Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK

Sektion Politische Rechte

13. Dezember 2013

Technische und administrative Anforderungen an die elektronischen Stimmabgabe

Inkrafttreten: 15.1.2014

V. 1.0

Inhaltsverzeichnis

1. Allgemeines

1.1 Referenzen

1.1.1 Bundesgesetz vom 17. Dezember 1976 über die politischen Rechte (BPR; SR 161.1)

1.1.2 Verordnung vom 24. Mai 1978 über die politischen Rechte (VPR; SR 161.11)

1.1.3 Anforderungskatalog Druckereien für Vote électronique (Dokument der BK)

1.1.4 Common Criteria Schutzprofil für Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte, Version 1.0 (BSI-CC-PP-0037-2008)

1.1.5 ISO/IEC 27001:2013 Standard

1.1.6 Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES; SR 943.03)

1.1.7 eCH-0059: Accessibility Standard Version 2.0, 13.04.2011

Die oben genannten Dokumente können bei folgenden Organisationen bezogen werden:

Gesetzestexte mit einer SR-Referenz	Bundesamt für Bauten und Logistik (BBL) Vertriebsstelle für Bundespublikationen CH-3003 Bern http://www.bundespublikationen.ch
ISO-Normen	Zentralsekretariat der Internationalen Organisation für Normung (ISO) Rue de Varembé 1 1211 Genève http://www.iso.org
Anforderungskatalog für Druckereien	Schweizerische Bundeskanzlei CH-3003 Bern www.bk.admin.ch > Themen > Politische Rechte > Vote électronique > Versuchsbedingungen
Common Criteria Schutzprofil	Bundesamt für Sicherheit in der Informationstechnik Postfach 200362 D-53133 Bonn, Deutschland https://www.bsi.bund.de
e-CH Standards	Verein eCH Mainaustrasse 30, Postfach, 8034 Zürich http://www.ech.ch

1.2 Abkürzungen

BK	Bundeskanzlei
BPR	Bundesgesetz über die politischen Rechte
BSI	Bundesamt für Sicherheit in der Informationstechnik (Deutschland)
CC	Common Criteria
DOS	Denial Of Service
DNS	Domain Name Server
EAL	Evaluation Assurance Level
ISO	International Organization for Standardization
MITM	Man In The Middle
PIN	Personal Identification Number
PP	Protection Profile
SAS	Schweizerische Akkreditierungsstelle
SFR	Security Functional Requirements
VPR	Verordnung über die politischen Rechte

1.3 Begriffsbestimmungen

1.3.1 Authentisierung

1.3.1.1 Clientseitiges Authentisierungsmerkmal

Alle für die einzelnen Stimmberechtigten individuell bereitsgestellten Informationen, die sie brauchen, um eine Stimme abgeben zu können (kann beispielsweise ein PIN sein, dessen Eingabe letztlich in der Erstellung einer Signatur der Stimme resultiert). Aufgrund des clientseitigen Authentisierungsmerkmals erstellt das verwendete technische Hilfsmittel eine Authentisierungsnachricht (beispielsweise die Signatur der Stimme), die an die Infrastruktur geschickt wird. Mithilfe der Authentisierungsnachricht und des serverseitigen Authentisierungsmerkmals (beispielsweise ein öffentlicher Schlüssel zur Überprüfung der Signatur) authentisiert die Infrastruktur den Absender einer Stimme als Stimmberechtigten. Clientseitige Authentisierungsmerkmale sollen schwer zu erraten sein.

1.3.1.2 Serverseitiges Authentisierungsmerkmal

Alle Informationen, um mithilfe einer Authentisierungsnachricht den Absender einer Stimme als Stimmberechtigten zu authentisieren.

1.3.1.3 Authentisierungsnachricht

Alle Informationen, die eine Benutzerplattform nach Eingabe des clientseitigen Authentisierungsmerkmals an die Infrastruktur schickt, damit diese den Absender einer Stimme als Stimmberechtigten authentisiert. Es soll in der Praxis unmöglich sein, eine Authentisierungsnachricht ohne Kenntnis eines clientseitigen Authentisierungsmerkmals zu generieren.

1.3.2 Systemteile

1.3.2.1 System

Oberbegriff für Funktionalität und Infrastruktur. Derjenige Teil des Systems, der aus der Benutzerplattform und der clientseitigen Software der Funktionalität besteht, wird als clientseitiges System bezeichnet. Derjenige Teil des Systems, der aus Serverplattform und der serverseitigen Software der Funktionalität besteht, wird als serverseitiges System bezeichnet.

1.3.2.2 Infrastruktur (I)

Hardware, Software, Netzwerkelemente, Räumlichkeiten, Services und Betriebsmittel jeglicher Art, die zum technischen Betrieb der serverseitigen Funktionalität unter Gewährleistung aller Anforderungen an die Sicherheit und erforderlich sind.

1.3.2.3 Funktionalität (F)

Serverseitige Software und clientseitige Software auf der Benutzerplattform, welche zur Gewährleistung aller Anforderungen an die Sicherheit speziell für die elektronische Stimmabgabe entwickelt wurde.

1.3.2.4 Benutzerplattform

Multifunktionales, programmierbares Gerät, das mit dem Internet verbunden ist und zur Stimmabgabe verwendet wird. Im Allgemeinen handelt es sich um einen handelsüblichen Computer, ein Smartphone oder ein Tablet.

1.3.3 Stimme

1.3.3.1 Stimme, wie sie die stimmende Person in die Benutzerplattform eingegeben hat

Eine Stimme, welche der Erfassung durch den Stimmenden an der Benutzerplattform entspricht, und insbesondere seither nicht manipuliert wurde. Sie entspricht immer dem Willen des Stimmenden, ausser diesem unterläuft bei der Eingabe ein Irrtum.

1.3.3.2 Registrierte Stimme

Eine Stimme wird als registriert bezeichnet, wenn die Infrastruktur von der endgültigen Stimmabgabe Kenntnis genommen hat.

1.3.3.3 Teilstimme

Bezeichnet bei Abstimmungen eine Vorlage, einen Gegenvorschlag oder eine Stichfrage und bei Wahlen die Wahl einer Liste oder die Wahl eines Kandidaten auf einer Liste.

1.3.3.4 Systemkonform abgegebene Stimme

Eine Stimme ist „systemkonform abgegeben“, wenn

1. ihr Absender sie endgültig abgegeben hat; und
2. das dazu verwendete clientseitige Authentisierungsmerkmal, beziehungsweise die daraus resultierende Authentisierungsnachricht einem serverseitigen Authentisierungsmerkmal entspricht, das in der Vorbereitungsphase des Urnengangs festgelegt und einem Stimmberechtigten zugewiesen wurde; und
3. die elektronische Urne noch keine Stimme enthält, die unter Verwendung desselben clientseitigen Authentisierungsmerkmals abgegeben wurde.

1.3.4 Risikobeurteilung

Oberbegriff für die sequentiell auszuführenden Tätigkeiten Risiken identifizieren, Risiken analysieren und Risiken bewerten

1.3.5 Systembetreiber

Organisation (Behörde oder Privatunternehmen), welche bei einem Urnengang für die Handhabung aller technischen Aspekte der Stimmabgabe die volle Verantwortung übernimmt. Dazu stellt er Personal, Organisation und Infrastruktur in angemessenem Umfang zur Verfügung. Die Gesamtheit der technischen, administrativen, rechtlichen und Führungstätigkeiten des Systembetreibers wird als Betrieb bezeichnet. Der Systembetreiber arbeitet auf Weisung des Kantonsverantwortlichen.

1.3.6 Klassifizierte Daten und Informationen

1.3.6.1 Vertrauliche Daten und Informationen

Daten und Informationen werden als vertraulich bezeichnet, wenn sie nur einzelnen namentlich bekannten Personen bekannt sein dürfen.

1.3.6.2 Geheime Daten und Informationen

Daten und Informationen werden als geheim bezeichnet, wenn sie vertraulich sind und keiner einzigen Person bekannt sein dürfen. Dazu gehören im Mindesten die Daten und Informationen, die es in ihrer Gesamtheit erlauben würden, das Stimmgeheimnis zu brechen oder vorzeitige Teilergebnisse zu erheben. Die vorliegende Definition kann von anderen Standards abweichen.

2. Anforderungen zur Ausgestaltung elementarer Abläufe

Die nachfolgenden Ziffern umfassen Anforderungen zur Ausgestaltung elementarer Abläufe. In der rechten Spalte finden sich Hinweise, bei welcher Überprüfung die jeweilige Anforderung im Vordergrund steht (I: Prüfung der Infrastruktur und des Betriebs; F: Prüfung der Funktionalität).

2.1 Abstimmungsvorgang

2.1.1	Das System muss benutzerfreundlich sein. Die Benutzerführung richtet sich nach allgemein bekannten Schemen.	F
2.1.2	Die Barrierefreiheit des clientseitigen Systems ist gemäss Standard eCH-0059 Version 2.0 von einer Stelle zu prüfen, die die Bundeskanzlei als fachkompetent anerkennt.	F
2.1.3	Die Stimmenden erklären, dass sie die Regeln der elektronischen Stimmabgabe und ihre Verantwortlichkeit zur Kenntnis genommen haben.	F
2.1.4	Die Stimmberechtigten müssen vor Abgabe ihrer Stimme ausdrücklich darauf aufmerksam gemacht werden, dass sie durch das Übermitteln der elektronischen Stimmen gültig an einem Volksentscheid teilnehmen. Vor der Stimmabgabe muss die stimmberechtigte Person bestätigen, dass sie von dieser Meldung Kenntnis nehmen konnte.	F
2.1.5	Zur elektronischen Stimmabgabe muss die stimmende Person unter Verwendung des clientseitigen Authentisierungsmerkmals gegenüber der zuständigen Behörde nachweisen, dass sie stimmberechtigt ist.	F
2.1.6	Die Stimmenden geben ihre Stimme in die Benutzerplattform ein und geben sie unter Verwendung des clientseitigen Authentisierungsmerkmals ab.	F
2.1.7	Das clientseitige System, wie es sich den Stimmenden präsentiert, beeinflusst diese nicht in ihrer Entscheidungsfindung.	F,I
2.1.8	Bis zur Willensbekundung, die Stimme definitiv abgeben zu wollen, können Stimmende ihre Stimme korrigieren. Der konventionelle Kanal steht ihnen vor der definitiven Abgabe weiterhin offen.	F
2.1.9	Die Benutzerführung darf nicht zu übereilter oder unüberlegter Stimmabgabe verleiten.	F
2.1.10	Das System erlaubt die Stimmabgabe nur, wenn die stimmende Person ihre Stimme explizit kontrolliert und bestätigt hat. Dazu wird ihm diese vor der endgültigen Abgabe erneut angezeigt.	F
2.1.11	Das System bietet den Stimmberechtigten vor der Stimmabgabe jederzeit die Möglichkeit, ihre Wahlhandlung zu beenden, ohne ihre Stimmberechtigung dabei zu verlieren.	F,I
2.1.12	Das System bietet den Stimmenden keine Funktion zum Ausdrucken der Stimme.	F

2.1.13	Die erfolgreiche Übermittlung der Stimme muss für die stimmende Person auf der Benutzerplattform erkennbar sein. Die Stimmenden erhalten eine Bestätigung, dass die abgegebenen Stimme an ihrem Bestimmungsort angekommen ist.	F,I
2.1.14	Den Stimmenden soll nach Abschluss der Stimmabgabe keinerlei Information zur abgegebenen Stimme angezeigt werden.	F
2.1.15	Es kann mithilfe desselben clientseitigen Authentisierungsmerkmals keine weitere Stimme abgegeben werden.	F,I

2.2 Vorbereitung von Authentisierungsmerkmalen, kryptografischen Schlüsseln und weiteren Systemparametern

2.2.1	Das Stimmregister wird in die Infrastruktur importiert.	F,I
2.2.2	Die Fragestellungen des Urnengangs (beispielsweise Abstimmungsvorlagen oder Kandidatenlisten) für alle betroffenen föderalen Ebenen und Wahlkreise werden in die Infrastruktur importiert und gespeichert.	F,I
2.2.3	In der Infrastruktur wird pro Stimmberechtigten das serverseitige Authentisierungsmerkmal bereitgestellt und gespeichert.	F
2.2.4	Bei Bedarf wird pro Stimmberechtigten das clientseitige Authentisierungsmerkmal in der Infrastruktur bereitgestellt und temporär gespeichert. (Dies ist nur notwendig, falls auf kein externes Authentisierungsmittel zurückgegriffen wird.)	F
2.2.5	Die verwendeten kryptografischen Schlüssel werden in der Infrastruktur bereitgestellt und gespeichert.	F
2.2.6	Der Systembetreiber setzt die für die Durchführung eines Urnengangs relevanten technischen Parameter.	I

