeit ein Code aufgeführt ist);

1.6 *öffentliche Parameter*: Daten, die einem Programm übergeben werden müssen, damit dieses korrekt funktioniert; bei den Daten handelt es sich um nicht vertrauliche Daten;

1.7 *externer Angreifer*: Person oder Gruppe von Personen, die nicht mit der Entwicklung und dem Betrieb des Systems vertraut ist und über durchschnittliche Ressourcen und Fachkenntnisse verfügt und von der ein Angriff ausgeht; ihre Beweggründe können Aktivismus oder finanziellen Gewinn umfassen;

1.8 *interner Angreifer:* Person oder Gruppe von Personen, die an der Entwicklung oder am Betrieb des Systems beteiligt ist und von der ein Angriff ausgeht; ihre Beweggründe können Aktivismus, finanziellen Gewinn oder die Absicht, ihrem Arbeitgeber zu schaden, umfassen;

1.9 *feindliche Organisation*: Gruppe von Personen, die über umfangreiche

Ressourcen und überdurchschnittliche Fachkenntnisse verfügt und von der ein Angriff ausgeht; sie kann dabei auch von einem Staat unterstützt werden; ihre Beweggründe können das Erlangen von Daten zu Profiling-Zwecken, die Störung eines Urnengangs oder die Beeinflussung der Ergebnisse des Urnengangs sein;

1.10 *Angreifer*: eine Person, Gruppe von Personen oder Organisation nach den Ziffern 1.7–1.9;

1.11 *elektronische Urne*: ein Speicherbereich, in dem die abgegebenen Stimmen bis zur Entschlüsselung und Auszählung gespeichert werden können.

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

2.1 Systemteilnehmende

Das kryptografische Protokoll regelt die Aufgaben der folgenden abstrakten Systemteilnehmenden:

- stimmberechtigte / stimmende Person
- Benutzerplattform
- Setup-Komponente
- nicht vertrauenswürdiges System (beliebige Komponenten unter Ausschluss der übrigen in dieser Ziffer aufgelisteten Komponenten; NV-System)
- Druckkomponente
- eine oder mehrere Gruppen von Kontrollkomponenten
- Prüferinnen und Prüfer
- technisches Hilfsmittel der Prüferinnen und Prüfer

2.2 Kommunikationskanäle

Das kryptografische Protokoll kann die folgenden Kommunikationskanäle zum Austausch von Nachrichten zwischen den Systemteilnehmenden vorsehen:

- stimmberechtigte / stimmende Person ↔ Benutzerplattform
- Benutzerplattform ↔ NV-System
- Setup-Komponente ↔ NV-System
- Kontrollkomponente ↔ NV-System
- NV-System → Druckkomponente
- NV-System → technisches Hilfsmittel der Prüferinnen und Prüfer
- Druckkomponente → stimmberechtigte / stimmende Person
- Setup-Komponente → technisches Hilfsmittel der Prüferinnen und Prüfer

- Prüferinnen und Prüfer ↔ technisches Hilfsmittel der Prüferinnen und Prüfer
- Bidirektionale Kanäle für die Kommunikation zwischen den Kontrollkomponenten

2.3 Angreifer

2.3.1 Das kryptografische Protokoll muss vor einem Angreifer Schutz bieten, der versucht, missbräuchlich auf die Stimmen und das Ergebnis einzuwirken, das Stimmgeheimnis zu brechen oder Teilergebnisse vorzeitig zu erheben (Ziffern 2.5-2.8).

2.3.2 Es muss die Annahme getroffen werden, dass ein Angreifer über folgende Fähigkeiten verfügt:

- Er kann sämtliche nicht vertrauenswürdigen Systemteilnehmenden (vgl. Ziffer 2.4) unter seine Kontrolle bringen, so dass sie alle geheimen Daten mit ihm teilen und uneingeschränkt nach seinen Anweisungen handeln.
- Er kann sämtliche Nachrichten, die auf nicht vertrauenswürdigen Kanälen ausgetauscht werden, mitlesen oder abfangen und selbst beliebig Nachrichten einspeisen.

2.4 Vertrauenswürdige und nicht vertrauenswürdige Systemteilnehmende und Kommunikationskanäle

2.4.1 Systemteilnehmende und Kommunikationskanäle gelten entweder als «vertrauenswürdig» oder als «nicht vertrauenswürdig». Die zulässigen Vertrauensannahmen für die einzelnen Systemteilnehmenden sind in Ziffer 2.9 geregelt.

2.4.2 Vertrauenswürdige Systemteilnehmende und Kommunikationskanäle werden als gegen Angreifer geschützt betrachtet. Für das kryptografische Protokoll darf namentlich von folgenden Annahmen ausgegangen werden:

- vertrauenswürdige Systemteilnehmende halten vertrauliche Daten unter Verschluss und führen ausschliesslich jene Operationen durch, die durch das kryptografische Protokoll vorgegeben sind; und
- vertrauenswürdige Kommunikationskanäle halten die übertragenen Nachrichten unter Verschluss und authentisch.

2.5 Anforderung an das kryptografische Protokoll: individuelle Verifizierbarkeit

Die stimmberechtigte Person erhält Beweise nach Artikel 5 Absatz 2 in Verbindung mit Artikel 6 Buchstaben a und b zur Bestätigung, dass der Angreifer:

- bis zur Registrierung einer als systemkonform abgegebenen Stimme keine Teilstimme der stimmberechtigten Person verändert oder unterschlagen

hat;

– nicht im Namen der stimmberechtigten Person missbräuchlich eine Stimme abgegeben hat, die in der Folge als systemkonform abgegebene Stimme registriert und gezählt worden ist.

2.6 Anforderung an das kryptografische Protokoll: universelle Verifizierbarkeit

Die Prüferinnen und Prüfer erhalten Beweise nach Artikel 5 Absatz 3 Buchstabe a in Verbindung mit Artikel 6 Buchstaben a und c zur Bestätigung, dass der Angreifer:

– nachdem die Stimmen als systemkonform abgegeben registriert worden sind, bis zur Berechnung des Ergebnisses keine Teilstimmen verändert oder unterschlagen hat;

– keine nicht systemkonform abgegebenen Stimmen oder Teilstimmen eingefügt hat, die bei der Berechnung des Ergebnisses berücksichtigt wurden.

2.7 Anforderung an das kryptografische Protokoll: Stimmgeheimnis und Fehlen vorzeitiger Teilergebnisse

2.7.1 Es muss sichergestellt sein, dass der Angreifer weder das Stimmgeheimnis brechen noch vorzeitige Teilergebnisse erheben kann, ohne zusätzlich die Stimmberechtigten oder deren Benutzerplattformen unter seine Kontrolle zu bringen.

2.7.2 Mit Ausnahme der stimmenden Person und ihrer Benutzerplattform gelten Systemteilnehmende, die über genügend Informationen verfügen, um das Stimmgeheimnis zu brechen oder vorzeitige Teilergebnisse zu erheben, nicht als gegen den Angreifer geschützt.

2.7.3 Es muss sichergestellt sein, dass der Angreifer die Benutzerplattformen nicht unbemerkt unter seine Kontrolle bringen kann, indem er die Software für die Benutzerplattformen auf dem Server manipuliert. Die stimmende Person muss die Möglichkeit haben, zu prüfen, ob ihre Benutzerplattform vom Server die korrekte Software mit den korrekten Parametern, insbesondere dem öffentlichen Schlüssel zur Verschlüsselung der Stimme, erhalten hat.

2.8 Anforderung an das kryptografische Protokoll: wirksame Authentisierung

Es muss sichergestellt sein, dass der Angreifer keine Stimme systemkonform abgeben kann, ohne die entsprechenden Stimmberechtigten unter seine Kontrolle zu bringen.

2.9 Aufzählung der vertrauenswürdigen und nicht vertrauenswürdigen Systemteilnehmenden

2.9.1 Für die Stichhaltigkeit der Beweise nach Ziffer 2.5

2.9.1.1 Die folgenden Systemteilnehmenden gelten als nicht vertrauenswürdig:

- Benutzerplattform
- NV-System
- drei von vier Kontrollkomponenten pro Gruppe, wobei offen gelassen werden muss, um welche drei es sich handelt
- ein signifikanter Anteil der Stimmberechtigten
- Prüferinnen und Prüfer
- technische Hilfsmittel der Prüferinnen und Prüfer

2.9.1.2 Die folgenden Systemteilnehmenden dürfen als vertrauenswürdig gelten:

- Setup-Komponente
- Druckkomponente
- eine von vier Kontrollkomponenten pro Gruppe, wobei offengelassen werden muss, um welche es sich dabei handelt

2.9.2 Für die Stichhaltigkeit der Beweise nach Ziffer 2.6

2.9.2.1 Die folgenden Systemteilnehmenden gelten als nicht vertrauenswürdig:

- Benutzerplattform
- NV-System
- drei von vier Kontrollkomponenten pro Gruppe, wobei offen gelassen werden muss, um welche drei es sich handelt
- ein signifikanter Anteil der Stimmberechtigten
- Setup-Komponente
- Druckkomponente

2.9.2.2 Die folgenden Systemteilnehmenden dürfen als vertrauenswürdig gelten:

- eine von vier Kontrollkomponenten pro Gruppe, wobei offengelassen werden muss, um welche es sich dabei handelt
- eine Prüferin oder ein Prüfer einer Gruppe, wobei offengelassen werden muss, um welche oder welchen es sich dabei handelt
- ein technisches Hilfsmittel einer vertrauenswürdigen Prüferin oder eines vertrauenswürdigen Prüfers, wobei offengelassen werden muss, um welches es sich dabei handelt

2.9.3 Für die Wahrung des Stimmgeheimnisses und das Fehlen vorzeitiger Teilergebnisse nach Ziffer 2.7

2.9.3.1 Die folgenden Systemteilnehmenden gelten als nicht vertrauenswürdig:

- NV-System
- drei von vier Kontrollkomponenten pro Gruppe, wobei offen gelassen werden muss, um welche drei es sich handelt
- ein signifikanter Anteil der Stimmberechtigten

2.9.3.2 Die folgenden Systemteilnehmenden dürfen als vertrauenswürdig gelten:

- Setup-Komponente
- Druckkomponente
- Benutzerplattform
- eine von vier Kontrollkomponenten pro Gruppe, wobei offengelassen werden muss, um welche es sich dabei handelt
- eine Prüferin oder ein Prüfer einer Gruppe, wobei offengelassen werden muss, um welche oder welchen es sich dabei handelt; Ziffer 2.7.2 geht dabei vor
- ein technisches Hilfsmittel einer vertrauenswürdigen Prüferin oder eines vertrauenswürdigen Prüfers, wobei offengelassen werden muss, um welches es sich dabei handelt; Ziffer 2.7.2 geht dabei vor

2.9.3.3 Wird eine gesamte Gruppe von Kontrollkomponenten bei einem privaten Systembetreiber eingesetzt, so gilt keine dieser Kontrollkomponenten als vertrauenswürdig.

