Physikalisch-Technische Bundesanstalt
Braunschweig und Berlin

Fachbereich Metrologische Informationstechnik

Laborbericht PTB-8.5-2004-1

Online-Wahlsysteme für nicht-parlamentarischen Wahlen: Anforderungskatalog

Online Voting Systems for Non-parliamentary Elections: Catalogue of Requirements

PTB-8.5-2004-1
Berlin, April 2004

Online-Wahlsysteme für nicht-parlamentarischen Wahlen: Anforderungskatalog

(Autoren/Bearbeiter: Volker Hartmann, Nils Meißner und Dieter Richter)
(Volker.Hartmann@ptb.de, Nils.Meissner@ptb.de, Dieter.Richter@ptb.de)

Der vorliegende Anforderungskatalog ist im Rahmen des vom deutschen Bundesministerium für Wirtschaft und Arbeit (BMWA) geförderten Projektes „Entwicklung von Konzepten für die Prüfung und Zertifizierung von Online-Wahlsystemen“, Förderkennzeichen 01 MD 248, an der Physikalisch-Technischen Bundesanstalt, Fachbereich „Metrologische Informationstechnik“, entstanden. Er wurde in den vom BMWA eingesetzten Arbeitsgruppen „Prüfung und Zertifizierung von Online-Wahlsystemen“[1] und „Rechtliche Rahmenbedingungen für Online-Wahlsysteme“[2] diskutiert. Zum Zeitpunkt der Herausgabe stellt er das abgestimmte Meinungsbild der an der Diskussion Beteiligten dar.

Im Anforderungskatalog werden technische und organisatorische Maßstäbe zur Umsetzung der wahlrechtlichen Grundsätze bei nicht-parlamentarischen Wahlen beschrieben. Er stellt eine Empfehlung für Entwickler als auch eine Orientierung für die Verfeinerung der Prüfschritte dar. Zukünftige technische Entwicklungen, neue Erkenntnisse im Allgemeinen sowie über Bedrohungspotentiale im Besonderen und praktische Erfahrungen können zu Erweiterungen oder Änderungen führen.

Berlin, im April 2004

Dieter Richter
(Projektleiter)

[1] In der Arbeitsgruppe sind nachfolgende Institutionen vertreten: Physikalisch-Technische Bundesanstalt (PTB) Berlin, Bundesamt für Sicherheit in der Informationstechnik (BSI) Bonn, Technische Universität Ilmenau, Technischer Überwachungsverein Informationstechnik (TÜV IT) Essen, T-Systems Darmstadt, Landesbetrieb für Datenverarbeitung und Statistik (LDS) Potsdam, Bundesministerium für Wirtschaft und Arbeit (BMWA) Berlin, Deutsches Zentrum für Luft- und Raumfahrt (DLR) Köln, Vereinigte Dienstleistungsgewerkschaft (ver.di) Berlin, Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI) Saarbrücken

[2] In der Arbeitsgruppe sind nachfolgende Institutionen vertreten: Bundesministerium für Wirtschaft und Arbeit (BMWA) Berlin und Bonn, Deutsche Lufthansa (DLH) Frankfurt, Bundesministerium des Innern (BMI) Berlin, T-Systems Darmstadt, Landesbetrieb für Datenverarbeitung und Statistik (LDS) Potsdam, Universität Osnabrück, Vereinigte Dienstleistungsgewerkschaft (ver.di) Berlin, Physikalisch-Technische Bundesanstalt (PTB) Berlin, Deutsches Zentrum für Luft- und Raumfahrt (DLR) Köln

Online Voting Systems for Non-parliamentary Elections: Catalogue of Requirements

(Authors/Editors: Volker Hartmann, Nils Meißner und Dieter Richter)
(Volker.Hartmann@ptb.de, Nils.Meissner@ptb.de, Dieter.Richter@ptb.de)

The catalogue of requirements which is now available has been drawn up at Physikalisch-Technische Bundesanstalt, Department of Metrological Information Technology, within the framework of the project "Development of concepts for testing and certification of online voting systems" funded by the German Ministry of Economics and Labour (BMWA). It has been discussed in the working groups "Testing and certification of online voting systems"[3] and "Legal framework conditions for online voting"[4], both established by BMWA. The catalogue represents the harmonised opinion of the participants at the point in time of its issue.

Based on basic electoral rules, the catalogue describes technical and operational standards for the implementation of non-parliamentary elections. It constitutes a recommendation for developers of systems and, simultaneously, gives an orientation for the refinement of test concepts. Future technological developments, new knowledge in general and on threats in particular as well as further practical experience may lead to extensions or amendments.

Berlin, April 2004

Dieter Richter
(project leader)

[3] Members of the working group are from following institutions: Physikalisch-Technische Bundesanstalt (PTB) Berlin, Bundesamt für Sicherheit in der Informationstechnik (BSI) Bonn, Technische Universität Ilmenau, Technischer Überwachungsverein Informationstechnik (TÜV IT) Essen, T-Systems Darmstadt, Landesbetrieb für Datenverarbeitung und Statistik (LDS) Potsdam, Bundesministerium für Wirtschaft und Arbeit (BMWA) Berlin, Deutsches Zentrum für Luft- und Raumfahrt (DLR) Köln, , Vereinigte Dienstleistungsgewerkschaft (ver.di) Berlin, Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI) Saarbrücken

[4] Members of the working group are from following institutions: Bundesministerium für Wirtschaft und Arbeit (BMWA) Berlin und Bonn, Deutsche Lufthansa (DLH) Frankfurt, Bundesministerium des Innern (BMI) Berlin, T-Systems Darmstadt, Landesbetrieb für Datenverarbeitung und Statistik (LDS) Potsdam, Universität Osnabrück, Vereinigte Dienstleistungsgewerkschaft (ver.di) Berlin, Physikalisch-Technische Bundesanstalt (PTB) Berlin, Deutsches Zentrum für Luft- und Raumfahrt (DLR) Köln

Inhaltsverzeichnis Seite

Table of Contents Page

Anforderungen an Online-Wahlsysteme für nicht-parlamentarischen Wahlen

Vorbemerkung

Zweck des Anforderungskataloges

Dieser Anforderungskatalog enthält Kriterien für die Umsetzung grundlegender wahlrechtlicher Bestimmungen auf Online-Wahlsysteme. Er definiert einen Standard, der sowohl Entwicklern und Prüfern von Online-Wahlsystemen als Orientierung dienen soll. Dieses Dokument hat keinen bindenden regulativen, sondern empfehlenden Charakter.

Mit der Veröffentlichung dieses Kataloges soll zur gegenwärtigen Diskussion um angemessene Rahmenbedingungen für technische Systeme zur Unterstützung von Online-Wahlsystmen beigetragen werden.

Der Katalog schreibt keine Methoden vor, die bei Online-Wahlsystemen zum Einsatz kommen sollen. Es wird auch nicht vorgegeben, ob bestimmte Anforderungen durch technische Verfahren oder organisatorische Maßnahmen abzusichern sind. Ebenso ist die Frage, wie die Erfüllung der Anforderungen nachgewiesen wird, nicht Gegenstand des Kataloges.

Status des Anforderungskataloges

Dieser Anforderungskatalog wurde in der PTB entworfen. Er ist in mehreren Versionen in den Arbeitsgruppen „Prüfung und Zertifizierung“ sowie „Rechtliche Rahmenbedingungen“, die von Bundesministerium für Wirtschaft und Arbeit für die Erörterung spezieller Fragen von Online-Wahlsystemen gebildet wurden, beraten worden. Die vorliegende Version berücksichtigt alle bislang bekannten Hinweise aus den Arbeitsgruppen.

Da praktische Erfahrungen mit Online-Wahlsystmen bisher kaum verfügbar sind, repräsentiert der Katalog das gegenwärtige Meinungsbild der Beteiligten. Zukünftige technische Entwicklungen und neue Erfahrungen im Allgemeinen sowie über Bedrohungen im Besonderen können zu Änderungen oder Ergänzungen dieses Kataloges führen.

Anwendungsbereich und Einschränkungen

Das Anwendungsfeld, das der Entwicklung der Anforderungen zu Grunde lag, ist durch gesetzlich geregelte, nicht-parlamentarische Wahlen wie z.B. Betriebsratswahlen, Personalratswahlen oder Aktionärswahlen, bestimmt. Die Anforderungen sind bei anderen, nicht gesetzlich geregelten, nicht-parlamentarischen Wahlen auch anwendbar. Jedoch kann dann die eine oder andere Anforderung abgeschwächt werden. Was die Anwendung auf parlamentarische Wahlen betrifft, sind die meisten Anforderungen

ebenfalls übertragbar. Jedoch ist eine sorgfältige Analyse noch erforderlich, wo Verstärkungen oder Erweiterungen geboten sind.

Bei der Ausarbeitung der Anforderungen ist angenommen worden, dass Wahlen ausschließlich in vernetzten Wahllokalen stattfinden. Die Durchführung von Wahlen von privaten Plätzen zu Hause oder an anderer Stelle ist explizit nicht in den Anforderungen eingeschlossen.

Methodische Herangehensweise

Der gesamte Wahlvorgang einschließlich Vor- und Nachbereitung sowie übergreifender Aspekte ist in neutral, d.h. unabhängig von Systemkonzepten, definierten Funktionseinheiten aufgeteilt worden. Diese Einheiten orientieren sich an einer abstrakten Wahlfunktionalität. Entsprechend ist der Detaillierungsgrad der Anforderungen beschränkt. Das Zerlegungsprinzip entspricht dem vorherrschenden Verständnis über die Funktionskomponenten von Online-Wahlsystemen. Die meisten der aufgestellten Funktionseinheiten sind genau einer Phase des Wahlprozesses zuzuordnen, einige sind phasenübergreifend. Es ist nicht zwingend, dass alle hier definierten Funktionen in allen Online-Wahlsystemen vorhanden sind.

Den definierten Funktionseinheiten sind dann Anforderungen zugeordnet worden. Eine durchaus denkbare, weitere Klassifizierung der zu einer Funktionseinheit gehörenden Anforderungen (z.B. nach funktionellen Anforderungen, Sicherheitsanforderungen und ergonomischen Anforderungen) ist in Erwägung gezogen, dann aber doch nicht realisert worden. Sie ist für den beabsichtigten Zweck dieses Kataloges nicht erforderlich. Darüber hinaus wäre eine solche Zuordnung nicht immer eindeutig, so dass dieser Katalog mit Problemen aus dem Bereich der IT-Terminologie überfrachtet worden wäre, die der interdisziplinären Diskussionen nicht förderlich sind. In den meisten Fällen ist der Charakter der Anforderung bezüglich der IT-bezogenen Qualittätskriterien aus der Darstellung selbst ableitbar.

Die Anforderungen sind detaillierter, als es rechtliche Rahmenbedingungen sein können. Sie sind aber andererseits hinreichend allgemeingültig, um sie unabhängig von speziellen Systemkonfigurationen beschreiben zu können. Auf Konfigurationsbeispiele wurde grundsätzlich verzichtet, um keine bestimmten Systeme zu favorisieren. Untersetzungen im Hinblick auf spezifische Online-Wahlsysteme und ihre Modelle sowie auf eine eventuelle Differenzierung hinsichtlich der Wahlart sind nicht Gegenstand des Kataloges. Sie sind zu einem späteren Zeitpunkt im Vorfeld der Prüfung abzuleiten.

Das Detaillierungsniveau der Anforderungsdefinitionen ist unterschiedlich. Es ist grundsätzlich versucht worden, die Anforderungen so spezifisch wie möglich zu entwerfen. Es gibt jedoch Aspekte, die wegen des unklaren rechtlichen Hintergrundes bzw. wegen der vielen möglichen, sehr unterschiedlichen technischen Lösungen nicht weiter eingeengt werden können. Es hat sich in der Tat herausgestellt, dass zur Zeit die gesetzliche Grundlage verschiedener Aspekte von Online-Wahlsystemen noch nicht oder nur grob definierbar ist. Das betrifft Fragen wie die Rolle von technischem

Personal, die Definition von so genannten Zwischenspeichern von Stimmen, die Nachprüfbarkeit von Wahlen, etc. für die Vielfalt von technischen Lösungen steht die Anonymisierung als Beispiel. Die bekannten und wahrscheinlich anwendbaren Methoden sind so unterschiedlich, dass die entsprechenden Anforderungen nur auf einem relativ allgemeinen Niveau dargestellt werden konnten.