2.3 Informationen und Hilfestellungen

2.3.1	Der Kantonsverantwortliche erstellt ein Konzept zur Information der Bürgerinnen und Bürger über die elektronische Stimmabgabe.	I
2.3.2	Das Konzept gewährleistet, dass die Informationen von den zuständigen Gremien autorisiert worden sind.	I
2.3.3	Auf dem Internet finden sich Ratschläge und Regeln zur Stimmabgabe sowie Informationen zur Verantwortlichkeit der Stimmberechtigen. Diese sollen einer überstürzten oder unüberlegten Handlungsweise entgegenwirken.	F,I
2.3.4	Den Stimmberechtigten wird mit Bezug auf die Sicherheitsmassnahmen auf zugängliche Weise erklärt, wodurch die Vertrauenswürdigkeit der elektronischen Stimmabgabe sichergestellt ist.	F
2.3.5	Den Stimmberechtigten wird erklärt, worauf sie achten müssen, damit sie ihre Stimme sicher abgeben können.	F
2.3.6	Den Stimmberechtigten wird erklärt, wie die Stimme in dem zur Stimmeingabe verwendeten Benutzerplattform auf allen Speichern gelöscht werden kann.	F
2.3.7	Die Stimmberechtigten können technischen Support anfordern.	I
2.3.8	Die Prüferinnen und Prüfer, beispielsweise eine zur Verifizierung eingesetzte Kommission, sollen 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 werden. Sie müssen in der Lage sein, die Vorgänge und ihre Bedeutung zu verstehen.	I

2.4 Vorbereitung zum Druck des Stimmmaterials

2.4.1	Das Stimmmaterial muss so konzipiert sein, dass die doppelte Stimmabgabe über einen konventionellen Abstimmungskanal ausgeschlossen werden kann.	F,I
2.4.2	Die Datei zum Druck des Stimmmaterials wird bereitgestellt, allenfalls unter Einbezug des clientseitigen Authentisierungsmerkmals.	F
2.4.3	Die Druckdatei wird an die Druckerei übermittelt.	F,I

2.5 Öffnen und Schliessen des elektronischen Stimmkanals

2.5.1	Der Systembetreiber initialisiert das System. (Die Initialisierung umfasst sämtliche Einstellungen, die gemäss Prozessdefinition kurz vor der Öffnung des elektronischen Stimmkanals erfolgen müssen und kann beispielsweise die Inbetriebnahme von Systemmonitoren oder das Zurücksetzen von Zählern und der elektronischen Urne[1] beinhalten.)	I
2.5.2	Der elektronische Stimmkanal wird für die Stimmberechtigten geöffnet.	F,I
2.5.3	Eine verfrühte Schliessung oder Öffnung des elektronischen Stimmkanals muss untersagt sein.	I
2.5.4	Der elektronische Stimmkanal wird für die Stimmberechtigten geschlossen.	F,I

2.6 Konformitätskontrolle und Ablage endgültig abgegebener Stimmen

2.6.1	Das System authentisiert unter Verwendung der empfangenen Authentisierungsnachricht und des serverseitigen Authentisierungsmerkmals den Absender der abgegebenen Stimme als Stimmberechtigten.	F
2.6.2	Das System überprüft, ob für den selben Stimmberechtigten bereits eine Stimme in der elektronischen Urne abgelegt worden ist.	F
2.6.3	Im Fall einer systemkonform abgegebenen Stimme legt das System die Stimme in der elektronischen Urne ab und informiert den Stimmenden über die erfolgreiche Stimmabgabe. Eine nicht systemkonform abgegebene Stimme wird nicht in der elektronischen Urne abgelegt. Die Wohlgeformtheit einer Stimme[2] kann nebst ihrer systemkonformen Abgabe ein Kriterium für die erfolgreiche Stimmabgabe bilden.	F

2.7 Auszählung der elektronischen Urne

2.7.1	Der Kantonsverantwortliche löst nach der Schliessung des elektronischen Stimmkanals frühestens am Abstimmungssonntag die Entschlüsselung der in der elektronischen Urne enthaltenen Stimmen aus.	F,I
2.7.2	Der Kantonsverantwortliche löst die Auszählung der entschlüsselten Stimmen aus und speichert für jeden Wahl- oder Abstimmungskreis das Ergebnis. Jede stärkere Form der Detaillierung ist unzulässig.	F,I
2.7.3	Der Kantonsverantwortliche protokolliert den Vorgang der Entschlüsselung der Stimmen und deren Auszählung.	I

[1] Als „elektronische Urne“ wird jener Speicherbereich bezeichnet, in dem die abgegebenen Stimmen bis zur Entschlüsselung und Auszählung gespeichert werden.

[2] Eine wohlgeformte Stimme repräsentiert eine vorgesehene Art einen Stimm- oder Wahlzettel auszufüllen. Wie und ob nicht-wohlgeformte Stimmen im Endergebnis berücksichtigt werden sollen, kann vorgängig definiert werden. Beispielsweise kann definiert werden, dass bei einer Abstimmungsfrage nur die vorgesehenen Antworten „ja“, „nein“ oder „leer“ das Abstimmungsergebnis beeinflussen können. Eine Antwort „ich will nicht abstimmen“ würde in dem Fall dazu führen, dass die Stimme nicht wohlgeformt ist. Ob nicht-wohlgeformte Stimmen gar nicht erst in der elektronischen Urne abgelegt werden können oder sie bei der Auszählung ignoriert werden oder ob sie gar im Endergebnis ausgewiesen werden, muss vorgängig definiert werden.

2.7.4	Von der Entschlüsselung der Stimmen bis zur Übermittlung der Abstimmungsergebnisses muss jeder Zugriff auf das System oder auf eine seiner Komponenten durch mindestens zwei Personen erfolgen; er muss schriftlich aufgezeichnet werden, und er muss von einer Vertretung der zuständigen Behörde kontrolliert werden können.	F,I
2.7.5	Das Abstimmungsergebnis wird an ein Drittsystem zur weiteren Verarbeitung übermittelt, insbesondere zur Konsolidierung mit den über die konventionellen Kanäle abgegebenen Stimmen.	F,I
2.7.6	Das System stellt die notwendigen Informationen zur Verfügung, damit unter Verwendung eines Stimmrechtsausweises festgestellt werden kann, ob der betreffende Stimmberechtigte, der persönlich oder brieflich stimmen will, bereits eine elektronische Stimme abgegeben hat. Im Fall von Versuchen mit stark beschränktem Elektorat (beispielsweise ausschliesslich mit Auslandschweizern) darf zum Schutz des Stimmgeheimnisses keine Liste, welche die Stimmberechtigten identifiziert, die eine elektronische Stimme abgegeben haben, an eine Stelle ausserhalb der Infrastruktur ausgehändigt werden. Stattdessen muss auf Anfrage hin bestätigt werden, ob von einzelnen Stimmberechtigten eine Stimme eingegangen ist. Alternativ kann das System eine Liste aushändigen, die anonyme Codes aufweist, die mit den verwendeten Stimmrechtsausweisen korrelieren.	F,I
2.7.7	Die Entschlüsselung und die Auszählung der Stimmen erfolgen unter Einbezug unabhängiger Organe oder Parteien. Sie können dadurch den geordneten Ablauf der Prozedur bezeugen.	I

2.8 Vertrauliche und geheime Daten

2.8.1	Es ist sichergestellt, dass weder Mitarbeiter noch Externe Daten kennen, die einen Bezug zwischen der Identität von Stimmenden und ihrer Stimme zulassen.	F,I
2.8.2	Es ist sichergestellt, dass weder Mitarbeiter noch Externe vor dem Zeitpunkt der Entschlüsselung der Stimmen Daten kennen, die die Erhebung vorzeitiger Teilergebnisse erlauben.	F,I
2.8.3	Es ist sichergestellt, dass Abstimmungsergebnisse zwischen dem Zeitpunkt der Entschlüsselung der Stimmen und dem Zeitpunkt der Publikation vertraulich behandelt werden.	F,I
2.8.4	Es ist sichergestellt, dass Daten vertraulich behandelt werden, die es erlauben festzustellen, ob Stimmberechtigte auf dem elektronischen Weg eine Stimme abgegeben haben.	F,I
2.8.5	Es ist sichergestellt, dass persönliche Daten aus dem Stimmregister vertraulich behandelt werden.	F,I
2.8.6	Es ist sichergestellt, dass die einzelnen Stimmen auch nach der Auszählung vertraulich behandelt werden.	I
2.8.7	Es ist sichergestellt, dass Abstimmungsergebnisse vertraulich behandelt werden, falls nur ein geringer Anteil der Stimmberechtigten eines Abstimmungskreises elektronisch abstimmen darf.	F,I
2.8.8	Nach der Erwahrung vernichtet der Systembetreiber gemäss einem dokumentierten Prozess sämtliche Daten, die im Rahmen des elektronischen Urnengangs angefallen sind, in Bezug zu den einzelnen eingegangenen Stimmen stehen und als vertraulich oder geheim klassifiziert sind.	I

2.9 Pflichten des Kantonsverantwortlichen

	Der Kantonsverantwortliche ist eine natürliche Person, der für einen Urnengang mit der elektronischen Stimmabgabe die Gesamtverantwortung übernimmt. Im Besonderen muss er: a. Massnahmen für die Informationssicherheit definieren, verabschieden und einführen (Informationssicherheitsrichtlinie, Basiskriterien für das Management von Informationssicherheitsrisiken, Geltungsbereich und Grenzen für das Management von Informationssicherheitsrisiken, Organisation des Risikomanagements); b. den Vertrag zur Durchführung des Urnengangs verfassen und Anforderungen an dessen Überwachung und Überprüfung festlegen; c. die Durchführung des Urnengangs bei einem Systembetreiber beauftragen; d. die Fristen zur Durchführung von kritischen Handlungen und Operationen festlegen; und e. die Durchführung des Urnengangs bei dem beauftragten Systembetreiber überwachen und überprüfen. Er kann bei der Durchführung eines Urnengangs mit der elektronischen Stimmabgabe beteiligt sein.	I

3. Sicherheitsanforderungen

Die Sicherheitsziele (vgl. Art. 3 Abs. 1) lassen sich nicht mit hundertprozentiger Gewissheit erreichen. In jedem Fall lassen sich Sicherheitsrisiken identifizieren. Auf der Basis einer methodischen Risikobeurteilung (Art. 3 Abs. 2 und Ziff. 6.4) ist der Nachweis zu erbringen, dass sich jegliche Sicherheitsrisiken in einem ausreichend tiefen Rahmen bewegen.

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

Ziffer 3.1 listet einige allgemeine Bedrohungen auf und bezieht sie auf die Sicherheitsziele. Sie sind bei der Identifizierung von Risiken zu berücksichtigen. In Abhängigkeit von den identifizierten Schwachstellen des Systems sind sie so weit als nötig zu konkretisieren und zu ergänzen.

Die Sicherheitsanforderungen sind in den Ziffern 3.2 – 3.15 zusammengefasst.

- Einerseits beziehen sie sich auf die Bedrohungen. Sicherheitsmassnahmen, die die Sicherheitsanforderungen nach besten Praktiken erfüllen, sind zur Gewährleistung der Sicherheitsziele in allen denjenigen Schwachstellen des Systems vorzusehen, die Bedrohungen ausgesetzt sind.
- Anderseits beziehen sie sich auf die Anforderungen zur Ausgestaltung elementarer Abläufe (vgl. Ziffer 2). Dies dient als Hilfestellung zum Verständnis, welche Schwachstellen bei der Umsetzung einer Sicherheitsanforderung zu berücksichtigen sind. Weitere Schwachstellen sind am konkreten System zu identifizieren und die Sicherheitsanforderungen in analoger Weise auf sie zu beziehen.

Ziffer 3.15 umfasst Sicherheitsanforderungen aus dem Schutzprofil (PP) des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) [4]. Dabei sind gewisse Abweichungen zulässig. Die Abweichungen und die Bezüge zu den Bedrohungen und den Anforderungen zur Ausgestaltung elementarer Abläufe sind in Ziffer 3.15 aufgeführt.