2.9.4 Für die Wirksamkeit der Authentifizierung nach Ziffer 2.8

2.9.4.1 Die folgenden Systemteilnehmenden gelten als nicht vertrauenswürdig:

- NV-System
- drei von vier Kontrollkomponenten pro Gruppe, wobei offen gelassen werden muss, um welche drei es sich handelt
- ein signifikanter Anteil der Stimmberechtigten
- Prüferinnen und Prüfer
- technische Hilfsmittel der Prüferinnen und Prüfer
- Benutzerplattform

2.9.4.2 Die folgenden Systemteilnehmenden dürfen als vertrauenswürdig gelten:

- Setup-Komponente
- Druckkomponente
- eine von vier Kontrollkomponenten pro Gruppe, wobei offengelassen werden muss, um welche es sich dabei handelt

2.10 Aufzählung der vertrauenswürdigen und nicht vertrauenswürdigen Kommunikationskanäle

2.10.1 Die folgenden Kommunikationskanäle gelten als nicht vertrauenswürdig:

- Benutzerplattform ↔ NV-System
- Setup-Komponente ↔ NV-System
- Kontrollkomponente ↔ NV-System
- NV-System → Druckkomponente
- NV-System → technisches Hilfsmittel der Prüferinnen und Prüfer
- bidirektionale Kanäle für die Kommunikation zwischen den Kontrollkomponenten

2.10.2 Die folgenden Kommunikationskanäle dürfen als vertrauenswürdig gelten:

- stimmberechtigte / stimmende Person ↔ Benutzerplattform
- technisches Hilfsmittel der Prüferinnen und Prüfer ↔ Prüferinnen und Prüfer
- Setup-Komponente → technisches Hilfsmittel der Prüferinnen und Prüfer
- Druckkomponente → stimmberechtigte / stimmende Person

2.11 Zusätzliche Anforderungen an die Stichhaltigkeit der Beweise

2.11.1 Die Wahrscheinlichkeit für den Angreifer, einen Beweis nach Ziffer 2.5 fälschen zu können, wenn er eine Teilstimme verändert, eine Teilstimme unterschlägt oder in fremdem Namen eine Stimme abgibt, darf höchstens 0.1% betragen.

2.11.2 Die Wahrscheinlichkeit für den Angreifer, einen Beweis nach Ziffer 2.6 fälschen zu können, wenn er durch Verändern und Unterschlagen von systemkonform abgegebenen Stimmen sowie durch Einfügen von nicht systemkonform abgegebenen Stimmen bewirkt, dass das berechnete Ergebnis um 0.1% vom korrekten Ergebnis abweicht, darf pro Vorlage, Listenwahl oder Kandidatenwahl höchstens 1% betragen.

2.11.3 Ist die Wahrscheinlichkeit für den Angreifer, einen Beweis nach Ziffer 2.6 fälschen zu können, nicht im kryptografischen Sinn vernachlässigbar[3], muss die Erfolgswahrscheinlichkeit durch mehrmaliges Auszählen beliebig reduziert werden können, indem die Prüferinnen und Prüfer zu jeder Auszählung einen zusätzlichen, unabhängigen Beweis nach Ziffer 2.6 erhalten.

[3] Dies entspricht etwa der Wahrscheinlichkeit, einen verschlüsselten Wert, der mit einem als sicher geltenden Algorithmus und entsprechender Parametrisierung verschlüsselt wurde, ohne Kenntnis des Schlüssels entschlüsseln zu können.

2.12 **Funktionale Anforderungen an den Prozess der Stimmabgabe mit Auswirkungen auf das kryptografische Protokoll**

2.12.1 Mit den Authentisierungsmerkmalen, die einer stimmberechtigten Person zugewiesen sind, kann nur eine Stimme abgegeben werden.

2.12.2 Die stimmende Person gibt ihre Stimme in die Benutzerplattform ein.

2.12.3 Die stimmende Person kann die Stimme bis zur Willensbekundung, sie abgeben zu wollen, verändern und anhand einer Übersicht prüfen.

2.12.4 Nachdem die stimmende Person die Möglichkeit hatte, die Stimme anhand der Übersicht zu prüfen, gibt sie in die Benutzerplattform ein, dass sie die Stimme in der eingegebenen Form abgeben will.

2.12.5 Die Beweise für die korrekte Stimmabgabe nach Ziffer 2.5 müssen sich in mindestens zwei sequenzielle Teilbeweise gliedern. Jede als Teilbeweis dargestellte Anzeige muss einen echten Beitrag an die Stichhaltigkeit des Beweises nach Ziffer 2.5 bilden.

2.12.6 Die Benutzerplattform zeigt der stimmenden Person den ersten Teilbeweis an, nachdem diese in die Benutzerplattform eingegeben hat, dass sie die Stimme abgeben will.

2.12.7 Die Benutzerplattform zeigt der stimmenden Person den nachfolgenden Teilbeweis erst dann an, wenn diese die Korrektheit des vorherigen Teilbeweises durch eine Eingabe in die Benutzerplattform bestätigt hat.

2.12.8 Indem die stimmende Person die Korrektheit des vorletzten Teilbeweises bestätigt, bekundet sie den Willen, die Stimme definitiv abgeben zu wollen.

2.12.9 Die Gruppe von Kontrollkomponenten registriert die Stimme als systemkonform abgegeben, wenn sie die Bestätigung, die Stimme definitiv abgeben zu wollen, erhalten hat.

2.12.10 Hat die stimmende Person den letzten Teilbeweis mit positivem Ergebnis geprüft, so ist die Stimmabgabe abgeschlossen. Der letzte Teilbeweis soll besonders leicht zu prüfen sein, indem sich die Prüfung möglichst auf die korrekte Anzeige eines einzigen Codes oder einer anderen einfachen Anzeige beschränkt.

2.12.11 Werden Stimmdaten importiert, so ist eine Setup-Komponente oder eine Druckkomponente ab jenem Zeitpunkt nicht mehr als vertrauenswürdig zu betrachten.

2.12.12 Werden in der Vorbereitung des Urnengangs vertrauliche Daten in ein Hilfsmittel der Prüferinnen und Prüfer importiert, so gelten für dieses dieselben Bestimmungen wie für Setup-Komponenten nach Ziffern 2 und 3.

2.13 **Anforderungen an die Definition und die Beschreibung des kryptografischen Protokolls**

2.13.1 Wo möglich werden Bausteine verwendet, die weltweit verbreitet sind und

vertieft durch kompetente Personen geprüft wurden. Als Massgabe können Standards, Referenzprojekte sowie wissenschaftliche Publikationen beigezogen werden. Abweichungen und Zweifelsfälle müssen im Rahmen der Risikobeurteilung nach Artikel 4 gesondert behandelt werden.

2.13.2 Handlungsanweisungen dürfen nicht unterspezifiziert sein. Die einzelnen Handlungsanweisungen müssen die Umsetzungsmöglichkeiten so weit eingrenzen, dass jede Umsetzung, die die Anweisung zulässt, auch mit der Erfüllung der Anforderungen an das kryptografische Protokoll konform ist.

2.14 Beweise über die Erfüllung der Anforderungen an das kryptografische Protokoll

2.14.1 Ein symbolischer und ein kryptografischer Beweis müssen belegen, dass das kryptografische Protokoll die Anforderungen in Ziffern 2.1-2.12 erfüllt.

2.14.2 Die Beweise müssen direkt auf die Protokollbeschreibung Bezug nehmen, die als Grundlage für die Systementwicklung dient.

2.14.3 Die Beweise dürfen bezüglich kryptografischer Grundkomponenten unter allgemein akzeptierten Sicherheitsannahmen geführt werden (beispielsweise «random oracle model», «decisional Diffie-Hellman assumption», «Fiat-Shamir heuristic»).

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

3.1 Der Betrieb der Setup-Komponente und mindestens einer Kontrollkomponente der Gruppe, die einen Teil des Schlüssels zur Entschlüsselung der Stimmen enthält, gehört in die direkte Zuständigkeit des Kantons und muss in dessen Infrastruktur erfolgen. Die Auslagerung an einen privaten Systembetreiber ist unzulässig.

3.2 Für die Wahl von Zufallswerten namentlich für Setup-Komponenten und Kontrollkomponenten ist die Verwendung von genügend Entropie sicherzustellen.

3.3 Prüferinnen oder Prüfer müssen die Beweise nach Ziffer 2.6 mindestens einmal prüfen und dazu ein technisches Hilfsmittel nach Ziffer 2 einsetzen.

3.4 Die betrieblichen Anforderungen für Setup-Komponenten nach Ziffer 3 gelten auch für technische Hilfsmittel der Prüferinnen und Prüfer. Die Prüferinnen und Prüfer können im Rahmen ihrer Verantwortung, die durch das kantonale Recht festgelegt wird, Abweichungen vorsehen.

3.5 Der Kanton kann mit Ausnahme der unter Ziffern 3.1 und 3.3 genannten Komponenten den Betrieb beliebiger Teile des Systems, einschliesslich der Kontrollkomponenten sowie der Druckkomponente an private Dienstleister delegieren. Ein privater Betreiber der Druckkomponente darf ausschliesslich betriebliche Aufgaben wahrnehmen, die für die Aufbereitung, Verpa-

ckung und Zustellung eine Voraussetzung bilden.

3.6 Vertrauenswürdige Komponenten (Setup-Komponenten, Druckkomponenten, technische Hilfsmittel der Prüferinnen und Prüfer sowie Kontrollkomponenten) müssen in einem beobachtbaren Prozess aufgesetzt, aktualisiert, konfiguriert und abgesichert werden.

3.7 Vor der Installation einer Software ist für sämtliche Programme anhand einer publizierten Referenz zu prüfen, ob es sich bei den Dateien um die korrekte und unverfälschte Version handelt.

3.8 Der Zeitpunkt für die Aktualisierung der gesamten Software von vertrauenswürdigen Komponenten ist so zu wählen, dass die dadurch erwarteten Vorteile gegenüber den möglichen Gefahren überwiegen.

3.9 Setup-Komponenten, Druckkomponenten und technische Hilfsmittel der Prüferinnen und Prüfer, die in irgendeiner Form an der Bearbeitung von kritischen Daten beteiligt sind, müssen während der gesamten Rechenzeit und bis zur Löschung allfälliger kritischer Daten oder bis zur sicheren Aufbewahrung im Vieraugenprinzip physisch überwacht werden. Sie dürfen höchstens über sichtbare physische Kabel untereinander verbunden sein, so dass bis zur Vernichtung der vertraulichen Daten ersichtlicherweise keine weiteren Maschinen auf sie zugreifen können.

3.10 Für die Installation oder die Aktualisierung von Software dürfen vertrauenswürdige Komponenten nicht mit dem Internet verbunden werden.

3.11 Im Grundsatz müssen kritische Daten nach ihrer Verwendung vernichtet werden. Beim Vorliegen guter Gründe ist als Alternative auch eine sichere Aufbewahrung des Datenträgers erlaubt.

3.12 Datenträger für den Datenaustausch oder die Aufbewahrung von Daten, wie USB-Sticks, müssen nach dem Aufspielen der Daten in die vertrauenswürdige Komponente entfernt werden und dürfen vor der Vernichtung der Daten nur dann wiederverwendet werden, wenn sich auf der vertrauenswürdigen Komponente vor dem Aufspielen der Daten keine kritischen Daten befunden haben.

Datenträger für den Datenaustausch müssen vor der Verwendung mithilfe einer Komponente, die entsprechend den Anforderungen an vertrauenswürdige Komponenten betrieben wird, neu formatiert und allfällige Daten darauf müssen vernichtet werden.

3.13 Es darf kein logischer Zugriff auf oder physischer Zugang zu vertrauenswürdigen Komponenten oder Datenträgern mit kritischen Daten möglich sein, ohne dass eine andere Person dies bemerkt, beispielsweise indem sie für die Gewährung des Zugriffs mitwirken muss (strenges Vieraugenprinzip).

3.14 Ein geglückter unerlaubter Zugriff auf eine Kontrollkomponente soll möglichst keinen Vorteil beim Versuch verschaffen, auf eine weitere Kontrollkomponente unbemerkt zuzugreifen. Zusätzlich zu den übrigen Anforderungen nach Ziffer 3 gelten dahingehend die folgenden Anforderungen:

– Hat eine Person physischen oder logischen Zugriff auf eine Kontrollkomponente, so darf sie keinen Zugriff auf eine andere Kontrollkomponente haben.
– Die Hardware, die Betriebssysteme und die Überwachungssysteme der Kontrollkomponenten sollen sich unterscheiden.
– Die Kontrollkomponenten sollen an unterschiedliche Netzwerke angeschlossen sein.
– Eine Kontrollkomponente muss durch ein physisches Gerät realisiert werden. Virtualisierung über mehrere physische Geräte ist nicht zulässig.

