ANFORDERUNGEN AN INTERNETBASIERTE VEREINSWAHLEN[1]

***Die unten aufgelisteten Anforderungen gelten unter nachfolgenden Vereinbarungen*:**

- Die Wahl erfolgt von einem internetfähigen Endgerät in privater oder Arbeitsumgebung.
- Die Wähleridentifizierung erfolgt durch nicht-geheimen Namen, Mitgliedsnummer o. ä., (im Folgenden als PIN bezeichnet).
- Die Wählerauthentifizierung erfolgt durch eine Wahl-PIN;
- Die Wahlurne und Wählerverzeichnis sind auf getrennten Servern installiert und befinden sich in unterschiedlichen Institutionen.
- Als alternative Wahlform ist die klassische Briefwahl für jeden Wähler möglich.
- Nominierungsverfahren der Wahlkandidaten und Festlegungen der berechtigten Wähler gehören nicht zum Anwendungsbereich des elektronischen Wahlsystems.
- Es gibt keine besonderen Vorschriften für die Langzeitarchivierung von Wahlergebnissen.
- Falls Teilkomponenten des Wahlsystems in anderen Softwareprodukten verwendet werden, dann gibt es für diese Teilkomponenten keine Nutzungseinschränkungen.
- Die Voraussetzungen zur Durchführung von Briefwahlen werden als gegeben angenommen. Es werden nur Anforderungen aufgestellt, die darüber hinaus erfüllt sein müssen.

A. Allgemeine Anforderungen an Systementwicklung und Wahldurchführung

(S-1) Es muss eine Systembeschreibung vorliegen, die mindestens den Systemaufbau, die Hardware- und Softwarekomponenten, die verwendeten Verfahren, die zugelassenen Internetendgeräte und die Umgebungsbedingungen enthält. Dies bedeutet insbesondere auch, dass der vollständige Source Code zur Prüfung vorgelegt werden muss. Außerdem muss der Hersteller eine Sicherheitsanalyse nachweisen.

(S-6) Die Software muss gemäß anerkannter Regeln der Technik entwickelt worden sein. Insbesondere muss sie wohl strukturiert und kommentiert, identifizierbar sowie jede Versi-

[1] Entwickelt für die Gesellschaft für Informatik e.V. (GI) unter Verwendung von
- „Online-Wahlsysteme für nicht-parlamentarischen Wahlen: Anforderungskatalog“, Laborbericht PTB-8.5-2004-1, April 2004;
- Council of Europe: Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting, September 2004;
- IEEE P 1583™, Draft 5.0: Standard for the Evaluation of Voting Equipment, August 2003

onsänderung nachvollziehbar sein. Die Dokumentation muss vollständig, widerspruchsfrei und verständlich sein.

(A-2) Der komplette Weg vom Entwurf bis zur Implementierung des Anonymisierungskonzeptes muss offen gelegt werden, je nach Wahlvorschriften für benannte Prüfstellen/Experten oder für die interessierte Öffentlichkeit. Die Implementierung muss mit Softwareprüfmethoden, die dem Stand der Technik entsprechen, als eine korrekte Umsetzung des theoretischen Konzeptes nachgewiesen worden sein.

(S-2) Angemessene Bedienanleitungen für die Wähler und den Wahlvorstand müssen verfügbar sein. Insbesondere müssen darin Informationen zum Schutz vor Manipulationen oder Ausspähungen am Internetendgerät den Wählern zur Verfügung gestellt werden.

(S-11) Alle Komponenten des Wahlsystems müssen auf Funktionssicherheit und Zusammenspiel getestet und darüber hinaus muss ein durchgängiger Funktionstest durchgeführt worden sein. Protokolle der Tests müssen vorliegen. Falls es die Vorschriften so verlangen, muss das Wahlsystem oder eine identische Kopie rechtzeitig und ausreichend lange außerhalb der eigentlichen Wahl für interessierte Personen zum Kennenlernen und Testen zur Verfügung stehen.

(A-3) Es muss eine angemessene Verwaltungsstrategie für die Schlüssel existieren, falls solche im Verfahren verwendet werden. Diese muss beschrieben sein.

(G-1) Für jeden Wähler muss rechtzeitig die PIN und WAHL-PIN zur Verfügung stehen. Die PIN muss eindeutig bekannt sein oder authentisch und unverfälscht übergeben werden. Die WAHL-PIN muss authentisch, unverfälscht und vertraulich übergeben werden.

(G-3) Es muss gesichert sein, dass der Wähler nur eine Wahloption – entweder Internetwahl oder Briefwahl - wahrnehmen kann.

(W-10) Das Löschen von Daten und das Deinstallieren des Systems darf erst dann erfolgen, wenn die aufgezeichneten Protokolle ausgewertet worden sind, ein weiterer Auswertungsbedarf nicht besteht und die nach den geltenden Vorschriften erforderliche Archivierung der Daten und Protokolle sichergestellt ist. Das Löschen der Daten muss endgültig und unumkehrbar sein.

