Bericht betreffend technischer Belange des E-Votings

Unterarbeitsgruppe 2 „Technik“ der Arbeitsgruppe zu E-Voting im Bundesministerium für Inneres

Dieser Bericht behandelt technische Aspekte des E-Voting. Dabei werden vor dem Hintergrund der Europarats-empfehlungen zu E-Voting diese in Relation zu aktuellen Gegebenheiten in Österreich gestellt. Mit Elementen wie Zentrales Melderegister (ZMR), Bürgerkarte oder elektronischer Zustellung ist Österreich in einer günstigen Situation, in der für Teilaspekte einer allfälligen Umsetzung von E-Voting bereits technische Infrastruktur besteht, die eine ökonomisch umsetzbare Basis bilden könnte. Dies wird in diesem Bericht besonders berücksichtigt.

Inhaltsverzeichnis

In die Unterarbeitsgruppe 2 „Technik“ zur Arbeitsgruppe „E-Voting“ im Bundesministerium für Inneres (BM.I) waren registriert:

Dipl.-Ing. Harald Brandstätter (BRZ), Dr. Thomas M. Buchsbaum (BMAA), Dipl.-Ing. Kurt Fleck (BRZ), Mag. Gabriela Forchtner (Österreichischer Städtebund), Dipl.-Ing. Robert Gottwald (BMI), Mag. Cornelius Granig (IBM), Mag. Robert Grim (BRZ), Astrid Grüner (Land Oberösterreich), Dipl.-Ing. Raimund Hartbauer (Comm-Unity), Michael Juren (Land Niederösterreich), Dr. Oswald Kessler (BMI), Hartmut Kosma (BMI), Mag. Robert Krimmer (WU Wien), Dr. Gerhard Kunnert (BKA), Dipl.-Ing. Herbert Leitold (A-SIT), Dr. Gottfried Luef (IBM), Prof. Dr. Erich Neuwirth (Uni Wien), Wolfgang Oberaigner (Magistrat Linz), Dipl.-Ing. Klaus Petermeier (Land Oberösterreich), Carl Markus Piswanger (BRZ) Prof. Dr. Reinhard Posch (CIO Bund), Prof. Dr. Alexander Prosser (WU Wien), Dr. Roland Rödl (Land Steiermark), Dipl.-Ing. Thomas Rössler (TU Graz), Mag. Robert Stein (BMI), Mario Taschner (BMI), Mag. Gregor Wenda (BMI), Dipl.-Ing. Johann Zeiner (Magistrat Wien)

Dieser Bericht wurde von Dipl.-Ing. Herbert Leitold (A-SIT) als Moderator der Unterarbeitsgruppe ausgefertigt.

Graz, 3. November 2004

Executive Summary

Der Bericht betrachtet E-Voting aus einem technischen Blickwinkel. Dabei werden aufbauend auf den Ansätzen der Europaratsempfehlungen zu E-Voting verschiedene Szenarien des E-Voting diskutiert und die technischen oder ökonomischen Konsequenzen der einzelnen Ansätze skizziert.

Dabei ist der Bericht technologieneutral und ist nicht als Empfehlung einzelner Ansätze zu verstehen. Dennoch werden sinnvolle konkrete Lösungsansätze in den Bericht aufgenommen. Der Bericht geht von einer breiten Verfügbarkeit der Bürgerkarte als Sicherheitsinfrastruktur in absehbarer Zeit aus. Deshalb geht der Bericht von diesem hohen Sicherheitsstandard aus. Weiters ist der Einsatz bestehender Infrastruktur auch aus Kostengründen nahe liegend. Dies bezieht sich etwa auf die Nutzung des ZMR als Basis einer Zentralen Wählerevidenz und weitere Synergien zur E-Government Strategie.

In allen Varianten stellt sich eine zentrale Wählerevidenz als notwendige Basis des E-Voting dar. Elektronische Wählerverzeichnisse können zentral oder dezentral geführt werden. Dezentrale Wählerverzeichnisse müssen für alle Berechtigten zugänglich sein. Mit zentraler Wählerevidenz bzw. darauf aufbauenden Wählerverzeichnissen lassen sich auch ohne E-Voting Verbesserungen erzielen, etwa in der elektronischen Umsetzung der Beantragung der Aufnahme in die Wählerevidenz bzw. Europawählerevidenz, und der Einsicht in eigene Daten der Bürgerinnen und Bürger im betreffenden Wählerverzeichnis bzw. in der jeweiligen Wählerevidenz über die Bürgerkarte.

Die gemeinsame technische E-Voting-Infrastruktur (z.B. Wählerevidenz, E-Voting Server, etc.) kann als Dienstleister für Gemeinden, Städte, Länder zur Verfügung stehen.[1]

Wesentliche technische Herausforderungen bei E-Voting sind vor allem die Wahrung des geheimen Wahlrechts und das Verhindern mehrfach abgegebener Stimmen, vor allem über die verschiedenen Medien “elektronisch“ und „Papier-Stimmzettel“.

Zur Verhinderung der mehrfachen Stimmabgabe kristallisieren sich technisch zwei Ansätze als viel versprechend heraus, wobei sie sich in notwendiger Ausstattung der Wahllokale bzw. in Alternativen bei Ausfällen der Komponenten, sowie bezgl. der von Wählerinnen und Wählern bei der Wahl einzusetzenden Komponenten (z.B. PCs, Internetzugang, o.ä.), unterscheiden:

- Zeitliche Trennung von E-Voting und konventioneller Stimmabgabe so weit vor dem Wahltag für konventionelle Stimmabgabe, dass dann die Wählerlisten um Personen bereinigt vorliegen, die elektronisch gewählt haben.
- Abbildung einer elektronischen Briefwahl so, dass Personen, die sich vorab zu E-Voting am Wahltag registriert haben, die Stimme dann auch nur mehr elektronisch abgeben können bzw. eine Papier-Stimme die Nachschau im elektronischen Wählerverzeichnis bedarf. Hier wären zumindest einige Wahllokale mit Online- oder Call Center Zugang zur Zentralen Wählerevidenz auszustatten, um bei Fehlern der technischen Komponenten (PCs, Internetzugang, etc.)

[1] dies schließt nicht aus, dass ggf. eigene Infrastrukturen aufgebaut werden

die Stimme an Komponenten im Wahllokal oder konventionell abgeben zu können.

Alternativen, bei denen am Wahltag sowohl elektronisch, als auch per Papierstimme gewählt werden können, bedingen eine Online-Ausstattung der Wahllokale – im allgemeinen Fall die Online-Ausstattung aller Wahllokale. Alternativen über telefonische Nachfrage in einem Call Center[2] sind dann möglich, wenn die Anzahl dieser Anfragen relativ gering ist (zB Abgabe Papierstimme bei technischen Problemen).

Der Bericht zeigt auch Übergangsszenarien auf, in denen die Stimmabgabe noch nicht elektronisch erfolgt, wie elektronische Wahlkarten als Alternative zu herkömmlichen Papier-Wahlkarten. Durch die Duplizierbarkeit dieser elektronischen Wahlkarten ergeben sich Kosten der technischen Ausstattung der Wahllokale sowie der österreichischen Vertretungsbehörden im Ausland, die den Mehrwert solcher Lösungen als gering erscheinen lassen.

Zur Geheim- und Anonymhaltung der abgegebenen Stimme bestehen verschiedene technische und wissenschaftliche Ansätze, die dies sicherstellen. Es besteht dazu in Österreich mit dem Konzept Bürgerkarte eine Sicherheitsinfrastruktur, die über e-card, Handy-Signatur oder Bankomatkarte absehbar breit ausgerollt sein wird und deshalb sinnvoller Weise einzusetzen sein wird. Darüber hinaus werden keine Präferenzen hinsichtlich einer Lösung zu Geheim-/Anonymhaltung ausgesprochen.

Es wird im Bericht auch klar gestellt, dass die Anforderung des persönlichen Ausübens des Wahlrechts, wie auch der unbeobachteten Stimmabgabe in der elektronisch durchgeführten Distanzwahl ebenso wenig technisch garantiert werden kann, wie etwa bei einer Briefwahl.

Den Wahlkommissionen und etwaigen Beobachtern muss auch analog zum derzeitigen papiergestützten System die Möglichkeit geboten werden, die elektronische Stimmabgabe, Öffnung der elektronischen Stimmen und die Auszählung zu überwachen. Insbesondere dürfen die abgegebenen Stimmzettel erst durch einen gemeinschaftlichen Akt der Wahlkommission zugänglich sein.

Der Bericht zeigt ebenso auf, dass sich mit der Informationstechnologie Möglichkeiten ergeben, die in der konventionellen Stimmabgabe nicht gegeben sind. Hier wird der Grad, in dem das Nutzen derartiger technischer Möglichkeiten keine unverhältnismäßige Ungleichheit der Medien zur Stimmabgabe darstellt, zu diskutieren sein und muss Vorgabe an die technische Ausformung sein. Beispiele, in denen technische Varianten möglich sind, wären das Zulassen einer bewusst ungültig abgegebenen Stimme (Ankreuzen von zwei Parteien) vs. eines technischen Verunmöglichens von oder eines Hinweises auf solche, ggf. versehentlich ausgelöste Situationen. Jedenfalls lässt sich im E-Voting die bewusste Abgabe eines leeren Stimmzettels abbilden.

Es werden jene Teilaspekte aufgezeigt, in denen durch bestehende Infrastruktur eine Basis für einen allfälligen Übergang zu E-Voting besteht. Dies sind etwa Synergien zu E-Government bei der Registrierung zu E-Voting oder das ZMR als Basis einer Zentralen Wählerevidenz. Dem stehen etwa bei der tatsächlichen elektronischen

[2] Die Publizität der Antwort muss gegeben sein; Antwort muss authentisch dem Protokoll beigelegt werden können

Stimmabgabe Bereiche gegenüber, in denen Entwicklungsbedarf oder weit reichende Tests und Pilotversuche notwendig erscheinen.

Unter Nutzung der aus dem E-Government bestehenden Infrastruktur kann in Anlehnung an herkömmliche Wahlkarten bzw. Briefwahlsysteme durch die Synergien folgendes Internet E-Voting Szenario effizient umsetzbar sein:

- Einrichten zentraler Wählerevidenz und zentraler Wählerverzeichnisse
- Wählerin oder Wähler registriert sich mit Bürgerkarte vorab zu E-Voting
    - Dabei wird elektronisches Äquivalent zu Wahlkarte ausgestellt und dies wird im Wählerverzeichnis vermerkt
    - Wählerin oder Wähler kann die Stimme dann nicht mehr ohne weiteres konventionell abgeben (siehe unten)
- Bei der Stimmabgabe erfolgt die Sicherung der abgegebenen Stimme und der Übertragung an zentrale E-Voting Server mit der Bürgerkarte.
    - Es bestehen Varianten in der technischen Ausgestaltung der Stimmabgabe, die hier nicht gelistet werden
    - Sind für E-Voting Wählerinnen und Wähler Stimmabgabe im Wahllokal (zB bei technischen Problemen) bzw. Umsetzung Wahlpflicht vorzusehen, wird elektronische Stimmabgabeberechtigung, bzw. tatsächliche Stimmabgabe, im Wählerverzeichnis vermerkt.
    - Dabei kann Stimmabgabe in Wahllokalen mit Online-Zugang oder alternativem Zugang[3] zum Wählerverzeichnis erfolgen, wobei die Antwort authentisch, allen Berechtigten zugänglich, sowie speicherbar sein muss.
- Auszählung der elektronischen Stimmen erfolgt über hinreichend große Satze an abgegebenen Stimmen

[3] z.B. telefonisch über Call Center

1. Einleitung

Mit der Fertigstellung der Europaratsempfehlungen (ER Empfehlungen) zu rechtlichen. Verfahrens- und technischen Standards zu E-Voting[4] besteht eine Basis, in der bereits technische Anforderungen an E-Voting definiert werden. Die ER Empfehlungen sind in den technischen Teilen insofern allgemein gehalten, als sie auf nationale Gegebenheiten und Infrastruktur nicht eingehen. Hier ist Österreich mit dem Konzept Bürgerkarte, den Modulen für Online-Applikationen (MOA), dem ZMR oder der elektronischen Zustellung weit fortgeschritten. Es werden deshalb in diesem Bericht die ER Empfehlungen in Relation zur Infrastruktur in Österreich gestellt und dargestellt, wie diese bei E-Voting allenfalls eingesetzt werden kann.