Für bestimmte Anforderungen ist das Attribut „hohe Kritikalität“ eingeführt worden. Hohe Kritikalität bedeutet im Kontext diese Kataloges, dass die jeweilige Anforderung wichtig für die Umsetzung der allgemeinen wahlrechtlichen Grundsätze ist und ihre Erfüllung nicht ohne technische Spezialkenntnisse oder -verfahren festgestellt werden kann, d.h. Fehler in den betroffenen Funktionen sind bei der Anwendung auf Grund der elektronischen oder softwaretechnischen Realisierung im Allgemeinen nicht oder nicht sicher erkennbar. Die Richtigkeit, Zuverlässigkeit oder der Schutz der entsprechenden Funktionen vor Manipulationen kann nicht mehr im bisherigen Sinne durch eine soziale oder wahlorganisatorische Kontrolle erfolgen. Es sind technische Sicherungs- und Prüfmaßnahmen erforderlich.

Anforderungen hoher Kritikalität sind gekennzeichnet. Anforderungen, die nicht als hoch kritisch benannt sind, sind im wahlrechtlichen Sinne nicht unwichtig. Ihre korrekte Umsetzung kann jedoch durch Wahlpersonal oder Wähler währen der Wahldurchführung hinreichend kontrolliert werden.

Die Beziehungen zwischen den einzelnen Funktionen einerseits und den wahltypischen Rollen und Objekten andererseits werden im Anhang A in einer Tabelle dargestellt. Diese Tabelle hat informativen Charakter. Darüber hinaus werden in Anhang B die Beziehungen zwischen den Funktionen und den rechtlichen Rahmenanforderungen hergestellt. Diese in Tabellenform angegebenen Beziehungen haben ebenfalls informativen Charakter, erklären aber auch in der Übersicht, warum bestimmte Anforderungen aufgestellt worden sind. Anhang C erklärt die verwendeten bzw. eingeführten Begriffe.

Quellen

Der Ausarbeitung des Katalogs ging eine Analyse verfügbarer Materialien voraus, die sich zumindest teilweise mit Anforderungen an Online-Wahlsysteme befassen. Ausgewertet wurden die folgenden Unterlagen: [CYBERVOTE], [NVSS], [RICHTLINIE], [VPR], [VSS]. Der vorliegende Katalog ist frei entworfen und in Diskussionen weiter entwickelt worden, so dass eine Quellenangabe bei einzelnen Anforderungen nicht mehr möglich ist.

Anforderungskatalog

Der Anforderungskatalog ist nach Wahlphasen geordnet aufgebaut. Funktionen bzw. Anforderungen, die nicht nur einer Wahlphase zugeordnet werden können, sind unter der Rubrik „Übergreifende Funktionen“ eingeordnet worden. Die folgenden Wahlphasen werden unterschieden und mit den eingeführten Kurzzeichen gekennzeichnet:

WV: Wahlvorbereitung
- **(WV1)** Erzeugung des Wählerverzeichnisses
- **(WV2)** Vorbereitung der Wähleridentifikation und –authentifizierung
- **(WV3)** Vorbereitung des Wahlvorschlages
- **(WV4)** Installation des Online-Wahlsystems und Herstellung der Betriebsbereitschaft

WH: Wahlhandlung
- **(WH1)** Wähleridentifikation und –authentifizierung
- **(WH2)** Wählerlistenmanagement
- **(WH3)** Behandlung des Stimmzettels
- **(WH4)** Transport der Stimme
- **(WH5)** Speicherung der Stimme

EW: Ermittlung des Wahlergebnisses
- **(EW1)** Abschluss der Wahlhandlung
- **(EW2)** Feststellung des Wahlergebnisses

NA: Nachbereitung und Aufbewahrung
- **(NA1)** Deinstallation des Wahlsystems
- **(NA2)** (Langzeit-)Archivierung
- **(NA3)** Aufbewahrung und Wartung des Wahlsystems

sowie

ÜF: Übergreifende Funktionen
- **(ÜF1)** Allgemeine Software- und Hardwarezuverlässigkeit,
- **(ÜF2)** zu Grunde liegendes Kommunikationssystem,
- **(ÜF3)** Anonymisierung der Stimmen,
- **(ÜF4)** Technische Beobachtung des Wahlsystems (technisches Audit).

Auch Datenschutzbestimmungen haben einen übergreifenden Charakter. Sie sind bei Online-Wahlen gundsätzlich zu beachten, da mit personenbezogenen Daten umgegangen wird. Die geltenden Regelungen sind in entsprechenden Gesetzen geregelt. Weitere Präzisierungen sind hier nicht erforderlich.

Bei ergonomischen Anforderungen liegen ebenfalls übergreifende Gesichtspunkte vor. Allerdings gibt es dann doch Differenzierungen bei einzelnen Funktionen, so dass der Einzelbenennung der ergonomischen Anforderungen in den jeweiligen Funktionen der Vorzug gegenüber der übergreifenden Darstellung gegeben wurde.

1 Wahlvorbereitung - WV

In der Wahlvorbereitung sind die nachfolgenden Funktionen relevant:

(WV1) Erzeugung des Wählerverzeichnisses,
(WV2) Vorbereitung der Wähleridentifikation und –authentifizierung,
(WV3) Vorbereitung des Wahlvorschlages,
(WV4) Installation des Online-Wahlsystems und Herstellung der Betriebsbereitschaft.

Die Wahlvorbereitungsphase endet mit der Eröffnung der Wahlhandlung.

1.1 Erzeugung des Wählerverzeichnisses (WV1)

Bei der Erzeugung des Wählerverzeichnisses (d.h. bei der Auswahl, der Festlegung und der Bestimmung der Wahlberechtigten) ist bisher nicht vorstellbar, dass Online-Wahlsystemkomponenten zum Einsatz kommen könnten. Daher erfolgt für diese Funktion keine Spezifikation von Anforderungen.

Für die Vorbereitung des Wählerlistenmanagements ergibt sich folgende Anforderung:

(WV1-1) Die elektronische Wählerliste muss den Inhalt der gültigen Wählerliste korrekt enthalten.

(WV1-2) Der Umgang mit der elektronischen Wählerliste muss leicht handhabbar sein.

1.2 Vorbereitung der Wähleridentifikation und Wählerauthentifizierung(WV2)

Diese Funktion umfasst die Vorbereitung und Ausgabe der notwendigen Wähleridentifikationsmittel und muss gewährleisten, dass jeder Wahlberechtigte sich zum Zeitpunkt der Wahl entsprechend dem angewendeten Identifikationsverfahren als wahlberechtigt ausweisen kann. Es bestehen die folgenden Anforderungen:

(WV2-1) Für jeden Wähler muss (spätestens zum Zeitpunkt der Wahl) sein Wähleridentifikationsmittel bereitstehen.

(WV2-2) Die Funktionssicherheit der technischen Wähleridentifikation muss gewährleistet sein.

(WV2-3) Es müssen Alternativen zur elektronischen Wähleridentifikation bereitgehalten werden, falls eine solche zur Anwendung kommt. Die Alternativen müssen den gestellten Anforderungen genügen.

(WV2-4) Die erforderlichen Verbindungen und Schnittstellen müssen abgestimmt sein (Hardware- und Softwarekompatibilität).

(WV2-5) Die Wähleridentifikationsmittel müssen authentisch und unverfälscht übersendet bzw. übergeben werden. Bei geheimen Wähler-identifikationsmitteln muss darüber hinaus Vertraulichkeit gewahrt werden.

(WV2-6) Der Wähler muss über den Umgang mit den Wähleridentifikationsmittel und die Bedeutung der Geheimhaltung klar und ausreichend informiert werden.

Die Anforderungen (WV2-4) und – im Falle einer elektronischen Übermittlung der Wähleridentifikationsmittel – auch (WV2-5) haben eine hohe Kritikalität.

1.3 Vorbereitung des Wahlvorschlages (WV3)

Nominierungsverfahren für Kandidaten und das Ausarbeiten der Stimmzettel erfolgen vor Einsatz des Online-Wahlsystems. Sie werden hier nicht behandelt.
Für die Übertragung der erarbeiteten Dokumente, insbesondere für die Vorbereitung der Darstellung des Stimmzettels sowie für die Anbindung an Steuerungs- und Stimmabgabefunktionen gilt die Anforderung:

(WV3-1) Das Online-Wahlsystem muss dokumentierte Schnittstellen und Hilfsmittel zur Einpflege der Stimmzettel-Daten zur Verfügung stellen. Die Durchführung muss leicht handhabbar sein.

1.4 Installation des Systems und Herstellen der Betriebsbereitschaft (WV4)

In diesem wichtigen Funktionskomplex in unmittelbarer Vorbereitung der Wahl ist abzusichern, dass

- die Wahlsysteme installiert sind,
- die Betriebsbereitschaft des Gesamtsystems sichergestellt ist,
- Systemdokumentationen verfügbar sind,
- Maßnahmen zur Einweisung in die Bedienung erfolgt sind; das betrifft insbesondere die Bedienhinweise für die Wähler, für den Wahlvorstand sowie Anleitungen für das technische Wahlpersonal.

Daraus ergeben sich die nachfolgenden Anforderungen:

(WV4-1) Es muss eine umfassende Systemdokumentation vorliegen, die insbesondere enthalten soll
- die Beschreibung der Architektur des Systems (System-Modell),
- die Beschreibung der enthaltenen Hardware- und Softwarekomponenten,

- die Beschreibung der zur Umsetzung der Systemfunktionalität verwendeten Verfahren,
- die Beschreibung der Umgebungsbedingungen.

(WV4-2) Anleitungen für die Wähler, den Wahlvorstand und das technische Wahlpersonal müssen vorhanden und für den jeweiligen Personenkreis angemessen sein.
Texte müssen ohne Veränderung anderer technischer Eigenschaften durch fremdsprachliche Texte ersetzbar oder ergänzbar sein.

(WV4-3) Die Zugangskontrolle zu allen Rechnern, die im Rahmen der Wahl eine Funktion haben, muss eindeutig geregelt sein und jeder Zugang muss zum Zwecke des Schutznachweises protokolliert werden.

(WV4-4) Die Aufgabenbereiche (Privilegien) des technischen Wahlpersonals und die dafür erforderliche Qualifikation müssen wohl definiert sein.

(WV4-5) Das komplette Wahlsystem muss rechtzeitig am Ort der Wahlhandlung bzw. der –durchführung bereitgestellt sein.

(WV4-6) Alle notwendigen Anschlüsse an das für die Wahldurchführung vorgesehene Kommunikationssystem müssen vorhanden sein.

(WV4-7) Es sind geeignete Vorkehrungen für das unbeobachtete Ausfüllen der Stimmzettel im Wahllokal zu treffen.

(WV4-8) Alle Komponenten müssen auf Funktionssicherheit und Zusammenspiel getestet werden.

(WV4-9) Es muss ein durchgängiger Funktionstest durchgeführt und protokolliert werden.

(WV4-10) Alle Teile des Online-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.

(WV4-11) Bei Ausfall von oder Fehlern in Komponenten müssen technische und/oder organisatorische Alternativen, die den gleichen Anforderungen unterliegen, zur Verfügung stehen.

(WV4-12) Es müssen Strategien, Software und/oder Hardware zum Zusammenführen und Auszählen der Stimmen bereitgestellt werden.

Die Anforderungen (WV4-8) bis (WV4-12) haben eine hohe Kritikalität.

2 Wahlhandlung - WH

Die Wahlhandlung umfasst als Funktionen:

(WH1) Wähleridentifikation und –authentifizierung,
(WH2) Wählerlistenmanagement,
(WH3) Behandlung des Stimmzettels,
(WH4) Transport der Stimme,
(WH5) Speicherung der Stimme.

2.1 Wähleridentifikation und -authentifizierung (WH1)

Die Anforderungen an die Wähleridentifikation und -authentifizierung hängen in großem Maße von den verwendeten Verfahren ab und sind auch in Abhängigkeit davon genau zu spezifizieren. Dabei existiert eine Vielfalt von Möglichkeiten.