3.15 Kontrollkomponenten müssen darauf ausgerichtet sein, unerlaubte Zugriffe zu erkennen und die verantwortlichen Personen zu alarmieren. Die verantwortlichen Personen sollen externe Überwachungsmassnahmen vorsehen, wie beispielsweise die Überwachung und die manipulationsresistente Protokollierung des Netzverkehrs oder die physische Überwachung mit Kameras, die ihrer Kontrolle unterliegen. Die verantwortlichen Personen müssen als besonders vertrauenswürdig und zuverlässig gelten.

3.16 Vertrauenswürdige Komponenten müssen ausschliesslich die vorgesehenen Operationen durchführen.

3.17 Die Software des technischen Hilfsmittels der Prüferinnen und Prüfer muss von einem anderen Systementwickler bezogen werden als jenem, der den grössten Teil der Software der übrigen Systembestandteile entwickelt hat. Die Publikation der Software des technischen Hilfsmittels unter einer Lizenz, die die Kriterien nach Open Source Software[4] erfüllt, kann eine Ausnahme begründen. Bringen Prüferinnen oder Prüfer mehrere technische Hilfsmittel zum Einsatz, so gilt diese Bestimmung für mindestens eines.

3.18 Alle Abläufe im Umgang mit vertrauenswürdigen Komponenten müssen schriftlich und für die betroffenen Personen leicht verständlich dokumentiert sein.

3.19 Jeder Zugriff und jede Verwendung einer vertrauenswürdigen Komponente oder eines Datenträgers mit kritischen Daten müssen protokolliert werden.

4. Stimmvorgang

4.1 Die stimmende Person erklärt, dass sie die Regeln der elektronischen Stimmabgabe und ihre Verantwortlichkeit zur Kenntnis genommen hat.

4.2 Die stimmende Person wird, bevor sie ihre Stimme abgibt, darauf aufmerksam gemacht, dass sie damit am Urnengang teilnimmt, wie wenn sie brieflich oder persönlich an der Urne abstimmen würde. Die stimmende Person

[4] vgl. dazu die Definition im Praxis-Leitfaden Open Source Software in der Bundesverwaltung, Version 1.0 vom 19.12.2019, Kap. 1; beziehbar bei: Schweizerische Bundeskanzlei, CH-3003 Bern; www.bk.admin.ch > Digitale Transformation und IKT Lenkung > Bundesarchitektur > Open Source Software (OSS).

kann ihre Stimme erst abgeben, nachdem sie bestätigt hat, dies zur Kenntnis genommen zu haben.

4.3 Die stimmende Person wird bei der Stimmabgabe aufgefordert, die Beweise nach Ziffer 2.5 anhand der Verifizierungsreferenz zu prüfen und allfällige Zweifel an deren Korrektheit beim Kanton zu melden.

4.4 Vor der definitiven elektronischen Stimmabgabe kann die stimmberechtigte Person ihre Stimme weiterhin über einen konventionellen Stimmkanal abgeben.

4.5 Das clientseitige System, wie es sich der stimmenden Person präsentiert, beeinflusst diese nicht in ihrer Entscheidungsfindung.

4.6 Die Benutzerführung verleitet nicht zu einer übereilten oder unüberlegten Stimmabgabe.

4.7 Das System bietet der stimmenden Person keine Funktion zum Ausdrucken der Stimme.

4.8 Der stimmenden Person wird nach Abschluss der Stimmabgabe keinerlei Information zum Inhalt der abgegebenen verschlüsselten Stimme angezeigt.

4.9 Einer stimmberechtigten Person, die keine Stimme abgeben kann, weil Drittpersonen unter missbräuchlicher Verwendung ihres Stimmmaterials eine Stimme abgegeben haben, kann der Kanton die Stimmabgabe weiterhin ermöglichen, indem er die missbräuchlich abgegebene Stimme für nichtig erklärt. Das Stimmgeheimnis nach Ziffer 2.7 ist zu wahren.

4.10 Für eine stimmberechtigte Person mit einer Behinderung dürfen Erleichterungen zur Überprüfung der Beweise vorgesehen werden. Ausschliesslich in einem solchen Fall darf von den Anforderungen nach Ziffer 2.9.1 abgewichen werden.

4.11 Solange das System keine Bestätigung der definitiven elektronischen Stimmabgabe registriert hat, kann eine stimmberechtigte Person ihre Stimme weiterhin über einen konventionellen Stimmkanal abgeben.

4.12 Die Verwendung eines von der elektronischen Stimmabgabe unabhängigen Authentisierungsmittels ist erlaubt. Auswirkungen auf die Integrität der Stimmrechtsprüfung sowie die Wahrung des Stimmgeheimnisses sind im Rahmen der Risikobeurteilung vertieft zu prüfen.

5. Vorbereitung des Urnengangs

5.1 Werden die Stimmregisterdaten aus einem Drittsystem importiert, das sich ausserhalb der Kontrolle des Kantons befindet, müssen die Daten verschlüsselt und signiert werden. Die Signatur muss bei Erhalt solcher Daten überprüft werden. Für die Zustellung an die Druckerei gehen die Bestimmungen nach Ziffer 7 vor.

5.2 Die Daten, die für die Prüfung der Beweise nach Ziffer 2.6 notwendig sind, werden an die Prüferinnen und Prüfer übergeben.

6. Anforderungen an die Stimmrechtsausweise

6.1 Sicherheitselemente auf dem Stimmrechtsausweis (Hydalamsiegel, Rubbelcode) dürfen nur verwendet werden, wenn ein Nachweis vorliegt, dass die verdeckte Information gut vor unerlaubtem Lesen geschützt ist.

6.2 Wird auf die Verwendung von Sicherheitselementen zum Schutz vertraulicher Informationen auf dem Stimmrechtausweis verzichtet, so müssen Organisationsabläufe zur Gewährleistung der Sicherheit vorhanden sein.

7. Anforderungen an Druckereien

7.1 Der Datenträger mit den Druckdaten zur Produktion der Stimmrechtsausweise wird immer von zwei Personen der Druckerei überbracht (Vieraugenprinzip). Die Daten können auch verschlüsselt und signiert zugestellt werden.

7.2 Die Daten auf dem Datenträger sind verschlüsselt. Die Verschlüsselung genügt den Anforderungen aus dem eCH-Standard 0014[5], Kapitel 7. Das Geheimelement zur Entschlüsselung wird den Verantwortlichen der Druckerei auf einem sicheren Zweitweg zugestellt.

7.3 Die Verantwortlichen der Druckerei, die den Datenträger entgegennehmen, unterschreiben eine Empfangsbestätigung.

7.4 Für den Datenträger mit den Druckdaten, die Komponente, auf der die kritischen Daten entschlüsselt werden, sowie alle Komponenten, die die kritischen Daten verarbeiten, gelten die Bestimmungen nach Ziffer 3 an die Druckkomponente.

7.5 Die Verantwortlichen der Druckerei nehmen eine Materialmengenkontrolle vor.

7.6 Nach dem Drucken der Stimmrechtsausweise vernichtet die Druckerei die erhaltenen Daten.

7.7 Nimmt die Druckerei auch die Verpackung und den Versand der Stimmrechtsausweise vor, so sind diese unverzüglich nach dem Druck zusammen mit dem Stimmmaterial zu verpacken.

7.8 Die Vertrauenswürdigkeit des Kanals zwischen der Druckerei und den Stimmberechtigten darf nur dann als gegeben erachtet werden, wenn die nach kantonalem Recht zuständigen Stellen das verpackte Stimmmaterial den Stimmberechtigten brieflich zustellen oder die persönliche Übergabe sicherstellen.

[5] eCH-0014: Standards und Architekturen für eGovernment Anwendungen Schweiz (SAGA.ch), Version 9.0 vom 09.12.2019; der Standard kann kostenlos bezogen und eingesehen werden beim Verein eCH, Mainaustrasse 30, Postfach, 8034 Zürich, www.ech.ch.

8. Informationen und Anleitungen

8.1 Die auf kantonaler Ebene verantwortliche Stelle erstellt ein Konzept zur Information der Bürgerinnen und Bürger über die elektronische Stimmabgabe.

8.2 Das Konzept gewährleistet, dass die Informationen von den zuständigen Gremien autorisiert werden.

8.3 Auf dem Internet finden sich Ratschläge und Anleitungen zur Stimmabgabe sowie Informationen zur Verantwortlichkeit der Stimmberechtigten. Diese wirken einer überstürzten oder unüberlegten Handlungsweise entgegen.

8.4 Den Stimmberechtigten werden die Verifizierbarkeit, weitere Sicherheitsmassnahmen sowie das Vorgehen bei Anomalien auf zugängliche Weise erklärt.

8.5 Den Stimmberechtigten wird erklärt, worauf sie achten müssen, damit sie ihre Stimme sicher abgeben können.

8.6 Den Stimmberechtigten wird erklärt, wie die Stimme in der zur Stimmeingabe verwendeten Benutzerplattform nach der Stimmabgabe auf allen Speichern gelöscht werden kann.

8.7 Die Stimmberechtigten können technischen Support anfordern.

8.8 Die Stimmberechtigten werden aufgerufen, falsch angezeigte Prüfcodes oder weitere Prüfungen mit negativem Ergebnis bei der auf kantonaler Ebene verantwortlichen Stelle zu melden. Dieser Aufruf wird insbesondere mit dem Stimmmaterial verbreitet.

8.9 Die Stimmberechtigten erhalten die nötigen Angaben, um die Authentizität der zur Stimmabgabe benutzten Internetseite, des Servers und der Software zu kontrollieren. Die Aussagekraft einer erfolgreichen Kontrolle muss durch den Einsatz kryptografischer Mittel gemäss besten Praktiken unterstützt werden.

8.10 Die für die sichere Stimmabgabe wesentlichen Informationen werden mit dem Stimmmaterial verschickt. Den Stimmberechtigten wird erklärt, dass sie sich im Zweifelsfall an die Informationen des Stimmmaterials halten sollen und nicht an die Informationen, die auf der Benutzerplattform angezeigt werden.

8.11 Den Stimmberechtigten wird erklärt, wie die Verifizierbarkeit und die Wahrung des Stimmgeheimnisses sichergestellt sind.

8.12 Bekannte Mängel und der mit ihnen verbundene Handlungsbedarf werden transparent kommuniziert.

8.13 Die Prüferinnen und Prüfer werden zu Prozessen, denen die Korrektheit des Ergebnisses, die Einhaltung des Stimmgeheimnisses und das Fehlen vorzeitiger Teilergebnisse unterliegen (beispielsweise Schlüsselgenerierung, Druck des Stimmmaterials, Entschlüsselung und Auszählung), angemessen informiert und geschult. Sie

sind in der Lage, die Vorgänge und ihre Bedeutung in den Kernpunkten zu verstehen.

9. Öffnen und Schliessen des elektronischen Stimmkanals

Der elektronische Stimmkanal steht nur im erlaubten Zeitraum zur Verfügung.

10. Konformitätskontrolle und Ablage endgültig abgegebener Stimmen

Eine nicht systemkonform abgegebene Stimme wird nicht in der elektronischen Urne abgelegt.

11. Auszählung der elektronischen Urne

11.1 Die Entschlüsselung der Stimmen und deren Auszählung dürfen frühestens am Abstimmungs- oder Wahlsonntag beginnen.

11.2 Der Kanton führt die Entschlüsselung und die Auszählung in der eigenen Infrastruktur durch.

11.3 Der Kanton sorgt für die Protokollierung der Entschlüsselung der Stimmen sowie deren Auszählung. Die Freigabe des Protokolls erfolgt durch die auf kantonaler Ebene verantwortliche Stelle.

11.4 Von der Entschlüsselung der Stimmen bis zur Übermittlung des Ergebnisses des Urnengangs erfolgt jeder Zugriff auf das System oder auf eine seiner Komponenten durch mindestens zwei Personen gemeinsam; er wird schriftlich aufgezeichnet und er muss von den Prüferinnen und Prüfern kontrolliert werden können.

11.5 Werden die Ergebnisdaten an ein Drittsystem übermittelt, das sich ausserhalb der Kontrolle des Kantons befindet, werden die Daten verschlüsselt und signiert.