Die ER Empfehlungen beschreiben Vorgaben für elektronische Verfahren in der Vorwahlphase, bei der Stimmabgabe und in der Auszählung. E-Voting wird als eine politische Wahl oder Volksabstimmung, in dem zumindest die Stimmabgabe elektronisch erfolgt, definiert. Dieser Bericht geht jedoch auch auf die Situation ein, in der die Stimmabgabe noch nicht elektronisch vorgenommen wird, da auch ohne die elektronische Stimmabgabe kurzfristig Effekte zu erzielen sind. Beispiele wären die elektronische Beantragung der Aufnahme in die Wählerevidenz bzw. Europawählerevidenz, und Beantragung oder elektronische Zustellung einer Wahlkarte, die für Bürgerinnen und Bürger Vereinfachungen in der Abwicklung ergeben können.

Es werden in diesem Bericht nicht alle technischen Anforderungen an ein Wahlsystem diskutiert, da einige Teile in den ER Empfehlungen entsprechend detailliert ausgeführt sind und in Österreich einfach anwendbar sind. Dazu werden in einem Anhang an den Bericht die technischen ER Empfehlungen angeführt und allenfalls kommentiert.

In Folge wird in Abschnitt 2 ein Überblick über bereits bestehende Infrastruktur gegeben. Dies dient als Einführung, um Leserinnen und Lesern, die nicht mit dem aktuellen Stand der aus dem E-Government bestehenden Ansätze vertraut sind, einen ersten Überblick zu geben. In Abschnitt 3 wird konkreter auf den Stand der Technik im E-Voting eingegangen. Es werden dabei die wesentlichsten Herausforderungen aufgezeigt, die in einem Einsatz des E-Voting zu lösen sind. In Abschnitt 4 wird konkreter diskutiert, wie in Österreich bestehende technische Infrastrukturen zur Verwendung im E-Voting anzupassen wären, welcher technische Entwicklungsbedarf allenfalls besteht. Abschließend wird im Anhang für die einzelnen ER Empfehlungen jeweils eine Stellungnahme unter Bezug auf österreichische Infrastruktur oder den Stand der Technik gegeben.

2. Bestehende Infrastruktur

Dieser Abschnitt beschreibt die technische Infrastruktur in Österreich, die bei einer allfälligen Einführung von E-Voting relevant ist. Bei einer allfälligen Entscheidung für E-Voting wäre die tatsächliche breite Verfügbarkeit der in diesem Bericht angeführten Vorraussetzungen zu prüfen.

[4] Vorlage zur Annahme durch das Ministerkomitee voraussichtlich am 30. September 2004

2.1 Zentrales Melderegister – ZMR

Das ZMR besteht seit 2002 und umfasst alle in Österreich gemeldeten Menschen. Es ist eine Evidenz, die etwa bereits Grundlage für Finanzausgleich, Volkszählung, (Europa-)Wählerevidenz oder Bürgerkarte ist. Es umfasst Identitätsdaten (Name, Geschlecht, Geburtsdaten, Staatsangehörigkeit, etc.) sowie die Wohnsitzdaten für Hauptwohnsitz oder weitere Wohnsitze (Strasse/Hausnummer/Stiege/Tür, Postleitzahl, etc.)

Das ZMR bzw. das Ergänzungsregister sind im Zusammenhang mit E-Voting somit die logische Basis für eine zentrale Wählerevidenz und die Wählerverzeichnisse. Wählerverzeichnisse, die für alle Berechtigten zugänglich sind, auf Basis einer Zentralen Wählerevidenz erscheinen sinnvoll.

2.2 Bürgerkarte

Das Konzept der österreichischen Bürgerkarte bildet im Kern eine Kombination aus:

- elektronischer Signatur und
- eindeutiger Identifikation

Einerseits kann die Bürgerin bzw. der Bürger mit Hilfe der Bürgerkarte eine elektronische Signatur leisten. Diese ist im Fall der sicheren Signatur nach Signaturgesetz der handschriftlichen Unterschrift äquivalent. Darüber hinaus enthält die Bürgerkarte in Form der so genannten Personenbindung die Person eindeutig identifizierende Daten – die so genannte Stammzahl, die für in Österreich gemeldete Personen aus dem ZMR abgeleitet ist, sowie Name und Geburtsdatum. Zur Identifikation selbst wird aus Datenschutzgründen eine Ableitung der Stammzahl, das bereichsspezifische Personenkennzeichen (bPK), herangezogen. So kann im elektronischen Verfahren unter Anwendung der Personenbindung eine Person über das bPK eindeutig identifiziert und über die elektronische Signatur authentifiziert werden.

Über diese Basisfunktionalitäten hinaus bietet die Bürgerkarte in Verbindung mit der für den Funktionsumfang maßgeblichen Schnittstellenspezifikation (Security Layer) weitere Funktionen, wie Signaturprüfung oder Ver- und Entschlüsselung von Daten[5]. Weiters sind über so genannte Infoboxen Speichermöglichkeiten gegeben.

Die Bürgerkarte ist technologieneutral definiert, sodass verschiedene Umsetzungen möglich sind. Beispiele sind die SV-Chipkarte e-card, angekündigt ist etwa auch die Bankomatkarte mit Signatur bzw. ist die Chipkarte a-sign premium des Zertifizierungsdiensteanbieters A-TRUST bereits als Bürgerkarte verfügbar. Im Rahmen der Bürgerkartenfunktion sieht das E-Government Gesetz für eine Übergangsfrist bis Ende 2007 auch so genannte Verwaltungssignaturen vor. Damit ist über die A1 Signatur das Handy als Bürgerkarte einsetzbar.

Im E-Voting ist die Bürgerkarte somit zur Identifikation und Authentifizierung von Wählerinnen und Wählern, aber auch für die Verschlüsselung einsetzbar. Die Software zur Bürgerkartenumgebung (Schnittstelle Security Layer) wird seit August 2004 über eine Generallizenz vom Bund kostenlos zur Verfügung gestellt.

[5] Ab Version 1.2 der Spezifikation Security Layer

2.3 Elektronische Zustellung

Die elektronische Zustellung stellt einen weiteren wesentlichen Standardbaustein im österreichischen E-Government dar. Damit können Zustellprozesse an Bürgerinnen und Bürger nach dem Zustellgesetz elektronisch abgewickelt werden. So zugestellte Dokumente sind von der Zustellart auch RSa-Zustellstücken gleichzusetzen. Bei der elektronischen Zustellung identifiziert sich die Empfängerin bzw. der Empfänger und bestätigt den Empfang und die Annahme des Zustellstücks über die Bürgerkarte (bPK und elektronische Signatur).

Die elektronische Zustellung bietet sich demnach für die Kommunikation mit den Wählerinnen und Wählern im Rahmen eines österreichischen E-Voting Systems an, etwa zur Zustellung einer elektronischen Wahlkarte.

2.4 MOA Module

In der Umsetzung von E-Government Anwendungen sind einzelne Verfahrenschritte unabhängig von Verfahren wiederkehrend ähnlich. Dazu zählen Server-seitig etwa die Identifikation über bPK, Erstellung von elektronischen Signaturen bzw. das Anbringen einer Amtssignatur, das Prüfen elektronischer Signaturen oder die Anbindung an elektronische Zustellung.

Es wurden dazu Module für Online Applikationen (MOA) entwickelt, die Organisationseinheiten der öffentlichen Verwaltung als auch der Privatwirtschaft[6] kostenfrei zur Verfügung gestellt werden. Es umfasst dies etwa MOA ID (Identifikation), MOA SS (Erstellung von Serversignaturen) und MOS SP (Signaturprüfung).

Für E-Voting Verfahren bestehen also aus dem E-Government Bausteine, die zu einer raschen und kosteneffizienten Umsetzung in Teilaspekten verwendet werden können.

2.5 Sicherheitsstandards

In der Akzeptanz von E-Voting ist der Nachweis der Einhaltung von Sicherheitsanforderungen ein wesentliches Kriterium. Es besteht eine Reihe von Standards, über die die unabhängige Prüfung der technischen Sicherheit und Zertifizierung von Systemen durchführbar ist.

Seit 1998 werden auf europäischer Ebene „Information Technology Security Evaluation Criteria – ITSEC“ im Rahmen eines Abkommens zur gegenseitigen Anerkennung von Zertifikaten[7] angewandt. Diese werden zunehmend von den „Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik“, ISO 15408 bzw. meist als Common Criteria bezeichnet, abgelöst. Common Criteria ist ebenfalls ein internationales Abkommen zur Anerkennung von Zertifikaten, dem Österreich 2003 als „Certificate Consuming Participant“ beigetreten ist. Beide Standards, ITSEC und Common Criteria, definieren Vertraulichkeitsstufen, über die das zu erreichende Prüf- und damit Sicherheitsniveau von Produkten vorgegeben werden kann.

---

[6] Allenfalls mit Einschränkungen hinsichtlich von den Modulen verwendeten Bibliotheken

[7] SOGIS Abkommen, Österreich hat dieses nicht unterzeichnet, was jedoch nicht gegen eine Anerkennung einer ITSEC Evaluierung spricht. ITSEC wird jedoch zunehmend durch Evaluierungen nach Common Criteria ersetzt

Common Criteria und ITSEC sind vor allem zur Prüfung und Bewertung von technischen Systemen mit klaren, überschaubaren Sicherheitsfunktionen geeignet, wie Chipkarten, Firewalls, Netzwerkkomponenten, Datenbanken oder Betriebssysteme. Für komplexere Systeme wie das Sicherheitsmanagement von Organisationen bestehen andere Standards und Werkzeuge, wie „Informationstechnologie - Leitfaden für das Management der Informationssicherheit“ ÖNORM A 7799, das deutsche IT Grundschutzhandbuch oder das Österreichische IT Sicherheitshandbuch.

Standards wie Common Criteria erlauben die technologieneutrale Definition von Sicherheitsanforderungen über Schutzprofile und die Prüfung von Produkten gegen diese. Dies kann bei E-Voting zur Feststellung der Vertrauenswürdigkeit von Systemen dienen, wie etwa die Schutzprofile für Signaturerstellungseinheiten die Prüfung der Erfüllung technischer Anforderungen aus Signaturgesetz und Signaturverordnung erleichtern.

Ebenso können über anerkannte Standards und Werkzeuge wie ÖNORM A 7799 oder das Österreichische IT Sicherheitshandbuch Vorgaben an Rechenzentren und Dienstleister definiert werden.

3. Stand der Technik und Herausforderungen

In diesem Abschnitt werden Szenarien zu E-Voting am Stand der Technik dargestellt. Es werden verschiedene Möglichkeiten technologieneutral aufgezeigt, ohne einzelne Technologien besonders hervorzuheben. Technische Konsequenzen einzelner Szenarien werden diskutiert.