Die Wähleridentifikation und –authentifizierung, d.h. das Ausweisen des Wählers als Wahlberechtigter, steht am Anfang der Wahlhandlung. Es gehören dazu die Kontrolle der Wähleridentität, das Feststellen der Wahlberechtigung und das Freigeben bzw. Sperren der Wahlhandlung des einzelnen Wählers.

Als Grundanforderungen stehen:

(WH1-1) Die Identifikation und Authentisierung des Wählers bzw. der Wahlberechtigung muss eindeutig und zuverlässig erfolgen.

(WH1-2) Es darf keine Beziehung vom Wähler zu seiner abgegebenen Stimme hergestellt werden können.

Anforderungen an die Kontrolle der Wähleridentität:

(WH1-3) Das Vorgehen bei der Kontrolle der Wähleridentität muss verständlich und leicht handhabbar sein.

(WH1-4) Für den Fall des Verlustes des Wähleridentifikationsmittels müssen alternative Identifikationsverfahren bereit stehen. Die Alternativen müssen den gestellten Anforderungen genügen.

Für das Feststellen der Wahlberechtigung ergeben sich folgende Anforderungen:

(WH1-5) Eine Unterbrechung der Verbindung des Wähleridentifikationssystems zur elektronischen Wählerliste darf die Wähleridentifikations- und Wählerauthentifizierungsfunktionen nicht beeinflussen.

Das Freigeben bzw. Sperren der Wahlhandlung erfordert:

(WH1-6) Eine Möglichkeit zum (automatischen oder manuellen) Freigeben bzw. Sperren
der Wahlhandlung muss vorhanden sein. Das Freigeben darf nur nach erfolgreicher Wähleridentifikation erfolgen, ansonsten muss das Wahlterminal gesperrt sein.

(WH1-7) Erfolgt das Freigeben bzw. Sperren der Wahlhandlung teilweise manuell, muss es leicht handhabbar sein und der Wahlvorstand muss jederzeit über den Freigabestatus informiert sein.

Mit Ausnahme von (WH1-3) sind alle Anforderungen von hoher Kritikalität.

2.2 Wählerlistenmanagement (WH2)

Das Wählerlistenmanagement beinhaltet das Führen der elektronischen Wählerliste während der Wahl. Es umfasst auch die Handhabung von Sonderfällen bei der Wähleridentifikation und die Erstellung der Stimmabgabevermerke. Die Funktion steht in engem Zusammenhang mit der Wähleridentifikation und –authentifizierung.

Folgende Anforderungen müssen für die Handhabung der elektronischen Wählerliste erfüllt sein:

(WH2-1) Die elektronische Wählerliste muss das Setzen von Stimmabgabevermerken erlauben. Stimmabgabevermerke müssen gegen Verlust geschützt werden.[5]

(WH2-2) Zulässige, auch kurzfristige Veränderungen der elektronischen Wählerliste (Korrektur und/oder Ergänzung) durch autorisierte Personen müssen möglich und leicht handhabbar sein.

(WH2-3) Die elektronische Wählerliste einschließlich der Stimmabgabevermerke muss gegenüber unberechtigten Veränderungen geschützt sein.

(WH2-4) Jede Veränderung der elektronischen Wählerliste muss protokolliert werden.

(WH2-5) Die elektronische Wählerliste muss vom Stimmenspeicher getrennt sein.

Sämtliche Anforderungen haben eine hohe Kritikalität.

2.3 Behandlung des Stimmzettels (WH3)

Der Umgang mit dem Stimmzettel ist ein wesentlicher Teil der Wahlhandlung. Im Einzelnen gehören zur Behandlung des Stimmzettels:
das Laden (Bereitstellen des zutreffenden Stimmzettels),

[5] Eine redundante Speicherung bietet sich als geeignete Maßnahme an.

- die Darstellung des Stimmzettels,
- das Ausfüllen des Stimmzettels,
- die endgültige Stimmabgabe sowie
- deren Bestätigung und die Rückmeldung an den Wähler.

Die Anforderungen an das Laden des Stimmzettels sind:

(WH3-1) Die Bereitstellung des für die jeweilige Wahl und – falls erforderlich – für die jeweilige Gruppe zutreffenden Stimmzettels (Authentizität des Stimmzettels) muss gesichert sein.

(WH3-2) Die Bereitstellung des unverfälschten Stimmzettels (Integrität des Stimmzettels) muss gesichert sein.

(WH3-3) Der Wahlvorstand muss die Authentizität und Integrität des Stimmzettels kontrollieren können.

Die Anforderungen (WH3-1) und (WH3-2) haben hohe Kritikalität.

Die Darstellung des Stimmzettels muss folgende Anforderungen erfüllen:

(WH3-4) Die Darstellung des Stimmzettels muss auf allen Wahlterminals einheitlich und gut erkennbar erfolgen. Sie muss alle notwendigen Angaben und nur diese enthalten.[6]

(WH3-5) Bei der Darstellung des Stimmzettels müssen dem Wähler alle Wahlvorschläge gleichmäßig und vollständig dargestellt werden. Insbesondere ist dies bei Stimmzetteln zu beachten, die die Bildschirmgröße überschreiten. Benachteiligungen für einzelne Wahlvorschläge sind durch geeignete Maßnahmen[7] auszuschließen.

(WH3-6) Die ggf. erforderliche Bedienung am Wahlterminal bei der Darstellung des Stimmzettels muss verständlich und leicht handhabbar sein.

Als Anforderungen an das Ausfüllen des Stimmzettels gelten:

(WH3-7) Die Vertraulichkeit bei dem Ausfüllen des Stimmzettels muss gewährleistet sein.

(WH3-8) Die Stimmabgabe muss gegen Manipulationen geschützt sein.

(WH3-9) Fehlbedienungen dürfen keinen Einfluss auf die abzugebende Stimme haben.

[6] Nach gegenwärtiger Auffassung soll die Darstellung des Stimmzettels, wo es möglich ist, identisch zur gewohnten Darstellung auf Papier sein.

[7] Geeignet sind nach gegenwärtiger Auffassung eine verkleinerte Gesamtdarstellung als erste Darstellung der Wahlvorschläge, ein ununterbrechbarer Zwangsdurchlauf durch alle Wahlvorschläge vor einer Stimmabgabe oder vergleichbare Maßnahmen.

(WH3-10) Fehlbedienungen müssen durch eindeutige Handlungshinweise korrigiert werden können, insbesondere muss die Möglichkeit zum Abbruch bzw. Neubeginn existieren.

(WH3-11) Die Möglichkeit zur ungültigen Stimmabgabe muss existieren.

(WH3-12) Die Navigation während der Stimmabgabe muss verständlich und leicht handhabbar sein.

Die Anforderungen (WH3-7) bis (WH3-9) haben eine hohe Kritikalität.

Für die endgültige Stimmabgabe, ist erforderlich:

(WH3-13) Die endgültige Stimmabgabe darf für jeden Wähler nur einmal möglich sein und nur an freigegebenen Wahlterminals erfolgen.

(WH3-14) Zur endgültigen Stimmabgabe muss eine ausdrückliche Bestätigungsfunktion existieren.

(WH3-15) Es dürfen keinerlei Merkmale der Wähleridentität bei der endgültigen Stimmabgabe verwendet werden.

(WH3-16) Nach der endgültigen Stimmabgabe müssen am Wahlterminal alle sichtbaren und internen Informationen über die abgegebene Stimme entfernt werden.

(WH3-17) Nach der endgültigen Stimmabgabe muss das Wahlterminal automatisch in den gesperrten Zustand gesetzt werden.

Mit Ausnahme von (WH3-14) haben diese Anforderungen eine hohe Kritikalität.

Zur Bestätigung der endgültigen Stimmabgabe ist erforderlich:

(WH3-18) Die endgültige Stimmabgabe und erfolgreiche Annahme durch das Online-Wahlsystem müssen dem Wähler transparent dargestellt werden.

(WH3-19) Die Bestätigung soll in angemessen kurzer Zeit erfolgen.

2.4 Transport der Stimme (WH4)

Mit der endgültigen Stimmabgabe beginnt der Transport der Stimme vom Wahlterminal zum Stimmenspeicher. Hierzu gehören:

- das Erstellen eines transportablen Stimmdatensatzes,
- die Sicherung (Zwischenspeicherung) von Stimme bzw. Stimmdatensatz, entweder als Puffer für den Fall von Kommunikationsunterbrechungen vorgesehen oder

konzeptionell geplant, z.B. für die Bündelung von Stimmdatensätzen für den Transport,
- das Weiterleiten des Stimmdatensatzes via Kommunikationssystem sowie
- die Rückmeldung an den Wähler.

Für das Erstellen eines transportablen Stimmdatensatzes gelten die Anforderungen:

(WH4-1) Der Stimmdatensatz muss dem abgestimmten und dokumentierten Format entsprechen.

(WH4-2) Der Stimmdatensatz muss genau den Inhalt der abgegebenen Stimme (bzw. der abgegebenen Stimmen) enthalten.

(WH4-3) Der Stimmdatensatz muss gegen unberechtigte Einsicht und Veränderung gesichert sein.

Für die Sicherung (Zwischenspeicherung) von Stimme bzw. Stimmdatensatz ist erforderlich:

(WH4-4) Die Zwischenspeicherung darf nur in einer Form erfolgen, die gegen unberechtigte Einsicht und Veränderung geschützt ist.

(WH4-5) Die Zwischenspeicherung darf nur für den unbedingt notwendigen Zeitraum erfolgen. Danach müssen die gespeicherten Daten endgültig und unumkehrbar gelöscht werden.

An den eigentliche Transport des Stimmdatensatzes wird folgende Anforderung gestellt:

(WH4-6) Es dürfen keine abgegebenen Stimmen vom Transport ausgeschlossen werden und vor Beginn der Auszählung müssen alle abgegebenen Stimmen im Stimmenspeicher vorhanden sein.

Die Anforderungen an das verwendete Kommunikationssystem befinden sich bei den übergreifenden Funktionen ÜF2.

Hinsichtlich der Rückmeldung an den Wähler wird über die Anforderungen (WH3-18) und (WH3-19) hinaus gefordert:

(WH4-7) Für den Fall einer nicht erfolgreichen Übermittlung einer Stimme muss ein Handlungsszenario für Wähler und Wahlpersonal existieren.

Die Anforderungen mit Ausnahme von (WH4-7) haben eine hohe Kritikalität.

2.5 Speicherung der Stimme (WH5)

Die Speicherung der Stimme beendet den Transport. Unter Speicherung ist in diesem Zusammenhang das Bereithalten der Stimmen zur Auszählung zu verstehen. Die Langzeitarchivierung, d.h. eine Speicherung über die Wahl hinaus, wird hier nicht betrachtet.

Bei der Übernahme der Stimme in den Stimmenspeicher ist zu beachten:

(WH5-1) Aus dem Stimmdatensatz ist genau der Inhalt der ursprünglichen Stimme (bzw. Stimmen) wieder herzustellen.

(WH5-2) Die Speicherung der Stimmen muss in einer Form erfolgen, die sie gegen unberechtigte Einsicht und Veränderungen schützt.

(WH5-3) Ein Verlust von Stimmdatensätzen ist auszuschließen.[8]

(WH5-4) Bei der Stimmenspeicherung muss eine Rückmeldung an die elektronische Wählerliste generiert bzw. abgesandt werden.

Für die Bereithaltung zur Auszählung ist erforderlich:

(WH5-5) Inkonsistente Zustände müssen sofort erkannt werden. Handlungsszenarien für solche Fälle müssen existieren.

(WH5-6) Eine Ausgabe von Ergebnisinformationen darf vor dem Abschluss der Wahlhandlung nicht möglich sein.

Alle Anforderungen haben hohe Kritikalität.

3 Ermittlung des Wahlergebnisses - EW

Die Ermittlung des Wahlergebnisses untergliedert sich in:

(EW1) den Abschluss der Wahlhandlung und
(EW2) die Feststellung des Wahlergebnisses.

3.1 Abschluss der Wahlhandlung (EW1)

Vor der Ermittlung des Wahlergebnisses ist die Wahlhandlung abzuschließen. Das Beenden der Wahlhandlung betrifft das Sperren des Wahlterminals für weitere Wahlhandlungen, das Abschalten der Kommunikationsverbindung für weitere wahlbezogene Übertragungen sowie das Sperren des Stimmenspeichers für die Annahme weiterer Stimmen.