B. Anforderungen an die Wahlserver

(S-3) Die Server müssen so betrieben werden, dass sie Energieschwankungen, mechanischen Stößen, Temperaturschwankungen, Feuchtigkeit und elektromagnetischen Einflüssen nicht ausgesetzt oder robust dagegen sind. Ein Sofortservice muss im Bedarfsfall verfüg-

bar sein. Defekte Baugruppen müssen durch baugleiche bzw. kompatible Teile ersetzbar sein.

(S-4) Für die eingesetzten Server müssen sichere Betriebssysteme und Sicherheitskonzepte realisiert sein, die dem aktuellen Bedrohungspotenzial entsprechen.

(S-8) Die wahlrelevante Software muss isoliert gegenüber anderer Software arbeiten, d.h. sie darf nicht Rückwirkungen solcher Software ausgesetzt sein und auch selber die wahlunabhängige Software nicht beeinflussen.

(S-5) Der Zugang bzw. Zugriff zu allen Servern und zu Protokollaufzeichnungen, die im Rahmen der Wahl eine Bedeutung haben, muss registriert werden. Jeder Zugriff auf den Server darf nur über das Vier-Augenprinzip geregelt sein.

(G-4) Die elektronische Wählerliste einschließlich der Stimmabgabevermerke muss gegenüber unberechtigten Veränderungen geschützt sein. Jede Veränderung der elektronischen Wählerliste muss protokolliert werden.

C Anforderungen an die Wahlsoftware

1. Allgemeine Anforderungen an das elektronische Wahlsystem und seine Sicherheit

(S-7) Die Software muss sämtliche Funktionen, die für die Erfüllung der gestellten Aufgabe nötig sind, effektiv und zuverlässig realisieren. Sie darf keine unbenutzten Programmteile oder andere, für Angriffe oder Fehlfunktionen anfällige Programmkonstrukte enthalten.

(S-9) Bei einer beabsichtigten oder unbeabsichtigten Unterbrechung der Wahl muss das System auf einen Zustand zurückgefahren werden, aus dem heraus die Wahlhandlung wieder aufgenommen werden kann. Alle wahlrelevanten Informationen müssen gesichert oder bei Fortsetzung wieder herstellbar sein.

(S-10) Der technische Systemzustand muss fortlaufend protokolliert werden, so dass der ordnungsgemäße Ablauf der Wahl beurteilt werden kann. Insbesondere muss das Wahlsystem während des Betriebes eine Selbstdiagnose durchführen und Softwareveränderungen erkennen. Alle erkannten Angriffsversuche müssen protokolliert werden. Es darf keine Möglichkeit geben, automatische Protokollierungsfunktionen abzustellen oder Protokolldaten unberechtigt zu verändern. Die Protokollierung muss auf eine Art und Weise erfolgen, die die geheime Wahl nicht verletzt.

2. Spezifische Funktionsanforderungen an das elektronische Wahlsystem

(W-1) Alle Teile des Wahlsystems, insbesondere der Stimmenspeicher, müssen vor Wahlbeginn in den definierten Anfangszustand versetzt werden. Dieses Setzen in den Anfangszustand darf nach Wahlbeginn nicht mehr durchführbar sein.

(W-2) Das Wahlsystem muss eine elektronische Wählerliste führen die zudem sicherstellt, dass jeder Wähler nur eine Stimme abgibt.

(W-2') Zulässige, auch kurzfristige Veränderungen der elektronischen Wählerliste (Korrektur und/oder Ergänzung) durch autorisierte Personen müssen möglich und leicht handhabbar sein, falls dies in den Wahlvorschriften vorgesehen ist.

(W-3) Über alle in der Systembeschreibung genannten Endgeräte muss die Identifizierung und Authentisierung durch den Wähler möglich sein.

(W-4) Das Wahlsystem muss den authentischen und unverfälschten Stimmzettel auf den in der Systembeschreibung genannten Endgeräten anbieten und Wahlentscheidungen annehmen, die gemäß geltender Vorschriften möglich sind. Die Möglichkeit zur ungültigen Stimmabgabe muss existieren, falls dies von den Wahlvorschriften verlangt wird.

(W-5) Das Zwischenspeichern von Stimmen außerhalb des hierzu vorgesehenen Wahlservers ist nicht erlaubt.

(W-5') Die Stimmenspeicherung muss so organisiert sein, dass inkonsistente Zustände nach jeder Einspeicherung einer Stimme erkannt werden. Handlungsszenarien für solche Fälle müssen existieren.

(W-6) Die erfolgreiche Einspeicherung einer Stimme muss zum Stimmabgabevermerk für diesen Wähler in der elektronischen Wählerliste führen.

(W-7) Die Wahlabschlussprozedur muss eindeutig festgelegt sein. Spätestens 15 Minuten nach dem festgelegten Endzeitpunkt der Wahl müssen die rechtzeitig begonnenen Wahlhandlungen beendet und die ggf. abgegebenen Stimmen gespeichert werden.