Generell kann E-Voting in den Einsatz elektronischer Mittel zur Stimmabgabe im Wahllokal (elektronische Wahlmaschinen), Aufstellung von spezifischen Wahlmaschinen an öffentlichen Plätzen (Kiosk-Systeme, am Wahltag typischerweise nicht unter physischer Aufsicht der Wahlbehörde) und die allgemeine Distanzwahl, etwa über das Internet klassifiziert werden. Es wird hier nur letzterer Fall – die allgemeine Distanzwahl über elektronische Mittel – betrachtet.

Der Abschnitt ist dazu in die Phasen „Vorwahlphase“, „Stimmabgabe“ und „Auszählung“ strukturiert. Allgemeine übergreifende Aspekte sind in den Abschnitten „Ausfall technischer Komponenten“ bzw. „Wahlbehörde, Wahlzeugen, Audit“ gegeben.

Nachdem das Wahlgeheimnis und damit das anonym Halten der abgegebenen Stimme einen besonderen Stellenwert einnimmt, wird die Trennung von Stimme und identifizierender Information in den einzelnen Phasen gesondert betrachtet.

3.1 Vorwahlphase

In der Vorwahlphase beschränken sich die Betrachtungen darauf, ob bzw. wie eine Registrierung zur elektronischen Stimmabgabe erfolgen kann. Die in den ER Empfehlungen ebenfalls behandelte nachträgliche Zustimmung der Kandidaten zu ihrer Nominierung ist für Österreich in der Form nicht relevant. Elektronische Nominierung der Kandidaten ohne nachträgliche Zustimmung wäre technisch relativ einfach umzusetzen, bedarf etwa Authentifizierung und Berechtigungsprüfung.

3.1.1 Wählerevidenz, Wählerverzeichnisse

Für ein Umsetzen des E-Voting ist die Einführung einer zentralen elektronischen Wählerevidenz (ZWE) notwendig. Wenngleich es theoretisch denkbar wäre, dezentrale Wählerevidenzen in den Gemeinden zu führen, scheint dies nicht praktikabel: Die dezentralen Systeme müssten in allen Gemeinden installiert oder über Dienstleister zusammengefasst werden und – je nach gewähltem Verfahrens des Zugangs zu E-Voting – am Wahltag hochverfügbar ausgestattet sein. Dies scheint nur an wenigen Stellen (Landeswahlbehörden) oder einer zentralen Stelle (Zentrale Wählerevidenz) effizient umsetzbar.

Technisch handelt es sich bei einer zentralen elektronischen Wählerevidenz um eine Datenbank, die mit Evidenzen mit ähnlichen Volumensanforderungen vergleichbar ist, etwa dem ZMR. Wählerverzeichnisse sind dementsprechend Auszüge aus dieser Datenbank (der Gemeinde, des Wahlsprengels).

Äquivalent lassen sich zentrale Wählerverzeichnisse auf Basis der zentralen Wählerevidenz einrichten. Wählerlisten in den Wahlsprengeln sind dann Auszüge aus diesem zentralen Wählerverzeichnis. Damit lassen sich relativ einfach Dienste, wie das Nachschaurecht im Wählerverzeichnis, elektronisch über die Bürgerkarte abbilden.

Der Übergang zu einer zentralen Wählerevidenz ist technisch etwa vergleichbar mit dem Übergang dezentraler Meldebestände zum ZMR, wobei hier im ZMR die entsprechende technische Infrastruktur bzw. der Datenbestand gemeldeter Personen besteht. Es ergibt sich also die Verwendung bzw. Anpassung bestehender Infrastruktur wie ZMR als sinnvollster Zugang.

3.1.2 Registrierung, Wahlkarte

Generell sind zwei Varianten des Zuganges zu E-Voting diskussionswert: Einerseits kann einer Wählerin oder einem Wähler die elektronische Stimmabgabe nur dann ermöglicht werden, wenn sie bzw. er sich vorab zu E-Voting registriert hat. Die zweite Variante wäre ein offenes System, bei dem die Wählerin oder der Wähler sich am Wahltag[8] spontan zur elektronischen Stimmabgabe entscheiden kann. Die beiden Szenarien unterscheiden sich vor allem in den Methoden, wie eine doppelte Stimmabgabe durch dieselbe Wählerin oder denselben Wähler – sowohl elektronisch und konventionell – zu verhindern sind, bzw. zu welchem Zeitpunkt die Identifikation der Wählerin bzw. des Wählers zu erfolgen hat.

Der Fall vorheriger Registrierung kann mit der Ausstellung einer Wahlkarte verglichen werden, wo dies bereits bisher bei konventionellen Wahlkarten zu einem Vermerk im Wählerverzeichnis führt. Die Anforderungen der Feststellung der Identität ist äquivalent zum E-Government Verfahren mit der Bürgerkarte gestaltbar. Die elektronische Wahlkarte muss authentisch sein, was unter Anwendung kryptographischer Verfahren gewährleistet werden kann[9]. Die Authentizität der elektronischen Wahlkarte muss für die Wählerin bzw. den Wähler einfach feststellbar sein.

Ein Verhindern der doppelten Stimmabgabe lässt sich ähnlich wie bei herkömmlichen Wahlkarten gestalten, bedarf aber besonderer Maßnahmen: Nachdem eine elektronische Wahlkarte nicht detektierbar beliebig duplizierbar ist, ist ein elektronisches

[8] bzw. dem für elektronische Stimmabgabe definierten Zeitraum
[9] Etwa über Amtsignatur wie im E-Government Verfahren

ungültig Machen nur über den zentralen Datenbestand – dem elektronischen Wählerverzeichnis – möglich. Lässt man also trotz Registrierung zur elektronischen Stimmabgabe die herkömmliche Stimmabgabe im Wahllokal zu, bedarf es eines Zugangs zum elektronischen Wählerverzeichnis, um auszuschließen, dass nicht bereits mit einer elektronischen Wahlkarte elektronisch gewählt wurde. Ebenso ist bei der elektronischen Stimmabgabe zu prüfen, dass die Wählerin oder der Wähler nicht bereits konventionell per Papierstimmzettel gewählt hat[10].

Ähnlich verhält es sich im Szenario ohne vorherige Registrierung zu E-Voting. Es ist im Wahllokal auszuschließen, dass nicht bereits elektronisch gewählt wurde bzw. vor elektronischer Stimmabgabe, dass nicht im Wahllokal abgestimmt wurde.

In beiden Szenarien – mit oder ohne vorheriger Registrierung zu E-Voting – ist also das Verhindern mehrfacher Stimmabgabe entweder über Online- oder alternativer Zugänge zum elektronischen Wählerverzeichnis aus den Wahllokalen[11] realisierbar, oder über zeitlich versetzte Wahlzeiten für elektronische und konventionelle Stimmabgabe.

Technisch einfacher ist die Situation, wenn Registrierung zu E-Voting den Ausschluss von einer konventionellen Stimmabgabe bedingt, also die Streichung von den im Wahllokal verwendeten Wählerverzeichnissen. In diesem Fall ist die Stimmabgabe nur mehr elektronisch möglich, ein Ausweichen auf Wählen per Papier-Stimmzettel ist nicht mehr möglich. Dies schließt nicht aus, dass bei technischen Problemen mit der Umgebung der Wählerin oder des Wählers[12] am Wahltag ein Ausweichen auf elektronische Stimmabgabe im Wahllokal ermöglicht wird. Da mit dem Ausschluss der Mehr-Medien Stimmabgabe[13] das Verhindern einer doppelten Stimmabgabe relativ einfach[14] sicherzustellen ist, sind hier nur jene Wahllokale mit Online-Möglichkeit und E-Voting Umgebung[15] auszustatten, die für ein solches Ausweichen ins Wahllokal vorzusehen sind.

Verfolgt ein elektronisches Wahlsystem in Österreich den Ansatz vorhergehender Registrierung, so erfolgt diese sinnvoller Weise auch elektronisch unter Anwendung der Bürgerkarte. Die Bürgerkarte bietet hier als elektronisches Ausweisdokument eine starke Authentifizierung und die eindeutige Identifikation.

3.1.3 Elektronische Wahlkarte, Ausdruck Wahlkarte oder Stimmzettel

Das E-Government Gesetz sieht vor, dass mit Amtssignatur versehene elektronische Bescheide auch im Ausdruck auf Papier die Beweiskraft behalten. Es wäre damit ein Szenario diskutierbar, in dem auch ohne Einführung eines E-Voting mit elektronischer Stimmabgabe die Beantragung und Ausstellung einer herkömmlichen Wahlkarte elektronisch erfolgt, die Wählerin oder der Wähler diese ausdruckt und zur konventionellen Stimmabgabe im Wahllokal verwenden kann.

---

[10] Wenn in der Variante vorheriger Registrierung die Wählerin bzw. der Wähler von der konventionellen Abgabe der Stimme ausgeschlossen (im Online- oder ausgedruckten Wählerverzeichnis markiert) wird, ist die vorherige Abgabe per Papierstimmzettel dadurch verhindert.

[11] oder einigen derart ausgestatteten Wahllokalen, in denen mit elektronischen Wahlkarten konventionell abgestimmt werden kann

[12] Diese Umgebung kann etwa der Heim-PC oder die Internetanbindung der Wählerin oder des Wählers umfassen, die am Wahltag defekt werden könnten.

[13] Papier-Stimmzettel und E-Voting

[14] nur in der „E-Voting Domäne“

[15] Etwa als Bürgerkarten-fähige Kiosk-Systeme

Technisch ist auch das Beibringen der elektronischen Wahlkarte auf elektronischem Wege mittels Datenträger möglich. Es ist dabei jedoch die Frage der im Wahllokal akzeptierten Datenträger bzw. Datenformate zu klären[16]. Ansonst könnten exotische Speichermedien eine Wahlteilnahme verhindern bzw. erschweren.

In diesen Szenarien – elektronische Wahlkarte oder selbst-ausgedruckte Wahlkarte – ist jedoch zu bedenken, dass das bisherige Konzept einzelner Wahlkarten für jede Wählerin oder jeden Wähler nicht mehr gegeben ist – es lassen sich einfach identische Kopien einer elektronischen Wahlkarte herstellen (ausdrucken). Mehrfach in verschiedenen Wahllokalen verwendete Kopien einer Wahlkarte wären zu verhindern. Dies wäre wiederum nur über Online-Prüfung gegen das elektronische Wählerverzeichnis erkennbar. Alternativ müsste aus technischer Sicht vor der Auszählung ein bundesweiter Abgleich der verwendeten Wahlkarten erfolgen – dazu müssten die mit Wahlkarte abgegebenen Stimmen getrennt gehalten werden und doppelt abgegebene Stimmen den Wahlkarten zuordenbar sein. Jedenfalls wäre in den Wahllokalen die Prüfung der Authentizität der ausgedruckten Wahlkarte vorzusehen. Diese Prüfung entspricht der Rekonstruktion ausgedruckter elektronisch signierter Bescheide[17].

Eine Kombination von durch Wählerinnen und Wählern selbst ausgedruckten Wahlkarten mit einer Briefwahl, indem die Wählerinnen und Wähler auch Stimmzettel ausdrucken, ist technisch nicht sinnvoll. Es wären durch unterschiedliche Papierqualitäten oder -sorten bzw. unterschiedliche Drucker identifizierende Merkmale der Stimme möglich. Selbiges gilt für die Wahlkuverts.

Das Konzept elektronischer Beantragung der Wahlkarte als Serviceangebot an Wählerinnen und Wähler scheint jedoch sinnvoll.