3.1 Bedrohungen

	Beschreibung	Betroffenes Sicherheitsziel
3.1.1	Malware verändert Stimme auf der Plattform des Benutzers	Korrektheit des Ergebnisses
3.1.2	Ein Angreifer leitet Stimme mittels DNS-spoofing[3] um	Korrektheit des Ergebnisses
3.1.3	Ein Angreifer verändert Stimme mit einer Man-in-the-middle[4] (MITM) Technik	Korrektheit des Ergebnisses
3.1.4	Ein Angreifer schickt mittels MITM bösartig veränderten Stimmzettel	Korrektheit des Ergebnisses
3.1.5	Administrator manipuliert Software, diese speichert Stimmen nicht	Korrektheit des Ergebnisses
3.1.6	Administrator verändert Stimmen	Korrektheit des Ergebnisses
3.1.7	Administrator fügt Stimmen ein	Korrektheit des Ergebnisses
3.1.8	Kriminelle Organisation dringt in System ein mit dem Ziel, das Ergebnis zu fälschen	Korrektheit des Ergebnisses (hier i.S.v.Ziff. 3.1.5/6/7/9)
3.1.9	Administrator kopiert Stimmunterlagen und benutzt sie	Korrektheit des Ergebnisses
3.1.10	Malware auf der Plattform des Benutzers schickt Stimme an die kriminelle Organisation	Schutz des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse
3.1.11	Stimme wird mittels DNS-spoofing umgeleitet	Schutz des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse
3.1.12	Ein Angreifer liest Stimme mittels MITM	Schutz des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse
3.1.13	Administrator benutzt Schlüssel und entschlüsselt nicht-anonyme Stimmen	Stimmgeheimnis und Ausschluss vorzeitiger Teilergebnisse
3.1.14	Bei der Prüfung auf Korrektheit der Verarbeitung / Auszählung wird das Stimmgeheimnis gebrochen	Schutz des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse
3.1.15	Administrator schaut vorzeitig unverschlüsselte Stimmen an	Schutz des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse
3.1.16	Kriminelle Organisation dringt in System ein mit dem Ziel, das Stimmgeheimnis zu brechen oder vorzeitige Teilergebnisse zu erheben	Schutz des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse (hier i.S.v. Bedrohungen, Ziff. 3.1.13/14/15).
3.1.17	Malware auf dem Computer des Stimmberechtigten macht Stimmabgabe unmöglich	Verfügbarkeit der Funktionalität
3.1.18	Malware beeinflusst Stimmberechtigte bei der Meinungsbildung	Schutz der Informationen für die Stimmberechtigten

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

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

3.1.19	Kriminelle Organisation führt einen denial-of-service[5] (DOS) Angriff durch	Verfügbarkeit der Funktionalität
3.1.20	Administrator macht eine fehlerhafte Konfiguration; es kann nicht bis zur Auszählung kommen	Verfügbarkeit der Funktionalität
3.1.21	Administrator manipuliert Informationswebsite bzw. Abstimmungsportal, verwirrt Stimmberechtigte	Schutz der Informationen für die Stimmberechtigten
3.1.22	Administrator sucht nach der Entschlüsselung nach vorgegebenem Wahlverhalten (nur möglich bei Wahlen)	Ausschluss von Beweisen zum Stimmverhalten in Infrastruktur
3.1.23	Kriminelle Organisation dringt in System ein mit dem Ziel, den Betrieb zu stören, die Informationen für die Stimmberechtigten zu manipulieren oder Beweise zum Stimmverhalten der Stimmenden zu bekommen	Verfügbarkeit der Funktionalität, Schutz der Informationen für die Stimmberechtigten, Ausschluss von Beweisen zum Stimmverhalten in Infrastruktur (hier i.S.v. Bedrohungen, Ziff. 3.1.20/21/22)
3.1.24	Administrator stiehlt Adressdaten der Stimmberechtigten	Schutz der persönlichen Informationen über die Stimmberechtigen

3.2 Feststellung / Entdeckung und Meldung von Sicherheitsereignissen und -schwächen; Handhabung von Sicherheitsereignissen und -verbesserungen

3.2.1	Ein Monitoringsystem der Infrastruktur muss Zwischenfälle entdecken und das zuständige Personal alarmieren. Das Personal behandelt Zwischenfälle gemäss vordefinierten Verfahren. Krisenszenarien und Rettungspläne dienen als Leitlinie (darin inbegriffen ein Plan, der gewährleistet, dass die auf den Urnengang bezogenen Aktivitäten weitergeführt werden können) und kommen bei Bedarf zur Anwendung.	F,I - 2.2.1/2/3/4/5/6 - 2.3.3/4/5/ - 2.5.2/3/4 - 2.6.1/2/3 - 2.7.1/4 - 2.8.1/2/3/4/5/6/8 - 3.1.5/6/7/8/9/13/14/15/16/19/20/21/22/23/24
3.2.2	Auf der Infrastruktur sind Protokolle der eingegangenen Stimmen anzufertigen und bei Bedarf bereitzustellen. Sie dienen als Belege für die vollständige, unverfälschte und ausschliessliche Berücksichtigung systemkonform abgegebener Stimmen. Im Fall einer Abweichung müssen sie der Suche nach der Ursache dienen.	F,I - 2.1.6/13 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/4 - 2.8.1/2/3/4/5/6/8 - 3.1.5/6/7/8/9/13/14/15/16/20/22/23
3.2.3	Auf der Infrastruktur sind manipulationsresistente Protokolle der Systemzugriffe anzufertigen und bei Bedarf bereitzustellen. 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. Im Fall einer Abweichung, beziehungsweise von Zweifeln müssen sie der Suche nach der Ursache dienen.	F,I - 2.1.6/13 - 2.2.1/2/3/4/5/6 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/15/16/19/20/21/22/23/24
3.2.4	Die elektronisch abgegebenen und ausgezählten Stimmen müssen zur Plausibilisierung des Ergebnisses mit den Protokollen der eingegangenen Stimmen auf der Infrastruktur verglichen werden.	F,I - 2.1.6/13 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/4 - 2.8.1/2/3/4/5/6/8 - 3.1.5/6/7/8/9/13/14/15/16/20/22/23

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

3.2.5	Es muss gewährleistet sein, dass im Falle einer Panne die Stimmen und die Daten, die ein reibungsloses Funktionieren des Verfahrens der Auszählung der Stimmen belegen, unversehrt auf der Infrastruktur gespeichert werden.	F,I - 2.1.6/13 - 2.2.1/2/3/4/5/6 - 2.4.2 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/3/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.8/20/23
3.2.6	Es müssen mit Hilfe von Authentisierungsmerkmalen Kontrollstimmen abgegeben werden können, die keinem Stimmberechtigten zugewiesen sind. Der Inhalt dieser Kontrollstimmen ist zu protokollieren. Die Auszählung der Kontrollstimmen ist mit den Protokollen der Kontrollstimmenabgabe zu vergleichen. Es muss sichergestellt werden, dass die Kontrollstimmen möglichst ähnlich gehandhabt werden wie systemkonform abgegebene Stimmen, gleichzeitig muss sichergestellt sein, dass sie nicht gezählt werden.	F,I - 2.1.6/13 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/4 - 2.8.1/2/3/4/5/6/8 - 3.1.1/2/3/4/5/6/7/8/9/13/14/15/16/17/18/21/23
3.2.7	Die Verfügbarkeit der Infrastruktur muss in gewählten Zeitabständen überprüft und protokolliert werden.	I - 3.1.19/20/23
3.2.8	Statistische Methoden sollen soweit die Datenbasis dies erlaubt zur Plausibilisierung des Ergebnisses eingesetzt werden können.	I - 2.1.6/13 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/4 - 2.8.1/2/3/4/5/6/8 - 3.1.5/6/7/8/9/13/14/15/16/20/22/23
3.2.9	Durch einen dokumentierten Prozess müssen die Teile des Wahlsystems, die vom Internet erreichbar sind, regelmässig aktualisiert werden um bekanntgewordene Schwachstellen zu eliminieren.	I - 3.1.5/6/7/8/9/13/14/15/16/19/21/22/23/24

3.3 Gebrauch kryptografischer Massnahmen und Schlüsselverwaltung

3.3.1	Elektronische Zertifikate müssen nach besten Praktiken verwaltet werden.	I 2.2.13 - 2.2.5/6 - 2.4.3 - 2.7.5 - 3.1.2/3/4/8/12/16/20/23
3.3.2	Zur Sicherstellung der Integrität von Datensätzen, welcher die Korrektheit des Ergebnisses unterliegen, müssen wirksame kryptografische Massnahmen zum Einsatz kommen, die dem Stand der Technik entsprechen.	I,F - 2.1.6 – 2.2.1/3/4/5/6 - 2.4.3 - 2.5.1 - 2.6.1/2/3 - 2.7.1/2/5/6 - 3.1.5/6/7/8/9/14/16
3.3.3	Zur Sicherstellung der Geheimhaltung von Datensätzen, welcher das Stimmgeheimnis und das Fehlen vorzeitiger Teilergebnisse unterliegen, müssen wirksame kryptografische Massnahmen zum Einsatz kommen, die dem Stand der Technik entsprechen.	I,F - 2.1.6 - 2.2.1/3/4/5/6 - 2.4.2/3 - 2.5.1 - 2.6.1/2/3 - 2.7.1/2/5/6 - 2.8.1/2/3/4/6/7/8 3.1.12/13/14/15/16
3.3.4	Stimmen dürfen von ihrer Erfassung bis zur Auszählung zu keinem Zeitpunkt in unverschlüsselter Form abgelegt oder weitergeleitet werden.	I,F 2.1.6/13 - 2.4.2/3 - 2.6.1/2/3 - 2.7.1 - 2.8.1/2 - 3.1.3/4/5/6/7
3.3.5	Beim Austausch von Stimmregister- und Ergebnisdaten müssen Verschlüsselung und Signatur zum Einsatz kommen. Die Signatur und die Datenintegrität sind bei Erhalt solcher Daten zu überprüfen.	I,F 2.2.1/2 - 2.4.3 - 2.7.5 - 2.8.3/7

3.3.6	Kryptografische Grundkomponenten dürfen nur dann zur Anwendung kommen, wenn die Schlüssellängen und Algorithmen den gängigen Standards entsprechen (z.B. FIPS 143-3, NIST, ECRYPT, ZertES). Die elektronische Signatur muss die Anforderungen einer fortgeschrittenen elektronischen Signatur nach dem ZertES erfüllen. Die Verifikation der Signatur muss mittels eines Zertifikats erfolgen, das von einem nach ZertES anerkannten Anbieter von Zertifizierungsdiensten ausgestellt worden ist.	I,F
3.3.7	Die Stimmberechtigten erhalten die nötigen Angaben, um die Authentizität der zur Stimmabgabe benutzten Internetseite und des Servers zu kontrollieren. Die Aussagekraft einer erfolgreichen Verifizierung muss durch den Einsatz kryptografischer Mittel gemäss besten Praktiken unterstützt werden.	I,F 2.1.13 - 2.2.5 - 3.1.2/3/4/11/12

3.4 Sicherer elektronischer und physischer Informationsaustausch

3.4.1	Sämtliche Komponenten der Infrastruktur müssen in einer separaten Netzwerkzone betrieben werden. Diese Netzwerkzone muss durch eine angemessene Routingkontrolle gegenüber dem übrigen Netzwerk geschützt werden.	I 2.8.1/2/3/4/5/6/7 - 3.1.6/7/8/9/13/14/15/16/20/22/23/24
3.4.2	Die Systeme müssen vor Angriffen (unabhängig von der Art der Angriffe oder ihrer Herkunft) geschützt sein.	I
3.4.3	Das System zur Auszählung der Stimmen muss innerhalb der Netzwerkzone, in dem die Infrastruktur betrieben wird, in einer eigenen Netzwerkunterzone betrieben werden, die von allen anderen Netzwerkunterzonen sicher abgetrennt ist.	I 7.2.1/2/3/4/5/6/7 - 2.8.1/2/3/4/5/6/7 3.1.6/7/8/9/13/14/ 15/16/20/22/23
3.4.4	Bearbeitungen im Zusammenhang mit der elektronischen Stimmabgabe müssen von sämtlichen anderen Anwendungen klar getrennt sein.	I 2.8.1/2/3/4/5/6/7 - 3.1.6/7/8/9/13/14/15/16/20/22/23/24

3.5 Tests der Funktionalität

3.5.1	Durch ein Testkonzept muss sichergestellt sein, dass sich die Funktionalität gemäss Spezifikation verhält. Das Konzept muss Testdrehbücher zu jeder Art von Test umfassen. Es regelt die Verantwortlichkeiten bei der Durchführung, der Protokollierung und der Berichterstattung. Es legt fest, unter welchen Bedingungen ein Test durchzuführen ist. Im Mindesten ist bei der Entwicklung jede sicherheitsrelevante Funktionalität zu testen, auch im Fall von geringfügigen Anpassungen.	I,F