11.6 Das System ermöglicht es, dass anhand des Stimmrechtsausweises festgestellt werden kann, ob jemand eine elektronische Stimme abgegeben hat.

11.7 Die Prüferinnen und Prüfer sind bei der Entschlüsselung und Auszählung anwesend.

11.8 Für die Komponenten, die zur Auszählung der Stimmen verwendet werden, gelten dieselben Anforderungen wie für Setup-Komponenten nach Ziffer 3.

11.9 Die Prüferinnen und Prüfer nehmen ihre Verantwortung nach Massgabe des kantonalen Rechts bei der Prüfung der Beweise nach Ziffer 2.6 wahr.

11.10 Die auf kantonaler Ebene verantwortliche Stelle unterbreitet den Prüferinnen und Prüfern sämtliche relevanten Indikatoren für die Korrektheit des Ergebnisses. Dazu gehören nebst der Beweisen nach Ziffer 2.6 insbesondere auch die Zahl und die Art von Anomalien, die durch Stimmberechtigte beim Kanton gemeldet wurden.

11.11 Der Kanton antizipiert allfällige Anomalien und erstellt dahingehend in Absprache mit den betroffenen Stellen einen Notfallplan, der das jeweilige

Vorgehen festlegt. Er schafft Transparenz gegenüber der Öffentlichkeit.

12. Vertrauliche Daten

12.1 Es ist sichergestellt, dass weder Mitarbeitende noch externe Personen Daten kennen, die einen Bezug zwischen der Identität der stimmenden Person und ihrer Stimme zulassen.

12.2 Es ist sichergestellt, dass weder Mitarbeitende noch externe Personen vor dem Zeitpunkt der Entschlüsselung der Stimmen Daten kennen, die die Erhebung vorzeitiger Teilergebnisse erlauben.

12.3 Der Kanton darf seinen Teil des Schlüssels zur Entschlüsselung der Stimmen, der ihm nach Ziffer 3.1 auf der von ihm betriebenen Kontrollkomponente vorliegt, nicht an private Unternehmen weiterleiten.

12.4 Der Kanton behandelt die Ergebnisse des Urnengangs zwischen dem Zeitpunkt der Entschlüsselung der Stimmen und dem Zeitpunkt der Publikation vertraulich.

12.5 Der Kanton sorgt dafür, dass Daten vertraulich behandelt werden, die es erlauben festzustellen, ob eine stimmberechtigte Person auf dem elektronischen Weg eine Stimme abgegeben hat.

12.6 Der Kanton sorgt dafür, dass persönliche Daten aus dem Stimmregister vertraulich behandelt werden. Er darf diese Daten nicht an private Unternehmen weiterleiten, wenn sie die Rolle eines Systembetreibers wahrnehmen.

12.7 Der Kanton behandelt die einzelnen Stimmen nach der Auszählung vertraulich.

12.8 Der Kanton sorgt dafür, dass Abstimmungs- und Wahlergebnisse kleiner Wahlkreise vertraulich behandelt werden.

12.9 Nach der Erwahrung werden gemäss einem vorgegebenen und dokumentierten Prozess sämtliche Daten vernichtet, die im Rahmen des elektronischen Urnengangs angefallen sind, in Bezug zu den einzelnen eingegangenen Stimmen stehen und als vertraulich klassifiziert sind.

13. Bedrohungen

13.1 Die in den Ziffern 13.3–13.39 aufgelisteten Bedrohungen sind allgemeiner Art und bilden eine minimale Grundlage. Sie beziehen sich auf die Sicherheitsziele und sind bei der Identifizierung von Risiken zu berücksichtigen. In Abhängigkeit der identifizierten Schwachstellen des Systems und bei der Risikobeurteilung der verschiedenen Stellen ist die Liste entsprechend der konkreten Konstellation und in Abhängigkeit der spezifischen Bedrohung zu konkretisieren und zu ergänzen.

13.2 Als mögliche Bedrohung gelten:

– versehentlich oder absichtlich verursachte Bedrohungen, die von internen oder externen Akteurinnen und Akteuren ausgehen, die elekt-

ronische oder physische Mittel einsetzen;

– Bedrohungen, die auf eine Fehlfunktion des Systems oder der systemunterstützenden Elemente zurückzuführen sind.

	Beschreibung	**Betroffenes Sicherheitsziel (nach Art. 4 Abs. 3)**
13.3	Malware verändert die Stimme auf der Benutzerplattform.	Korrektheit des Ergebnisses
13.4	Ein externer Angreifer leitet die Stimme mittels Domain-Name-Server-Spoofing (DNS-Spoofing)[6] um.	Korrektheit des Ergebnisses
13.5	Ein externer Angreifer verändert die Stimme mit einer Man-in-the-middle-Technik (MITM[7]-Technik).	Korrektheit des Ergebnisses
13.6	Ein externer Angreifer schickt mittels MITM bösartig veränderte Stimmzettel.	Korrektheit des Ergebnisses
13.7	Ein interner Angreifer manipuliert die Software, diese speichert die Stimmen nicht.	Korrektheit des Ergebnisses
13.8	Ein interner Angreifer verändert die Stimmen.	Korrektheit des Ergebnisses
13.9	Ein interner Angreifer fügt Stimmen ein.	Korrektheit des Ergebnisses
13.10	Eine feindliche Organisation dringt in das System ein mit dem Ziel, das Ergebnis zu fälschen.	Korrektheit des Ergebnisses
13.11	Ein interner Angreifer kopiert Stimmunterlagen und benutzt sie.	Korrektheit des Ergebnisses

[6] Auch DNS-Poisoning genannt. Bezeichnet einen Angriff, bei dem es gelingt, die Zuordnung zwischen einem Hostnamen und der zugehörigen IP-Adresse zu fälschen.

[7] 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 physisch oder logisch zwischen den beiden Kommunikationspartnern, hat dabei mit seinem System vollständige Kontrolle über den Datenverkehr zwischen zwei oder mehreren Netzwerkteilnehmerinnen und -teilnehmern und kann die Informationen nach Belieben einsehen und sogar manipulieren.

	Beschreibung	**Betroffenes Sicherheitsziel (nach Art. 4 Abs. 3)**
13.12	Ein externer Angreifer nutzt Social-Engineering-Methoden, um die Aufmerksamkeit der stimmenden Person an den Sicherheitsvorkehrungen vorbeizulenken (individuelle Verifizierbarkeit).	Korrektheit des Ergebnisses
13.13	Ein externer Angreifer dringt elektronisch, physisch oder mittels Social Engineering in die Infrastruktur des Kantons ein und entnimmt sicherheitsrelevante Daten während der Einstellung der Parameter des Urnengangs.	Korrektheit des Ergebnisses
13.14	Ein externer Angreifer dringt elektronisch, physisch oder mittels Social Engineering in die Infrastruktur der Druckerei ein und entnimmt die Codes der Stimmrechtsausweise.	Korrektheit des Ergebnisses
13.15	Ein externer Angreifer dringt elektronisch, physisch oder mittels Social Engineering in die Infrastruktur der Post ein und entwendet Stimmrechtsausweise.	Korrektheit des Ergebnisses
13.16	In der individuellen Verifizierbarkeit tritt ein Fehler auf.	Korrektheit des Ergebnisses
13.17	In der universellen Verifizierbarkeit tritt ein Fehler auf.	Korrektheit des Ergebnisses
13.18	Ein technisches Hilfsmittel der Prüferinnen und Prüfer weist einen Fehler auf.	Korrektheit des Ergebnisses

	Beschreibung	**Betroffenes Sicherheitsziel (nach Art. 4 Abs. 3)**
13.19	Eine Backdoor[8] wird über eine Softwareabhängigkeit in das System eingeführt und von einem externen Angreifer ausgenutzt, um auf das System zuzugreifen.	Korrektheit des Ergebnisses, Wahrung des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse, Erreichbarkeit und Funktionsfähigkeit des Stimmkanals, Schutz der für die Stimmberechtigten bestimmten Informationen vor Manipulationen, keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten
13.20	Malware auf der Benutzerplattform schickt die Stimme an eine feindliche Organisation.	Wahrung des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse
13.21	Die Stimme wird mittels DNS-Spoofing umgeleitet.	Wahrung des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse
13.22	Ein externer Angreifer liest die Stimme mittels MITM.	Wahrung des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse
13.23	Ein interner Angreifer benutzt den Schlüssel und entschlüsselt nicht-anonyme Stimmen.	Wahrung des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse
13.24	Bei der Prüfung auf Korrektheit der Verarbeitung und der Auszählung wird das Stimmgeheimnis gebrochen.	Wahrung des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse
13.25	Ein interner Angreifer liest die Stimmen vorzeitig, ohne die Stimmen entschlüsseln zu müssen.	Wahrung des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse
13.26	Eine feindliche Organisation dringt ins System ein mit dem Ziel, das Stimmgeheimnis zu brechen oder vorzeitige Teilergebnisse zu erheben.	Wahrung des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse

[8] Backdoor bezeichnet einen Teil einer Software, der es ermöglicht, unter Umgehung der normalen Zugriffssicherung Zugang zum Computer oder einer sonst geschützten Funktion eines Computerprogramms zu erlangen.

	Beschreibung	**Betroffenes Sicherheitsziel (nach Art. 4 Abs. 3)**
13.27	Ein Fehler im Verschlüsselungsprozess macht diesen funktionsunfähig oder reduziert seine Wirksamkeit.	Wahrung des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse
13.28	Malware auf der Benutzerplattform macht die Stimmabgabe unmöglich.	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals
13.29	Eine feindliche Organisation führt einen Denial-of-Service-Angriff (DOS-Angriff)[9] durch.	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals
13.30	Ein interner Angreifer nimmt eine fehlerhafte Konfiguration vor; es kommt nicht bis zur Auszählung.	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals
13.31	Ein interner Angreifer fälscht die kryptografischen Beweise der universellen Verifizierbarkeit.	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals
13.32	Ein technischer Fehler des Systems führt dazu, dass das System zum Zeitpunkt der Auszählung nicht verfügbar ist.	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals
13.33	Ein technisches Hilfsmittel der Prüferinnen und Prüfer funktioniert zum Zeitpunkt der Auszählung nicht.	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals
13.34	Eine feindliche Organisation dringt ins System ein mit dem Ziel, den Betrieb zu stören, die Informationen für die Stimmberechtigten zu manipulieren oder Beweise zum Stimmverhalten der stimmenden Personen zu stehlen.	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals, Schutz der für die Stimmberechtigten bestimmten Informationen vor Manipulationen, keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten
13.35	Ein interner Angreifer stiehlt Adressdaten der Stimmberechtigten.	Schutz der persönlichen Informationen über die Stimmberechtigen

[9] Englisch für Dienstverweigerung. Bezeichnet in der digitalen Datenverarbeitung die Nichtverfügbarkeit eines Dienstes, der eigentlich verfügbar sein sollte.

	Beschreibung	Betroffenes Sicherheitsziel (nach Art. 4 Abs. 3)
13.36	Malware beeinflusst Stimmberechtigte bei der Meinungsbildung.	Schutz der für die Stimmberechtigten bestimmten Informationen vor Manipulationen
13.37	Ein interner Angreifer manipuliert die Informationswebsite bzw. das Abstimmungsportal und täuscht so die Stimmberechtigten.	Schutz der für die Stimmberechtigten bestimmten Informationen vor Manipulationen
13.38	Ein interner Angreifer schreibt Stimmberechtigten vor, ob und wie sie abzustimmen oder zu wählen haben. Nach der Entschlüsselung findet er in der Infrastruktur Belege, dass sich die Stimmberechtigten an die Instruktionen gehalten haben.	Keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten
13.39	Ein externer Angreifer schreibt Stimmberechtigten vor, ob und wie sie abzustimmen oder zu wählen haben und verlangt von ihnen einen Beleg, dass sie sich an die Instruktionen gehalten haben.	Keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten

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

14.1 Ein Monitoringsystem der Infrastruktur erkennt die Zwischenfälle, die die Sicherheit oder die Verfügbarkeit des Systems gefährden könnten, und alarmiert das zuständige Personal. Das Personal behandelt Zwischenfälle gemäss vordefinierten Verfahren. Krisenszenarien und Rettungspläne dienen als Leitlinie (darin inbegriffen ist ein Plan, der gewährleistet, dass die auf den Urnengang bezogenen Aktivitäten weitergeführt werden können) und kommen bei Bedarf zur Anwendung.