(W-8) Die Ermittlung der für einen Kandidaten abgegebenen Stimmen darf erst nach Wahlabschluss erfolgen. Davor darf die Feststellung entsprechender Zwischenergebnissen nicht möglich sein.

(W-9) Die summarische Ermittlung der Ergebnisse und die Einbeziehung aller einzelnen Stimmen muss nachweisbar korrekt sein. Falls weitere Auswertungen vorgesehen sind, müs-

sen die dafür verwendeten Verfahren den geltenden Vorschriften entsprechen und korrekt sein.

(W-9') Das System muss eine Abgleichfunktion bzgl. der laut Wählerverzeichnis abgegebenen Stimmen und der Anzahl der Stimmen in der Urne zur Verfügung stellen.

3. Anonymisierungsanforderungen

(A-1) Das verwendete Anonymisierungskonzept einschließlich der mathematischen Verfahren muss nachweislich das Wahlgeheimnis sichern, insbesondere müssen die eingesetzten Verfahren effizient, robust und über den geforderten Geheimhaltungszeitraum stabil sein.

(A-4) Bei keinem Teilschritt der Wahl und in keinem Systemzustand darf die Trennung von Wähler und Stimmeninhalt gefährdet werden.

(A-5) Bei der Stimmabgabe darf keine nachweisbare Beziehung vom Wähler zum Inhalt seiner abgegebenen Stimme hergestellt werden können. Insbesondere dürfen PIN und WAHL-PIN oder Teile von ihnen bei der Stimmabgabe bzw. Absendung der Stimme nur nach angemessener Verschlüsselung dieser Daten verwendet werden.

(A-6) Das Wahlsystem darf es dem Wähler nicht ermöglichen, die tatsächliche Wahlentscheidung zu beweisen. Im Zusammenhang mit der endgültigen Stimmabgabe müssen am Endgerät alle sichtbaren und intern gespeicherten Informationen automatisch entfernt werden. Ggf. muss der Wähler Hinweise erhalten, wie er dies am Endgerät kontrollieren kann.

(A-7) Die abgegebene Stimme muss bei Transport und Speicherung bis zur Auszählung gegen Einsicht gesichert sein. Es darf auch nicht möglich sein, über indirekte Informationen (z.B. Reihefolge der Stimmabgabe) Schlüsse über das Wahlverhalten von einzelnen Personen oder Wählergruppen zu ziehen.

(A-8) Bei der Feststellung des Wahlergebnisses darf die Anonymisierung der abgegebenen Stimmen nicht gefährdet werden. Das gilt grundsätzlich auch bei der Zusammenführung von Stimmen oder Teilergebnissen aus der Internet- und der Briefwahl.

(A-9) In automatisch aufgezeichneten Protokollen dürfen sich keine Informationen über Wähler sowie über Stimminhalte befinden.

4. Spezielle Anforderungen zum Schutz der Allgemeinheit und Gleichheit der Wahl

(G-2) Die Identifikation und Authentisierung des Wählers muss eindeutig und zuverlässig erfolgen. Eine Kommunikationsunterbrechung darf die Eindeutigkeit und Zuverlässigkeit nicht beeinträchtigen.

(G-5) Bei der Darstellung des Stimmzettels sind Präferenzen oder Benachteiligungen für einzelne Wahlvorschläge durch geeignete Maßnahmen auszuschließen.

(G-6) Stimmen dürfen nur von autorisierten Wählern und innerhalb der festgelegten Zeiten angenommen werden. Für jeden Wähler darf nur eine Stimme in das Ergebnis eingehen. Nach dem Wahlabschluss darf es nicht möglich sein, weitere Stimmen abzugeben bzw. zu speichern.

(G-7) Abgegebene Stimmen müssen beim Transport und bei der Speicherung gegen Löschung, Veränderung oder Vervielfältigung geschützt sein. Es dürfen keine abgegebenen Stimmen unbemerkt verloren gehen oder vom Transport und Speicherung ausgeschlossen werden. Für den Fall einer nicht erfolgreichen Übermittlung oder Speicherung einer Stimme muss ein Handlungsszenario für den Wähler existieren.

5. Ergonomische und Bedienbarkeitsanforderungen

(E-1) Das Wahlsystem muss für den Wähler verständlich und leicht handhabbar sein. Fehlbedienungen, die zu einem nicht definierten oder unklaren Zustand des Systems führen, dürfen keinen Einfluss auf die abgegebene Stimme haben und müssen durch eindeutige Handlungshinweise korrigiert werden können.

(E-2) Die Darstellung des Stimmzettels muss auf den angegebenen internetfähigen Endgeräten so erfolgen, dass die Wahlvorschläge gut erkennbar sind. Die Darstellung zusätzlicher Einblendungen durch die Wahlsoftware muss verhindert werden, wenn dies von den Wahlvorschriften verlangt wird.

(E-3) Für die Stimmabgabe muss eine ausdrückliche Bestätigungsfunktion existieren.

(E-4) Die erfolgreiche Annahme und Speicherung der Stimme durch das Wahlsystem muss dem Wähler deutlich dargestellt werden.