3.6 Informationssicherheitsrichtline

3.6.1	Der Kantonsverantwortliche muss eine Informationssicherheitsrichtlinie erlassen und kommunizieren, die für den gesamten Betrieb des Systems einen verbindlichen Sicherheitsrahmen definiert. Diese Richtline muss in geplanten Zeitintervallen überprüft und wenn nötig angepasst werden.	I

3.7 Organisation der Informationssicherheit

3.7.1	Alle Rollen und Verantwortlichkeiten für den Betrieb des Systems müssen präzise definiert, zugeordnet und kommuniziert werden.	I - 3.1.5/6/7/8/9/13/14/ 15/16/20/21/22/23
3.7.2	Für Einrichtungen zur Informationsverarbeitung der Infrastruktur muss ein Autorisierungsprozess eingerichtet werden.	I - 3.1.5/6/7/8/9/13/14/ 15/16/20/21/22/23
3.7.3	Die Risiken im Zusammenhang mit Dritten (Auftragnehmer jedweder Art wie Lieferanten, Dienstleister, etc.) müssen identifiziert und über angemessene vertragliche Vereinbarungen soweit nötig reduziert werden. Die Einhaltung der Vereinbarungen muss während ihrer Laufzeit angemessen überwacht und überprüft werden.	I

3.8 Verwaltung der immateriellen und materiellen Ressourcen

3.8.1	Alle immateriellen und materiellen Ressourcen im Sinne des Begriffs Asset in der Norm ISO/IEC 27001:2013, die im Zusammenhang mit der elektronischen Stimmabgabe relevant sind (Organisation als Ganzes, insbesondere deren Organisationsprozesse und die in diesen Prozessen bearbeiteten Informationen als solche; Datenträger, Einrichtungen zur Informationsverarbeitung der Infrastruktur; Räumlichkeiten der Infrastruktur) müssen in einem Inventar erfasst werden. Über das Personal muss eine Liste geführt werden. Das Inventar und die Personalliste müssen aktuell gehalten werden. Jeder immateriellen und materiellen Ressource muss eine Person zugewiesen werden, die für diese Ressource die Verantwortung übernimmt.	I 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2 - 2.5.1 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/ 15/16/19/20/21/22/23/24
3.8.2	Der zulässige Gebrauch von immateriellen und materiellen Ressourcen muss definiert werden.	I 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2 - 2.5.1 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/ 15/16/19/20/21/22/23/24
3.8.3	Für Informationen müssen Klassifizierungsleitlinien erlassen und kommuniziert werden.	I 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2 - 2.5.1 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/ 15/16/19/20/21/22/23/24
3.8.4	Für die Kennzeichnung und Handhabung von Information müssen Verfahren eingerichtet werden.	I 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2 - 2.5.1 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/ 15/16/19/20/21/22/23/24

3.9 Vertrauenswürdigkeit des Personals

3.9.1	Zur Gewährleistung der Vertrauenswürdigkeit des Personals vor, während und nach Beendigung der Anstellung oder bei Rollenwechseln müssen angemessene Richtlinien und Verfahren eingerichtet und kommuniziert werden.	I 3.1.5/6/7/8/9/13/14/ 15/16/20/21/22/23
3.9.2	Für die Gewährleistung der Vertrauenswürdigkeit des Personals müssen die Entscheidungsträger des Personals die volle Verantwortung übernehmen.	I 3.1.5/6/7/8/9/13/14/ 15/16/20/21/22/23
3.9.3	Das gesamte Personal muss über ein ausgeprägtes Informationssicherheitsbewusstsein verfügen. Dazu muss ein aufgabengerechte Ausbildungs- und Trainingsprogramm eingerichtet und betrieben werden.	I 3.1.5/6/7/8/9/13/14/ 15/16/20/21/22/23

3.10 Physische und umgebungsbezogene Sicherheit

3.10.1	Die Sicherheitsperimeter der verschiedenen Räumlichkeiten der Infrastruktur (Räume für die verschiedenen Personengruppen des Personals, Serverräume, etc.) müssen klar definiert sein.	I 3.1.5/6/7/8/9/13/14/ 15/16/19/21/22/23/24
3.10.2	Für den physischen Zugang zu diesen verschiedenen Räumlichkeiten der Infrastruktur müssen Zugangsberechtigungen definiert, eingerichtet und angemessen kontrolliert werden.	I 3.1.5/6/7/8/9/13/14/ 15/16/23
3.10.3	Zur Gewährleistung der Sicherheit von Geräten innerhalb und ausserhalb der Räumlichkeiten der Infrastruktur müssen angemessene Richtlinien und Verfahren definiert und deren Einhaltung überwacht und überprüft werden.	I 3.1.5/6/7/8/9/13/14/ 15/16/19/21/22/23/24

3.11 Management der Kommunikation und des Betriebs

3.11.1	Die Bedienabläufe für die wichtigsten Systemaktivitäten müssen detailliert beschrieben werden.	I 2.2.1/2/3/4/5/6 - 2.3.8 - 2.4.2/3 - 2.5.1/2/3 - 2.7.1/2/3/4/5/6/7 - 3.1.20
3.11.2	Produktive Systeme dürfen nur gemäss einem dokumentierten Verfahren zum Änderungsmanagement geändert werden.	I 3.1.5/6/7/8/9/13/14/ 15/16/19/20/21/22/23/24
3.11.3	Pflichten und Verantwortlichkeitsbereiche müssen so aufgeteilt werden, dass die mit Betrieb und Kommunikation verbundenen Risiken personellen Ursprungs auf Restrisiken reduziert werden, die mit den Risikoakzeptanzkriterien kompatibel sind.	I - 2.2.1/2/3/4/5/6 - 2.3.8 - 2.4.2/3 - 2.5.1/2/3 - 2.7.1/2/3/4/5/6/7 - 3.1.20
3.11.4	Zum Schutz vor Schadsoftware müssen angemessene Massnahmen getroffen werden.	I 3.1.5/6/7/8/9/13/14/ 15/16/19/20/21/22/23/24
3.11.5	Es muss ein detaillierter Plan für die Datensicherung erstellt und umgesetzt werden. Die korrekte Funktion der Datensicherung muss regelmässig überprüft werden.	I 2.1.6/13 - 2.2.1/2/3/4/5/6 - 2.4.2 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/3/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.8/20/23
3.11.6	Es müssen angemessene Massnahmen zum Schutz des Netzwerks und der Sicherheit von Netzwerkservices definiert und umgesetzt werden.	I 3.1.5/6/7/8/9/13/14/ 15/16/19/20/21/22/23/24

3.11.7	Die Verfahren zur Handhabung von Wechseldatenträgern und zur Entsorgung von Datenträgern müssen detailliert geregelt werden.	I - 2.8.1/2/3/4/5/6/7/8 - 3.1.8/9 - 3.1.13/14/15/16 - 3.1.22/23/24
3.11.8	Die Massnahmen zur Überwachung und Protokollierung der Systembenutzung, der Tätigkeiten von Administratoren und zur Störungsprotokollierung müssen detailliert beschrieben, umgesetzt, überwacht und überprüft werden.	I 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2/3 - 2.5.1/2/3/4 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/ 15/16/20/21/22/23/24

3.12 Zuteilung, Verwaltung und Entzug von Zugangs- und Zugriffsrechten

3.12.1	Es muss gewährleistet sein, dass während des Urnengangs jede nachträgliche Änderung nur mit Zustimmung des Kantonsverantwortlichen erfolgt.	F,I - 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2 - 2.5.1 - 2.7.4 - 3.1.5/6/7/8/20/23
3.12.2	Zugang zu und Zugriff auf Infrastruktur und Funktionalität müssen auf der Basis einer Risikobeurteilung detailliert geregelt und dokumentiert werden. In Hochrisikobereichen muss das Vieraugenprinzip eingesetzt werden	I 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2 - 2.5.1 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/ 15/16/19/20/21/22/23/24
3.12.3	Es muss gewährleistet sein, dass Informationen auf der Website zur elektronischen Stimmabgabe und/oder diesbezügliche Informationsseiten nicht ohne Berechtigung geändert werden können.	F,I 2.3.3/3/4/5/6 - 3.1.21/23
3.12.4	Während des Urnengangs müssen sachfremde Zugriffe jeglicher Art auf die Infrastruktur ausgeschlossen sein.	F,I 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2/3 - 2.5.1/2/3/4 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/ 15/16/20/21/22/23/24
3.12.5	Es muss sichergestellt sein, dass keines der Elemente des clientseitigen Authentisierungsmerkmals 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.	F,I – 2.1.5/6/15 - 2.2.3/4 - 2.4.1/2/3 - 2.6.1/2 - 2.7.1/2/4/5/6 - 2.8.1/4/5 - 3.1.5/6/7/8/9/13/14/15/16

3.13 Anforderungen an Druckereien

3.13.1	Druckereien richten sich bei der Erfüllung ihrer Aufgaben nach den im Anforderungskatalog Druckereien festgelegten Bestimmungen.	

3.14 Beschaffung, Entwicklung und Wartung von Informationssystemen

3.14.1	Für die Softwareinstallation auf produktiven Systemen müssen angemessene Verfahren detailliert beschrieben und umgesetzt werden.	I 3.1.5/6/7/8/9/13/14/ 15/16/19/20/21/22/23/24
3.14.2	Zur Behandlung technischer Schwachstellen müssen angemessene Verfahren detailliert beschrieben und umgesetzt werden. Teilen der Infrastruktur, die über das Internet erreichbar sind, muss besondere Aufmerksamkeit zukommen.	I - 3.1.5/6/7/8/9/13/14/ 15/16/19/20/21/22/23/24

3.15 Anforderungen aus dem Schutzprofil des BSI

Die Anforderungen aus dem Schutzprofil des BSI [1.1.4] sind zusätzlich umzusetzen. Bei ihrer Interpretation ist die Terminologie des Schutzprofils massgeblich.

Bei inhaltlichen Widersprüchen zwischen der deutschen und der englischen Version des Schutzprofils sind die Bestimmungen der englischen Version massgebend. Die VEleS geht im Falle von Widersprüchen zum Schutzprofil stets vor.

Die folgenden Abweichungen vom Schutzprofil sind zulässig oder zwingend einzuhalten:

3.15.1	OE.Wahlvorbereitung[6] sieht unter anderem vor, dass „Wähler“ die in der „Wahlberechtigungsliste“ enthaltenen Einträge überprüfen und allenfalls eine Berichtigung verlangen können. Dies muss in Analogie für Stimmberechtigte hier nicht umgesetzt werden.
3.15.2	Es soll keine Registrierung der Stimmberechtigten erfolgen müssen. Die Einträge im Stimmregister sind für die Erteilung der Stimmberechtigung massgebend.
3.15.3	OE.ServerRaum sieht vor, dass nur der Wahlvorstand den Serverraum betreten darf. Diese Anforderung darf abgeschwächt werden im Sinn, dass nur vom Kantonsverantwortlichen festgelegte Berechtigte unter Aufsicht den Serverraum betreten dürfen.
3.15.4	O.Korrektur sieht vor, dass die Stimmenden ihre Stimme bis zur endgültigen Abgabe beliebig oft korrigieren können. Diese Anforderung darf folgendermassen abgeschwächt werden: Bis zur Willensbekundung, die Stimme definitiv abgeben zu wollen, können Stimmende ihre Stimme korrigieren.. (Ziff. 2.1.8 geht vor.)
3.15.5	Es dürfen in gut begründeten Fällen alternative IT-Sicherheitsmassnahmen (im Sinne der Terminologie nach CC; engl. Security Functional Requirements) zum Einsatz kommen.

Die nachfolgende Liste bezieht die Sicherheitsziele (im Sinne der Terminologie nach CC; engl. Security Objectives) auf die Bedrohungen und die Anforderungen zur Ausgestaltung elementarer Abläufe der vorliegenden Verordnung.

O.StimmberechtigterWähler	F,I 2.1.5 - 2.2.1/2/3/4 - 2.4.2 - 2.6.1 - 3.1.7/8/9
O.Beweis	F,I 2.1.12 - 3.1.22
O.IntegritätNachricht	F – 2.1.6/13 – 2.2.5 – 2.4.3 – 3.1.2/3/4
O.Wahlgeheimnis	F – 2.1.6 – 2.2.5 – 2.8.1/2 – 3.1.12/13
O.GeheimNachricht	F - 2.1.6 - 2.2.5 - 2.8.1/4 - 3.1.9
O.AuthentizitätServer	F,I - 2.1.6 - 2.2.5 - 2.4.2 - 3.1.2/3/4/12
O.ArchivierungIntegrität	F,I - 2.2.5 - 2.7.2/3/4 - 3.1.6/7/8
O.ArchivierungWahlgeheimnis	F,I - 2.7.2 - 2.8.1/6/8 - 3.1.13/14/16/22
O.Abbruch	F - 2.1.11
O.WahlBeenden	F - 2.5.3/4 - 3.1.20

[6] Die hier genannten Anforderungen aus dem Schutzprofil beginnen entweder mit „O.“. Die Verwendung des Bezeichners „O.“ hat ihren Ursprung im Begriff „security objective“ und jene von „OE.“ hat ihren Ursprung in „security objectives for the operational environment“.