Zu überlegen wäre allenfalls die elektronische Zustellung von Wahlkarten an Auslandsösterreicherinnen und Auslandsösterreicher für die Briefwahl in der derzeitigen Form. Die Authentizitätsprüfung und die Prüfung von nur einzelner Stimmabgabe können hier zentral erfolgen. Jedenfalls sind hier Wahlunterlagen, wie amtlicher Stimmzettel und Stimmkuvert, weiterhin auf Papier zuzusenden, womit sich der Mehrwert relativiert. Allenfalls ergeben sich Vorteile in der Logistik, wenn diese in großen Mengen identischen Unterlagen zentral versandt werden[18].

Verfolgt ein elektronisches Wahlsystem in Österreich den Ansatz vorhergehender Registrierung, so ist diese sinnvoller Weise auf elektronischem Wege unter Anwendung der Bürgerkarte zu sehen. Die Bürgerkarte bietet hier als elektronisches Ausweisdokument eine starke Authentifizierung und die eindeutige Identifikation.

3.1.4 Benachrichtigung der Wählerinnen und Wähler

Die Zustellung einer elektronischen Wahlkarte, bzw. die Benachrichtigung über die erfolgreiche Registrierung für eine elektronische Wahlteilnahme, kann unter Anwendung der elektronischen Zustellung erfolgen. So ist der Empfang des Zustellstücks durch die Wählerin oder den Wähler nachweislich.

---

[16] z.B. USB-Stick, div. Diskettenformate, Bürgerkarte, etc.

[17] vgl. § 20 E-Government Gesetz

[18] identische Unterlagen sind derzeit in der Praxis nicht bei allen Wahlen gegeben (z.B. dzt. bei NR-Wahl mit bis zu 43 Stimmzettel)

3.1.5 Ort der Stimmabgabe

Für den Fall, dass E-Voting nur aus dem Ausland eingeführt werden sollte bedeutet dies unter technischen Aspekten E-Voting für alle Österreicherinnen und Österreicher, da der geographische Ort der Stimmabgabe über das Internet üblicherweise nicht nachvollziehbar ist.[19]

3.1.6 Geheim-/Anonym-Haltung der Stimme

Wenngleich in der Vorwahlphase noch keine Stimmabgabe erfolgt, bestehen technische Ansätze, in denen die Anonymität der Stimmabgabe bereits hier vorbereitet wird. Über so genannte blinde Signaturen[20] können in der Registrierung nach erfolgter eindeutiger Identifikation und Authentifizierung anonyme Wahlkarten[21] ausgestellt werden, die zwar die Berechtigung der Wählerin oder des Wählers zur Stimmabgabe nachweisen, in denen allerdings keine identifizierenden Informationen mehr enthalten sind. Dieses Szenario wurde etwa in den Wahltests an der WU Wien erprobt.

Werden über anonyme Wahlkarten bereits vor der Stimmabgabe die identifizierenden Informationen unterdrückt, ist im Prozess der Stimmabgabe auch nicht mehr feststellbar, welche Wählerin bzw. welcher Wähler die Stimme abgibt. Eine allenfalls noch mögliche Wahlpflicht kann dann nicht mehr umgesetzt werden, da hier nur bekannt ist, wer eine anonyme Wahlkarte erhalten hat, nicht jedoch wer damit auch eine Stimme abgegeben hat.

3.2 Stimmabgabe

Für die Stimmabgabe selbst geht der Bericht von einer Distanzwahl aus, bei der die Wählerinnen und Wähler eigene Geräte wie Personalcomputer, Mobiltelefone oder Handhelds verwenden. Kiosk-Systeme oder die elektronische Stimmabgabe im Wahllokal lassen sich entsprechend aus den Anforderungen für die Distanzwahl ableiten. Die Umsetzung ist typischerweise jedoch einfacher, da die technische Umgebung bekannt ist.

Elektronische Verfahren unterscheiden sich hinsichtlich Gewährleistung des persönlichen Wahlrechts und Unbeobachtbarkeit nicht grundsätzlich von anderen Distanzwahlverfahren, wie bspw. der Briefwahl. Ähnlich der Briefwahl kann mit rein technischen Mitteln nicht sichergestellt werden, in welcher Umgebung eine Stimme abgegeben wird und ob es dabei zu einer Beobachtung oder Beeinflussung kommt. Es wird deshalb dieser technisch nicht lösbare Aspekt hier nicht diskutiert.

3.2.1 Identifikation, Authentifizierung

Den Überlegungen zu Registrierung und elektronischer Wahlkarte in der Vorwahlphase im vorherigen Abschnitt folgend, lassen sich die eindeutige Identifizierung der Wählerinnen und Wähler und die Prüfung der Wahlberechtigung entweder zeitlich abgesetzt in der Vorwahlphase oder unmittelbar vor der Stimmabgabe durchführen. In ersterem Fall ist ein Analogon zur herkömmlichen Wahlkarte gegeben. Diese kann

[19] was auch bei den derzeitigen Postbriefwahlen nicht unbedingt nachvollziehbar ist

[20] Unter „blinden Signaturen“ versteht man kryptographische Verfahren, über die die Authentizität eines Stücks bestätigt werden kann, ohne jedoch Inhalt und Urheber des Stücks offen zu legen. Die bestätigende Stelle signiert „blind“, sieht also Inhalt oder Urheber nicht, womit etwa Protokolle zu anonyme Wahlkarten möglich sind.

[21] Eine anonyme Wahlkarte bestätigt die Berechtigung zur Stimmabgabe, gibt aber die Identität der Wählerin bzw. des Wählers nicht preis.

allenfalls anonymisiert sein, sofern ein Nachweis der Ausübung des Wahlrechts bei Wahlpflicht nicht geführt werden muss.

Technisch unterscheiden sich die Verfahren dadurch, dass im Fall einer elektronischen Wahlkarte diese in der technischen Umgebung der Wählerin oder des Wählers nicht-flüchtig bis zum Wahltag zu speichern ist. Dies kann in herkömmlichen Speichermedien[22] oder in der Wählerin oder dem Wähler am Wahltag zugänglichen Online-Archiven erfolgen[23].

Mittel zur Authentifizierung – dem Nachweis einer behaupteten Identität – sind elektronische Signaturen.

Eindeutige Identifikation und Authentifizierung sowie Infoboxen zur Speicherung sind in der Bürgerkarte vorgesehen.

3.2.2 Elektronischer Stimmzettel und Software zur Stimmabgabe

Wesentlich ist, dass die Authentizität des elektronischen Stimmzettels gewährleistet ist und dies vor Abgabe der Stimme prüfbar ist. Hier wären etwa entsprechende Serverzertifikate[24] der Wahlbehörde zur elektronischen Signatur der Stimmzettel[25] technische Mittel.

Ebenso müssen die zur Stimmabgabe bzw. zur Registrierung zu E-Voting verwendeten Softwarekomponenten authentisch sein. Wiederum sind hier Serverzertifikate oder elektronisch signierte Software technische Mittel.

3.2.3 Geheim-/Anonym-Haltung der Stimme

Die Geheimhaltung der Stimme bis zur Auszählung ist über Verschlüsselung zu erreichen. Hier gibt es Standardverfahren, die Geheimhaltung stellt damit technisch kein wesentliches Problem dar.

Wesentliche Herausforderung im E-Voting ist, eine abgegebene Stimme nicht auf eine Wählerin oder einen Wähler zurückführen zu können. Es ist die Stimme somit von identifizierenden Informationen zu trennen. Dabei können identifizierende Informationen Primärinformationen wie Name, digitales Zertifikat oder bPK aus der Identifikation und Authentifizierung mit der Bürgerkarte sein, aber auch aus indirekt identifizierenden Informationen, wie genauer Zeitpunkt der Stimmabgabe, Internetadressen, Telefonnummer, oder aus über Schadprogramme wie Viren oder Würmer aus der technischen Umgebung der Wählerin oder des Wählers gesammelten Daten, stammen. Es wird in Folge nicht weiter zwischen diesen Kategorien unterschieden, da ein Wahlsystem gewährleisten muss, dass keine dieser Information mit der entschlüsselten Stimme assoziiert wird.

Es sind aus der wissenschaftlichen Literatur oder aus kommerziellen Systemen, wie sie auch in Pilotprojekten eingesetzt wurden, verschiedene Lösungsansätze bekannt,

---

[22] PC Festplatte, USB-Stick, etc.

[23] Entsprechende Zugriffkontrolle und sichere Verwahrung im Online-Archiv vorausgesetzt

[24] Etwa über Object Identifier (OID) der öffentlichen Verwaltung, wie im E-Government

[25] Hier darf die Signatur der Wahlbehörde nach Stimmabgabe nicht zu identifizierbaren Stimmen führen. Es ist also die Signatur der Wahlbehörde vom ausgefüllten Stimmzettel zu trennen oder alle signierte Stimmzettel müssen den selben Signaturwert aufweisen.

die dem Anspruch der anonymen Stimmabgabe genügen. Diese lassen sich in drei Klassen teilen: Organisatorische Maßnahmen, spezielle kryptographische Protokolle und spezielle Hardware.

Der erste Ansatz, ist, Anonymisierung durch organisatorische Vorgaben an Wahlbehörden oder deren Dienstleister zu delegieren. Solche Vorgaben können sein, dass vor der Entschlüsselung der elektronischen Stimme diese von den identifizierenden Informationen wie elektronische Wahlkarten, Absenderadressen oder Zeitmarken zu trennen und verschlüsselt in einer elektronischen Wahlurne zu sammeln sind. Solche Vorgaben sind vergleichbar mit der Behandlung von per Briefwahl abgegebenen Stimmen.

Im zweiten Ansatz sind aus der Wissenschaft eine Reihe von kryptographischen Protokollen bekannt, die technisch sicherstellen sollen, dass die Stimmabgabe anonym gehalten werden kann. Die Wesentlichsten sind Protokolle basierend auf blinden Signaturen, kryptographischen Mix-Netzwerken oder Homomorphismus. Die Details dieser Protokolle werden hier nicht weiter ausgeführt. Es sind in der Umsetzung vor allem die Skalierbarkeit in Bezug auf große Anwendermengen (Wählerinnen und Wähler) und die Abbildbarkeit des Wahlsystems (z.B. Vorzugsstimmen, Landeswahlkreise und Stimmbezirke) zu beachten.

Ein weiterer Ansatz ist, spezielle Hardware Security Module zu verwenden, die die abgegebenen Stimmen entschlüsseln. Dabei werden jedoch nicht einzelne Stimmen klartextlich bereitgestellt, sondern nur eine entsprechend große Menge als Block entschlüsselt freigegeben oder die gesamte Auszählung vom Hardware Security Modul selbst vorgenommen. Damit müssen außerhalb des Hardware Security Moduls die verschlüsselte Stimme und identifizierende Information wie eine elektronische Wahlkarte nicht notwendigerweise getrennt gehalten werden. Dies ist vergleichbar einem Sammeln von per Briefwahl einlangenden verschlossenen Wahlkuverts zusammen mit den Wahlkarten.

In allen Ansätzen ist die Verfügbarkeit der Stimmen auch im Fehlerfall zu berücksichtigen. Eine entsprechend redundante Auslegung der Systeme, Zweitsysteme zu den verwendeten kryptographischen Schlüsseln oder die laufende Sicherung der abgegebenen Stimmen bis zur Auszählung sind zu gewährleisten.