Fehler bei der Registrierung der Stimme in den Kontrollkomponenten und in der Urne müssen erkannt werden. Dabei müssen weitere Informationen im Zusammenhang mit dem Fehler verfügbar sein, um die Ursache zu erkennen und zu beheben. Festgestellte Vorfälle sind der auf kantonaler Ebene verantwortlichen Stelle zu melden.

14.2 Auf der Infrastruktur werden Protokolle erstellt, deren Erfassung, Übertragung und Speicherung gegen Manipulationen resistent sind (Systemprotokolle). Die Protokolle sind untereinander konsistent und ermöglichen bei der Untersuchung von vermuteten Manipulationen oder Fehlern die Rückverfolgung der relevanten Ereignisse. Sie dienen als Belege für die

vollständige, unverfälschte und ausschliessliche Berücksichtigung systemkonform abgegebener Stimmen sowie für die Einhaltung des Stimmgeheimnisses und das Fehlen vorzeitiger Teilergebnisse.

Der Inhalt der Protokolle umfasst mindestens die folgenden Ereignisse:

- Start und Ende der Audit-, Identifizierungs- und Authentisierungsprozesse;
- Start, Neustart und Ende der Abstimmungs- oder Wahlphase;
- Start der Auszählung mit der Ergebnisermittlung;
- Durchführung und Ergebnisse allfälliger Selbsttests;
- festgestellte Störungen in den Elementen der IT-Infrastruktur, die die Betriebsfähigkeit beeinträchtigen.

Von jedem Ereignis werden das Datum und die Uhrzeit, die Art des Ereignisses, den möglichen Verursacher und das Ergebnis im Sinne von Misserfolg oder Erfolg dokumentiert.

Die Systemprotokolle werden der auf kantonaler Ebene verantwortlichen Stelle so zur Verfügung gestellt, dass diese die Informationen interpretieren kann.

14.3 Das Monitoring und die Erfassung von Systemprotokollen unterliegen einem ständigen Verbesserungsprozess. Der Verbesserungsprozess beinhaltet einen offenen Dialog zwischen den beteiligten Akteurinnen und Akteuren sowie eine regelmässige und objektive Beurteilung der Wirksamkeit der eingesetzten Instrumente und Prozesse. Die Ergebnisse dieser Evaluationen werden dabei berücksichtigt.

14.4 Das Monitoring und die Erfassung von Systemprotokollen beeinträchtigen die Wirksamkeit der Massnahmen zur Gewährleistung des Stimmgeheimnisses in keiner Weise.

14.5 Es ist gewährleistet, dass im Falle einer Panne die Stimmen und die Daten, die ein reibungsloses Funktionieren des Verfahrens bei der Auszählung der Stimmen belegen, unversehrt auf der Infrastruktur gespeichert werden.

14.6 Nach einer Panne des Systems oder einem Ausfall von Kommunikations- oder Speichermedien, geht das System in einen Wartungsmodus über, in dem die Möglichkeit besteht, in einen sicheren Zustand zurückzukehren. Begonnene Stimmvorgänge werden unterbrochen. Die stimmende Person kann die Stimmabgabe erst dann wieder aufnehmen, wenn sich das System wieder in einem sicheren Zustand befindet.

14.7 Es ist möglich, mit Hilfe von Authentisierungsmerkmalen Kontrollstimmen abzugeben, die keiner stimmberechtigten Person zugewiesen sind. Der Inhalt dieser Kontrollstimmen wird protokolliert. Die Auszählung der Kontrollstimmen wird mit den Protokollen verglichen.

Es ist sichergestellt, dass die Kontrollstimmen möglichst ähnlich gehandhabt werden wie systemkonform abgegebene Stimmen, gleichzeitig ist

sichergestellt, dass sie nicht gezählt werden.

14.8 Die Verfügbarkeit der Infrastruktur wird in gewählten Zeitabständen überprüft und protokolliert.

14.9 Statistische Methoden können, soweit sie verfügbar sind und soweit die Datenbasis dies erlaubt, zur Plausibilisierung des Ergebnisses eingesetzt werden.

14.10 Durch einen vorgegebenen und dokumentierten Prozess werden die Teile des Systems, die vom Internet erreichbar sind, regelmässig aktualisiert, um bekanntgewordene Schwachstellen zu eliminieren.

14.11 Die Massnahmen für das Monitoring und zur Protokollierung der Systembenutzung, der Tätigkeiten von Administratoren und zur Störungsprotokollierung werden detailliert beschrieben, umgesetzt, überwacht und überprüft.

15. Einsatz von kryptografischen Massnahmen und Schlüsselverwaltung

15.1 Elektronische Zertifikate werden nach besten Praktiken verwaltet.

15.2 Zur Sicherstellung der Integrität von Datensätzen, welcher die Korrektheit des Ergebnisses sowie die Geheimhaltung geheimer und vertraulicher Daten unterliegt, einschliesslich der Identifikations- und Authentifizierungsdaten der Behörden, kommen wirksame kryptografische Massnahmen zum Einsatz, die dem Stand der Technik entsprechen.

15.3 Zur Sicherstellung der Geheimhaltung geheimer und vertraulicher Daten kommen in der Infrastruktur wirksame kryptografische Massnahmen zum Einsatz, die dem Stand der Technik entsprechen. Solche Daten werden auf Datenträgern immer verschlüsselt abgespeichert.

15.4 Kryptografische Grundkomponenten kommen nur dann zur Anwendung, wenn die Schlüssellängen und Algorithmen den gängigen Standards entsprechen (z. B. NIST, ECRYPT, ZertES). Die elektronische Signatur erfüllt die Anforderungen einer fortgeschrittenen elektronischen Signatur nach dem Bundesgesetz vom 18. März 2016[10] über die elektronische Signatur (ZertES). Die Verifikation der Signatur erfolgt mittels eines Zertifikats, das von einem nach ZertES anerkannten Anbieter von Zertifizierungsdiensten ausgestellt wird.

16. Sicherer elektronischer und physischer Informationsaustausch

16.1 Sämtliche Komponenten der Infrastruktur werden in einer separaten Netzwerkzone betrieben. Diese Netzwerkzone wird durch eine angemessene Routingkontrolle gegenüber dem übrigen Netzwerk geschützt.

16.2 Die Systeme sind vor Angriffen, unabhängig von der Art der Angriffe oder ihrer Herkunft, geschützt.

[10] SR **943.03**

16.3 Die elektronische Stimmabgabe ist von sämtlichen anderen Anwendungen klar getrennt.

17. Tests des Systems

17.1 Die Funktionen, die für die Sicherheit des Systems relevant sind (Sicherheitsfunktionen), werden getestet, und die Tests werden mit Testplänen, erwarteten und tatsächlichen Testergebnissen dokumentiert.

Der Testplan:

- legt die auszuführenden Tests fest;
- beschreibt die Szenarien für jeden Test, einschliesslich allfälliger Abhängigkeiten von den Ergebnissen anderer Tests.

Die erwarteten Ergebnisse müssen die Ergebnisse aufzeigen, die bei erfolgreicher Testausführung erwartet werden.

Die tatsächlichen Ergebnisse müssen mit den erwarteten Ergebnissen übereinstimmen.

17.2 Es wird eine Analyse der Testabdeckung erstellt. Diese umfasst den Nachweis, dass:

- die in der Testdokumentation definierten Tests und die funktionalen Spezifikationen der Schnittstellen übereinstimmen;
- alle Schnittstellen vollständig getestet wurden.

17.3 Es wird eine Analyse der Testtiefe durchgeführt. Diese umfasst den Nachweis, dass:

- die in der Testdokumentation definierten Tests und die Teilsysteme, die sich auf Sicherheitsfunktionen und Module beziehen, die eine Rolle bei der Gewährleistung der Sicherheit spielen, übereinstimmen;
- alle Teilsysteme, die mit den in den Spezifikationen genannten Sicherheitsfunktionen zusammenhängen, getestet wurden;
- alle Module, die bei der Gewährleistung der Sicherheit eine Rolle spielen, getestet wurden.

18. Organisation der Informationssicherheit

18.1 Alle Rollen und Verantwortlichkeiten für den Betrieb des Systems werden präzise definiert, zugeordnet und kommuniziert.

18.2 Für Einrichtungen zur Informationsverarbeitung der Infrastruktur wird ein Autorisierungsprozess eingerichtet.

18.3 Die Risiken im Zusammenhang mit Dritten (Auftragnehmer wie Lieferanten, Dienstleister usw.) werden identifiziert und über angemessene vertragliche Vereinbarungen soweit nötig reduziert. Die Einhaltung der Vereinbarungen wird während ihrer Laufzeit angemessen überwacht und überprüft.

19. Verwaltung der immateriellen und materiellen Ressourcen

19.1 Alle immateriellen und materiellen Ressourcen im Sinne des Begriffs Asset in der Norm ISO/IEC 27001, 2013, Information technology – Security techniques – Information security management systems – Requirements[11], die im Zusammenhang mit der elektronischen Stimmabgabe relevant sind (Organisation als Ganzes, insbesondere die Organisationsprozesse und die in diesen Prozessen bearbeiteten Informationen, Datenträger, Einrichtungen zur Informationsverarbeitung der Infrastruktur und Räumlichkeiten der Infrastruktur) werden in einem Inventar erfasst. Über das Personal wird eine Liste geführt. Das Inventar und die Personalliste sind aktuell zu halten. Jeder immateriellen und materiellen Ressource wird eine Person zugewiesen, die dafür die Verantwortung übernimmt.

19.2 Der zulässige Gebrauch von immateriellen und materiellen Ressourcen wird definiert.

19.3 Für Informationen werden Klassifizierungsleitlinien erlassen und kommuniziert.

19.4 Für die Kennzeichnung und Handhabung von Information werden Verfahren eingerichtet.

20. Vertrauenswürdigkeit des Personals

20.1 Zur Gewährleistung der Vertrauenswürdigkeit des Personals vor, während und nach Beendigung der Anstellung oder bei Rollenwechseln werden angemessene Richtlinien und Verfahren eingerichtet und kommuniziert.

20.2 Für die Gewährleistung der Vertrauenswürdigkeit des Personals übernehmen die Personalverantwortlichen die volle Verantwortung.

20.3 Das gesamte Personal verfügt über ein ausgeprägtes Informationssicherheitsbewusstsein. Dazu wird ein aufgabengerechtes Ausbildungs- und Trainingsprogramm eingerichtet und betrieben.

21. Physische und umgebungsbezogene Sicherheit

21.1 Die Sicherheitsperimeter der verschiedenen Räumlichkeiten der Infrastruktur sind klar definiert.

21.2 Für den physischen Zugang zu diesen verschiedenen Räumlichkeiten der Infrastruktur werden Zugangsberechtigungen definiert, eingerichtet und angemessen kontrolliert.

21.3 Zur Gewährleistung der Sicherheit von Geräten innerhalb und ausserhalb der Räumlichkeiten der Infrastruktur werden angemessene Richtlinien und Verfahren definiert und deren Einhaltung überwacht und überprüft.

21.4 Sämtliche Daten werden ausschliesslich in der Schweiz bearbeitet, dazu

[11] Die Norm kann gegen Bezahlung bezogen werden beim Zentralsekretariat der Internationalen Organisation für Normung (ISO), Chemin de Blandonnet 8, CP 401, 1214 Vernier oder unter www.iso.org.

gehört auch die Aufbewahrung.