O.Wahlende	F - 2.5.4 - 3.1.20
O.WahlgeheimnisWahlvorstand	F - 2.7.2 - 2.8.1/6/7 - 3.1.13/14/16
O.IntegritätWahlvorstand	F - 2.5.1/2/4 - 2.7.4 - 3.1.5/6/7/8
O.Zwischenergebnis	F - 2.7.1 - 2.8.2/3 - 3.1.15/16
O.Übereilungsschutz	F - 2.1.10
O.Korrektur	F - 2.1.8
O.Rückmeldung	F - 2.1.13 - 3.1.17
O.Störung	F,I - 2.2.6 - 2.5.1 - 3.1.19/20
O.Protokoll	F,I - 2.1.6/13 - 2.2.1/2/3/4/5/6 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9 - 3.1.13/14/15/16/19/20/21/22/23/24
O.OneVoterOneVote	F,I - 2.1.5/8/11/13/15 - 2.2.1/2/3/4 - 2.4.1 - 2.6.1/2/3 - 2.7.6 - 3.1.7/8/17
O.AuthWahlvorstand	F - 2.2.1/2/3/4/5/6 - 2.4.2 - 2.5.1/2/4 - 2.7.1/2/4/5 - 2.8.1/2/3/4/5/6/7
O.StartStimmauszählung	F - 2.5.4 - 2.7.1/2 - 3.1.15/16
O.Stimmauszählung	F - 2.2.6 - 2.5.1 - 2.7.2 - 3.1.5/7/8 - 3.1.20
OE.Wahlvorbereitung	F,I - 2.2.1/2/3/4/5/6 - 2.3.1/3 - 2.4.2/3 - 2.5.1 - 2.8.1/2/3/4/5/6/7/8 - 3.1.7/8/20
OE.Beobachten	F - 2.1.6
OE.Wahlvorstand	I - 2.2.1/2/6 - 2.3.2 - 2.5.1/2/4 - 2.7.1/2/3/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/15/16/20/21/22/23/24
OE.AuthDaten	F,I - 2.2.1/2/3/4 - 2.4.2/3 - 2.8.1/5 - 3.1.8/9
OE.Endgerät	F,I - 2.1.3 - 2.3.3/4 - 3.1.1 - 3.1.10
OE.Wahlserver	I - 3.1.8 - 3.1.16 - 3.1.23
OE.Verfügbarkeit	I - 3.1.19
OE.ServerRaum	I - 3.1.5/6/7/8/9/13/14/15/16/23
OE.Speicherung	I - 2.1.6/13 - 2.2.1/2/3/4/5/6 - 2.4.2 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/3/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.8/20/23
OE.Systemzeit	I - 2.1.6/13 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/4 - 2.8.1/2/3/4/6/8 - - 3.1.5/6/7/8/9/13/14/15/16/20/22/23
OE.Protokollschutz	I - 2.1.6/13 - 2.2.1/2/3/4/5/6 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/15/16/19/20/21/22/23/24
OE.AuthentizitätServer	F - 2.3.3/4/5 - 2.4.2 - 3.1.2/3/4/12
OE.ArchivierungIntegrität	F,I - 2.2.5 - 2.7.2/3/4 - 3.1.6/7/8
OE.ArchivierungWahlgeheimnis	F,I - 2.7.2 - 2.8.1/6/8 - 3.1.13/14/16/22
OE.GeschützteKommunikation	I - 3.1.5/6/7/8/9/13/14/15/16/22/23/24
OE.Zwischenspeicherung	F - 2.3.6

4. Verifizierbarkeit

Die Artikel 4 und 5 legen die Bestimmungen zur Verifizierbarkeit fest. Diese Ziffer gibt die Bestimmungen auf formellere Weise wieder, um die Kriterien für beide Formen der Verifizierbarkeit zu verdeutlichen.

Dazu wird unter Ziffer 4.1 ein reduziertes abstraktes Modell zur Beschreibung eines Urnengangs bestimmt. Auf der Grundlage jenes Modells enthält Ziffer 4.2 Ausführungen und weiterführende Bestimmungen zu Artikel 4. Ziffer 4.3 zeigt das vollständige abstrakte Modell auf. Ziffer 4.4 enthält Ausführungen und weitergehende Bestimmungen zu Artikel 5.

4.1 Reduziertes abstraktes Modell zu Art. 4

In der verwendeten Abstraktion ist ein Urnengang durch ein kryptografisches Protokoll[7] definiert. Es besteht aus dem Nachrichtenaustausch zwischen den folgenden Systemkomponenten:

Stimmberechtigte/ Stimmende	Stimmberechtigte erhalten vom System oder von der Druckerei vorgängig zum Urnengang ihr clientseitiges Authentisierungsmerkmal. Um eine Stimme abzuschicken teilen sie der Benutzerplattform ihr clientseitiges Authentisierungsmerkmal und ihre Stimme mit.
Benutzerplattform	Sie erstellt die Authentisierungsnachricht und schickt sie zusammen mit der verschlüsselten Stimme ans serverseitige System. Dazu verwendet sie öffentliche Parameter, die sie vorgängig vom System erhalten hat. Sie zeigt den Stimmenden Nachrichten vom serverseitigen System bei Bedarf an.
Vertrauenswürdiges technisches Hilfsmittel der Stimmberechtigten	Stimmende können als Alternative ihre Stimme und/oder ihr clientseitiges Authentisierungsmerkmal auch einem vertrauenswürdigen technischen Hilfsmittel mitteilen. Dieses kann beliebige Aufgaben der Benutzerplattform übernehmen.
System (hier immer serverseitig)	Es generiert und schickt den Stimmberechtigten vorgängig zum Urnengang (eventuell über die Druckerei) ihr clientseitiges Authentisierungsmerkmal und der Benutzerplattform öffentliche Parameter, damit diese die Authentisierungsnachricht und die verschlüsselte Stimme erstellen kann. Es beurteilt, ob Stimmen systemkonform abgegeben worden sind, entschlüsselt sie unter Wahrung des Stimmgeheimnisses und berechnet das Ergebnis des Urnengangs.
Druckerei	Sie kann zum Druck des clientseitigen Authentisierungsmerkmals und der vertraulichen Daten, mit deren Hilfe die Stimmenden von der individuellen Verifizierbarkeit Gebrauch machen können (Verifizierungsreferenz), eingesetzt werden. Sie erhält die entsprechenden Daten vom System und schickt sie weiter an die Stimmberechtigten.

Das Protokoll kann zum Austausch von Nachrichten folgende Kommunikationskanäle vorsehen:

- Stimmende ↔ Benutzerplattform
- Stimmende ↔ vertrauenswürdiges technisches Hilfsmittel
- Vertrauenswürdiges technisches Hilfsmittel ↔ Benutzerplattform
- Benutzerplattform ↔ System
- System ↔ Druckerei
- Druckerei → Stimmberechtigte

[7] Ein kryptografisches Protokoll ist ein Protokoll mit kryptografischen Sicherheitsfunktionen zur Erreichung von Sicherheitszielen. Die kryptographischen Protokolle sind in der Modellebene angesiedelt und enthalten so keine direkten Implementierungen sondern nur abstrakte Sicherheitsfunktionen.

Systemkomponenten und Kommunikationskanäle sind entweder vertrauenswürdig oder nicht vertrauenswürdig. Vertrauenswürdige Systemkomponenten halten geheime Daten ohne Ausnahme unter Verschluss und führen ausschliesslich jene Operationen durch, die durch das Protokoll vorgegeben sind. Vertrauenswürdige Kanäle stellen sicher, dass die übertragenen Nachrichten geheim bleiben. Ausserdem kann der Nachrichtenempfänger darauf vertrauen, dass der Absender einer Nachricht jener Systemkomponente entspricht, der durch die Definition des Kanals vorgegeben ist.

Zusätzlich formalisiert die verwendete Abstraktion einen Angreifer. Er kann sämtliche nicht vertrauenswürdigen Systemkomponenten und Kommunikationskanäle bösartig verändern und unter seine Kontrolle bringen. Bösartig veränderte Systemkomponenten teilen dem Angreifer alle geheimen Daten mit und handeln uneingeschränkt nach seinen Anweisungen. Ebenfalls kann er alle Nachrichten, die auf nicht vertrauenswürdigen Kanälen ausgetauscht werden, mitlesen oder abfangen und selbst beliebig Nachrichten einspeisen.

Vertrauensannahmen im abstrakten Modell (individuelle Verifizierbarkeit des Protokolls):

Für die individuelle Verifizierbarkeit wird in diesem Modell angenommen, dass vertrauenswürdige technische Hilfsmittel, das System und die Druckerei vertrauenswürdig sind. Die Benutzerplattformen und ein signifikanter Anteil der Stimmberechtigten werden als nicht vertrauenswürdig angenommen. Unter den Kommunikationskanälen werden einzig Benutzerplattform ↔ System und System ↔ Druckerei als nicht vertrauenswürdig angenommen.

Sicherheitsziel im abstrakten Modell (individuelle Verifizierbarkeit des Protokolls):

Der Angreifer kann unter den gegebenen Vertrauensannahmen folgende Ziele nicht erreichen, ohne dass ein Stimmender die Möglichkeit hat, einen erfolgten Angriff mit grosser Wahrscheinlichkeit zu erkennen:

- Verändern der Stimme vor der Registrierung
- Unterschlagen der Stimme vor der Registrierung
- Abgeben einer Stimme

Zur Erreichung der Sicherheitsziele kommen im Protokoll ausschliesslich kryptografische Bausteine zum Einsatz, die als sicher gelten.

Individuelle Verifizierbarkeit des Systems in der Umsetzung:

Das System setzt ein kryptografisches Protokoll um, das das Sicherheitsziel zur individuellen Verifizierbarkeit im abstrakten Modell erfüllt. Wo notwendig wird die Annahme der Vertrauenswürdigkeit der Systemkomponenten und Kommunikationskanäle durch entsprechende Sicherheitsmassnahmen gerechtfertigt.

Ziffer 4.2 bezieht die Bestimmungen von Art. 4 auf das Sicherheitsziel im abstrakten Modell und führt sie wo nötig aus. Ausserdem enthält sie Sicherheitsanforderungen zu den im abstrakten Modell als vertrauenswürdig angenommenen Systemkomponenten und Kommunikationskanälen.

4.2 Ergänzende Bestimmungen zur individuellen Verifizierbarkeit

4.2.1	(Zu Art. 4 Abs. 2) Der Beweis muss nicht in einer einzigen Transaktion erfolgen. Er kann auch auf mehrere Nachrichten, die der Stimmende während des Stimmabgabeprozesses erhält, verteilt sein. (In diesem Fall bestätigt die letzte dieser Nachrichten die Registrierung als systemkonform abgegebene Stimme.) Falls die stimmende Person sich vor der definitiven Stimmabgabe (und somit vor Erhalt der letzten Nachricht) entscheidet den Prozess abzubrechen, muss ihr nach wie vor die konventionelle Stimmabgabe zur Verfügung stehen.
4.2.2	(Zu Art. 4 Abs. 2) Diese Anforderung ist so umzusetzen, dass das Risiko des Stimmenkaufs gegenüber der brieflichen Stimmabgabe nicht signifikant vergrössert wird.
4.2.3	(Zu Art. 4 Abs. 3) Das Ziel liegt darin zu verhindern, dass nicht vertrauenswürdige Systemkomponenten unbemerkt eine Stimme abgeben können. Die Bestimmung ist dahingehend zu interpretieren und das Protokoll dementsprechend zu prüfen.