Es werden hier im Sinne der Technologieneutralität keine Ansätze favorisiert. Aktuell besteht über anonyme Stimmabgabe über die Bürgerkarte hinausgehend in Österreich auch keine spezifische Infrastruktur im Produktionsbetrieb, die ein Verfahren als besonders ökonomisch hervorhebt. Verschiedene Verfahren werden national und international in Tests und Pilotversuchen erprobt, etwa auch in Österreich in den Wahltests an der WU Wien.

3.2.4 Übereilungsschutz vs. Nachweis der abgegebenen Stimme

Im E-Voting kann ein Übereilungsschutz rechtliche Forderung sein. Auch die Nachvollziehbarkeit, dass die elektronisch abgegebene Stimme in der Zählung berücksichtigt wird, kann für das Vertrauen in ein System notwendig sein. Gleichzeitig wird auch bei E-Voting gefordert sein, dass ein Nachweis der abgegebenen Stimme auch den Wählerinnen und Wählern nicht möglich ist, etwa um Stimmenkauf zu verhindern. Dies muss so ausgeformt werden, dass es keine gegenläufigen Forderungen ergibt.

Ein Übereilungsschutz kann durch entsprechende Willensakte, wie das wiederholte Betätigen eines Bestätigungsknopfes, abgebildet werden. Hier reichen etwa bei Internet-Voting die technischen Möglichkeiten bis zur nochmaligen Anzeige der abgegebenen Stimme, bevor diese durch eine Bestätigung endgültig in die elektronische Urne übermittelt wird. Abschließend wird zur Nachvollziehbarkeit eine Bestätigung notwendig sein, dass die Stimme tatsächlich übernommen wurde.

Hier ist darauf zu achten, dass vor allem in den abschließenden Meldungen des elektronischen Wahlsystems kein Hinweis auf die abgegebene Stimme gegeben ist.

Hinsichtlich eines evident Haltens der Stimme durch die Wählerin oder den Wähler sind die technischen Möglichkeiten bei der Distanzwahl insofern eingeschränkt, als ein Abbild (etwa Ausdruck, Screenshot oder Photo des Bildschirm) zwar teilweise technisch erschwert, jedoch nicht verhindert werden kann. Etwa kann die Funktionsleiste mit der Druck-Funktion bei einigen Webbrowsern ausgeblendet werden. In der unkontrollierten Umgebung einer Distanzwahl kann aber etwa ein Screenshot ebenso wenig technisch verhindert werden, wie in der Briefwahl eine Kopie oder Photo des Stimmzettels. Dies ist jedoch von einem vom Wahlsystem bereitgestellten Nachweis der Stimme zu unterscheiden[26].

Die elektronische Stimmabgabe ist eine wesentliche psychologische Veränderung für die Wählerinnen und Wähler. Es ist nicht mehr eine Gruppe von Personen für das ordnungsgemäße Sammeln und Auszählen der Stimmzettel verantwortlich, sondern ein für die Einzelne oder den Einzelnen nicht durchschaubares System. Die Möglichkeit, dass bei E-Voting Wählende das korrekte Eingehen der eigenen Stimme in den Zählprozess nachvollziehen können, scheint technisch möglich. Inwieweit derartige technische Möglichkeiten auch in eine Umsetzung einfließen sollen, wäre der allgemeinen Diskussion zu unterziehen.

3.2.5 Besondere technische Möglichkeiten zur Unterstützung

Die Informationstechnologie bietet technische Möglichkeiten, Wählerinnen und Wähler bei der Stimmabgabe zu unterstützen. Es werden hier nur einige Varianten dargestellt, die mit dem Medium Papierstimmzettel nicht möglich sind. Inwieweit hier die technischen Möglichkeiten auch mit den Wahlgrundsätzen vereinbar sind, etwa Möglichkeiten geschaffen werden, die eine wesentliche Ungleichheit zur konventionellen Stimmabgabe eröffnen, wird hier nicht bewertet. Vielmehr werden diese aus einer technischen Sichtweise zur Diskussion gestellt – eine allfällige Umsetzung hat den rechtlichen und inhaltlichen Vorgaben zu folgen.

Jedenfalls lassen sich bei E-Voting leere Stimmzettel oder selbst formulierte Bemerkungen umsetzten. Auch die willentliche oder die versehentliche Abgabe einer ungültigen Stimme ist möglich, indem durch das E-Voting System keine Prüfung der Gültigkeit vorgenommen wird. Konträr kann ein E-Voting System auch auf eine ungültige Stimme hinweisen, um versehentlich ungültige Stimmen zu verhindern oder bewusst ungültige Stimmen grundsätzlich nicht zu zulassen. Die tatsächliche Ausformung ist keine technische Frage, sondern hat den Vorgaben zu folgen.

[26] Eine Bestätigung, dass eine Stimme in die elektronische Urne gelangt ist, scheint unbedenklich, im Gegensatz zu einer Bestätigung, die die abgegebenen Stimme bzw. das Stimmverhalten enthält

Ebenso sind sowohl die Abgabe einer Vorzugsstimme ohne Parteistimme, wie auch mit Parteistimme möglich. In der Darstellung der Listen ist bei typischen PC- oder Laptopbildschirmen eine Darstellung, die dem amtlichen Stimmzettel entspricht, vorstellbar, allenfalls eine wahlweise Vergrößerung der Vorzugsstimmenbereiche durch die Wählerinnen und Wähler möglich. Bei anderen Technologien wie Personal Digital Assistent (PDA) oder Handy-Bildschirmen werden mit derzeitiger Technologie bzw. schon aufgrund der Größe typischer Nationalratswahl-Stimmzettel diese nicht ohne Blättern zu den Vorzugsstimmen darstellbar sein.

In der Darstellung der Stimmzettel bestehen vor allem bei Internet-Wahlen Technologien, über die eine Gleichbehandlung der Parteien im Layout auch bei unterschiedlichen Ausgabemedien, wie bspw. unterschiedliche Bordschirmauflösungen, sichergestellt werden kann. Beispiele dafür sind Extensibel Markup Langauge (XML) mit Stylesheets oder die Darstellung von Tabellen in Hypertext Markup Language (HTML). Mit Ansätzen wie der Web Accessible Initiative (WAI) ist auch die entsprechende Darstellung für Sehbehinderte möglich, wie auch mit Internet Technologien durch die Benutzer die für sie am besten wahrnehmbare Darstellung gewählt werden kann. Hier ist die grundsätzliche Gleichbehandlung der Parteien in der Präsentation des Stimmzettels von der von Wählerinnen und Wählern selbst gewählten Darstellungshilfen zu trennen[27].

Technisch denkbar sind auch Ausfüllhilfen bis hin zu über den elektronischen Stimmzettel verlinkten Online-Informationen zu Parteiprogrammen oder den einzelnen Personen der Listen. Es ist dies technisch nicht besonders komplex, stellt aber einen klaren Unterschied zu den Möglichkeiten, die Wählerinnen und Wähler, die konventionell abstimmen, am Wahltag haben. Außerdem ist dabei die Gefahr einer Beeinflussung des Wahlverhaltens der Wählerinnen bzw. der Wähler zu bedenken[28].

Technische besteht die Möglichkeit bereits abgegebene Stimmen nachträglich bis zu einem bestimmten Zeitpunkt zu ändern. Dies wird etwa in Ländern angedacht, die diese Möglichkeit auch bei der Briefwahl vorsehen, bedingt aber, dass die einzelne Stimme bis zu diesem Zeitpunkt der Wählerin oder dem Wähler zuordenbar ist.

3.2.6 Ausstattung der Wahllokale

Im organisatorischen Umfeld eines E-Voting Systems lässt sich auch hinsichtlich der Wahlzeiten unterscheiden, die sich dann vor allem auf die Führung der Wählerverzeichnisse auswirken. Findet die elektronische Wahl zeitlich vor der Möglichkeit zur Stimmabgabe im Wahllokal statt, lassen sich am Wahltag aktuelle Wählerverzeichnisse offline zur Verfügung stellen, in denen Wählerinnen und Wähler, die bereits elektronisch abgestimmt haben, nicht mehr aufscheinen. Eine Alternative, E-Voting nach dem Wahltag zu ermöglichen, scheint vorerst wenig diskussionswert – es würde die Bekanntgabe von Hochrechnungen oder vorläufiger Wahlergebnisse am Wahltag verzögern.

Bei Überlappung der zugelassenen Zeit für elektronische und konventionelle Stimmabgabe sind, im Sinne der Überlegungen in der Vorwahlphase zur Verhinderung doppelter Stimmabgabe, im Wahllokal Online Zugänge zu elektronisch aktuellen

[27] Ein Vergrößern von Ausschnitten im Web-Browser bei Sehbehinderungen ist etwa vergleichbar mit dem Verwenden einer Lupe beim Papier-Stimmzettel.

[28] siehe auch ER Empfehlung: Verfahrensempfehlungen, Punkt 14

Wählerverzeichnissen zu gewährleisten, wenn es der Wählerin oder dem Wähler auch nach Registrierung zu E-Voting freistehen soll, konventionell abzustimmen.

Es wäre zu definieren, ob alle oder nur einige Wahllokale die entsprechend technische Ausstattung haben müssen, um den Online-Zugang zu aktuellen Wählerverzeichnissen und das Lesen einer elektronischen Wahlkarte[29] zu ermöglichen. Bei Internet-Wahlsystemen wäre die Ausstattung etwa vergleichbar mit der, die Wählerinnen und Wähler in der Distanzwahl einsetzen (z.B. PC und Zugang zu Bürgerkartenumgebung wie Chipkartenleser oder Handy-Signatur). Zusätzlich wäre in diesen Wahllokalen dann die Online-Einsicht in das Wählerverzeichnis durch die Wahlbehörde notwendig, wenn alternativ die Möglichkeit, konventionell mit Papier-Stimmzettel abzustimmen, gewährleistet werden soll. Hat die Nachschau im Wählerverzeichnis nur für eine beschränkte Anzahl von Wählerinnen und Wählern zu erfolgen – etwa für zu E-Voting Registrierte, die durch technische Probleme nicht elektronisch abstimmen können – kann dies beispielsweise auch telefonisch über Call Center erfolgen. Das Call Center hat in ein zentrales Wählerverzeichnis Einsicht, in das eine erfolgte Stimmabgabe eingetragen wird[30].

3.3 Auszählung

Die Auszählung elektronisch gesammelter Stimmen ist technisch keine große Herausforderung. Es ist jedoch die Wahrung der Anonymität der abgegebenen Stimme auch hier sicher zu stellen. Über die Überlegungen zur Anonymität bei der Stimmabgabe hinausgehend sind Vorgaben zu treffen, die vor allem auch keinen indirekten Rückschluss auf das Wahlverhalten ermöglichen. Hier sind äquivalent zu sehr kleinen Wahlsprengeln Regelungen für ein Zusammenfassen sehr kleiner Mengen an Stimmen vorzusehen. Mit den Mitteln der Analyse elektronischer Daten sind über die rein geographische Analyse weitere Parameter zu bedenken. Ein willkürliches Zusammenfassen von Stimmen zur Auszählung ist zu verhindern[31].

Inwieweit eine gesonderte Bekanntgabe von elektronisch und konventionell abgegebenen Stimmen etwa für statistische Zwecke zu unterstützen ist, ist keine technische Frage und allenfalls über organisatorische Vorgaben zu klären.

Die Archivierung der elektronisch abgegebenen Stimmen, etwa zur Kontrolle bei Wahlanfechtung, ist vorzusehen. Dies stellt technisch kein besonderes Problem dar. Selbst für den Fall einer höchstgerichtlich angeordneten Reproduktion des Wahlergebnisses stehen so die archivierten Stimmen vollständig zur Verfügung.