[8] Eine redundante Speicherung bietet sich als geeignete Maßnahme an.

(EW1-1) Die Abschlussprozedur muss eindeutig festgelegt sein.

(EW1-2) Vor dem Abschalten bzw. Sperren der Komponenten müssen alle abgegebenen Stimmen transportiert und gespeichert und die entsprechenden Rückmeldungen an die Wähler sowie an die elektronische Wählerliste erfolgt sein. Es dürfen keine abgegebenen Stimmen verloren gehen.

(EW1-3) Nach dem Sperren darf es nicht möglich sein, weitere Stimmen abzugeben bzw. zu speichern.

(EW1-4) Der ordnungsgemäße Abschluss ist zu überprüfen und zu dokumentieren.

(EW1-5) Das Abschließen muss leicht handhabbar sein.

Die Anforderungen (EW1-2) und (EW1-3) sind von hoher Kritikalität.

3.2 Feststellung des Wahlergebnisses (EW2)

Die Feststellung des Wahlergebnisses umfasst:
- die summarische Ermittlung der Ergebnisse, d.h. das Auszählen aller abgegebenen gültigen und ungültigen Stimmen,
- gegebenenfalls die Ermittlung von Sitzverteilungen, Minderheitenvertretungen etc.,
- die Überprüfung des Ergebnisses,
- die Ergebnisübertragung.

Die Ermittlung der Ergebnisse erfordert:

(EW2-1) Die Ermittlung der Ergebnisse darf erst nach dem Abschließen des Stimmenspeichers erfolgen.

(EW2-2) Die summarische Ermittlung der Ergebnisse muss korrekt sein.

(EW2-3) Falls weitere Auswertungen der summarischen Ergebnisse vorgesehen sind, müssen die dafür verwendeten Verfahren den geltenden Vorschriften entsprechen und korrekt sein.

(EW2-4) Die Bedienung bei der Ermittlung der Ergebnisse und weiteren Auswertungen muss leicht handhabbar sein.

Die Anforderungen haben bis auf (EW2-4) hohe Kritikalität.

Anforderungen an die Überprüfbarkeit des Ergebnisses:

(EW2-5) Die Korrektheit des summarischen Ergebnisses und der abgeleiteten Auswertungen muss nachprüfbar sein.

(EW2-6) Die Einbeziehung aller einzelnen Stimmen muss nachprüfbar sein.

Die Anforderungen haben eine hohe Kritikalität.

Anforderungen an die Ergebnisübertragung:

(EW2-7) Bei der Berichterstellung sowie bei der Ergebnisübertragung darf keine Änderung bzw. kein Verlust der gespeicherten Stimmen oder des Ergebnisses erfolgen.

4 Nachbereitung und Aufbewahrung - NA

Zum Komplex der Nachbereitung und Aufbewahrung gehören:

(NA1) die Deinstallation des Wahlsystems,
(NA2) die(Langzeit-)Archivierung sowie
(NA3) die Aufbewahrung und Wartung des Wahlsystems.

4.1 Deinstallation des Wahlsystems (NA1)

Nach der Ermittlung und Protokollierung der Wahlergebnisse sowie ggf. der Ergebnisübertragung muss das Wahlsystem deinstalliert werden. Dazu gehört das Herunterfahren und das Abmelden aller Systemkomponenten sowie das Entfernen der Komponenten aus dem Wahllokal.

Anforderungen:

(NA1-1) Vor dem Löschen muss die Archivierung von allen für die gerichtliche Nachprüfbarkeit erforderlichen Daten sichergestellt werden.

(NA1-2) Das Löschen der Daten muss endgültig und unumkehrbar sein.

4.2 (Langzeit-)Archivierung (NA2)

Die (Langzeit-)Archivierung ist notwendig, um über einen Zeitraum von im allgemeinen fünf Jahren die gerichtliche Nachprüfbarkeit abzusichern.
Als Funktionen werden die Regelung der Archivierung und die Aufhebung des Archivs gesehen.

Anforderungen an die Regelung der Archivierung:

(NA2-1) Die Archivierung muss redundant erfolgen.

(NA2-2) Die archivierten Daten müssen vor Änderungen geschützt sein.

(NA2-3) Jeder Zugriff zu den archivierten Daten darf nur durch autorisierte Personen und nach einem geregelten Verfahren erfolgen und muss protokolliert werden.

(NA2-4) Es muss alle zur gerichtlichen Nachprüfbarkeit erforderliche Software und Hardware aufbewahrt werden.

(NA2-5) Inkonsistenzen, die während der Archivierung entstehen, müssen festgestellt werden.

(NA2-6) Die Regelung der Archivierung ist zu dokumentieren.

Die Anforderungen (NA2-1), (NA2-2) und (NA2-5) sind von hoher Kritikalität.

Die Aufhebung eines Archivs ist für die Durchführung und die Gültigkeit einer Wahl kaum relevant und wird daher nicht weiter durch Anforderungen untersetzt.

4.3 Aufbewahrung und Wartung des Wahlsystems (NA3)

Die Aufbewahrung und Wartung des Wahlsystems ist für die Durchführung und die Gültigkeit einer Wahl nicht relevant, da entsprechende Maßnahmen bei der Installation des Wahlsystems vorgesehen sind, die unabhängig von der zwischenzeitlichen Lagerung oder Benutzung der Komponenten sind. Die Funktion wird daher nicht durch Anforderungen untersetzt.

Sollten die Maßnahmen bei der Installation abgeschwächt werden unter Hinweis auf den Ausschluss einer anderen zwischenzeitlichen Verwendung, sind an dieser Stelle zweckmäßige Anforderungen aufzustellen.

5 Übergreifende Funktionen - ÜF

Online-Wahlsysteme haben Funktionen bzw. an sie sind Anforderungen zu stellen, die nicht genau einer Wahlphase zugeordnet werden können. Es sind:

(ÜF1) die allgemeine Software- und Hardwarezuverlässigkeit,
(ÜF2) das zu Grunde liegende Kommunikationssystem,
(ÜF3) die Anonymisierung der Stimmen und
(ÜF4) die technische Beobachtung des Wahlsystems (technisches Audit).

5.1 Allgemeine Software- und Hardwarezuverlässigkeit (ÜF1)

Zur Gewährleistung der Zuverlässigkeit sind allgemeine Software- und Hardwareanforderungen zu stellen. Diese Anforderungen betreffen grundlegende Softwareeigenschaften, die sich im Wesentlichen auf die Einhaltung des Standes der Technik beziehen. Die Anforderungen an die Hardware zielen vor allem auf den allgemeinen Schutz vor äuße-

ren bzw. Umgebungseinflüssen. Darüber hinaus sind Anforderungen für den Fall von Unterbrechungen der Wahlhandlung durch „höhere Gewalt“ erforderlich.

(ÜF1-1) Der Hersteller muss einen Nachweis über die Qualität seiner Entwicklungsprozesse gemäß einschlägiger Normen führen.

(ÜF1-2) Das Online-Wahlsystem muss isoliert gegenüber allen wahlsystemfremden Anwendungen arbeiten. Die Online-Wahl darf in keiner Weise durch andere Hard- oder Softwarekomponenten beeinflusst werden.

Die Software muss weiterhin folgenden Grundanforderungen genügen:

(ÜF1-3) Die Software muss sämtliche Funktionen, die für die Erfüllung der gestellten Aufgabe nötig sind, angemessen realisieren sowie zuverlässig ausführen.

(ÜF1-4) Die Software muss unter Beachtung der anerkannten Regeln des Softwareengineering entwickelt worden sein. Insbesondere muss sie wohl strukturiert und kommentiert sein, um die Prüfung zu ermöglichen.

(ÜF1-5) Jedes Programm muss eindeutig identifizierbar sein.

(ÜF1-6) Die Programmdokumentation muss vollständig, widerspruchsfrei, eindeutig und angemessen sowie verständlich und übersichtlich sein.

Hardware-Anforderungen:

(ÜF1-7) Die Hardware muss eine ausreichende Stossfestigkeit aufweisen sowie ausreichend resistent gegenüber Temperaturschwankungen, Feuchtigkeit und elektromagnetischen Einflüssen sein.

(ÜF1-8) Die verwendeten Bauteile müssen eine angemessen lange Lebensdauer erwarten lassen können. Defekte Bauteile müssen durch baugleiche bzw. kompatible Teile ersetzbar sein.

Anforderungen im Zusammenhang mit der Absicherung von im Wahlablauf vorgesehenen sowie nicht geplanten Unterbrechungen der Wahlhandlung:

(ÜF1-9) Abgegebene Stimmen dürfen nicht verloren gehen, verfälscht werden oder deanonymisierbar sein.

(ÜF1-10) Die elektronische Wählerliste darf während der Unterbrechung der Wahlhandlung nicht verändert werden.

(ÜF1-11) Alle wahlrelevanten Informationen müssen gesichert oder bei Fortsetzung wieder herstellbar sein.

(ÜF1-12) Wahlrelevante Handlungen am Wahlterminal dürfen während der Unterbrechung der Wahlhandlung nicht möglich sein.

(ÜF1-13) Das System muss auf einen Zustand zurückgefahren werden, aus dem heraus die Wahlhandlung wieder aufgenommen werden kann.

Diesen Anforderungen kommt eine hohe Kritikalität zu.

5.2 Kommunikationssystem (ÜF2)

Das zu Grunde liegende Kommunikationssystem, das auch außerhalb des Wahlsystems existiert und verwendet wird, muss bestimmten Mindestanforderungen genügen. Darüber hinaus gibt es Anforderungen, die sich an das Online-Wahlsystem richten.

Allgemeine Anforderung an das Kommunikationssystem:

(ÜF2-1) Eine hohe Verfügbarkeit des Kommunikationssystems muss sich in einer Online-Wahlverfahren vergleichbaren Praxis bestätigt haben.

Spezifische Anforderungen an das Wahlsystem, die im Zusammenhang mit der Kommunikation stehen:

(ÜF2-2) Während der Kommunikation müssen die Systemkomponenten des Online-Wahlsystems den Nachweis der Unverfälschtheit (Datenintegrität) und die unzweifelhafte Zuordnung von Sendern und Empfängern (Datenauthentizität) gemäß geltender technischer Standards bieten.

(ÜF2-3) Bei Kommunikationsunterbrechungen muss das Online-Wahlsystem in einen Zustand geführt werden, aus dem heraus die Kommunikation wieder aufgenommen werden kann.

(ÜF2-4) Für den Fall von wahlbehindernden Kommunikationsunterbrechungen müssen Alternativen für die Weiterführung der Wahl vorbereitet sein.

(ÜF2-5) Alle Kommunikationsunterbrechungen müssen so protokolliert werden, dass Gefahren wie:
- der Verlust oder die Veränderung von Stimmen,
- die Veränderung von Wählerlisteneintragungen oder
- die Deanonymisierung

beurteilbar sind.
Informationen über Wähler sowie Stimminhalte sind von der Protokollierung ausdrücklich auszuschließen.

(ÜF2-6) Für die eingesetzte Technik müssen Sicherheitskonzepte realisiert sein, die dem aktuellen technischen Stand und dem angenommenen Bedrohungspotential entsprechen.

Die wahlspezifischen Anforderungen haben eine hohe Kritikalität.

5.3 Anonymisierung (ÜF3)

Für die Anonymisierung sind verschiedene Verfahren bekannt. Die konkreten Anforderungen hängen wesentlich von den Verfahren ab.

Auf Grund der Abhängigkeit von den Verfahren können hier nur grundsätzliche Anforderungen für die Sicherung der Anonymisierung aufgestellt werden:

(ÜF3-1) Das verwendete Konzept einschließlich der mathematischen Verfahren muss nachweislich (d.h. gemäß Expertenbeurteilung auf der Basis des Standes der Technik bzw. einschlägiger Fachliteratur) die geforderte Anonymisierungsfunktion sichern, insbesondere müssen die eingesetzten Verfahren robust und über den geforderten Geheimhaltungszeitraum stabil sein.

(ÜF3-2) Das verwendete Konzept einschließlich der mathematischen Verfahren muss für die konkrete Wahl geeignet sein.

(ÜF3-3) Der komplette Weg vom Entwurf bis zur Implementation muss offengelegt werden.