4.2.4	(Zu Art. 4 Abs. 4) Der Beweis ist stichhaltig, wenn er den Stimmenden dazu dient, Manipulationen ihrer Stimme im Sinne des Sicherheitsziels und unter den gegebenen Vertrauensannahmen erkennen zu können. Dadurch kann der Angreifer Stimmende nicht irreführen, indem er mithilfe der nicht vertrauenswürdigen Systemkomponenten einen Beweis anfertigt, der die Stimmenden im Glauben lässt, dass ihre Stimme so, wie sie die stimmende Person in die Benutzerplattform eingegeben hat, als systemkonform abgegebene Stimme registriert wurde. Die Erfolgswahrscheinlichkeit des Angreifers, einen solchen Beweis durch korrektes Raten erstellen zu können (analog für den Beweis zur Bestätigung, dass keine Stimme abgegeben wurde), darf höchstens 0.1% betragen.
4.2.5	(Zu Art. 4 Abs. 4) Für Stimmberechtigte mit einer Behinderung dürfen Erleichterungen zur Überprüfung der Beweise vorgesehen werden. Ausschliesslich hinsichtlich dieses Falls darf vom Sicherheitsziel abgewichen werden. Namentlich darf die Stichhaltigkeit der Beweise in diesem Fall von der Vertrauenswürdigkeit der Benutzerplattform abhängen. Dies erlaubt beispielsweise das Einscannen der Verifizierungsreferenz vorgängig zur Stimmabgabe. Diese Erleichterungen dürfen sich ausschliesslich an eine kleine Gruppe von Stimmberechtigten richten, die den Beweis ohne solche Erleichterungen nicht in seiner vollen Stichhaltigkeit interpretieren können. Stimmberechtigte, für die dies nicht zutrifft, sollen grundsätzlich dazu animiert werden, Beweise gemäss der vorgesehenen Prozedur zu überprüfen.
4.2.6	(Zu Art. 4 Abs. 5) Falls die Stimmenden zum Verifizieren ein besonderes technisches Hilfsmittel benutzen, muss dieses spezifisch für das sichere Speichern von Geheimelementen und Ausführen von kryptografischen Operationen entwickelt worden sein, wie zum Beispiel Geräte, die zum sicheren Homebanking eingesetzt werden. Ausserdem müssen sich die Stimmenden durch die Abgabe von Teststimmen von der korrekten Funktionsweise des Hilfsmittels überzeugen können.
4.2.7	(Zu Art. 4 Abs. 5) Zusätzlich zum Anforderungskatalog für Druckereien gilt die folgende Bestimmung: Alle Maschinen, die in irgendeiner Form an der Bearbeitung von unverschlüsselten oder unsignierten Daten der Verifizierungsreferenz beteiligt sind, müssen während der gesamten Rechenzeit im Vieraugenprinzip physisch überwacht werden. Es sind nur Netzwerkverbindungen zulässig, deren Teilnehmende über physische Kabel so verbunden sind, dass bis zur Vernichtung der vertraulichen Daten ersichtlicherweise keine weiteren Maschinen auf sie zugreifen können.
4.2.8	(Zu Art. 4 Abs. 5) Für das serverseitige System gelten keine zusätzlichen Bestimmungen. Bei der Umsetzung der Anforderungen zur Ausgestaltung elementarer Abläufe und der Sicherheitsanforderungen (vgl. Art. 2 und Ziff. 2 und 3) ist allerdings zu berücksichtigen, dass die Vertraulichkeit der Daten, die mit der Verifizierungsreferenz in Verbindung stehen, für die Korrektheit des Ergebnisses, das Stimmgeheimnis und den Ausschluss vorzeitiger Teilergebnisse entscheidend ist.
4.2.9	(Zu Art. 4 Abs. 4) Die Vertrauenswürdigkeit des Kanals zwischen Druckerei und Stimmberechtigten darf nur dann als gegeben erachtet werden, wenn die Informationen durch die Schweizerische Post zugestellt oder sie zwischen den beteiligten Personen persönlich übergeben werden.

4.3 Vollständiges abstraktes Modell zu Art. 5

Das vollständige abstrakte Modell versteht das System als nicht vertrauenswürdig. Stattdessen sieht es Prüferinnen und Prüfer vor, die auf der Grundlage eines vertrauenswürdigen Hilfsmittels und auf der Grundlage von unabhängigen „Kontrollkomponenten“ die korrekte Ergebnisermittlung beurteilen.

Damit identifiziert es die folgenden zusätzlichen Systemkomponenten:

Kontrollkomponente	Sie interagiert mit dem System und den übrigen Kontrollkomponenten so, dass dieses zum Schluss des Urnengangs einen stichhaltigen Beweis anfertigen kann, der die korrekte Ergebnisermittlung bestätigt.
Prüferinnen und Prüfer	Sie erhalten nach der Auszählung vom System einen Beweis zur Bestätigung der korrekten Ergebisermittlung.
Technisches Hilfsmittel der Prüferinnen und Prüfer	Die Prüferinnen und Prüfer können zur Beurteilung des Beweises ein technisches Hilfsmittel verwenden.

Das kryptografische Protokoll kann die folgenden zusätzlichen Kommunikationskanäle zum Austausch von Nachrichten vorsehen:

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

Vertrauensannahmen im abstrakten Modell (vollständige Verifizierbarkeit des Protokolls):

Es kommen mehrere Kontrollkomponenten zum Einsatz, die in einer oder wenigen Gruppen zusammengefasst sind. Eine einzelne Kontrollkomponente muss - gleich wie das System - als nicht vertrauenswürdig angenommen werden. Es darf jedoch die Annahme gelten, dass mindestens eine Kontrollkomponente pro Gruppe vertrauenswürdig ist, allerdings ohne festzulegen um welche es sich dabei handelt. Die Menge der Gruppen von Kontrollkomponenten bildet den vertrauenswürdigen Systemteil. Seine Vertrauenswürdigkeit ist durch die Vertrauenswürdigkeit mindestens einer Kontrollkomponente in jeder seiner Gruppen definiert. Die Stichhaltigkeit des Beweises, den eine Prüferin oder ein Prüfer infolge von Art. 5 erhält, darf nur von der Vertrauenswürdigkeit des vertrauenswürdigen Systemteils und seines technischen Hilfsmittels abhängen. Weiter wird angenommen, dass mindestens eine vertrauenswürdige Prüferin oder ein vertrauenswürdiger Prüfer mithilfe eines vertrauenswürdigen technischen Hilfsmittels den Beweis überprüft. Allfällige weitere Prüferinnen oder Prüfer und deren technische Hilfsmittel gelten als nicht vertrauenswürdig. Unter den zusätzlichen Kommunikationskanälen darf einzig jener zwischen den Prüferinnen und Prüfern und ihrem technischen Hilfsmittel als vertrauenswürdig angenommen werden. Das System ist als nicht vertrauenswürdig zu betrachten.

Sicherheitsziel im abstrakten Modell (vollständige Verifizierbarkeit des Protokolls):

- Der Angreifer kann unter den Vertrauensannahmen zur vollständigen Verifizierbarkeit des Protokolls folgende Ziele nicht erreichen, ohne dass ein Stimmender oder eine vertrauenswürdige Prüferin oder ein vertrauenswürdiger Prüfer die Möglichkeit hat, einen erfolgten Angriff mit grosser Wahrscheinlichkeit zu erkennen:
  - Verändern der Stimme vor der Registrierung durch den vertrauenswürdigen Systemteil
  - Unterschlagen der Stimme vor der Registrierung durch den vertrauenswürdigen Systemteil
  - Abgeben einer Stimme
  - Verändern einer systemkonform abgegebenen Stimme, deren Abgabe durch den vertrauenswürdigen Systemteil registriert wurde
  - Unterschlagen einer systemkonform abgegebenen Stimme, deren Abgabe durch den vertrauenswürdigen Systemteil registriert wurde
  - Einfügen einer Stimme
- Der Angreifer kann unter den Vertrauensannahmen zur vollständigen Verifizierbarkeit des Protokolls weder das Stimmgeheimnis brechen noch vorzeitige Teilergebnisse erheben, ohne dazu die Stimmberechtigten oder deren Benutzerplattformen bösartig zu verändern.

Zur Erreichung der Sicherheitsziels kommen ausschliesslich kryptografische Bausteine zum Einsatz, die als sicher gelten.

Vollständige Verifizierbarkeit des Systems in der Umsetzung: Es gelten dieselben Bestimmungen wie für die individuelle Verifizierbarkeit.

Ziffer 4.4 bezieht die Bestimmungen von Art. 5 auf das Sicherheitsziel im abstrakten Modell und führt sie wo nötig aus. Ausserdem enthält sie Sicherheitsanforderungen zu den im abstrakten Modell als vertrauenswürdig angenommenen Systemkomponenten und Kommunikationskanälen.

4.4 Ergänzende Bestimmungen zur vollständigen Verifizierbarkeit

4.4.1	(Zu Art. 5 Abs. 1) Der Einsatz von Prüferinnen und Prüfern dient der Transparenz. Die Stimmerechtigten sollen davon ausgehen können, dass Prüferinnen und Prüfer im Zweifelsfall auf Unregelmässigkeiten aufmerksam machen würden. Es wird jedoch bewusst offen gelassen, aus welchen Kreisen Personen mit der Rolle als Prüferin oder Prüfer zu mandatieren sind.
4.4.2	(Zu Art. 5 Abs. 3) Aufgrund der Informationen im vertrauenswürdigen Systemteil (darunter kann sich die verschlüsselte Stimme selbst befinden) können Prüferinnen und Prüfer feststellen, ob eine Stimme als Eingabe für die Ergebnisermittlung in unveränderter Form berücksichtigt wurde. Stimmende müssen somit darauf vertrauen können, dass die Daten im vertrauenswürdigen Systemteil nicht entfernt oder manipuliert werden. In der technischen Literatur finden sich dazu Vorschläge, die verschlüsselten Stimmen auf einem elektronischen „schwarzen Brett“ (engl. *public board*) zu publizieren. Ein schwarzes Brett wird durch den Einbezug mehrerer vertrauenswürdigen Komponenten realisiert, so dass Einträge nur unbemerkt gestrichen oder verändert werden, wenn mehrere dieser Komponenten bösartig verändert sind. Mithilfe einer vertrauenswürdigen Benutzerplattform können Stimmende zu jedem Zeitpunkt nachvollziehen, dass sich ihre Stimme in der Menge der abgegebenen Stimmen befindet. Am Schluss der Abstimmung enthält das schwarze Brett das Ergebnis und den Beweis der korrekten Ergebnisermittlung, der im Rahmen der universellen Verifizierbarkeit angefertigt wird. Die Stimmenden könnten dadurch im Geist einer maximal möglichen Transparenz die Rolle der „Prüferinnen und Prüfer“ einnehmen. Verschiedene Risikoerwägungen, die nicht zuletzt mit der praxisorientierten Annahme zusammenhängen, dass Benutzerplattformen als nicht vertrauenswürdig betrachtet werden dürfen, können dafür sprechen, die für die Verifizierbarkeit relevanten Daten des vertrauenswürdigen Systemteils nicht uneingeschränkt zu veröffentlichen. Es ist daher zulässig die Daten einem eingeschränkten Kreis von Prüferinnen und Prüfern zur Verfügung zu stellen. In der Terminologie der technischen Literatur kann die Anforderung daher so verstanden werden: *Stimmende erhalten von den für das schwarze Brett zuständigen Komponenten einen Beweis zur Bestätigung, dass sie ihre Stimme (bzw. Daten, die für die universelle Verifizierung ausreichend sind) erhalten haben. Seine Stichhaltigkeit darf nicht von der Vertrauenswürdigkeit einer* nicht *vertrauenswürdigen Benutzerplattform oder des Systems abhängen. Die* Prüferinnen und Prüfer *erhalten spätestens nach der Ergebnisermittlung (aber vor der Publikation) Zugang zum schwarzen Brett und stellen fest, dass das Ergebnis jede Stimme auf dem schwarzen Brett gemäss den geltenden Regeln berücksichtigt.*
4.4.3	(Zu Art. 5 Abs. 3 Bst. b) Das Ziel liegt darin zu verhindern, dass nicht vertrauenswürdige Systemkomponenten unbemerkt eine Stimme abgeben können. Die Bestimmung ist dahingehend zu interpretieren und das Protokoll dementsprechend zu prüfen.
4.4.4	(Zu Art. 5 Abs. 3 Bst. c) Die Vertraulichkeit der Daten zu einer allfälligen Verifizierungsreferenz darf somit auch innerhalb der Infrastruktur nur vom vertrauenswürdigen Systemteil abhängen.
4.4.5	(Zu Art. 5 Abs. 4) Die Unabhängigkeit und Isolation des technischen Hilfsmittels müssen gewährleisten, dass die Bewertung des Beweises nicht vom System beeinflusst werden kann. Es wird jedoch bewusst offengelassen, ob die technischen Hilfsmittel und die entsprechenden Programme vom System oder den Prüferinnen und Prüfern bereit gestellt werden sollen. Die Prüferinnen und Prüfer sollen jedoch leicht nachvollziehen können, dass das Hilfsmittel korrekt funktioniert. Dies kann beispielsweise dadurch erreicht werden, dass die Prüferinnen und Prüfer die Programme selber schreiben oder zumindest vorgängig analysieren könnten. Vor dem Verifizieren könnten sie das Hilfsmittel gemeinsam mit den Systemverantwortlichen frisch aufsetzen und die Programme zum Verifizieren kompilieren und installieren. Grundsätzlich sollen Programme zum Verifizieren im Dienste der Transparenz leicht zu schreiben sein.