22. Management der Kommunikation und des Betriebs

22.1 Pflichten und Verantwortlichkeitsbereiche werden so aufgeteilt, dass die mit Betrieb und Kommunikation verbundenen Risiken personellen Ursprungs auf Restrisiken reduziert werden, die mit den Risikoakzeptanzkriterien kompatibel sind.

22.2 Zum Schutz vor Schadsoftware werden angemessene Massnahmen getroffen.

22.3 Es wird ein detaillierter Plan für die Datensicherung erstellt und umgesetzt. Die korrekte Funktion der Datensicherung wird regelmässig überprüft.

22.4 Es werden angemessene Massnahmen zum Schutz des Netzwerks und der Sicherheit von Netzwerkservices definiert und umgesetzt.

22.5 Die Verfahren zur Handhabung von Wechseldatenträgern und zur Entsorgung von Datenträgern werden detailliert geregelt.

23. Zuteilung, Verwaltung und Entzug von Zugangs- und Zugriffsrechten

23.1 Es muss gewährleistet sein, dass während des Urnengangs jede nachträgliche Änderung von Zugangs- und Zugriffsrechten nur mit der Zustimmung der auf kantonaler Ebene verantwortlichen Stelle erfolgt.

23.2 Der Zugang zu und der Zugriff auf die Infrastruktur und die Software werden auf der Basis einer Risikobeurteilung detailliert geregelt und dokumentiert. In Hochrisikobereichen sowie für alle manuellen Operationen im Zusammenhang mit der elektronischen Urne (z. B. Öffnung des Stimmkanals, Schliessung des Stimmkanals, Start der Auszählung) gilt das Vieraugenprinzip.

Manuelle Operationen im Zusammenhang mit der elektronischen Urne (z. B. Öffnung des Stimmkanals, Schliessung des Stimmkanals, Start der Auszählung) werden explizit authentifiziert.

23.3 Es muss gewährleistet sein, dass Informationen auf der Website zur elektronischen Stimmabgabe und diesbezügliche Informationsseiten nicht ohne Berechtigung geändert werden können.

23.4 Während des Urnengangs müssen sachfremde Zugriffe jeglicher Art auf die Infrastruktur ausgeschlossen sein.

23.5 Es muss sichergestellt sein, dass keines der Elemente der clientseitigen Authentisierungsmerkmale bei der Zustellung systematisch abgefangen, verändert oder umgeleitet werden kann. Zur Authentisierung müssen Massnahmen und Technologien zum Einsatz kommen, die das Risiko des systematischen Missbrauchs durch Dritte hinreichend minimieren.

24. Entwicklung und Wartung von Informationssystemen

24.1 Entwicklung

24.1.1 Es wird ein Lebenszyklusmodell definiert. Das Lebenszyklusmodell:

- wird für die Entwicklung und Wartung der Software verwendet;
- sieht die notwendigen Kontrollen bei der Entwicklung und Wartung der Software vor;
- wird dokumentiert.

24.1.2 Es wird eine Liste der eingesetzten Entwicklungswerkzeuge sowie der Konfigurationsoptionen, die für den Einsatz der einzelnen Entwicklungswerkzeuge gewählt wurden, erstellt.

24.1.3 Die Dokumentation der Entwicklungswerkzeuge umfasst:

- eine Definition des Entwicklungswerkzeugs;
- eine Beschreibung aller Konventionen und Richtlinien, die bei der Implementierung des Entwicklungswerkzeugs verwendet werden;
- eine eindeutige Beschreibung der Bedeutung aller Konfigurationsoptionen für die Anwendung des Entwicklungswerkzeugs.

24.1.4 Es wird festgelegt, welche Implementierungsstandards angewendet werden.

24.1.5 Die Software wird so spezifiziert und implementiert, dass die Sicherheitsfunktionen nicht umgangen werden können.

24.1.6 Die Sicherheitsfunktionen werden so spezifiziert und implementiert, dass sie vor Manipulation geschützt sind.

24.1.7 Die Sicherheitsarchitektur der Software wird dokumentiert. Die Dokumentation:

- weist einen Detaillierungsgrad auf, welcher der Beschreibung der Sicherheitsfunktionen entspricht;
- beschreibt die Sicherheitsdomänen, auf die sich die Sicherheitsfunktionen richten;
- beschreibt, wie die Initialisierungsprozesse gesichert werden;
- weist die Erfüllung der Ziffern 24.1.5 und 24.1.6 nach.

24.1.8 Die funktionalen Spezifikationen werden dokumentiert. Die Dokumentation:

- bildet die gesamte Software ab;
- beschreibt den Zweck und die Anwendung aller Schnittstellen;
- identifiziert und beschreibt alle Parameter, die mit den Schnittstellen verbunden sind;
- beschreibt alle Aktionen, die mit Schnittstellen verbunden sind;

– beschreibt alle direkten Fehlermeldungen, die durch den Aufruf der einzelnen Schnittstellen entstehen können.

24.1.9 Die Nachvollziehbarkeit zwischen funktionalen Spezifikationen und Sicherheitsanforderungen wird bis auf die Ebene der Schnittstellen sichergestellt.

24.1.10 Alle Sicherheitsfunktionen sind im Quellcode implementiert.

24.1.11 Die Nachvollziehbarkeit zwischen dem gesamten Quellcode und den Spezifikationen der Sicherheitsfunktionen ist sichergestellt und deren Übereinstimmung ist erwiesen.

24.1.12 Die Sicherheitsfunktionen werden so konzipiert und implementiert, dass sie gut strukturiert sind. Die interne Struktur wird beschrieben und enthält eine Begründung, die:

– die Merkmale angibt, die zur Beurteilung von «gut strukturiert» und von «Komplexität» verwendet werden;

– aufzeigt, dass alle Sicherheitsfunktionen gut strukturiert und nicht zu komplex sind.

24.1.13 Die Spezifikationen umfassen folgende Aspekte:

– eine Beschreibung der Struktur der Software in Form von Teilsystemen;

– eine Beschreibung der Sicherheitsfunktionen als Module sowie für jedes Modul die Zielsetzung und eine Beschreibung, wie das Modul zu den anderen Modulen in Beziehung steht; die Beschreibung der sicherheitsrelevanten Module umfasst auch die verfügbaren Schnittstellen, die Rückgabewerte dieser Schnittstellen und die Schnittstellen der anderen Module, die sie zur Interaktion mit ihnen verwenden;

– eine Beschreibung aller Teilsysteme, die mit den Sicherheitsfunktionen zusammenhängen einschliesslich der möglichen Wechselwirkungen untereinander;

– eine Abbildung der mit Sicherheitsfunktionen verbundenen Teilsysteme auf ihre Module für den Nachweis, dass alle Schnittstellen dem in der Spezifikation beschriebenen Verhalten entsprechen.

24.1.14 Die Software wird mit einer eindeutigen Kennzeichnung versehen.

24.1.15 Die Dokumentation des Konfigurationsmanagements enthält:

– eine Beschreibung, wie Konfigurationselemente identifiziert werden;

– einen Konfigurationsmanagementplan, der beschreibt, wie das Konfigurationsmanagementsystem bei der Entwicklung der Software eingesetzt wird und welche Verfahren für die Übernahme von Änderungen oder neuen Elementen angewendet werden;

– einen Nachweis, dass die Verfahren für die Übernahme eine angemessene Prüfung der Änderungen für alle Konfigurationselemente vorsehen.

24.1.16 Das Konfigurationsmanagementsystem:

- identifiziert alle Konfigurationselemente eindeutig;
- stellt automatisierte Massnahmen bereit, damit nur autorisierte Änderungen an Konfigurationselementen vorgenommen werden;
- unterstützt die Entwicklung der Software durch automatisierte Verfahren;
- stellt sicher, dass die Person, die für die Abnahme des Konfigurationselements verantwortlich ist, nicht dieselbe Person ist, die es entwickelt hat;
- identifiziert die Konfigurationselemente, aus denen sich die Sicherheitsfunktionen zusammensetzen;
- unterstützt die Prüfung aller Änderungen an der Software mit automatisierten Verfahren, einschliesslich der Protokollierung des Verfassers sowie des Datums und der Uhrzeit der Änderung;
- stellt ein automatisiertes Verfahren zur Identifizierung aller Konfigurationselemente bereit, die von einer Änderung an einem bestimmten Konfigurationselement betroffen sind;
- kann die Version des Quellcodes identifizieren, auf dessen Basis die Software generiert wird.

24.1.17 Alle Konfigurationselemente werden im Konfigurationsmanagementsystem inventarisiert.

24.1.18 Das Konfigurationsmanagementsystem wird in Übereinstimmung mit dem Konfigurationsmanagementplan verwendet.

24.1.19 Es wird eine Konfigurationsliste erstellt, die die folgenden Elemente enthält:

- die Software;
- Nachweise der erforderlichen Überprüfungen zur Einhaltung der Sicherheit;
- die Teile, aus denen die Software besteht;
- den Quellcode;
- Berichte über Sicherheitsmängel und über den Stand der Behebung.

Für jedes Element, das für Sicherheitsfunktionen relevant ist, wird die Entwicklerin oder der Entwickler genannt. Jedes Element wird eindeutig identifiziert.

24.1.20 Die Dokumentation zur Sicherheit der Softwareentwicklung umfasst:

- die Beschreibung der physischen, verfahrenstechnischen, personellen und sonstigen Sicherheitsmassnahmen, die zum Schutz und zur Integrität der Ausgestaltung und der Implementierung der Software in ihrer Entwicklungsumgebung erforderlich sind;
- den Nachweis, dass die Sicherheitsmassnahmen das erforderliche

Schutzniveau bieten, um die Integrität der Software zu wahren.

24.2 Betrieb

24.2.1 Es wird ein Betriebshandbuch erstellt, das für jede Benutzerrolle folgende Aspekte enthält:

- eine Beschreibung der Funktionen, auf die die Benutzerin oder der Benutzer zugreifen kann, und der Berechtigungen, die in einer sicheren Umgebung kontrolliert werden müssen, einschliesslich entsprechender Warnungen;
- eine Beschreibung, wie die verfügbaren Schnittstellen auf sichere Weise genutzt werden können;
- eine Beschreibung der verfügbaren Funktionen und Schnittstellen, insbesondere aller Sicherheitsparameter, die unter der Kontrolle der Benutzerin oder des Benutzers stehen unter Hervorhebung der für die Sicherheit relevanten Werte;
- eine präzise Darstellung aller Typen von Sicherheitsereignissen in Bezug auf die auszuführenden, für die Benutzerin oder den Benutzer zugänglichen Funktionen, einschliesslich der Anpassungen der Sicherheitseigenschaften von Elementen, die der Kontrolle der Sicherheitsfunktionen unterliegen;
- Beschrieb der Sicherheitsmassnahmen, die umzusetzen sind, um die betrieblichen Sicherheitsziele zu erreichen.

24.2.2 Das Betriebshandbuch muss alle möglichen Betriebsarten der Software aufzeigen, dies einschliesslich der Wiederaufnahme des Betriebs nach der Entdeckung von Fehlern sowie der Beschrieb der Folgen und Auswirkungen von Fehlern auf die Aufrechterhaltung des sicheren Betriebs.

24.2.3 Das Betriebshandbuch muss präzise und zweckmässig sein.

24.3 Zuverlässige und nachvollziehbare Kompilierung und Deployment

24.3.1 Der Vorbereitungsprozess beschreibt alle Schritte, die notwendig sind für:

- eine sichere Abnahme der Systembestandteile in Übereinstimmung mit dem Verfahren für die Bereitstellung;
- eine sichere Aufbereitung der Betriebsumgebung in Übereinstimmung mit den betrieblichen Sicherheitszielen;
- eine sichere Installation der Software in der Betriebsumgebung.

24.3.2 Die Bereitstellung des Software oder von Teilen des Systems wird dokumentiert und umfasst alle Prozesse, die zur Aufrechterhaltung der Sicherheit bei der Bereitstellung der Software erforderlich sind.