(ÜF3-4) Die Implementation muss mit Softwaretestmethoden (inkl. Code-Inspektionen), die den Stand der Technik repräsentieren, als eine korrekte Umsetzung des theoretischen Konzeptes nachgewiesen worden sein.

(ÜF3-5) Die eingesetzten Verfahren müssen effizient arbeiten.

Sollten im Rahmen der Anonymisierung Schlüssel eingesetzt werden, gilt zusätzlich folgende Anforderung an das Schlüsselmanagement:

(ÜF3-6) Es muss eine angemessene Verwaltungsstrategie für die Schlüssel existieren.

Die Anforderungen (ÜF3-1) bis (ÜF3-4) sowie (ÜF3-6) haben eine hohe Kritikalität.

5.4 Technische Beobachtung (ÜF4)

Die technische Beobachtung der Komponenten des Wahlsystems (technisches Audit) ist für die gerichtliche Nachprüfbarkeit von Wahlen notwendig. Unter technischer Beobachtung wird dabei das Protokollieren von Zuständen und insbesondere von Havarien, Unterbrechungen und Auftreten von Systemfehlern verstanden. Ausdrücklich vom Zustandsprotokoll auszuschließen sind dabei Informationen über Wähler sowie Stimminhalte.

Anforderungen:

(ÜF4-1) Der technische Systemzustand muss fortlaufend protokolliert werden.

(ÜF4-2) Im Zustandsprotokoll dürfen sich keine Informationen über Wähler sowie über Stimminhalte befinden.

(ÜF4-3) Im Wahlablauf vorgesehene sowie nicht geplante Unterbrechungen, Havarien und andere abnormale Zustände sind so zu protokollieren, dass Gefahren wie:
- der Verlust oder die Veränderung von Stimmen,
- die Veränderung von Wählerlisteneintragungen oder
- die Deanonymisierung

beurteilbar sind.

(ÜF4-4) Es darf keine Möglichkeit geben, die Protokollierungsfunktion abzustellen oder Protokolldaten unberechtigt einzusehen oder zu verändern.

Die Anforderung (ÜF4-4) hat eine hohe Kritikalität.

Anhang A

Verbindung zwischen Funktionen und wahlspezifischen Rollen bzw. Objekten

In Tabelle 1 werden die bestehenden Beziehungen zwischen den wahlspezifischen Rollen und Objekten einerseits und den nach Wahlphasen geordneten Funktionsgruppen andererseits dargestellt. Dabei markiert (●) eine hohe Kritikalität.

Wahlspezifische Rollen sind durch Personen bzw. Ämtern auszufüllen. Es gibt die Wähler, den Wahlvorstand (einschließlich der Ämter in der Vorbereitung bzw. der Wahlhelfer in der Durchführung) und technisches Wahlpersonal mit Spezialkenntnissen für den technischen Service.
Wahltypische Objekte sind die elektronische Wählerliste, die Wähleridentifikationsmittel (z.B. Chipkarte, PIN, TAN), der (unausgefüllter) Stimmzettel; die (abgegebene) Stimme, der Stimmdatensatz als Objekt des Transportes, die Stimmenspeicher (Wahlurne) und das Wahlergebnis.
Die Rollen und Objekte werden über die Wahlphasen „Wahlvorbereitung“, „Wahlhandlung“, „Ermittlung des Wahlergebnisses", sowie „Nachbereitung und Aufbewahrung des Systems“ betrachtet.

Aus Sicht der Rollen wird beispielsweise deutlich, dass der Wahlvorstand bei den Anforderungen zu fast allen Funktionen betroffen ist. Die für den Wähler kritische Funktionen liegen insbesondere in der Phase der Wahlhandlung. Die Tabelle zeigt aber auch, dass neben bestimmten Konzentrationen eine recht breite Verteilung der Beziehungen besteht.

Rolle / Objekt Funktionsgruppe	Wähler	Wahlvorstand	Technisches Wahlpersonal	Wählerliste	Wähleridentifikationsmittel	Stimmzettel	(abgegebene) Stimme	Stimmdatensatz	Stimmenspeicher	Wahlergebnis
1. Wahlvorbereitung										
1.1 Erzeugen des Wählerverzeichnisses	○	○		○						
1.2 Vorbereitung Wähleridentifikation / -authentifizierung	○	●	○	○	●					
1.3 Vorbereitung des Wahlvorschlages		○				○				
1.4 Installation/Herstellen der Betriebsbereitschaft		●	●			○			●	
2. Wahlhandlung										
2.1 Wähleridentifikation / -authentifizierung	●	●		●	●					
2.2 Wählerlistenmanagement		●		●						
2.3 Behandlung des Stimmzettels	●	○				●	●			
2.4 Transport der Stimme	○	○	●				●	●		
2.5 Speicherung der Stimme			○	●			●	●	●	
3. Ermittlung des Wahlergebnisses										
3.1 Abschluss der Wahlhandlung		○					●		●	
3.2 Feststellung des Ergebnisses		○					●		●	●
4. Nachbereitung / Aufbewahrung										
4.1 Deinstallation		○	○							
4.2 (Langzeit-)Archivierung		○	○	●		●	●		○	●
4.3 Aufbewahrung / Wartung des Wahlsystems		○	○							

Tabelle 1: Zusammenhang zwischen Rollen bzw. Objekten und Funktionsgruppen

Anhang B

Verbindung zwischen Funktionen und rechtlichen Aspekten

Online-Wahlsysteme müssen den allgemeinen Wahlgrundsätzen:

- geheime Wahl,
- gleiche und allgemeine Wahl,
- unmittelbare Wahl,
- freie Wahl

genügen.

Darüber hinaus ist die gerichtliche Nachprüfbarkeit zu gewährleisten. In diesem Zusammenhang geht es um:

- die Sicherstellung der Nachprüfbarkeit des Wahlergebnisses,
- die Nachprüfbarkeit des ordnungsgemäßen Wahlablaufs.

In Tabelle 2 werden die Beziehungen zwischen den rechtlichen Aspekten einerseits und den nach Wahlphasen geordneten Funktionsgruppen andererseits dargestellt. Dabei markiert (●) eine hohe Kritikalität.

Die Tabelle ermöglicht eine Einordnung der Funktionen hinsichtlich ihrer rechtlichen Bedeutung.

rechtliche Aspekte Funktionsgruppe	***allgemeine Wahlgrundsätze***	geheime Wahl	gleiche und allgemeine Wahl	unmittelbare Wahl	freie Wahl	***gerichtliche Nachprüfbarkeit***	Nachprüfbarkeit des Wahlergebnisses	Nachprüfbarkeit der Ordnungsmäßigkeit
1. Wahlvorbereitung								
1.1 Erzeugen des Wählerverzeichnisses								○
1.2 Vorbereitung Wähleridentifikation / -authentifizierung		○	●	○				○
1.3 Vorbereitung des Wahlvorschlages								
1.4 Installation/Herstellen der Betriebsbereitschaft		●	○				○	●
2. Wahlhandlung								
2.1 Wähleridentifikation / -authentifizierung		●	●					○
2.2 Wählerlistenmanagement			●				○	○
2.3 Behandlung des Stimmzettels		●	●	●	●			○
2.4 Transport der Stimme		●	○					●
2.5 Speicherung der Stimme		●	●					●
3. Ermittlung des Wahlergebnisses								
3.1 Abschluss der Wahlhandlung			●				●	●
3.2 Feststellung des Ergebnisses		●	●				●	●
4. Nachbereitung / Aufbewahrung								
4.1 Deinstallation		●						○
4.2 (Langzeit-)Archivierung		●					○	○
4.3 Aufbewahrung / Wartung des Wahlsystems								
5. Übergreifende Funktionen								
5.1 Allgemeine Software- und Hardware-Anforderungen		●	○	○	○			○
5.2 Kommunikation		●	●					●
5.3 Anonymisierung		●			○			●
5.4 Technische Beobachtung								●

Tabelle 2: Zusammenhang zwischen rechtlichen Aspekten und Funktionsgruppen

Anhang C

Glossar

Verwendete Begriffe der IT-Sicherheit

Authentisierung: Echtheitsprüfung, Verifizierung, Nachweis (Prüfung und Bestätigung) einer angegebenen, behaupteten Identität eines Kommunikationspartners (Subjekt oder Objekt) oder einer Gruppenzugehörigkeit und Sicherstellung, dass diese Identität über die Dauer einer Kommunikationsbeziehung erhalten bleibt mit dem Ziel, Daten (und Programme) einem Urheber (Sender) verbindlich zuordnen zu können (Schutz vor Täuschung).
Die ursprünglich in Nuancen verschiedenen Begriffe "Authentifizierung" (eigentlich: Bezeugen der Echtheit) und "Authentisierung" (eigentlich: Beglaubigung, Rechtsgültigmachung) werden heute meist bedeutungsgleich nebeneinander gebraucht. ([POHL])

Authentizität: überprüfbare Echtheit der vorgegebenen Identität eines Nutzers, Prozesses oder Gerätes ([NIST])

Funktionssicherheit: Schutz vor unbeabsichtigten Ereignissen, d.h. die Eigenschaft eines Systems, trotz aufgetretener Systemfehler nicht in unkontrollierbare Systemzustände zu geraten, in denen das System selbst oder seine Umwelt in Gefahr gebracht werden (*FailSafe*), und zugleich noch weitestgehend konform zu seiner Spezifikation zu reagieren *(Fault Tolerance*). (gemäß [BSI], [DIN])

Integrität: Sicherheitsziel des Schutzes vor beabsichtigten oder versehentlichen Versuchen, Daten auf eine nicht autorisierte Weise zu ändern (Datenintegrität) oder die Ausführung einer Systemfunktion auf nicht autorisierte Weise zu beeinträchtigen (Systemintegrität) ([NIST]).

Verfügbarkeit: Eigenschaft eines Systems oder einer Systemresource, auf Nachfrage durch eine autorisierte Instanz entsprechend der Systemspezifikationen zugänglich und verwendbar zu sein. ([CC])

Vertraulichkeit: der Schutz von Informationen vor unsachgemäßer oder unautorisierter Freigabe ([CC])

Zuverlässigkeit: Eigenschaft eines Systems oder einer Systemresource, entsprechend seiner Spezifikation korrekt zu arbeiten. ([BSI])

Verwendete und eingeführte wahlspezifische Begriffe

Anonymisierung: Im Zusammenhang mit Wahlsystemen: Gewährleistung einer Trennung von Stimmeninhalt und Informationen über die Person, die die Stimme abgibt, so dass keine Verbindungen oder Rückschlüsse erkennbar sind oder hergestellt werden können.

Elektronische Wählerliste: Elektronische Realisierung der Wählerliste, die während des Wahlvorganges z.B. für die Feststellung der Wahlberechtigung, für das Eintragen von Stimmabgabevermerken, für das Hinzufügen von Wahlberechtigten verwendet wird.

Endgültige Stimmabgabe: Unumkehrbare Übergabe der Wahlentscheidung an das System. (Sie entspricht bei herkömmlichen Wahlen dem Einwurf des Stimmzettels in die Wahlurne.)

Kritikalität (hohe): Bedeutung einer Anforderung, die dann vorliegt, wenn ihre Realisierung wichtig für die Umsetzung der allgemeinen wahlrechtlichen Grundsätze ist und ihre Erfüllung nicht ohne technische Spezialkenntnisse oder -verfahren festgestellt werden kann.

Stimmabgabe: Prozess der Wahlhandlung des Wählers (vom Erhalt des Stimmzettels bis einschließlich der *endgültigen Stimmabgabe*)

Stimmdatensatz: Für den Transport aufbereitete Form einer oder mehrerer Stimmen

Stimmenspeicher: Speicherungssystem, in dem die abgegebenen Stimmen für die Auszählung aufbewahrt werden (entspricht bei herkömmlicher Wahl der Wahlurne)

Technisches Wahlpersonal: Servicepersonal mit (informations-)technischen Spezialkennt-nissen, das zur Sicherung des technischen Betriebs des Online-Wahlsystems erforderlich ist.