Es lassen sich im Wesentlichen drei verschiedene Ansätze zu Kontroll- oder Nachzählungen unterscheiden:

- Wiederholte Zählungen mit denselben Systemen basierend auf derselben elektronischen Datenbasis werden nur dann unterschiedliche Ergebnisse zeigen, wenn nicht Fehler in einer Zählung auftreten (Defekte). Solche Fehler

[29] Schon bisher sind für Wahlkartenwählerinnen und Wahlkartenwählern flächendeckend ausgewählte Wahllokale vorgesehen. Für die Einführung elektronischer Wahlkarten alleine betreffen so die dafür zu ergreifenden technischen Ausstattungsmaßnahmen vorwiegend diese Wahllokale sowie österreichische Vertretungsbehörden im Ausland (je nach Wahl ggf. auch alle Wahllokale).

[30] Die Publizität der Antwort an de Wahlbehörde muss gegeben sein, um die Antwort authentisch dem Protokoll beilegen zu können

[31] etwa ein Rastern von Stimmen die über einen bestimmten elektronischen Kanal, zu bestimmter Zeit, o.ä. eingelangt sind, etc.

sind eher unwahrscheinlich und mit heutigem Stand der Informationstechnologie untypisch.
- Erfolgen Nachzählungen mit verschiedenen Systemen, wird die korrekte Funktion eines Systems weitgehend verifiziert, systematische Fehler in der Zähl-Logik oder der Implementierung werden allenfalls nicht erkannt – etwa systematische Fehler in den Algorithmen.
- Mit Kontroll- oder Nachzählungen basierend auf verschiedenen Systemen und bewusst unterschiedlichen Methoden und Algorithmen werden Implementierungsfehler eines Ansatzes erkannt.

Wenngleich das Zählen elektronischer Stimmen keine technisch große Herausforderung darstellt, können etwa Kontrollzählungen über unabhängige Systeme das Vertrauen in E-Voting steigern.

3.4 Ausfall technischer Komponenten

Technische Systeme besitzen gewisse Fehler- und Ausfallswahrscheinlichkeiten. Dabei sind am Stand der Technik Fehler, die eine abgegebene Stimme in der Übermittlung oder Speicherung ändern oder unverfügbar machen, ausschließbar. Nicht ausschließen kann man jedoch den Ausfall einzelner Komponenten oder Kommunikationsverbindungen.

In der Betrachtung der Ausfallswahrscheinlichkeit kann man grob in drei Kategorien unterscheiden: Erstens zentrale Systeme wie Rechenzentren oder Zentrale Wählerevidenz. Zweitens Dezentrale Systeme geringen Volumens in kontrollierten Umgebungen. Dies sind etwa Wahllokale in Gemeindeämtern oder größeren Schulen. Drittens stark dezentrale Systeme in unkontrollierten Umgebungen.

Für zentrale Systeme wie Rechenzentren sind sichere Umgebungen, redundante Ausführung der Komponenten und Kommunikationsverbindungen oder je nach Kritikalität der Anwendung Verteilung an verschiedene Standorte Stand der Technik. Hier kann auch das Restrisiko eines Komplettausfalls am Wahltag bewertet und entsprechende Notfallprozeduren können geplant werden. Hochverfügbarkeit ist hier bei zentralen Diensten typisch gegeben, etwa beim ZMR.

In dezentralen Systemen in kontrollierten Umgebungen, in denen typisch Rechner- und Kommunikationsinfrastruktur besteht, etwa in Wahllokalen in Gemeindeämtern oder Schulen, sind Zweit- und Reservesysteme planbar, bei PCs typisch auch vorhanden. Auch alternative Kommunikationsverbindungen, die eine Mindestqualität zur Verfügung stellen, sind typisch gegeben[32] oder können für die Wahl beigestellt werden[33]. Es sind hier also die Wahrscheinlichkeiten eines Komplettausfalls minimierbar. Je nach Ausformung des E-Voting Systems sind kurzfristige Ausfälle auch relativ unkritisch[34].

[32] Etwa Modem-Einwahlverbindungen

[33] Etwa Modem-Einwahlverbindungen, Funknetze oder GPRS oder UMTS Mobilverbindungen

[34] Wenn ein System zur Zulassung zur Wahl mit Wahlkarte Nachschau in zentraler Wählerevidenz fordert, ist etwa ein Ausfall im Wahllokal im Sekunden- bis Minutenbereich, den Wählerin und Wähler abwarten muss, tolerierbar. Werden elektronische Wählerlisten lokal gehalten und mit „E-Voting Wählerinnen und Wählern“ des Heimatsprengels laufend upgedated, stellen auch hier kurzfristige Ausfälle nur geringes Risiko dar.

Anders verhält es sich bei Wahllokalen in privatem Umfeld (Gasthäuser, etc.) und vor allem bei den privaten Komponenten der Wählerinnen und Wähler. Die Vollvernetzung aller Wahllokale mit Reservekomponenten stellt kurzfristig wesentliche Kosten dar. Systeme, die nicht die Ausstattung aller Wahllokale mit IT-Infrastruktur benötigen, scheinen hier mittelfristig eher umsetzbar.

Bei den privaten Komponenten der Wählerinnen und Wähler ist mit Ausfällen oder auch Fehlkonfigurationen am Wahltag zu rechnen. Als gangbare Möglichkeiten zeichnen sich hier ab, dass entweder die elektronische Stimmabgabe vor dem Wahltag zu erfolgen hat, bei Problemen also am Wahltag konventionell gewählt werden kann, oder alternativ einige entsprechend ausgestattete Wahllokale[35] die Stimmabgabe elektronisch oder konventionell mit Papier-Stimmzettel erlauben.

3.5 Wahlbehörde, Wahlzeugen und Audit

In der Distanzwahl ist eine direkte und unmittelbare Kontrolle der geheimen, unbeobachteten Stimmabgabe durch die Wahlbehörde nicht mehr in der Form wie in einem konventionellen Wahllokal möglich. Es sind jedoch Maßnahmen vorzusehen, wodurch die technischen Prozesse nachvollziehbar und sowohl in einer nachträglichen Prüfung als auch bei einer Wahlbeobachtung während der Wahl verständlich dargestellt werden.

Verschlüsselung der Stimme vor Abgabe ermöglicht es, die Wahlkommission im elektronischen Medium abzubilden. Geben nämlich die Wahlkommissionsmitglieder vor der Wahl nur ihre öffentlichen Kommissions-Schlüssel bekannt und werden die abgegebenen Stimmen mit diesen öffentlichen Schlüsseln codiert, so sind die abgegebenen Stimmen auch für die Administratoren des Wahlsystems nicht einseh- oder änderbar. Das Bekannt geben (oder Anwenden) der privaten Schlüssel der Kommissionsmitglieder nach der Wahl und die dadurch mögliche Decodierung der Stimmen entspräche damit dem Öffnen der Urne in einem papierbasierten System.

Dies umfasst die Verständlichkeit des Prozesses einer Stimmabgabe[36], wie auch die Beobachtung des gesamten Wahlvorganges. Für letzteres sind einige Möglichkeiten vorstellbar, etwa Zählmechanismen der in einzelnen Phasen befindlichen Stimmen[37].

Konkrete Vorgaben für das Audit sind in den ER Empfehlungen gegeben und werden im Anhang dieses Berichts detailliert.

Zur Gewährleistung der Sicherheit und der Revisionsfähigkeit der Systeme wird eine entsprechende unabhängige Prüfung de Komponenten vorzusehen sein. Hier können je nach Kritikalität der Komponenten etwa Verpflichtungen zu Bescheinigungen, Gütesiegel, Gutachten, oder formelle Zertifizierungen vorgesehen werden.

---

[35] Vor allem Online-Fähigkeit zur Verhinderung doppelter Stimmabgabe.

[36] etwa: Wählerin/Wähler authentifiziert sich, gibt Stimme ab, verschlüsselte Stimme gelangt in elektronische Urne

[37] Etwa Zähler für Wählerinnen und Wähler im Prozess der Stimmabgabe, Anzahl abgebrochener Stimmabgaben/Fehler, Zähler für abgeschlossene Stimmabgaben und Stimmen in elektronischer Urne

4. Aktueller Stand, technischer Entwicklungsbedarf

In diesem Abschnitt wird dargestellt, in welchen Bereichen die technischen Konzepte wie weit konsolidiert sind, um bei allfälliger politischer Entscheidung einer Einführung des E-Voting Teilaspekte kurz- bis mittelfristig umsetzen zu können, respektive wo es noch Lücken, Entwicklungsbedarf oder die Notwendigkeit großflächiger Tests gibt.

4.1 Vorwahlphase

Die für eine sinnvolle Umsetzung von E-Voting notwendige Einführung einer zentralen elektronischen Wählerevidenz baut sinnvoller Weise auf die im E-Government verwendeten Register, wie ZMR und Ergänzungsregister, auf. Die dabei erforderlichen Erweiterungen, wie die Aufnahme der Wahlausschließungsgründe oder die Prozeduren zur Aufnahme nicht in Österreich gemeldeter Wählerinnen und Wähler, Auslandsösterreicherinnen und Auslandsösterreichern sowie in Österreich lebenden EU-Bürgerinnen und EU-Bürgern im Ergänzungsregister, stellen kein wesentliches technisches Problem dar, sodass dies als technisch relativ schnell umsetzbar zu bewerten ist.

Für den Fall einer notwendigen Registrierung zur elektronischen Wahl, sofern ein österreichisches E-Voting System dies vorsieht[38], ist dieser Vorgang technisch vergleichbar mit den bestehenden E-Government Verfahren (zum Beispiel Verfahren zur Ausstellung einer elektronischen Meldebestätigung oder dem elektronischen Antrag einer Strafregisterbescheinigung). Hier ist die Komplexität diesen Verfahren vergleichbar. Werden bereits in der Registrierung technischen Vorkehrungen getroffen, um im weiteren Verlauf der Wahl bestimmte Sicherheitsparameter zu erfüllen[39], steigt die Komplexität entsprechend diesen Vorkehrungen.

Das Ausfolgen einer elektronischen Wahlkarte ist über die elektronische Zustellung möglich. Als Zugang zur konventionellen Wahl wäre für eine elektronische Wahlkarte das Verhindern deren mehrfacher Verwendung zur konventionellen Stimmabgabe organisatorisch zu lösen. Im Zusammenspiel mit der Briefwahl aus dem Ausland besteht hier auch noch keine Basis für ein Selbst-Ausdrucken des Stimmzettels.

Zusammenfassend ist die Infrastruktur für die Vorwahlphase eines E-Voting weit fortgeschritten. Auch der Zwischenschritt der elektronischen Beantragung einer Wahlkarte stellt mit der Infrastruktur aus dem E-Government, wie Bürgerkarte und MOA, kein technisches Problem dar. Für eine elektronisch zugestellte Wahlkarte und deren Verwendung im Wahllokal oder bei Briefwahl im „Selbstausdruck“ bedarf es Verfahren zum Ausschluss derer Mehrfachverwendung.

4.2 Stimmabgabe

Für die Stimmabgabe besteht mit der Bürgerkarte eine Infrastruktur zur Identifikation von Wählerin oder Wähler bzw. zur Verschlüsselung der Stimmen[40].

Für die Wahrung der Anonymität der Stimme bestehen verschiedene Ansätze. Neben den in Österreich parallel zu ÖH-Wahlen an der WU Wien und parallel zur Bun-

[38] Es sind auch Systeme denkbar, in denen sich Wählerinnen oder Wähler am Wahltag spontan für E-Voting ohne vorherige Registrierung entscheiden

[39] Etwa die in den Wahltests der WU-Wien eingesetzten Protokolle zur Anynomhaltung der Stimme.