24.3.3 Es ist eine zuverlässige und überprüfbare Kompilierung mit angemessenen Sicherheitsmassnahmen durchzuführen. Damit ist sichergestellt, dass der

ausführbare Code eine überprüfbare und getreue Darstellung des Quellcodes ist, der einer öffentlichen Kontrolle und unabhängigen Prüfungen unterzogen wurde. Die Kompilierung erlaubt es, eine Beweiskette für die Überprüfung der Software anzulegen, und umfasst insbesondere:

- den Nachweis, dass die Kompilierumgebung so ausgestaltet ist, wie sie auf der öffentlichen Plattform beschrieben ist (Gesamtheit der Werkzeuge mit der jeweiligen Version, Betriebssystem und allfälligen Konfigurationen); allfällige Abweichungen sind zu dokumentieren und zu begründen;
- den Nachweis, dass die Software gemäss den auf der öffentlichen Plattform verfügbaren Anweisungen kompiliert wurde; wird bei der Kompilierung ein Mangel in den Instruktionen festgestellt, so ist dieser zu protokollieren und die Dokumentation anschliessend anzupassen;
- den Nachweis, dass der zur öffentlichen Kontrolle vorgelegte und geprüfte Quellcode tatsächlich derjenige ist, der zur Kompilierung verwendet wurde;
- den Nachweis, dass keine anderen als die in den Instruktionen vorgesehenen Elemente eingeführt wurden;
- den Nachweis, dass alle kryptografischen Signaturen der Abhängigkeiten gegen eine bewährte, öffentliche und vertrauenswürdige Referenz (z. B. Maven Central Repository) verifiziert wurden;
- den Nachweis, dass eine Analyse der Schwachstellen in Bezug auf Abhängigkeiten durchgeführt wurde und dass, sofern für die Software relevante Schwachstellen vorhanden sind, diese die Software nicht angreifbar machen;
- den Nachweis, dass die allenfalls eingeführten Parameter das System nicht angreifbar machen.

24.3.4 Es ist ein zuverlässiges und überprüfbares Deployment mit angemessenen Sicherheitsmassnahmen durchzuführen. Damit ist sicherzustellen, dass:

1. der produktiv eingesetzte Code eine überprüfbare und getreue Darstellung des Quellcodes ist, der einer öffentlichen Kontrolle und unabhängigen Prüfungen unterzogen wurde; und
2. dass die Produktionsumgebung mit derjenigen übereinstimmt, die der öffentlichen Kontrolle und unabhängigen Prüfungen unterzogen wurde.

Das Deployment erlaubt es, eine Beweiskette für die Überprüfung der Software anzulegen, und umfasst insbesondere:

- den Nachweis, dass die Produktionsumgebung mit derjenigen übereinstimmt, die der öffentlichen Kontrolle und unabhängigen Überprüfungen unterzogen wurde; allfällige Abweichungen (Firmware-Version, Konfigurationsdateien usw.) sind zu dokumentieren und zu begründen;

- den Nachweis, dass die in der Produktionsumgebung eingesetzte Software tatsächlich diejenige ist, die im zuverlässigen und überprüfbaren Kompilierungsverfahren erstellt wurde;
- den Nachweis, dass die allenfalls eingeführten Parameter das System nicht angreifbar machen.

24.3.5 Die Qualität der Nachweise der zuverlässigen und überprüfbaren Kompilierung und des zuverlässigen und überprüfbaren Deployments wird durch die Anwesenheit von mindestens zwei Zeuginnen oder Zeugen verschiedener Institutionen oder durch technische Verfahren zur Feststellung des Wahrheitsgehalts nach dem Stand der wissenschaftlichen Erkenntnisse und Erfahrungen bestätigt.

24.3.6 Die Nachweiskette der zuverlässigen und überprüfbaren Kompilierung und des zuverlässigen und überprüfbaren Deployments wird öffentlich zugänglich gemacht.

24.4 Systematische Behebung von Mängeln

24.4.1 Es werden Prozesse zur Behebung von Mängeln definiert. Die Prozesse umfassen:

- eine Dokumentation dieser Prozesse, insbesondere im Hinblick auf die Rückverfolgbarkeit von Mängeln für alle Versionen der Software sowie der Methoden, die verwendet werden, damit die Systembenutzerinnen und -benutzer über die Informationen über die Mängel, die Korrekturen und zu möglichen Korrekturmassnahmen verfügen;
- die Pflicht, die Art und die Auswirkungen aller Sicherheitsmängel, Informationen zum Stand der Arbeiten zur Lösungsfindung sowie die beschlossenen Korrekturmassnahmen zu beschreiben;
- eine Beschreibung der Instrumente, mit denen die Systembenutzerinnen und -benutzer die Möglichkeit erhalten, den Softwareentwicklerinnen und -entwicklern Berichte und Anfragen zu vermuteten Mängeln in der Software bekanntmachen zu können;
- ein Verfahren, das eine zeitnahe Reaktion und ein automatischer Versand von Berichten über Sicherheitsmängel und entsprechenden Korrekturen an registrierte Systembenutzerinnen und -benutzer, die vom Mangel betroffen sein könnten, erfordert.

24.4.2 Es wird ein Prozess für die Behandlung der gemeldeten Mängel definiert.

Dieser Prozess stellt sicher, dass alle gemeldeten und bestätigten Mängel behoben werden und dass die Prozesse zur Behebung den Systembenutzerinnen und -benutzern mitgeteilt werden.

Er sieht Vorkehrungen vor, die sicherstellen, dass eine Behebung von Sicherheitsmängeln keine neuen Sicherheitsmängel nach sich zieht.

24.4.3 Es werden Richtlinien für die Einreichung und die Behebung von Mängeln definiert. Diese umfassen:

- eine Anleitung, wie Systembenutzerinnen und -benutzer vermutete Sicherheitsmängel an die Entwicklerin oder den Entwickler melden können;
- eine Anleitung, wie sich Systembenutzerinnen und -benutzer bei der Entwicklerin oder beim Entwickler registrieren können, um Berichte über Sicherheitsmängel und die Behebungen zu erhalten;
- die Angabe von spezifischen Kontaktstellen für alle Berichte und Anfragen zu Sicherheitsfragen, die die Software betreffen.

24.5 Qualitätssicherung

Es wird regelmässig und objektiv geprüft, ob die durchgeführten Abläufe sowie die dazugehörenden Arbeitsprodukte mit der Beschreibung der umzusetzenden Abläufe, Normen und Prozesse übereinstimmen. Abweichungen werden bis zu ihrer Behebung weiterverfolgt.

25. Qualität Quellcode und Dokumentation

Der Quellcode und die Dokumentation erfüllen, mindestens die folgenden Qualitätskriterien:

25.1 Nachvollziehbarkeit

25.1.1 Als Nachvollziehbarkeit wird die Stringenz von den Anforderungen bis hin zur Implementierung verstanden.

25.1.2 Alle Anforderungen an das kryptografische Protokoll sind über sämtliche Arbeitsergebnisse im Zusammenhang mit dem Softwareentwicklungsprozess hinweg nachvollziehbar.

25.1.3 Für die Verbindung zwischen den rechtlichen Anforderungen und dem Protokoll, den Spezifikationen sowie der Dokumentation der Architektur gibt es einen Beschrieb.

25.2 Vollständigkeit

25.2.1 Als Vollständigkeit gilt die vollständige Umsetzung der geforderten Funktionen.

25.2.2 Die Software enthält keine mehrdeutigen Verweise (Input, Funktion, Output). Wird dasselbe Element referenziert, wird dazu immer die gleiche Bezeichnung verwendet.

25.2.3 Alle referenzierten Daten und alle verwendeten Funktionen sind in den Spezifikationen definiert.

25.2.4 Es werden alle in den Spezifikationen definierten Funktionen verwendet.

25.2.5 Für jeden Entscheidungspunkt (z. B. bedingte Ausführung) sind die möglichen Alternativen in den Spezifikationen definiert.

25.2.6 Alle Parameter sind in den Spezifikationen definiert und validiert (keine implizite Parameterübergabe).

25.2.7 Alle schwerwiegenden, gemeldeten Fehler werden behoben, bevor mit dem nächsten Schritt im Entwicklungszyklus fortgefahren wird.

25.2.8 Das kryptografische Protokoll, die Spezifikation, das Design und der Quellcode sind aufeinander abgestimmt.

25.3 Kohärenz

25.3.1 Als Kohärenz gilt die Verwendung einheitlicher Verfahren und Notationen bei der Konzeption und der Implementierung.

25.3.2 Die Darstellungen in der Dokumentation entsprechen einer Konvention, die die Softwareentwicklerin oder der Softwareentwickler erstellt hat.

25.3.3 Die Funktionen und die Variablen entsprechen einer Namenskonvention, die die Softwareentwicklerin oder der Softwareentwickler erstellt hat.

25.3.4 Input und Output von Funktionen werden nach einer Konvention behandelt, die die Softwareentwicklerin oder der Softwareentwickler erstellt hat.

25.3.5 Fehler werden nach einer Konvention behandelt, die die Softwareentwicklerin oder der Softwareentwickler erstellt hat.

25.3.6 Die verwendeten Variablentypen sind kohärent.

25.4 Einheitlichkeit der Kommunikation

25.4.1 Als Einheitlichkeit der Kommunikation gilt die Verwendung von standardisierten Protokollen und Schnittstellenroutinen.

25.4.2 Die Regeln für die Kommunikation mit anderen Systemen sind definiert.

25.4.3 Die Kommunikation basiert auf standardisierten Kommunikationsmethoden.

25.5 Einheitlichkeit der Daten

25.5.1 Als Einheitlichkeit der Daten gilt die Eigenschaft, die die Verwendung einer standardisierten Darstellung der Daten ermöglicht.

25.5.2 Die Standarddarstellung der Daten für die Kommunikation mit anderen Systemen wird formell festgelegt.

25.5.3 Für Konvertierungen zwischen den verschiedenen Darstellungen werden Standards festgelegt.

25.5.4 Die Konvertierungsfunktionen sollten in einem Modul zentralisiert werden.

25.6 **Erlernbarkeit**

25.6.1 Als Erlernbarkeit gilt die Eigenschaft der Software, die es den Benutzerinnen und Benutzern ermöglicht, sich die Bedienung der Software leicht anzueignen.

25.6.2 Personen, die das System betreiben und anwenden, werden geschult und mit der notwendigen Dokumentation bedient.

25.6.3 Die Schulung beinhaltet die Möglichkeit, an einem dafür vorgesehenen System zu trainieren.

25.6.4 Hilfestellungen zur Bedienung sind leicht zugänglich.

25.7 **Bedienbarkeit**

25.7.1 Als Bedienbarkeit gilt die Nutzungsqualität bei der Interaktion mit dem System.

25.7.2 Die Software ist benutzerfreundlich. Die Benutzerführung richtet sich nach allgemein bekannten Schemen.

25.7.3 Der clientseitige Teil der Software entspricht dem Accessibility Standard eCH-0059[12].

25.8 **Fehlertoleranz**

25.8.1 Mit der Fehlertoleranz wird die Weiterführung des Betriebs unter Ausnahmebedingungen ermöglicht.

25.8.2 Fehler werden erkannt und behandelt, damit das Programm ohne Unterbrechung weiterlaufen kann.

25.8.3 Die Fehlerbehandlung (einschliesslich der Erfassung im Protokoll) erfolgt auf derjenigen Ebene, die für die Weiterführung des Betriebs am relevantesten ist. Ein Fehler, der in einer Ebene nicht bearbeitet werden kann, wird in die nächsthöhere Ebene übertragen.

25.8.4 Für die Inputparameter werden Gültigkeitsbedingungen definiert.

25.8.5 Alle Inputparameter werden vor Beginn der Ausführung überprüft.

25.9 **Modularität**

25.9.1 Als Modularität gilt die Eigenschaft der Software, die eine Struktur von hochgradig unabhängigen Modulen bietet.

25.9.2 Die Aufgabe der einzelnen Module wird klar definiert.

25.9.3 Die Aufgabe der einzelnen Module sollte eng und fokussiert sein und die Aufgaben zweier Module sollten sich nicht überschneiden.