Wähleridentifikation: Verfahren zur Feststellung der Identität und der Wahlberechtigung einer Person

Wählerauthentifizierung: Verfahren zur Verifizierung der vorgegebenen Identität eines Wählers

Wählerlistenmanagement: Handlungen im Zusammenhang mit Zugriffen auf die *elektronische Wählerliste*

Wahlterminal: Gerät oder Komponente eines Gerätes zur Darstellung des Stimmzettels und
zur *Stimmabgabe*

Zwischenspeicherung: Zwischenzeitliche elektronische Speicherung von Stimmen bzw. *Stimmdatensätzen* nach der *endgültigen Stimmabgabe* und vor der Speicherung der Stimmen in den *Stimmenspeicher*.

Anhang D

Literaturverzeichnis

[BSI] Bundesamt für Sicherheit in der Informationstechnik: Integrierte Gebäudesysteme - Technologien, Sicherheit und Märkte, SecuMedia Verlags–GmbH, 2002

[CC] Common Criteria (ISO 15408) / IT-Sicherheits Datenbanken, http://bibliothek.commoncriteria.de

[CYBERVOTE] CyberVote, an innovative cyber voting system for Internet terminals and mobile phones, IST-1999-20338, www.eucybervote.org/reports.html

[DIN] DIN EN 61508-4: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme, Teil 4: Begriffe und Abkürzungen

[NIST] Gary Stoneburner: Underlying Technical Models for Information Technology Security, Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-33, 2001

[NVSS] Network Voting System Standards (Public draft 2 – 12.04.2002), www.fec.gov/pages/vss/comments/NetworkVotingSystemStandards.pdf

[POHL] Pohl, Hartmut, Prof. Dr., ISIS - InStitut für InformationsSicherheit, Köln, Fachbereich Angewandte Informatik - Kommunikationstechnik, FH Rhein-Sieg, St. Augustin, http://www.kes.info/lexikon/lexdata/authentifizierung.htm

[RICHTLINIE] Richtlinie für die Bauart von Wahlgeräten, Anhang zu: Verordnung zur Änderung der Bundeswahlgeräteverordnung und der Europawahlordnung, Vom 20. April 1999, Bundesgesetzblatt Jahrgang 1999 Teil I Nr. 20, ausgegeben zu Bonn am 23. April 1999, S. 753 ff.

[VPR] Verordnung über die politischen Rechte vom 24. Mai 1978 (Stand am 28.Januar 2003), 161.11, http://www.admin.ch/ch/d/sr/161_11/

[VSS] Voting System Standards, www.fec.gov/pages/vss/vss.html

Requirements of Online Voting Systems for Non-parliamentary Elections

Preliminary notes

Purpose of the Catalogue

This catalogue of requirements provides criteria for the implementation of basic legal electoral rules which are to be met by online voting systems. Its purpose is to define a standard which may serve as an orientation for both, developers and examiners of online voting systems. This document is a recommendation, but not of a mandatory regulating character.

Furthermore, the catalogue has been made publicly available in order to contribute to the ongoing discussions on online voting systems.

This catalogue does not prescribe any method to be used for meeting the requirements. It is not even prescribed whether particular requirements are to be met by technical measures or by non-technical operational measures. The way of how the requirements may be validated is also not within the aim of this catalogue.

Status of the Catalogue

The catalogue of requirements was drawn up by PTB. It was discussed in several versions in the working groups "Examination and Certification" and "Legal Framework Conditions", established by the Federal German Ministry of Economics and Labour for the discussion of special online voting issues. In the version now available, all comments received so far from the members of the working groups have been considered.

Since practical experience is hardly available so far, the catalogue represents the current opinion of the contributing persons. Future technical developments and new experience gathered in general as well as from particular threats may lead to amendments or extensions of this catalogue.

Scope and restrictions

The scope of application that were in mind when developing the requirements is given by legally prescribed, non-parliamentary elections such as, e.g., shop committee, staff council and shareholder elections. The requirements are also applicable to any other non-parliamentary type of election not regulated by law, but one or the other requirement may be weakened. As to the application in parliamentary elections, most of the catalogue is also valid. Particular analysis, however, is still necessary to decide on potential extensions of the requirements.

For the definition of the requirements, it has been assumed that elections take place exclusively at networked polling stations. Applications allowing voting from home or any other private place are explicitly not included in the definition.

Methodological approach

The entire voting procedure including preparation and wrap-up as well as cross-sectional aspects has been divided into functional units, which are defined independently of any system concepts. They are oriented to an abstract voting functionality. Accordingly, the level of detail is low. The applied modular principle is conform with the prevailing understanding of the functional components of online voting systems. Most of the predetermined functional units can be assigned exactly to one phase of the voting process, and some are of a cross-sectional nature. It is not compelling for all functional units here defined to be implemented in any particular online voting system.

Then requirements have been defined with respect to functional units. Further classification of the requirements (e.g., with respect to IT quality criteria as functional requirements, security requirements, ergonomic requirements) was under discussion but has not been realised so far as on the one hand, it is not necessary for the intended purpose of this catalogue, and, on the other hand, it would not in any case be unambiguous, so that this catalogue might become fraught with problems which are not of relevance here. Moreover, the more the description of requirements is interfused by IT terminology the more difficult is an interdisciplinary discussion. In most cases, the nature of the requirements with respect to IT quality criteria can be easily recognised from their wording.

The requirements of this catalogue are more detailed than basic legal rules are. However, they are of a sufficiently general nature to be described independently of particular system configurations. The catalogue does not use configuration examples in order not to indirectly favour any such configuration. Necessary reductions with regard to specific voting system models, system configurations or kinds of election are not the subject of this catalogue. They are to be derived at a later time as a run-up to examinations.

The level of detail used in the definition of the requirements is different. Basically, it has been tried as specific as possible. However, there are aspects, which cannot be confined in requirements due to an unclear legal background or many possible, different technical solutions. It has turned out, indeed, that the legal background of several aspects of online voting systems is currently not yet or only roughly definable. This concerns issues such as the role of technical staff, the definition of a so-called intermediate storage of votes, the verifiability of elections, etc. As regards the variety of different technical solutions, the anonymisation of votes is such an example. The methods known and probably applicable are so different that the corresponding requirement could only be developed on a relative generic level.

The attribute “highly critical” has been introduced for certain requirements. In the context of this catalogue, high criticality means that the particular requirement is

important for the implementation of the general principles of electoral laws, and that its conformance cannot be evaluated without specific technical know-how and/or methods, i.e., in general, functional failures, security gaps, etc. are not or not surely evident during the application due to the electronic and/or software nature of the components. The correctness, reliability and the protection of the functional components from manipulations cannot be assured any longer by a societal supervision or organisational measures. Technical securing and testing are necessary to replace conventional measures.

Requirements of high criticality are indicated. Requirements which are not referred to as highly critical, are not unimportant but their implementation can be adequately checked during the execution of elections by the electoral committee or the voters.

The relation between the individual functions on the one hand and the election-typical roles and objects on the other is tabulated in Annex A. This table is of an informative character. Moreover, a table in Annex B shows the relation between the functions and the fundamental legal requirements and is also of an informative character. It explains in a rough overview why certain requirements were laid down. Annex C contains the terminology used.

Sources

Before this catalogue has been drawn up, an analysis of available material that deals at least partly with requirements for online voting systems was carried out. The following available sources have been analysed: [CYBERVOTE], [NVSS], [RICHTLINIE], [VPR], [VSS]. The existing catalogue has been designed freely and developed further in discussions so that an indication of sources for its individual requirements is not possible anymore.

Catalogue of Requirements

The catalogue of requirements has been arranged according to the election phases. Functions and/or requirements, which cannot be assigned to a particular phase, have been classified as “cross-sectional". In the following, the assignment of functions to election phases is shown. The abbreviations used are employed throughout this catalogue.

PE: Preparation of election
- **(PE1)** Preparation of register of voters
- **(PE2)** Provision of means for voter identification and authentication
- **(PE3)** Preparation of ballot
- **(PE4)** Installation of voting system up to and including readiness for service

VP: Voting phase
- **(VP1)** Voter identification and authentication
- **(VP2)** Management of the register of voters
- **(VP3)** Ballot handling
- **(VP4)** Vote transmission
- **(VP5)** Vote storage

DR: Determination of election result
- **(DR1)** Termination of vote casting
- **(DR2)** Vote counting

WS: Wrap-up and safe-keeping
- **(WS1)** Dismantling and disassembly of voting system
- **(WS2)** (Long-term) archiving
- **(WS3)** Safe-keeping and maintenance of voting system

Furthermore, requirements for the following cross-sectional aspects are considered:

CF: Cross-sectional functions
- **(CF1)** General reliability of software and hardware,
- **(CF2)** Communication system underlying the voting system,
- **(CF3)** Anonymisation of votes,
- **(CF4)** Technical observation of voting system (technical audit).

Requirements for the protection of human-related data basically have also a cross-sectional character and have to be considered in the design of voting systems. It is, however, assumed that the existing regulations cover this aspect to an appropriate extent so that no further requirements need to be defined here.

Furthermore, ergonomic requirements basically are also of a cross-sectional nature. They have, however, been developed in connection with the individual functions in order to better individualise the particular features.

1 Preparation of Election - PE

In the preparatory phase of the election, the following functions are of relevance:

PE: Preparation of election
- **(PE1)** Preparation of register of voters
- **(PE2)** Provision of means for voter identification and authentication
- **(PE3)** Preparation of ballot
- **(PE4)** Installation of voting system up to and including readiness for service

This phase ends with the opening of vote casting.

1.1 Preparation of register of voters (PE1)

For the preparation of the register of voters (i.e. for the ascertainment of the persons eligible to vote), it is not conceivable so far to use components of an online voting system. This is why requirements for this function have not been specified.

When preparing the management of the register of voters, the following requirements are to be met:

(PE1-1) The electronic register of voters shall correctly reflect the register of voters valid.

(PE1-2) The electronic register of voters shall be easily manageable.

1.2 Provision of means for voter identification and authentication (EP2)

This function covers the preparation and distribution of the necessary voter identification means. It shall be guaranteed that each person eligible to vote holds the necessary means of identification that allows him/her to participate in the election. The following requirements are applicable:

(PE2-1) To <u>each</u> voter, the voter identification means shall be available at the time of vote casting at the latest.

(PE2-2) The functional safety of the technical voter identification shall be ensured.

(PE2-3) Alternatives to the electronic voter identification shall be held ready, where appropriate. The alternatives shall also meet the definded requirements.

(PE2-4) The necessary connections and interfaces shall have been harmonised (hardware and software compatibility).

(PE2-5) The voter identification means shall be sent or handed over authentically and must not be altered during this process. In addition, if the voter identification means are secret, privacy shall be protected.

(PE2-6) The voter shall be clearly and comprehensively informed about handling the voter identification means and the significance of secrecy.

The requirements (PE2-4) and - in the case of electronic transmission of the voter identification means - also (PE2-5) are of high criticality.

1.3 Preparation of ballot (PE3)

The procedures of candidate nomination and the preparation of the ballots are assumed to have been terminated before the voting system is used. So they are not dealt with here.
As to the transmission of ballots designed in particular for the preparation of the ballot presentation and for incorporation into control and casting functions of the voting systems, the following requirement is applicable:

(PE3-1) The voting system shall have documented interfaces and supporting means to assist the input of the ballot data. The execution shall be easily manageable.

1.4 Installation of voting system up to and including readiness for service (PE4)

This important complex of functions relates to the direct preparation of vote casting. It shall be ensured that

- the voting systems are installed,
- the readiness for service of the complete system is guaranteed,
- the necessary system documentation is available,
- the operating instructions are available or suitable educational measures have been carried out, in particular for the operations to be carried out by voters, by election officials and by the technical service.

The following requirements result:

(PE4-1) A comprehensive system documentation shall be available, which, in particular, should contain
- the description of the architecture of the system (system model),
- the description of the hardware and software components integrated,
- the description of the methods used for the realisation of the system functionality,
- the description of the environmental conditions.

(PE4-2) Guides for the voters, for the election officials and for the technical service shall be available and appropriate for the subgroup of persons concerned.
Texts shall be replaceable or supplementable by foreign language texts without any changes of other technical characteristics.

(PE4-3) The access control for all computers, having a function in the election context shall be clearly regulated, and each access shall be logged for the purpose of security verification.

(PE4-4) The fields of duty (privileges) of the technical service and the necessary qualification shall be well defined.

(PE4-5) The complete voting system shall be available in due time at the place where the votes are cast or at any other location.

(PE4-6) All necessary accesses to the communication system used for the election process shall be available.