4.4.6	(Zu Art. 5 Abs. 4 Bst. a und b) Eine Stimme gilt nur dann als systemkonform abgegeben, wenn das dazu verwendete clientseitige Authentisierungsmerkmal einem serverseitigen Authentisierungsmerkmal entspricht, das in der Vorbereitungsphase des Urnengangs festgelegt und einem Stimmberechtigten „zugewiesen“ wurde. Der Beweis muss daher die Bestätigung beinhalten, dass keine unzugewiesenen Authentisierungsmerkmale zum Abgeben von Stimmen erstellt wurden. Dazu müssen während der Vorbereitung des Urnengangs den Kontrollkomponenten oder den Prüferinnen und Prüfern entsprechende Daten als Vergleichsbasis übergeben worden sein. Die Prüferinnen und Prüfer müssen feststellen, dass die Anzahl der Authentisierungsmerkmale der (offiziellen) Anzahl der zugelassenen Stimmberechtigten entspricht. In diesem Fall dürfen die Authentisierungsmerkmale als einem Stimmberechtigten „zugewiesen“ gelten. Dadurch ist zwar noch nicht sichergestellt, dass clientseitige Authentisierungsmerkmale vertrauenswürdiger Stimmberechtigter nicht missbräuchlich zur Abgabe einer systemkonformen Stimme verwendet wurden. Infolge des entsprechenden Punktes im Sicherheitsziel des abstrakten Modells, bzw. Art. 5 Abs. 3, Bst. b können die Stimmberechtigten dies allerdings feststellen.
4.4.7	(Zu Art. 5 Abs. 5) Der Beweis ist stichhaltig, wenn er den Stimmenden oder den Prüferinnen und Prüfern dazu dient, Manipulationen der Stimmen im Sinne des Sicherheitsziels und unter den gegebenen Vertrauensannahmen erkennen zu können. Dadurch kann der Angreifer die Prüferinnen und Prüfer nicht irreführen, indem er mithilfe der nicht vertrauenswürdigen Systemkomponenten einen Beweis zur Rechtfertigung eines manipulierten Ergebnisses anfertigt, bzw. dessen Anfertigung beeinflusst. Im Rahmen der universellen Verifizierbarkeit gelten die folgenden Bestimmungen: Das ersatzlose Unterschlagen einer systemkonform abgegebenen Stimme, deren Abgabe durch den vertrauenswürdigen Systemteil registriert wurde, müssen Prüferinnen und Prüfer in jedem Fall erkennen können. Das Einfügen einer Stimme, ohne dass eine andere unterschlagen wird, müssen Prüferinnen und Prüfer in jedem Fall erkennen können. Die Erfolgswahrscheinlichkeit 0.1% der Teilstimmen zu manipulieren (beispielsweise durch Unterschlagen und gleichzeitigem Einfügen), so dass sie nicht mehr den Sinn des im Rahmen der individuellen Verifizierung generierten Beweises wiedergeben, darf höchstens 1% betragen. Ist die Wahrscheinlichkeit nicht im kryptografischen Sinn vernachlässigbar[8], muss die Unsicherheit durch mehrmaliges Auszählen unter Verwendung neuer Zufallswerte hinreichend reduziert werden können.
4.4.8	(Zu Art. 5 Abs. 5) Wird die Applikation, die auf der Benutzerplattform zur Verschlüsselung der Stimme verwendet wird, vom System bereitgestellt, dann ist sie auch dem serverseitigen System zuzurechnen. Es muss verhindert werden, dass durch eine serverseitige Manipulation der Applikation das Stimmgeheimnis von vertrauenswürdigen Stimmenden ohne bösartiges Verändern ihrer Benutzerplattform gebrochen wird. Stimmende sollen deshalb die Möglichkeit haben, sich mithilfe einer vertrauenswürdigen Plattform zu überzeugen, dass die Applikation ihre Stimme mit dem korrekten Schlüssel verschlüsselt verschickt. Dies kann beispielsweise durch den Einsatz von Browser-Technologie erreicht werden, die es erlaubt, den Quellcode der Benutzerapplikation einzusehen. Stimmende können sich so überzeugen, dass der verwendete öffentliche Schlüssel jenem des Urnengangs entspricht, und dass die Applikation ausschliesslich die vorgesehenen Operationen vornimmt. Alternativ könnte der Quellcode durch eine Gruppe von Kontrollkomponenten signiert sein.
4.4.9	(Zu Art. 5 Abs. 5) Im Sinne des Sicherheitsziels muss verhindert werden, dass das serverseitige System den Inhalt einer abgegebenen Stimme in Zusammenarbeit mit einem nicht vertrauenswürdigen Stimmberechtigten lernen kann. Dazu muss sichergestellt werden, dass dieser eine abgegebene verschlüsselte Stimme auch nicht nach äusserlichem Anpassen als seine eigene abgeben kann mit dem Ziel, durch den Beweis, den er im Rahmen der individuellen Verifizierbarkeit erhält, den Inhalt der Stimme zu lernen.

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

4.4.10	(Zu Art. 5 Abs. 5) Als Folge der Anforderung betreffend der Gewährleistung des Stimmgeheimnisses und des Fehlens vorzeitiger Teilergebnisse dürfen private Schlüssel zum Entschlüsseln von Stimmen mindestens während der Öffnungszeit des elektronischen Abstimmungskanals keiner Systemkomponente vorliegen. Es ist jedoch zulässig, dass sie bei Beteiligung aller Kontrollkomponenten einer Gruppe berechnet werden können. Es ist auch zulässig eine Gruppe von Kontrollkomponenten so vorzusehen, dass sie in Form einer Gruppe von Menschen umgesetzt wird. Jedes Mitglied dieser Gruppe könnte auf einem portablen Speichermedium einen Teil des privaten Schlüssels halten. Zur Wahrung des Stimmgeheimnisses darf nach der Entschlüsselung der private Schlüssel nur dann vorliegen, wenn die Stimmen anonym abgegeben werden und unter den gegebenen Vertrauensannahmen keine Verschlüsselung einer Stimme mit der Identität eines Stimmenden in Verbindung gebracht werden kann. Weiter ist es infolge der Anforderung betreffend des Fehlens vozeitiger Teilergebnisse nicht zulässig, wenn Stimmen während der Öffnungszeit des elektronischen Stimmkanals ausserhalb der Benutzerplattform zu irgendeinem Zeitpunkt in unverschlüsselter Form vorliegen.
4.4.11	(Zu Art. 5 Abs. 6) Ob ernsthafte Fehlverhalten des Systems erkannt werden können, hängt von der Vertrauenswürdigkeit des „vertrauenswürdigen Systemteils“ ab. Zu solchen Fehlverhalten zählen fehlerhafte Berechnungen, die das Ergebnis beeinflussen, das Brechen des Stimmgeheimnisses oder die Erhebung vorzeitiger Teilergebnisse. Die Umsetzung bekannter Vorschläge aus der technischen Literatur gewährleistet dabei eine besonders hohe Vertrauenswürdigkeit. Die Vorschläge gehen so weit, dass ernsthafte Fehlverhalten nur dann nicht bemerkt werden, wenn ausnahmslos jede Kontrollkomponente einer Gruppe (beispielsweise infolge unbemerkter Manipulationen) nicht korrekt funktioniert. Funktioniert jedoch nur eine einzige Kontrollkomponente korrekt, kann jedes ernsthafte Fehlverhalten des Systems erkannt werden. Die Kontrollkomponenten werden in der Abstraktion im Englischen oft „Trustees“ genannt. In der Abstraktion werden Trustees als Instanzen dargestellt, die imstande sind komplexe Berechnungen anzustellen und private Elemente geheim zu halten. Die Berechnungen können das beweisbar korrekte Mischen und Wiederverschlüsseln von Stimmen (zu deren Anonymisierung; jeder Trustee entspricht einem Mischknoten eines Wiederverschlüsselungsnetzes), das Führen eines vertrauenswürdigen elektronischen schwarzen Bretts oder die Erstellung der PKI und mithilfe deren verteilten privaten Schlüssels das beweisbar korrekte Entschlüsseln von Stimmen beinhalten. In der Abstraktion werden die Trustees oft wie Menschen dargestellt, die rechnen können wie Maschinen. Ob sie die Geheimelemente unter Verschluss halten, bzw. sie nicht benutzen um Nachrichten zu versenden, die missbräuchlich verwendet werden können, wird einzig von ihrem Willen abhängig gemacht, nicht mit dem Angreifer zusammenarbeiten zu wollen. In der Praxis muss zwar zwischen der Maschine und dem Menschen, der sie konfiguriert und überwacht, unterschieden werden. Die Beschreibung des kryptografischen Protokolls darf jedoch die Kontrollkomponenten wie autonome Trustees darstellen.
4.4.12	(Zu Art. 5 Abs. 6) Die Software von Kontrollkomponenten soll einfach zu analysieren sein und sich möglichst auf elementare kryptografische Funktionen beschränken.
4.4.13	(Zu Art. 5 Abs. 6) Die Kontrollkomponenten müssen in einem beobachtbaren Prozess aufgesetzt, aktualisiert, konfiguriert und abgesichert werden.
4.4.14	(Zu Art. 5 Abs. 6) Die Kontrollkomponenten müssen sich möglichst unterscheiden und ihr Betrieb muss unabhängig von den übrigen Kontrollkomponenten erfolgen. Dies dient dem Ziel, dass ein geglückter unerlaubter Zugriff möglichst keinen Vorteil beim Versuch verschafft, auf eine weitere Kontrollkomponente unbemerkt zuzugreifen (Implementierung von „Trustees“; siehe Ziff. 4.4.12). Dadurch bleibt die Vertrauenswürdigkeit einer Gruppe von Kontrollkomponenten weiterhin gewährleistet. Dazu sind mindestens die folgenden Massnahmen vorzusehen: Der Betrieb und die Überwachung der Kontrollkomponenten sollen in der Verantwortung unterschiedlicher Personen liegen. Die Hardware und die Überwachungssysteme der Kontrollkomponenten sollen sich unterscheiden. Die Kontrollkomponenten sollen an unterschiedliche Netzwerke angeschlossen sein. Sie dürfen physisch und logisch nur für Personen zugänglich sein, die für den Betrieb und die Überwachung einer spezifischen Kontrollkomponente verantwortlich sind. Zugriffsversuche durch Verantwortliche anderer Kontrollkomponenten müssen erkannt und dem Verantwortlichen der entsprechenden Kontrollkomponenten gemeldet werden.

4.4.15	(Zu Art. 5 Abs. 6) Die Kontrollkomponenten müssen ausschliesslich die vorgesehenen Operationen durchführen. Sie 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 unter ihrer Kontrolle liegt. Die verantwortlichen Personen müssen als besonders vertrauenswürdig und zuverlässig gelten.
4.4.16	(Zu Art. 5 Abs. 6) Es sollen mindestens vier Kontrollkomponenten pro Gruppe mit unterschiedlichen Betriebssystemen zum Einsatz kommen. Falls es sich bei den Kontrollkomponenten um Geräte handelt, die spezifisch für das sichere Ausführen von kryptografischen Operationen entwickelt und geprüft worden sind (Hardware-Sicherheits-Modul, HSM), darf eine Gruppe aus zwei Kontrollkomponenten von unterschiedlichen Herstellern bestehen. Es dürfen beide HSMs dasselbe Betriebssystem verwenden.
4.4.17	(Zu Art. 5 Abs. 6) Eine HSM muss über ein vertrauenswürdiges Zertifikat verfügen zur Bestätigung, dass die Geheimelemente unzugänglich sind und dass sie jede Verwendung der Geheimelemente so registriert, dass die verantwortliche Person eine missbräuchliche Verwendung erkennen kann. Das Zertifikat muss mindestens in Analogie zu einer Prüftiefe von EAL4 nach Common Criteria oder FIPS 140-2 level 3 entsprechen. Es ist zulässig, eine HSM mit Software zu ergänzen, die in einem geschützten Bereich läuft. Das Zertifikat muss sich in diesem Fall auch auf die Zuverlässigkeit des geschützten Bereichs beziehen. Die Software und ihre korrekte Installation sind zu prüfen.