[40] Mit Security Layer Version 1.2 über XML-Verschlüssellungsfunktionen

despräsidentenwahl 2004 durchgeführten Wahltests in Österreich sind erste Erfahrungen aus den internationalen Pilotversuchen mit Distanzwahl gegeben[41].

Nachdem Stimmabgabe und Wahrung der Anonymität der abgegebenen Stimme die kritischste Phase des E-Voting ist, scheinen hier weitere intensive Tests in großem Maßstab erforderlich. Die Stimmabgabe ist somit ein Bereich in dem, wenngleich wissenschaftlich intensiv behandelt, noch technischer Entwicklungsbedarf besteht.

4.3 Auszählung

In der Auszählung bestehen bei elektronischem Vorliegen der Stimmen keine technischen Probleme, sofern die Stimmen von identifizierenden Elementen getrennt sind. Archivierung und Nachzählen sind ebenso kein wesentliches technisches Problem.

4.4 Wahlbehörde, Wahlzeugen und Audit

Im Bereich der Wahlbehörden und der Überwachung einer elektronischen Wahl besteht die technische Infrastruktur in den Wahllokalen derzeit meist noch nicht. Es wären Wahllokale flächendeckend, wenngleich nicht notwendigerweise alle, zumindest mit Onlinezugängen zu aktuellen Wählerverzeichnissen auszustatten.

4.5 Konkretisierungsbedarf der ER-Empfehlungen

Die technischen Empfehlungen des Europarats stellen Anforderungen an E-Voting Systeme dar und sind keine Standards im eigentlichen Sinn. Es wären hier Detail-Spezifikationen und allenfalls Standards zu erstellen.

Im Bereich der Sicherheitsempfehlungen wäre es sinnvoll, diese weiter in Schutzprofile zu konkretisieren. Vor allem die zu erreichenden Vertraulichkeitsstufen der Produkte sind zu definieren, um die für E-Voting zu erreichenden Prüftiefen einer unabhängigen Evaluierung der Systeme festzulegen.

[41] Etwa Internet-Wahltest in Schweiz (Referenden im Kanton Genf), den Niederlanden (Wahlen zum Europaparlament) und Regionalwahlen im Vereinigten Königreich, oder auch Pilotversuche über Telefon in den Niederlanden und dem Vereinigten Königreich

Anhang: ER Empfehlungen vs. Situation in Österreich

In diesem Anhang werden die technischen Teile der Europaratsempfehlungen in Relation zu in Österreich bestehender Infrastruktur gestellt bzw. vor allem die möglichen Synergien zu den Ansätzen aus dem E-Government aufgezeigt.

Es werden dazu die Zitate der ER Empfehlungen in „*Arial 10 pt italic blau*“ dargestellt. Es sei hier auch darauf hingewiesen, dass zu den ER Empfehlungen umfangreiche Erläuterungen als Explanatory Memoranda vorhanden sind.

Wenn die ER Empfehlungen keine besondere Behandlung einer spezifisch österreichischen Situation bedingen oder keiner spezifischen Infrastruktur bedürfen, werden keine gesonderten Stellungnahmen dazu gegeben. Die entsprechenden ER Empfehlungen werden als Referenz trotzdem wiedergegeben.

Technische Aspekte in rechtlichen und Verfahrens-Empfehlungen

Nachfolgend ein Auszug einiger rechtlicher und Verfahrens- Empfehlungen der ER Empfehlungen, die konkret vor dem Österreichischen Hintergrund kommentiert werden können.

ad. Appendix I – Rechtliche Empfehlungen:

Allgemeines Recht zu Wählen

> *1. The voter interface of an e-voting system should be understandable and easily usable.*
>
> *2. Possible registration requirements for e-voting should not pose an impediment to the voter to participate in e-voting.*
>
> *3. E-voting systems should be designed, as far as it is practicable, to maximise the opportunities that such systems can provide for persons with disabilities.*

Die breite Zugänglichkeit des Systems und speziell die Zugänglichkeit für Personen mit Behinderungen ist ein wesentliches Kriterium für den Entwurf der Benutzerschnittstelle des E-Voting Systems. Beispielsweise ist in diesem Zusammenhang die Anwendung der Leitlinien der Web Accessibility Initiative (WAI) des World Wide Web Konsortiums zu nennen. Näheres dazu ist in den Erläuterungen zu den technischen Empfehlungen der ER Empfehlung, Abschnitt Zugänglichkeit, Punkt 1 bis 5, im nächsten Kapitel des Anhangs zu finden.

III. Reliability and security

> *[…]*
>
> *34. The e-voting system should maintain availability and integrity of the votes. It should also maintain the confidentiality of the votes and keep them sealed until the counting process. If stored or communicated outside controlled environments, the votes should be encrypted.*

Diese Forderung kann durch kryptographische Verfahren, wie Verschlüsselung und Signatur, sicher gestellt werden. Für die Geheimhaltung der Stimme stellt die Formulierung „sealed“ der ER-Empfehlung einen Kompromiss dar, wo in kontrollierbaren Umgebungen – etwa Wahlmaschinen im Wahllokal –Vertraulichkeit der Stimme nicht notwendiger Weise durch Verschlüsselung sicher zu stellen ist[42]. Bei Kommunikation der Stimme außerhalb kontrollierter Umgebungen – etwa über das Internet – ist Verschlüsselung zwingend vorgeschrieben. Das Konzept der österreichischen Bürgerkarte bietet dazu alle notwendigen Basisfunktionalitäten. Auch Ver- und Entschlüsselungsmethoden werden in der Version 1.2 der Bürgerkartenumgebung zur Verfügung stehen. Somit sind Wählerinnen und Wähler in der Lage, im Falle der Forderung die Stimmen bereits vor der Übermittlung der Stimme zu verschlüsseln und dies unter Anwendung ihrer Bürgerkarte durchzuführen. So kann eine sichere End-zu-End Verschlüsselung zwischen Wählerin bzw. Wähler und Wahlbehörde bzw. elektronischer Urne gewährleistet werden.

> *35. Votes and voter information (i.e. information relating to persons) should remain sealed as long as the data is held in a manner where they can be associated. Authentication information should be separated from the voter's decision at a pre-defined stage in the election process.*

Wie schon in dem Hauptteil dieses Berichts behandelt, existieren dazu verschiedene wissenschaftliche und technische Ansätze. Ein möglicher Weg dies zu gewährleisten ist die geeignete Anwendung kryptographischer Verfahren wie Signatur und Verschlüsselung. Mit der österreichischen Bürgerkarte sind die Wählerinnen und Wähler in der Lage, derartige kryptographische Methoden in einem E-Voting Verfahren anzuwenden.

ad. Appendix II - Operational standards:

II. Voter registration

> *[…]*
>
> *4. There should be a voters register which is regularly updated. The voter should be able to check as a minimum the information which is held about him/her on the register, and request corrections.*

Es bietet sich an, auf Basis der in Österreich elektronisch geführten Register, wie zentrales Melderegister (ZMR) oder Ergänzungsregister, eine Zentrale Wählerevidenz (ZWE) aufzubauen.

> *5. The possibility of creating an electronic register and introducing a mechanism allowing online application for voter registration and, if applicable, for application to use e-voting, should be considered. When participation in e-voting requires a separate application by the voter and/or additional steps, all these communications should be able to be carried out in an electronic, and, where possible, interactive way.*

Im Falle einer österreichischen E-Voting Lösung, die eine vorhergehende Registrierung der Wählerin oder des Wählers zur elektronischen Wahl bedingt, ist auf Basis einer Zentralen Wählerevidenz eine elektronische Registrierung unter Verwendung

[42] Etwa auch physischer Schutz durch Bauform und Plombieren der Wahlmaschine.

bestehender Komponenten bereits existierender E-Government Applikationen einfach möglich. Auch die Aufnahme von Auslandsösterreicherinnen und Auslandsösterreichern bzw. in Österreich lebenden EU-Bürgerinnen und EU-Bürgern in der Wählerevidenz bzw. in der Europawählerevidenz ist so möglich. Technische Komponenten wie Bürgerkarte, elektronischer Zustelldienst, etc. erlauben schon heute die Realisierung ähnlicher Online-Verfahren.

[…]

Technische Empfehlungen

Die Stellungnahmen zu den ER Empfehlungen folgen deren Struktur und Nummerierung.

Zugänglichkeit

1. Measures shall be taken to ensure that the relevant software and services can be used by all voters and, if necessary, provide access to alternative ways of voting.

2. Users shall be involved in the design of e-voting systems, particularly to identify constraints and test ease of use at each main stage of the development process.

3. Users shall be supplied, whenever required and possible, with additional facilities, such as special interfaces, or other equivalent resources, such as personal assistance. User facilities shall comply as much as possible with the guidelines set out in the Web Accessibility Initiative (WAI).

4. Consideration shall be given, when developing new products, to their compatibility with existing ones, including those using assistive technologies for people with disabilities.

5. The presentation of the voting options shall be optimised for the voter

Bereits aus dem Aktionsplan eEurope 2002 ist die Übernahme der WAI-Leitlinien für Webseiten der öffentlichen Verwaltung durch die Mitgliedstaaten vorgesehen. Konsequenterweise ist dies auch bei E-Voting Systemen zu verfolgen. Aus einer Entschließung des Rates Telekommunikation der Europäischen Union vom März 2002[43] sind die EU Mitgliedstaaten auch aufgefordert, Pläne zur Umsetzung der WAI-Leitlinien vorzulegen, die Leitlinien bei der Finanzierung der Entwicklung von öffentlichen Web-Inhalten zu berücksichtigen und den Dialog mit den Zielgruppen zu verstärken.

Die Einbeziehung von Benutzern in das Design ist sinnvolle Praxis, um den Zugang zu E-Voting nicht nur Technologie-affinen hinreichend benutzerfreundlich und einfach zu gestalten.

Speziell beim Entwurf von Wahlsystemen ist auf eine breite Zugänglichkeit zu achten. Dies bezieht sich sowohl auf den Zugang und die Verfügbarkeit der für die Teilnahme an elektronischen Wahlen notwendigen Komponenten (Software, etc.), als auch auf Darstellung und Repräsentation des Wahlsystems gegenüber den Wählerinnen und Wählern selbst. Hier ist bei der Darstellung und Repräsentation besonders auf ein Design zu achten, das einfach und klar ist, und das auch älteren Wählerinnen und Wählern, oder solchen mit Sehbehinderung oder anderen Einschränkun-

[43] Entschließung des Rates vom 25. März 2002 über den Aktionsplan eEurope 2002: Zugänglichkeit öffentlicher Webseiten und ihres Inhalts (2002/C 86/02)

gen eine einfache, selbstständige Bedienung ermöglicht. Die Web Accessibility Initiative (WAI) des World Wide Web Konsortium hat sich dies zum Ziel gesetzt und formuliert entsprechende Empfehlungen. (vgl. dazuTeil der rechtlichen Vorgaben der ER Empfehlungen: „*E-voting systems should be designed, as far as it is practicable, to maximise the opportunities that such systems can provide for persons with disabilities.*“)

Interoperabilität

> *6. Open standards shall be used to ensure that the various technical components or services of an e-voting system, possibly derived from a variety of sources, interoperate.*

Interoperabilität gewährleistet Unabhängigkeit von einzelnen Produkten bzw. von einzelnen Herstellern und Systemen und vermeidet die damit verbundenen finanziellen Risken eines Vendor Lock-In. Es ist die Möglichkeit der freien Wahl zwischen verschiedenen Systemen wünschenswert. Durch die Verwendung von Komponenten verschiedener Hersteller besteht auch die Möglichkeit, Komponenten einfach zu ersetzen und gegeneinander zu prüfen.