(PE4-7) Appropriate precautions for the unobserved marking of ballots shall be taken at the polling station.

(PE4-8) All components shall be tested for reliability and interoperability.

(PE4-9) An end-to-end function test shall be carried out, and the results shall be recorded.

(PE4-10) All the components of the voting system, in particular the vote storage, shall be set to a defined initial state. The function to set the initial state shall no longer be usable after the voting phase has started.

(PE4-11) In case of component failure, technical or organisational alternatives which are subject to the same requirements shall be available.

(PE4-12) Strategies and software and/or hardware shall be available for the collection and counting of votes.

The requirements (PE4-8) through (PE4-12) are highly critical.

2 Voting Phase - VP

The voting phase includes the following functions:

(VP1) Voter identification and authentication,
(VP2) Management of the register of voters,
(VP3) Ballot handling,
(VP4) Vote transmission,

(VP5) Vote storage.

2.1 Voter identification and authentication (VP1)

The requirements for voter identification and authentication depend to a great extent on the methods and means used. They are to be specified accordingly.

Voter identification and authentication is the beginning of the voting phase. Each person must prove his/her eligibility to vote.

The basic requirements are:

(VP1-1) The identification and authentication of the voter and of his/her eligibility to vote shall be unambiguous and reliable.

(VP1-2) Connections between the voter identity and vote must not be recognisable.

Requirements for the voter identity check:

(VP1-3) The handling of the voter identity check shall be comprehensible and easily manageable.

(VP1-4) In case of loss of the voter identification means, alternative identification methods shall be available. The alternative methods shall comply with the same requirements.

For the check of the eligibility to vote, the following requirements apply:

(VP1-5) An interruption of the connection between voter identification system and electronic register of voters must not affect the function of identification and authentication.

Blocking and deblocking of vote casting require:

(VP1-6) A switch or any other component that (automatically or manually) blocks and deblocks vote casting shall be available. Deblocking shall be allowed only after successful identification and authentication of a voter, and shall end with the completion of vote casting at the latest. At any other time, vote casting shall be blocked.

(VP1-7) If blocking and deblocking are carried out (partially) manually, this shall be easily manageable, and the election officials shall be informed of the blocking state at any time.

Except for (VP1-3), all requirements are highly critical.

2.2 Management of the register of voters (VP2)

The management of the register of voters consists of the administration of this electronic register during the election. It also covers the handling of special cases of voter identification and the generation of vote casting marks. This function is closely related to the voter identification and authentication.

The following requirements have to be met for the management of the electronic register of voters:

(VP2-1) The electronic register of voters shall permit vote casting marks to be set. These vote casting marks shall be protected against loss.[9]

(VP2-2) Eligible short-term changes of the electronic register of voters (corrections and/or amendments) by authorised persons shall be allowed and easily manageable.

(VP2-3) The electronic register of voters including the vote casting marks shall be protected against unauthorized modification .

(VP2-4) Any change of the electronic register of voters shall be logged.

(VP2-5) The electronic register of voters shall be separated from vote storage.

All requirements are highly critical.

2.3 Ballot handling (VP3)

The handling of the ballot is an essential part of the voting phase. In detail, the following actions are implicated:

- loading (provision of the appropriate ballot),
- presentation of ballot,
- ballot marking,
- completion of vote casting as well as
- its confirmation and feedback to the voter.

The requirements for ballot loading are:

(VP3-1) The provision of the appropriate ballot for the election in question and – if required – for the group of voters concerned shall be ensured (authenticity of ballot).

(VP3-2) The provision of the unaltered ballot shall be ensured (integrity of ballot).

[9] A redundant storage is a suitable measure.

Formatiert: Englisch (Großbritannien)

Formatiert: Englisch (Großbritannien)

Formatiert: Englisch (Großbritannien)

Formatiert: Englisch (Großbritannien)

Formatiert: Englisch (Großbritannien)

Formatiert: Englisch (Großbritannien)

(VP3-3) The election officials shall be able to check the authenticity and integrity of the ballot.

The requirements (VP3-1) and (VP3-2) are of high criticality.

The presentation of the ballot shall meet the following requirements:

(VP3-4) The presentation of the ballot shall be uniform and well readable on all voting terminals. It shall contain all necessary information, and only this.[10]

(VP3-5) All candidates on the ballot shall be completely and equally presented to the voter. This must be observed in particular if the size of the ballot exceeds the size of the screen. Discriminations of candidates shall be avoided by appropriate measures.[11]

(VP3-6) The operations to be carried out by the voter at the voting terminal during the presentation of the ballot shall be comprehensible and easily manageable.

The following requirements for ballot marking shall be valid:

(VP3-7) During ballot marking confidentiality shall be guaranteed.

(VP3-8) Vote casting shall be protected against manipulation.

(VP3-9) Maloperations shall not influence the vote to be cast.

(VP3-10) Maloperations shall be correctable following unambiguous guidance. It shall in particular be possible to abort the process and to start anew.

(VP3-11) It shall be possible to cast an invalid vote.

(VP3-12) Navigation during vote casting shall be comprehensible and easily manageable.

The requirements (VP3-7) to (VP3-9) are of high criticality.

For the completion of vote casting, the following requirements are necessary:

(VP3-13) The completion of vote casting shall be possible only once for each voter and shall only be allowed at voting terminals that are deblocked.

(VP3-14) The completion of vote casting shall be explicitly confirmed by the voter.

[10] As to the present opinion, the representation of the ballot should be identical to the usual presentation on paper wherever possible.

[11] Automatic scrolling through the entire ballot, automatic overview of all candidates at the first display of the ballot, or comparable measures are appropriate as regards the present opinion.

(VP3-15) In connection with the completion of vote casting, particulars of the voter's identity must not be used.

(VP3-16) After completion of vote casting, all visible and internal information about the vote cast shall be immediately removed from the voting terminal.

(VP3-17) After completion of vote casting, the voting terminal shall be immediately and automatically blocked.

Except for (VP3-14), these requirements are of high criticality.

For the confirmation of the completion of vote casting, the following are required:

(VP3-18) The completion of vote casting and successful reception by the voting system shall be transparently displayed to the voter.

(VP3-19) The confirmation shall be given immediately.

2.4 Vote transmission (VP4)

The completion of vote casting is at the same time the initial step of vote transmission from the voting terminal to the vote storage. Vote transmission includes:

- the generation of a transportable vote data set,
- saving (intermediate storing) votes or vote data sets, either intended as a buffer in case of communication interruptions or conceptionally planned, e.g., to bundle vote data sets for transmission,
- the actual transmission of vote data sets via the communication system, as well as
- feedback to the voter.

The following requirements apply to the generation of a transportable vote data set:

(VP4-1) The vote data set shall be in the format defined and harmonised.

(VP4-2) The vote data set shall contain exactly the content of the vote(s) cast.

(VP4-3) The vote data set shall be protected from unauthorised access and modification.

Saving (intermediate storing) votes or vote data sets requires:

(VP4-4) The intermediate storage shall be protected from unauthorised access and modification.

(VP4-5) Intermediate storage shall only be for the time period absolutely necessary. After storage, the data shall be finally and irreversibly deleted.

The following requirement applies to the actual transmission of vote data sets:

(VP4-6) Votes cast must not be excluded from transmission, and before starting vote counting, all votes cast shall have been received by the vote storage.

The requirements for the underlying communication system are provided at the cross-sectional functions CF2 (underlying communication system used by voting system).

With regard to the feedback to the voter, in addition to the requirements (VP3-18) and (VP3-19), it is required:

(VP4-7) In case of failed transmission of a vote data set, a handling procedure shall be available to the voter and the election officials.

Except for (VP4-7), the requirements are of high criticality.

2.5 Vote storage (VP5)

The transport is completed by vote storage. Storage in this context means holding the votes ready for counting. Long-term archiving, i.e., storage after the election, is not considered here.

With respect to the reception of the votes by the vote storage, it is to be considered:

(VP5-1) The exact contents of the original vote(s) shall be extracted from the vote data set.

(VP5-2) The vote storage shall be protected from unauthorised access and modification.

(VP5-3) The loss of votes is to be avoided.[12]

(VP5-4) As part of the vote storage process, feedback to the electronic register of voters shall take place.

To hold the votes ready for counting requires:

(VP5-5) Inconsistent states shall be immediately detected. Handling procedures for such cases shall be available.

(VP5-6) Any output of voting results shall not be possible before vote casting is closed.

All requirements are of high criticality.

[12] A redundant storage is a suitable measure.

3 Determination of election result - DR

The determination of the election result is subdivided into:

(DR1) Termination of vote casting
(DR2) Counting of votes

3.1 Termination of vote casting (DR1)

The termination of vote casting has to be accomplished before the votes are counted. The termination includes the blocking of the voting terminal for further voting, the disconnection of further vote-related communication and the blocking of further inputs into the vote storage.

(DR1-1) The regulation of blocking shall be defined unambiguously.

(DR1-2) Before blocking or disconnecting the components, all votes cast shall be transmitted and stored, and the appropriate feedback to the voters and to the electronic register of voters shall have been accomplished. No votes cast shall get lost.

(DR1-3) After the blocking, no further vote casting shall be allowed and no further votes shall be put into the vote storage.

(DR1-4) The proper blocking shall be checked and documented.

(DR1-5) The blocking shall be easily manageable.

The requirements (DR1-2) and (DR1-3) are of high criticality.

3.2 Counting of votes (DR2)

Counting of votes includes:
- counting all valid and invalid votes cast,
- if required, the allotment of seats, representation of minorities, etc.,
- check of the results,
- transmission of results.

The counting of votes requires:

(DR2-1) The determination of results shall start only after the vote storage has been permanently blocked.

(DR2-2) The vote counting shall be correct.

(DR2-3) If further analysis of the results is part of the voting system, the methods used shall meet the applicable rules, and shall be correct.

(DR2-4) Any manual operation shall be easily manageable.

Except for (DR2-4), the requirements are of high criticality.

Requirements of result checking:

(DR2-5) The correctness of vote counting and any further analysis shall be verifiable.

(DR2-6) The inclusion of all individual votes shall be verifiable.

The requirements are of high criticality.

Requirements for the transmission of results:

(DR2-7) So far part of the voting system: The generation of reports and transmission of results shall be protected from manipulations.

4 Wrap-up and safe-keeping - WS

The complex of wrap-up and safe-keeping includes:

(WS1) Dismantling and disassembly of voting system
(WS2) (Long-term) archiving
(WS3) Safe-keeping and maintenance of the voting system

4.1 Dismantling and disassembly of voting system (WS1)

After determining and checking the results and putting them on record, the voting system will be dismantled. This includes shutting down, logging off all system components and removing the components from the polling station.

Requirements:

(WS1-1) Archiving of all data necessary for judicial verification shall be performed before deleting any information.

(WS1-2) The deletion of data shall be finally and irreversibly accomplished.

4.2 (Long-term) archiving (WS2)

(Long-term) archiving is necessary to ensure judicial verification during the next five years, in general.

The requirements concern the regulation of archiving and the breaking-up of the archive.

Requirements for the regulation of archiving:

(WS2-1) Any information shall be redundantly stored.

(WS2-2) Data archived shall be protected from changes.

(WS2-3) Any access to data archived shall be allowed by authorised persons only by a prescribed procedure and put on record.

(WS2-4) All software and hardware necessary for judicial verification shall be archived.

(WS2-5) Inconsistencies arising during archiving shall be detected.

(WS2-6) The regulation of archiving shall be documented.

The requirements (WS2-1), (WS2-2) and (WS2-5) are of high criticality.

The breaking-up of archives is hardly of importance for the execution and validity of an election, therefore no further requirements are defined.

4.3 Safe-keeping and maintenance of voting system (WS3)

Requirements for safe-keeping and maintenance of the voting system are necessary because requirements for the installation of the voting system have been defined, which are independent of the use or storage of the system components in the meantime.
If the requirements for installation are weakened, appropriate requirements are to be laid down.

5 Cross-sectional functions - CF

There are functions of online voting systems and requirements for functions which cannot be assigned to just one election phase. These are:

(CF1) the general reliability of software and hardware,
(CF2) the underlying communication system,
(CF3) the anonymisation of the votes and
(CF4) the technical observation of the voting system (technical audit).