5. Prüfkriterien für die Systeme und ihren Betrieb (Zulassung von mehr als 30 Prozent des kantonalen Elektorats)

Jede der Ziffern 5.1 – 5.6 entspricht einer externen Prüfung des Systems. Die zuständigen Organisationen erstellen im Erfolgsfall einen Beleg zuhanden des Kantons, der die Prüfung in Auftrag gibt. Der Kanton legt den Beleg seinem Gesuch um Zulassung durch die BK bei. Die einzureichenden Belege sind unter Ziffer 6 zusammengefasst.

5.1 Prüfung des kryptografischen Protokolls

5.1.1	Prüfkriterien: Das Protokoll muss das Sicherheitsziel unter den Vertrauensannahmen im abstrakten Modell gemäss Ziffer 4 erfüllen. Dazu müssen ein kryptografischer und ein symbolischer Beweis vorliegen. Die Beweise dürfen bezüglich kryptografischer Grundkomponenten unter allgemein akzeptierten Sicherheitsannahmen geführt werden (beispielsweise „random oracle model“, „decisional Diffie-Hellman assumption“, „Fiat-Shamir heuristic“). Das Protokoll soll sich möglichst auf existierende und bewährte Protokolle abstützen.
5.1.2	Zuständigkeiten: Die Beweise müssen von hochspezialisierten Institutionen erbracht oder geprüft werden. Die Wahl einer Organisation muss vorgängig von der BK gutgeheissen werden. Konkretes Vorgehen: 1. Der Kanton meldet der BK den Einsatz eines neuen Protokolls oder eine Änderung am bestehenden. Der Kanton kann Vorschläge machen, welche Institution, allenfalls welche Person, die Prüfung vornehmen soll. 2. Die BK beurteilt den Vorschlag. 3. Die BK informiert den Kanton über ihren Entscheid. Im Fall von individuell verifizierbaren Systemen können infolge der starken Vertrauensannahmen simple Protokolle zum Einsatz kommen. In diesem Fall kann die BK vom Beizug einer externen Organisation absehen.
5.1.3	Dauer der Gültigkeit eines Belegs: Eine komplette Überprüfung muss vor der ersten Inbetriebnahme erfolgen. Das Protokoll muss bei jeder Änderung des Protokolls und bei gravierendenden neuen Erkenntnissen der Forschung bezüglich der Sicherheit von verwendeten kryptografischen Elementen neu überprüft werden.

5.2 Prüfung der Funktionalität

5.2.1	Prüfkriterien: Die Funktionalität muss die in Ziffern 2, 3 und 4 aufgeführten Anforderungen erfüllen, beziehungsweise die vorgegebenen Zielsetzungen adäquat unterstützen. Allenfalls muss ein Protokoll gemäss Art. 4 oder Art. 5 umgesetzt sein. Es soll sichergestellt sein, dass die im Protection Profile (PP) des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) aufgeführten Security Functional Requirements (SFR) oder gleichwertige Mittel als Sicherheitsmassnahmen umgesetzt sind. Die Funktionalität ist in Anlehnung an den Formalismus der Common Criteria (CC) nach den EAL2 Hauptkriterien zu prüfen.
5.2.2	Zuständigkeiten: Die Prüfung erfolgt durch eine von der schweizerischen Akkreditierungsstelle (SAS) akkreditierten Institution.
5.2.3	Dauer der Gültigkeit eines Belegs: Die Funktionalität ist bei jeder wesentlichen Änderung, wie beispielsweise nach einer Änderung am kryptografischen Protokoll, neu zu prüfen.

5.3 Prüfung der Infrastruktur und des Betriebs

5.3.1	Prüfkriterien: Das System und sein Betrieb müssen die in Ziffern 2, 3 und 4 aufgeführten Anforderungen erfüllen, beziehungsweise die vorgegebenen Zielsetzungen adäquat unterstützen. Die Informationssicherheit des Systems und seines Betriebs müssen durch Einrichtung, Implementierung, Betrieb, Überwachung, Überprüfung, Pflege und Verbesserung eines Informationssicherheitsmanagement-Systems (ISMS) nach ISO/IEC 27001:2013 (Information technology – Security techniques – Information security management systems – Requirements) gewährleistet sein. Der Geltungsbereich des ISMS muss alle diejenigen Organisationseinheiten des Systembetreibers umfassen, die rechtlich, administrativ und betrieblich für das System verantwortlich sind.
5.3.2	Zuständigkeiten: Die Wirksamkeit und Angemessenheit des ISMS muss durch die Vorlage des durch eine Zertifizierungsstelle ausgestellten Zertifikats, das die Zertifizierung des ISMS nach ISO/IEC 27001:2013 bescheinigt, nachgewiesen werden. Zusätzlich muss die Zertifizierungsstelle bescheinigen, dass die in Ziffern 2, 3 und 4 beschriebenen Anforderungen erfüllt werden, soweit diese nicht bereits durch den Audit nach ISO/IEC 27001:2013 abgedeckt werden. Die Zertifizierungsstelle muss durch die Schweizerische Akkreditierungsstelle (SAS) für die Durchführung von ISO/IEC 27001:2013 Audits akkreditiert sein.
5.3.3	Dauer der Gültigkeit eines Belegs: Wiederholungsaudits müssen in den durch ISO 27001:2013 festgelegten Abständen durchgeführt werden. Ein gültiges Zertifikat muss bei jedem Einsatz vorliegen. Infolge eines Entscheids auf eine Überwachungsmassnahme, welche dem sicheren und unabhängigen Einsatz von Kontrollkomponenten dient, zu verzichten oder sie wesentlich anzupassen, ist ebenfalls ein Wiederholungsaudit vorzunehmen. Wird eine neue Version des Standards ISO/IEC 27001:2013 publiziert, muss spätestens nach Ablauf der Übergangsfrist eine gültige Zertifizierung des ISMS nach der neuen Version nachgewiesen werden. Der Geltungsbereich des ISMS darf dabei nicht reduziert werden.

5.4 Prüfung der Kontrollkomponenten

5.4.1	Prüfkriterien: Die Kontrollkomponenten müssen die in Ziffer 4 festgehaltenen Anforderungen erfüllen, beziehungsweise die vorgegebenen Zielsetzungen adäquat unterstützen. Funktionen, deren Vertrauenswürdigkeit für die Stichhaltigkeit der im Rahmen der Verifizierbarkeit vorgesehenen Beweise massgeblich ist, sind anhand des Quellcodes und des kryptografischen Protokolls eingehend zu prüfen. Es soll sichergestellt sein, dass die im Protection Profile (PP) des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) aufgeführten Security Functional Requirements (SFR) oder gleichwertige Mittel als Sicherheitsmassnahmen umgesetzt sind. Die Funktionalität ist in Anlehnung an den Formalismus der Common Criteria (CC) nach den EAL4 Hauptkriterien zu prüfen. Basiskomponenten, wie beispielsweise Software, die dem sicheren und unabhängigen Einsatz von Kontrollkomponenten dient, die eingesetzten Betriebssysteme oder die eingesetzten Server müssen erwiesenermassen besten Standards entsprechen.
5.4.2	Zuständigkeiten: Die Prüfung erfolgt durch eine von der SAS akkreditierte Institution.
5.4.3	Dauer der Gültigkeit eines Belegs: Kontrollkomponenten sind in den folgenden Fällen neu zu prüfen: – bei jeder Änderung am Quellcode der Funktionen, deren Vertrauenswürdigkeit für die Stichhaltigkeit der im Rahmen der Verifizierbarkeit vorgesehenen Beweise massgeblich sind; und – beim Verzicht oder wesentlichen Anpassungen an Mechanismen, die dem sicheren und unabhängigen Einsatz von Kontrollkomponenten dienen; und – im Fall einer HSM muss das Aufspielen der Funktionen, deren Vertrauenswürdigkeit für die Stichhaltigkeit der im Rahmen der Verifizierbarkeit vorgesehenen Beweise massgeblich sind, in jedem Fall im Rahmen einer Prüfung stattfinden. Werden neue Versionen von Basiskomponenten eingesetzt (neue Server, Patches zu Betriebssystem oder Software, die dem sicheren und unabhängigen Einsatz von Kontrollkomponenten dient), muss keine neue Kontrolle erfolgen, sofern die Basiskomponenten weiterhin erwiesenermassen besten Standards entsprechen.

5.5 Prüfung des Schutzes gegen Versuche in die Infrastruktur einzudringen

5.5.1	Prüfkriterien: Kompetente Angreifer aus dem Internet dürfen nicht in die Infrastruktur eindringen können, um sich Zugang zu wichtigen Daten zu verschaffen oder um die Kontrolle über wichtige Funktionen zu übernehmen. Dazu versucht eine spezialisierte Institution im Rahmen eines Penetrationstests, ob sie auf der Grundlage der Systemdokumentation in die Infrastruktur eindringen kann, indem sie bekannte Schwachstellen der eingesetzten Technologien ausnutzt. Als Systemdokumentation müssen der Institution mindestens Dokumente zur Architektur, zum Datenfluss und zu den eingesetzten Technologien vorliegen. Sie prüft im Mindesten Schwachstellen, die im Open Web Application Security Project (OWASP) dokumentiert sind.
5.5.2	Zuständigkeiten: Die Prüfung erfolgt durch eine von der SAS akkreditierte Institution.
5.5.3	Dauer der Gültigkeit eines Belegs: Nach drei Jahren muss eine neue Prüfung erfolgen.

5.6 Prüfung einer Druckerei

5.6.1	Prüfkriterien: Eine Druckerei muss zusätzlich zu den im Anforderungskatalog an Druckereien aufgeführten Bestimmungen die Anforderung gemäss Ziffer 4.2.5 umsetzen.
5.6.2	Zuständigkeiten: Die Prüfung erfolgt durch eine von der SAS akkreditierte Institution.
5.6.3	Dauer der Gültigkeit eines Belegs: Nach zwei Jahren muss eine neue Prüfung erfolgen. Infolge eines Entscheids auf eine Massnahme zu verzichten oder sie wesentlich anzupassen, ist ebenfalls eine Wiederholung der Prüfung vorzunehmen.

6. Einzureichende Belege zur Zulassung

6.1	Der gesuchstellende Kanton reicht die Belege zu den Überprüfungen ein (vgl. Art. 7), die er von den zuständigen Institutionen erhalten hat. Beim Beleg zur Prüfung gemäss Ziffer 5.3 muss es sich um ein gültiges Zertifikat nach ISO/IEC 27001:2013handeln.
6.2	Der Kanton kann über mehrere Urnengänge hinaus die Gültigkeit eines Belegs geltend machen. In diesem Fall begründet der Kanton, weshalb er hinsichtlich des aktuellen Urnengangs keine Wiederholung der entsprechenden Prüfung vorgenommen hat. Dazu gibt er sämtliche vorgenommenen und geplanten Änderungen am System bis zum Zeitpunkt des Urnengangs an. Er zeigt dadurch auf, dass es sich um geringfügige Anpassungen handelt, die keinen negativen Einfluss auf die Risikobeurteilung haben.
6.3	Der Kanton reicht sämtliche Testprotokolle, die aus der Umsetzung des Testkonzepts (Ziff. 3.5) resultieren, ein. Er verpflichtet sich, weitere Testprotokolle nachzureichen, falls ein Test erst kurz vor dem Urnengang durchgeführt wird.
6.4	Der Kanton reicht seine aktuelle Risikobeurteilung (Art. 3) ein und verpflichtet sich, auf Veränderungen in der Einschätzung von Risiken umgehend hinzuweisen. Sämtliche Risiken, die sich für die Erfüllung der Sicherheitsziele ergeben, müssen über eine Risikobeurteilung bestimmt werden. Ferner müssen auch Risiken beurteilt werden, die das Umfeld der elektronischen Stimmabgabe in Administration und Öffentlichkeit betreffen. Die Beurteilung muss gemäss einer Methodik erfolgen, die die Einhaltung folgender Tätigkeiten vorsieht: – Risiken identifizieren – Risiken analysieren – Risiken bewerten Die Details der verwendeten Methodik sowie die vom Kanton vorgegebenen Risikoakzeptanzkriterien müssen dokumentiert werden. Für Risiken, die sich aus dem Betrieb des Systems ergeben, müssen bei der Risikoidentifikation im Fall einer Zulassung von mehr als 30 Prozent des kantonalen Elektorats die methodischen Anforderungen von ISO/IEC 27001:2013 vollumfänglich eingehalten werden.