12 eCH-0059: Accessibility Standard Version 3.0 vom 25.06.2020; der Standard kann kostenlos bezogen und eingesehen werden beim Verein eCH, Mainaustrasse 30, Postfach, 8034 Zürich; http://www.ech.ch.

25.9.4 Die Module teilen keine Daten über einen gemeinsamen volatilen Speicher (z. B. globale Variable).

25.10 **Einfachheit**

25.10.1 Als Einfachheit gilt die Implementierung der Funktionen auf die verständlichste Art. Im Allgemeinen bedeutet dies, dass Praktiken vermieden werden, die die Komplexität erhöhen.

25.10.2 Im Design wird ein Top-Down-Ansatz (hierarchische Struktur) gewählt.

25.10.3 Das Design sieht keine Verdoppelung von Funktionen zwischen den Modulen vor.

25.10.4 Das Design sieht keine globalen Daten vor, d. h. keine Daten, die von allen verwendet werden können, ohne als Parameter übergeben zu werden.

25.10.5 Komplizierte boolesche Kombinationen im Quellcode werden vermieden.

25.10.6 Im Quellcode werden keine Variablen für andere als die ursprünglich vorgesehenen Zwecke wiederverwendet.

25.10.7 Im Quellcode wird die Anzahl von Verschachtelungen so weit wie möglich beschränkt.

25.10.8 Die zyklomatische und kognitive Komplexität im Quellcode wird so weit wie möglich beschränkt.

25.11 **Prägnanz**

25.11.1 Als Prägnanz gilt, wenn eine Funktion mit einem Minimum an Instruktionen im Quellcode implementiert werden kann.

25.11.2 Die Software enthält keine überflüssigen Abschnitte im Quellcode (sogenannten «Dead Code») .

25.11.3 Der Quellcode enthält keine überflüssigen Variablen.

25.11.4 Der Quellcode enthält keine Wiederholungen.

25.12 **Verständlichkeit**

25.12.1 Als Verständlichkeit gilt, wenn die Adressatinnen und Adressaten die Zielsetzung, Annahmen, Einschränkungen, Input und Output, Komponenten und Status der Software erkennen können.

25.12.2 Klassen, Funktionen und komplexe Verarbeitungsschritte werden im Quellcode nach einer von der Softwareentwicklerin oder dem Softwareentwickler festgelegten Konvention kommentiert.

25.12.3 Variablen und Funktionen werden mit aussagekräftigen Namen bezeichnet.

25.12.4 Pro Zeile wird eine Anweisung erstellt. Anweisungen, die sich auf mehrere Zeilen beziehen, und mehrere Anweisungen pro Zeile sind zu vermeiden.

25.13 **Instrumentierung**

25.13.1 Als Instrumentierung gilt eine Eigenschaft der Software, die es erlaubt, ihre Nutzung zu messen oder Fehler zu erkennen.

25.13.2 Die Unit-Tests[13] decken alle möglichen Pfade und die zulässigen Werte der Inputparameter ab.

25.13.3 Die Integrationstests decken alle Module ab.

25.13.4 Die Softwaretestszenarien decken alle Module ab.

25.13.5 Fehler und notwendige Informationen werden in Logs protokolliert.

26. Prüfkriterien für die Systeme und ihren Betrieb

26.1 Prüfung des kryptografischen Protokolls (Art. 10 Abs. 1 Bst. a)

26.1.1 Gegenstand: Es wird geprüft:

- ob die Anforderungen in Artikel 5 in Verbindung mit den Artikeln 6–8 und Ziffer 2 des Anhangs erfüllt sind; diese Beurteilung erfolgt insbesondere anhand der kryptografischen und symbolischen Beweise;
- ob und inwiefern sich das kryptografische Protokoll auf existierende und bewährte Protokolle und Bausteine abstützt;
- welche Vertiefungen und Verbesserungen zu einer Stärkung der Sicherheit beitragen könnten.

26.1.2 Zuständigkeiten: Die Prüfung erfolgt durch Expertinnen und Experten aus der Kryptografie. Die Bundeskanzlei gibt die Prüfung in Auftrag und kontrolliert die auftragsgemässe Erfüllung.

26.1.3 Zeitpunkt der Prüfung:

- Eine komplette Überprüfung erfolgt vor der ersten Inbetriebnahme.
- Die Prüfung wird nach zwei bis drei Jahren erneut durchgeführt.
- Die Prüfung findet bei jeder Änderung des Protokolls und bei relevanten neuen Erkenntnissen der Forschung bezüglich der Sicherheit von verwendeten kryptografischen Elementen sowie der Bedrohungslage neu statt.

[13] Bei einem Unit-Test testet der Entwickler ein Modul unabhängig vom Rest des Programms, um sicherzustellen, dass das Modul die funktionalen Spezifikationen erfüllt und unter allen Umständen korrekt funktioniert. Diese Überprüfung wird bei kritischen Anwendungen als unerlässlich angesehen.

26.2 Prüfung der Software des Systems (Art. 10 Abs. 1 Bst. b)

26.2.1 Gegenstand: Es wird geprüft:

- ob das nach Ziffer 26.1 geprüfte kryptografische Protokoll umgesetzt ist; die korrekte Umsetzung von Funktionen vertrauenswürdiger Komponenten muss besonders eingehend geprüft werden;
- ob die Software des Systems die Anforderungen dieser Verordnung erfüllt und die vorgegebenen Zielsetzungen adäquat unterstützt;
- ob die Software mit dem Standard eCH-0059 konform ist; die Prüfung kann sich auf ein gültiges Zertifikat stützen, das von einer von der Bundeskanzlei anerkannten Institution ausgestellt wurde und die Konformität mit dem Standard belegt.

26.2.2 Zuständigkeiten: Die Prüfung erfolgt durch Expertinnen und Experten aus der Kryptografie und der Softwareentwicklung. Die Prüfung wird von der Bundeskanzlei in Auftrag gegeben.

26.2.3 Zeitpunkt der Prüfung:

- Eine komplette Überprüfung erfolgt vor der ersten Inbetriebnahme.
- Die Prüfung wird nach zwei bis drei Jahren erneut durchgeführt.
- Die Prüfung findet bei jeder wesentlichen Änderung neu statt, insbesondere:
  - nach einer Änderung am kryptografischen Protokoll;
  - bei jeder Änderung am Quellcode der Funktionen, deren Vertrauenswürdigkeit für die Stichhaltigkeit der im Rahmen der Verifizierbarkeit vorgesehenen Beweise massgeblich sind;
  - bei relevanten neuen Erkenntnissen der Forschung bezüglich der Sicherheit von verwendeten kryptografischen Elementen sowie der Bedrohungslage;
  - beim Verzicht oder bei wesentlichen Anpassungen an Mechanismen, die dem sicheren Einsatz von vertrauenswürdigen Komponenten nach Ziffer 2 dienen.

26.3 Prüfung der Sicherheit von Infrastruktur und Betrieb (Art. 10 Abs. 1 Bst. c)

26.3.1 Gegenstand: Es wird geprüft, ob:

- das System und sein Betrieb beim Kanton, beim Systembetreiber und bei der Druckerei die Anforderungen dieser Verordnung erfüllen und die vorgegebenen Zielsetzungen adäquat unterstützen;
- die Basiskomponenten, wie beispielsweise Software, die dem sicheren und unabhängigen Einsatz von Kontrollkomponenten dient, die eingesetzten Betriebssysteme oder die eingesetzten Server erwiesenermassen besten Standards entsprechen.

26.3.2 Zuständigkeiten: Die Prüfung erfolgt durch Expertinnen und Experten aus der Kryptografie und dem Betrieb von hochsicheren Systemen. Die Prüfung wird von der Bundeskanzlei in Auftrag gegeben.

26.3.3 Zeitpunkt der Prüfung:

- Eine komplette Überprüfung erfolgt vor der ersten Inbetriebnahme.
- Die Prüfung wird nach zwei bis drei Jahren erneut durchgeführt.
- Die Prüfung findet bei jeder wesentlichen Änderung neu statt, insbesondere:
  - nach einer Änderung am kryptografischen Protokoll;
  - beim Verzicht oder bei wesentlichen Anpassungen an Mechanismen, die dem sicheren Einsatz von vertrauenswürdigen Komponenten nach Ziffer 2 dienen;
  - bei einer wesentlichen Änderung der Prozesse oder der Infrastruktur.
- Werden neue Versionen von Basiskomponenten eingesetzt (neue Server, Patches zu Betriebssystem oder Software, die dem sicheren und unabhängigen Einsatz von vertrauenswürdigen Komponenten nach Ziffer 2 dient), muss keine neue Kontrolle erfolgen, sofern die Basiskomponenten weiterhin erwiesenermassen besten Standards entsprechen.

26.4 Prüfung des Schutzes gegen Versuche, in die Infrastruktur einzudringen (Art. 10 Abs. 1 Bst. d)

26.4.1 Gegenstand: Es wird geprüft, ob es den Expertinnen und Experten im Auftrag der Bundeskanzlei gelingt, im Rahmen eines Tests die Infrastruktur des Online-Systems einzudringen und sich Zugang zu wichtigen Daten zu verschaffen oder die Kontrolle über wichtige Funktionen zu übernehmen.

Die Tests werden auf der Grundlage von potenziellen Schwachstellen durchgeführt, die nach einer methodischen Analyse der öffentlich zugänglichen Unterlagen, insbesondere nach Artikel 11, entdeckt wurden. Die Expertinnen und Experten prüfen im Mindesten Schwachstellen, die im Open-Web-Application Security-Project (OWASP) dokumentiert sind.

26.4.2 Zuständigkeiten: Die Prüfung erfolgt durch Sicherheitsexpertinnen und -experten. Die Prüfung wird von der Bundeskanzlei in Auftrag gegeben.

26.4.3 Zeitpunkt der Prüfung:

- Eine komplette Überprüfung erfolgt vor der ersten Inbetriebnahme.
- Die Prüfung wird nach zwei bis drei Jahren erneut durchgeführt.
- Die Prüfung findet bei jeder wesentlichen Änderung der Infrastruktur neu statt.
- Die Prüfung findet bei relevanten neuen Erkenntnissen bezüglich der

Sicherheit der eingesetzten Betriebsmittel sowie der Bedrohungslage statt.

26.5 Prüfung des Informationssicherheitsmanagement-Systems (Art. 10 Abs. 2)

26.5.1 Gegenstand: Es wird geprüft, ob das ISMS des Systembetreibers mit der Norm ISO/IEC 27001, 2013, Information technology – Security techniques – Information security management systems – Requirements konform ist. Der Geltungsbereich des ISMS umfasst alle Organisationseinheiten des Systembetreibers, die rechtlich, administrativ und betrieblich für das System verantwortlich sind.

26.5.2 Zuständigkeiten: Die Zertifizierungsstelle ist durch die Schweizerische Akkreditierungsstelle für die Durchführung von Audits nach der Norm ISO/IEC 27001, 2013, Information technology – Security techniques – Information security management systems – Requirements akkreditiert. Die Prüfung wird vom Kanton oder vom Systembetreiber in Auftrag gegeben; der Kanton sorgt für die Durchführung der Prüfung.

26.5.3 Dauer der Gültigkeit eines Belegs: Wiederholungsaudits werden in den durch die Norm ISO/IEC 27001, 2013, Information technology – Security techniques – Information security management systems – Requirements festgelegten Abständen durchgeführt. Ein gültiges Zertifikat und die entsprechende «Statement of Applicability» liegt bei jedem Einsatz des Systems vor. Wird eine neue Version des Standards ISO/IEC 27001, 2013, Information technology – Security techniques – Information security management systems – Requirements publiziert, so wird spätestens nach Ablauf der Übergangsfrist eine gültige Zertifizierung des ISMS nach der neuen Version nachgewiesen. Der Geltungsbereich des ISMS darf dabei nicht reduziert werden.