5.1 General reliability of software and hardware (CF1)

To guarantee reliability, general software and hardware requirements are to be laid down. They relate to fundamental software qualities, such as the compliance with the

current state of technology. The hardware requirements aim first of all at the general protection from external and environmental influences. In addition, requirements are necessary for interruptions of vote casting due to force majeure.

(CF1-1) The manufacturer shall give proof of the quality of the development processes in accordance with relevant standards.

(CF1-2) The voting system shall work isolated from all external applications. Casting shall not be affected by any other hardware or software component.

Furthermore, the software shall comply with the following basic requirements:

(CF1-3) The software shall adequately implement all functions necessary for fulfilling the given task, and reliably execute it.

(CF1-4) The software shall have been developed taking the recognised rules of software engineering into account. In particular, it shall be well structured and commented to make inspection feasible.

(CF1-5) Every program shall be unambiguously identifiable.

(CF1-6) The software documentation shall be exhaustive, consistent, unambiguous and appropriate as well as comprehensible and concise.

Hardware requirements:

(CF1-7) The hardware shall show adequate shock resistance and be adequately resistant to temperature variations, humidity and electromagnetic influences.

(CF1-8) The components used shall have an adequate lifetime. Faulty components shall be replaceable by parts of identical or compatible construction.

Requirements in connection with the safeguarding during interruptions of vote casting, whether intended or not intended:

(CF1-9) Votes cast shall not get lost or altered, and must not lose their anonymity during an interruption.

(CF1-10) The electronic register of voters must not be changed during an interruption.

(CF1-11) All election-relevant information shall be secured or reproducible when vote casting is resumed.

(CF1-12) During an interruption election-relevant activities must not be possible at the voting terminal.

(CF1-13) The system shall be set back to a state from which vote casting can be resumed.

These requirements are of high criticality.

5.2 Underlying communication system used by voting system (CF2)

The underlying communication system used by the voting system shall satisfy a certain minimum standard. In addition, there are requirements for the voting system concerning the communication.

General requirement for the communication system:

(CF2-1) High availability of the communication system shall have been confirmed by a practice comparable to online voting.

Specific requirements of the voting system as regards communication:

(CF2-2) The system components of the voting system shall give proof of the genuineness (data integrity) and the unquestionable determination of transmitters and receivers (data authenticity) in accordance with the technical standards applicable.

(CF2-3) In the case of communication interruption, the voting system shall be set to a state from which the communication can be resumed.

(CF2-4) In the case of an interruption of communication embarrassing the election, alternatives shall be available so that the election can continue.

(CF2-5) All communication interruptions shall be logged in such a way that risks such as
- loss or modification of votes,
- modification of entries in the register of voters or
- loss of anonymity

are assessable.
Information about voters and votes are to be strictly excluded from the logging.

(CF2-6) For the devices used for communication security concepts complying with the state of the art in relation to the threat potential accepted shall be realised.

The election-specific requirements are of high criticality.

5.3 Anonymisation of votes(CF3)

Different methods for anonymisation are known. The specific requirements essentially depend on these methods. Due to this dependence, only fundamental requirements for the protection of anonymity can be given here:

(CF3-1) The concept used including the mathematical methods shall demonstrably ensure the required anonymisation (i.e., in accordance with expert judgements on the basis of the state of the art or the relevant literature).The methods used shall in particular be robust and stable for the period of secrecy prescribed.

(CF3-2) The concept used including the mathematical methods shall be appropriate for the particular election.

(CF3-3) The entire development of the software from the design up to the implementation and maintenance shall be disclosed.

(CF3-4) The implementation shall be proved to be correct with respect to the theoretical concept by software test methods (including code inspections) which represent the state of the art.

(CF3-5) The methods used shall be efficient.

If keys are used in the context of the anonymisation, the following requirement applies to key management:

(CF3-6) A appropriate strategy for key management shall be availabe.

The requirements (CF3-1) through (CF3-4) and (CF3-6) are of high criticality.

5.4 Technical observation (CF4)

The technical observation of the components of the voting system (technical audit) is necessary for the judicial verifiability of elections. Technical observation is understood as logging of system states and, in particular, of break-downs, interruptions and system failures. Information about voters and votes are to be explicitly excluded from logging.

Requirements:

(CF4-1) The technical state of the system shall be continuously logged.

(CF4-2) Information about voters and votes must not be logged.

(CF4-3) Planned or unintended interruptions, break-downs and other abnormal states shall be logged in such a way that risks such as
- loss or modification of votes,

- modification of entries in the register of voters or
- loss of anonymity

are assessable.

(CF4-4) It must not be possible to turn off the logging function or to access or modify logging data unauthorised.

The requirement (CF4-4) is of high criticality.

Annex A

Relation between functions and election-specific roles or objects

The relations existing between the election-specific roles and objects on the one hand and the functional units arranged by electoral phases on the other, are given in table 1. High criticality is marked with a black dot (●).

Election-specific roles are held by persons or, in the abstract, by offices. There are

- voters,
- election officials (including the offices preparing the election, and persons with supporting functions) and
- technical service personnel with special knowledge.

Election-typical objects are

- the electronic register of voters,
- the voter identification means (e.g., smart card, PIN, TAN),
- the (unfilled) ballot;
- the vote (cast),
- the vote data set as an object for transmission,
- the vote storage (ballot box) and
- the election result.

The roles and objects are considered in the election phases "Preparation of election", "Voting phase", "Determination of election result", and "Wrap-up and safe-keeping".

From the perspective of the roles, it is, for example, apparent that the election officials are concerned with the requirements for almost all functions. The functions critical for the voter are those of the voting phase in particular. However, the table also shows that besides a certain concentration, a rather wide distribution of the relations exists.

Role / Object Functional Unit	Voters	Election Officials	Technical Service	Register of Voters	Voter Identification Means	Ballots	Votes (Cast)	Vote Data Sets	Vote Storage	Election Results
1. Preparation of election										
1.1 Preparation of register of voters	○	○		○						
1.2 Provision of means for voter identification and authentication	○	●	○	○	●					
1.3 Preparation of ballot		○				○				
1.4 Installation of voting system		●	●			○			●	
2. Voting phase										
2.1 Voter identification and authentication	●	●		●	●					
2.2 Management of register of voters		●		●						
2.3 Ballot handling	●	○				●	●			
2.4 Vote transmission	○	○	●				●	●		
2.5 Vote storage			○	●			●	●	●	
3. Determination of election result										
3.1 Termination of vote casting		○					●		●	
3.2 Vote counting		○					●		●	●
4. Wrap-up and safe-keeping										
4.1 Dismantling and disassembly		○	○							
4.2 (Long-term) archiving		○	○	●		●	●		○	●
4.3 Safe-keeping and maintenance of voting system		○	○							

Table 1: Relation between roles or objects and functional units

Annex B

Relation between functions and legal aspects

Online voting systems must comply with the general fundamental principles such as

- secrecy
- equality
- generality,
- direct voting and
- free voting.

In addition, the judicial verifiability is to be guaranteed. In this context, two aspects are important:

- verifiability of the election result,
- verifiability of the proper election process.

The relations between the legal aspects on the one hand and the functional units arranged by electoral phases on the other, are given in table 2. High criticality is marked with a black dot (●).

The table allows the functions to be classified according to their legal importance.

Legal Aspects / Functional Unit	***General Electoral Principles***	Secrecy of Election	Equality and Generality of Election	Directness of Election	Freedom of Election	***Judicial Verifiability***	Verifiability of Election Result	Verifiability of Election Process
1. Preparation of Election								
1.1 Preparation of register of voters								○
1.2 Provision of means for voter identification and authentication		○	●	○				○
1.3 Preparation of ballot								
1.4 Installation of voting system		●	○				○	●
2. Voting phase								
2.1 Voter identification and authentication		●	●					○
2.2 Management of register of voters			●				○	○
2.3 Ballot handling		●	●	●	●			○
2.4 Vote transmission		●	○					●
2.5 Vote storage		●	●					●
3. Determination of election result								
3.1 Termination of vote casting			●				●	●
3.2 Vote counting		●	●				●	●
4. Wrap-up and safe-keeping								
4.1 Dismantling and disassembly		●						○
4.2 (Long-term) archiving		●					○	○
4.3 Safe-keeping and maintenance of voting system								
5. Cross-sectional functions								
5.1 General reliability of software and hardware		●	○	○	○			○
5.2 Communication system		●	●					●
5.3 Anonymisation		●			○			●
5.4 Technical observation								●

Table 2: Relation between legal aspects and functional units

Appendix C

Glossary

Terms used from the field of IT security

Authentication: Verifying the alleged identity of a user, process, or device ([NIST])

Availability: A requirement to assure that systems work promptly and service is not denied to authorised users ([NIST])

Confidentiality: Prevention of unauthorised disclosure of information ([CC])

Functional safety: Protection from unintentional events, i.e. the characteristic of a system not to get into uncontrollable states in which the system itself or its environment is endangered despite system failures that might occur (*fail safe*), and to simultaneously behave as far as possible in conformity with its specification (*fault tolerance*) (in accordance with [BSI], [DIN])

Integrity: Security objective that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has not been altered in an unauthorised manner) or system integrity (the quality a system has when performing its intended function in an unimpaired manner and free from unauthorised manipulation) ([NIST]).

Reliability: Characteristic of a system or a system resource to correctly work according to its specification ([BSI])

Election-specific terms used from the field of voting or newly introduced

Anonymisation: In connection with voting systems: Separation of the vote from any information about the voter in such a way that no connection exists or might be established.
Criticality (high): (High) Significance of a requirement with respect to its importance for the implementation of fundamental electoral principles in combination with the fact that the fulfilment of the requirement cannot be checked without special technical know-how or procedures.

Completion of vote casting: Irreversible transfer of the voter's decision to the system (corresponds to the insertion of the ballot paper into the ballot box in conventional elections).

Electronic register of voters: Electronic version of the register of voters used during the election process, e.g., for the determination of the person's eligibility to vote, for registering voting marks, for the addition of voters eligible to vote.

Intermediate storage: Intermediate electronic storage of votes or *vote data sets* after *completion of vote casting* but before the votes are stored in the *vote storage.*

Management of the register of voters: Actions in connection with accesses to the *electronic register of voters*

Technical service: Service staff with special (information-) technical know-how, which is necessary for ensuring the technical operation of the online voting system.

Vote casting: Voter's actions from the reception of the ballot up to the *completion of vote casting*

Vote data set: Set of data containing one or more votes that is formatted for transmission.

Vote storage: Storage system, in which the votes cast are kept for vote counting (corresponds to the ballot box in conventional elections).

Voter authentication: Procedure for verifying the identity of a voter.

Voter identification: Procedure for the determination of the identity of a person and his/her eligibility to vote.

Voting terminal: Device or component of a device for the presentation of the ballot and for carrying out *vote casting.*

Appendix D

References

[BSI] Bundesamt für Sicherheit in der Informationstechnik: Integrierte Gebäudesysteme - Technologien, Sicherheit und Märkte, SecuMedia Verlags–GmbH, 2002

[CC] The Common Criteria Evaluation and Validation Scheme, Acronymns and Terms, http://niap.nist.gov/cc-scheme/terms.html#A

[CYBERVOTE] CyberVote, an innovative cyber voting system for Internet terminals and mobile phones, IST-1999-20338, www.eucybervote.org/reports.html

[DIN] DIN EN 61508-4: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektroni-scher/programmierbarer elektronischer Systeme, part 4: Begriffe und Abkürzungen

[NIST] Gary Stoneburner: Underlying Technical Models for Information Technology Security, Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-33, 2001

[NVSS] Network Voting System Standards (Public draft 2 – 12.04.2002), www.fec.gov/pages/vss/comments/NetworkVotingSystemStandards.pdf

[RICHTLINIE] Richtlinie für die Bauart von Wahlgeräten, Anhang zu: Verordnung zur Änderung der Bundeswahlgeräteverordnung und der Europawahlordnung, Vom 20. April 1999, Bundesgesetzblatt Jahrgang 1999 Teil I Nr. 20, ausgegeben zu Bonn am 23. April 1999, S. 753 ff.

[VPR] Verordnung über die politischen Rechte vom 24. Mai 1978 (Stand am 28.Januar 2003), 161.11, http://www.admin.ch/ch/d/sr/161_11/

[VSS] Voting System Standards, www.fec.gov/pages/vss/vss.html