Die österreichischen E-Government Initiativen bauen aus eben diesen Gründen vorrangig auf offene Standards und offene Schnittstellen auf.

Das Konzept offene Standards und offene Schnittstellen ist von Open Source zu unterscheiden. Die Offenlegung der Quellcodes von Produkten erlaubt die Einsicht durch die breite Öffentlichkeit. Eine generelle qualifizierte Aussage, inwieweit die Möglichkeit einer Prüfung durch die Öffentlichkeit mehr Vertrauen oder höhere Qualität oder Sicherheit, als eine Akkreditierung oder Evaluierung durch Prüfstellen, die typischerweise ebenfalls Einsicht in Design und Quellcodes nehmen, ist nicht möglich.

> *7. At present, the Election Mark-up Language (EML) standard is such an open standard and in order to guarantee interoperability, EML shall be used whenever possible for e-election and e-referendum applications. The decision of when to adopt EML is a matter for member states. The EML standard valid at the time of adoption of this Recommendation, and supporting documentation are available on the Council of Europe website.*
>
> *8. In cases which imply specific election or referendum data requirements, a localisation procedure shall be used to accommodate these needs. This would allow for extending or restricting the information to be provided, whilst still remaining compatible with the generic version of EML. The recommended procedure is to use structured schema languages and pattern languages.*

Die Vorraussetzung für Interoperabilität sind offene Standards und definierte Schnittstellen. Die Election Markup Language (EML) ist eine unter OASIS[44] vor allem unter Betreiben der E-Government Initiativen des Vereinigten Königreichs[45] entwickelte Sammlung von XML-Schemata, die die Datenbeschreibung zwischen Komponenten eines E-Voting Systems spezifizieren. Eine Lokalisierungsprozedur zur Anpassung an nationale Spezifika ist definiert.

Österreich nimmt über die IKT-Stabstelle des Bundes als „Contributer “ an OASIS teil. XML ist auch wesentlicher Bestandteil der österreichischen E-Government Initia-

[44] OASIS: Internationales Komitee, das Standards und Spezifikationen für E-Business entwickelt. http://www.oasis-open.org

[45] United Kingdom, Office of the e-Envoy, neuerdings E-Government Unit

tiven. Eine Ausrichtung eines allfälligen österreichischen E-Voting Systems auf XML erscheint deshalb schon alleine aus den Synergien zu E-Government sinnvoll. EML bildet hier eine Basis. Dabei sollte auf Erfahrungen aus Pilotversuchen zurückgegriffen werden, in den EML eingesetzt wurde[46].

Systembetrieb

> *9. The competent electoral authorities shall publish an official list of the software used in an e-election or e-referendum. Member states may exclude from this list data protection software for security reasons. At the very least it shall indicate the software used, the versions, its date of installation and a brief description. A procedure shall be established for regularly installing updated versions and patches of the relevant protection software. It shall be possible to check the state of protection of the voting equipment at any time.*
>
> *10. Those responsible for operating the equipment shall draw up a contingency procedure. Any backup system shall conform to the same standards and requirements as the original system.*
>
> *11. Sufficient backup arrangements shall be in place and permanently available to ensure that voting proceeds smoothly. The staff concerned shall be ready to intervene rapidly according to a procedure drawn up by the competent electoral authorities.*
>
> *12. Those responsible for the equipment shall have procedures to ensure that during the polling period the voting equipment and its use satisfy requirements. The backup services shall be regularly supplied with monitoring protocols.*
>
> *13. Before each election or referendum, the equipment shall be checked and approved in accordance with a protocol drawn up by the competent electoral authorities. The equipment shall be checked to ensure that it complies with specifications. The findings shall be submitted to the competent electoral authorities.*
>
> *14. Any technical operations shall be subject to a formal change control procedure. Any critical changes to key equipment shall be announced.*
>
> *15. Key e-election or e-referendum equipment shall be located in a secure area and that area shall, throughout the election or referendum period, be guarded against interference of any sort and from anyone. During the election or referendum period a physical disaster recovery plan shall be in place. Furthermore, any data retained after the election or referendum period shall be stored securely.*
>
> *16. Where incidents that could threaten the integrity of the system occur, those responsible for operating the equipment shall immediately inform the competent electoral authorities, who will take the necessary steps to mitigate the effects of the incident. The level of incident which shall be reported shall be specified in advance by the electoral authorities.*

Jene Teile dieser Empfehlungen, die nicht spezifisch auf E-Voting abzielen, sind in professionellem Rechenzentrumsbetrieb Stand der Technik. Mit der Umsetzung von einschlägigen Standards wie ÖNORM A 7799 oder dem Österreichischen IT Sicherheitshandbuch sind die wesentlichen, sicherheitstechnischen Aspekte obiger Empfehlungen abgedeckt. Die in den Empfehlungen zu definierenden Prozeduren wären gesondert auf das verwendete E-Voting System abzustimmen.

Sicherheit

Der Teil Sicherheit der ER Empfehlungen wurde bereits vornehmlich von der österreichischen Delegation in der ad hoc Gruppe zu E-Voting des Europarat entwickelt.

[46] Pilotversuche bei Regionalwahlen im Vereinigten Königreich und bei Referenden im Kanton Genf

Die Empfehlungen wurden an die Methodik der Entwicklung eines Common Criteria Schutzprofils angelehnt, um damit bereits die weitere Entwicklung eines solchen vorzubereiten.

Allgemeine Sicherheitsanforderungen

> *17. Technical and organisational measures shall be taken to ensure that no data will be permanently lost in the event of a breakdown or a fault affecting the e-voting system.*
>
> *18. The e-voting system shall maintain the privacy of individuals. Confidentiality of voters registers stored in or communicated by the e-voting system shall be maintained.*
>
> *19. The e-voting system shall perform regular checks to ensure that its components operate in accordance with its technical specifications and that its services are available.*
>
> *20. The e-voting system shall restrict access to its services, depending on the user identity or the user role, to those services explicitly assigned to this user or role. User authentication shall be effective before any action can be carried out.*

In Empfehlung 20 wird unter dem Begriff „User“ nicht zwischen Wählerinnen bzw. Wählern und Personal des Systembetreibers (Administratoren, Wartung, etc.) unterschieden. Für Wählerinnen und Wähler scheint ein Abstellen auf die Bürgerkarte die sinnvollste Möglichkeit zur Authentifizierung zu sein.

> *21. The e-voting system shall protect authentication data so that unauthorized entities cannot misuse, intercept, modify, or otherwise gain knowledge of authentication data or part of it. In uncontrolled environments, authentication based on cryptographic mechanisms is advisable.*

Die Formulierung stellt einen Kompromiss zwischen Wahlmaschinen im Wahllokal und der Distanzwahl dar. In ersterem Fall können allenfalls organisatorische Maßnahmen technische ersetzen. Für die Distanzwahl („uncontrolled environments“) sind kryptographische Verfahren vorgesehen, die in Österreich durch die elektronische Signatur mit der Bürgerkarte gewährleistet sind.

> *22. Identification of voters and candidates in a way that they can unmistakably be distinguished from other persons (unique identification) shall be ensured.*

Zur eindeutigen Identifikation von Wählerinnen und Wählern sollte wiederum auf das Konzept Bürgerkarte zurückgegriffen werden, da damit die eindeutige Identifikation über das bPK durch die auf der Bürgerkarte aufgebrachte Personenbindung gewährleistet ist.

> *23. E-voting systems shall generate reliable and sufficiently detailed observation data so that election observation can be carried out. The time at which an event generated observation data shall be reliably determinable. The authenticity, availability and integrity of the data shall be maintained.*
>
> *24. The e-voting system shall maintain reliable synchronised time sources. The accuracy of the time source shall be sufficient to maintain time marks for audit trails and observations data, as well as for maintaining the time limits for registration, nomination, voting, or counting.*
>
> *25. Electoral authorities have overall responsibility for compliance with these security requirements which shall be assessed by independent bodies.*

Sicherheitsanforderungen in der Vorwahlphase

> *26. The authenticity, availability and integrity of the voters registers and lists of candidates shall be maintained. The source of the data shall be authenticated. Provisions on data protection shall be taken into account.*

In den ER Empfehlungen wurden jeweils Vorgaben für die Verfügbarkeit, Authentizität und Integrität der in einer Phase (Vorwahl, Stimmabgabe, Auszählung) gehaltenen Daten bzw. zwischen den Phasen kommunizierten Daten gegeben. Für Sicherstellung der Authentizität und Integrität bieten sich etwa Signaturen bzw. Amtssignaturen etwa über MOA SS an.

> *27. The fact that candidate nomination and, if required, the decision of the candidate and/or the competent electoral authority to accept a nomination has happened within the prescribed time limits shall be ascertainable.*

Der zweite Teil (zur nachträglichen Zustimmung des Kandidaten) ist für Österreich nicht relevant. In Österreich kann von der Zustimmung der Kandidaten im Zuge der Einbringung eines Wahlvorschlages ausgegangen werden

> *28. The fact that voter registration has happened within the prescribed time limits shall be ascertainable.*

Österreicherinnen und Österreicher mit Hauptwohnsitz in Österreich müssen sich nicht zur Wahl registrieren, sondern werden in der Wählerevidenz geführt.

Auslandsösterreicherinnen und Auslandsösterreicher bzw. EU-Bürgerinnen und EU-Bürger mit Hauptwohnsitz in Österreich müssen sich in die Wählerverzeichnisse bzw. Europa-Wählerevidenzen und Wählerverzeichnisse eintragen. Hier sind Fristen zu verifizieren bzw. bestehen Reklamationsverfahren mit Fristen.

Wird aber in einem künftigen österreichischen E-Voting System vorgesehen, dass sich Wählerinnen und Wähler für den Wahlgang per E-Voting vorab gesondert registrieren müssen, so ist die Nachweisbarkeit der zeitgerechten Registrierung zu gewährleisten.

Sicherheitsanforderungen bei der Stimmabgabe

> *29. Data communicated from the pre-voting stage (e.g. voters registers and lists of candidates) shall be maintained in integrity. Data-origin authentication shall be carried out.*

Die Empfehlungen definieren für alle Daten, die von einer Phase in eine andere kommuniziert werden, dass die Integrität sichergestellt und die Datenquelle authentifiziert werden soll. Zur Sicherstellung der Datenintegrität kann auf verschiedene, gängige und standardisierte Verfahren zurückgegriffen werden, die auf kryptographischen Verfahren basieren. Zur Authentifizierung des Ursprungs sind elektronische Signaturen das Mittel der Wahl, damit wird auch die Integrität der Daten gewährleistet.

> *30. It shall be ensured that the e-voting system presents an authentic ballot to the voter. In the case of remote e-voting, the voter shall be informed about the means to verify that a connection to the official server has been established and the authentic ballot been presented.*

Zur Sicherstellung der Authentizität von den Wählerinnen und Wählern zugestellten Stimmzetteln sind elektronische Signaturen sinnvoll, etwa über MOA SS. Die Authentizität des empfangenen Stimmzettels kann durch Signaturprüfung festgestellt werden. Dies sollte automatisch vor der Stimmabgabe erfolgen.

> *31. The fact that a vote has been cast within the prescribed time limits shall be ascertainable.*
>
> *32. Sufficient means shall be provided to ensure that the systems that are used by the voters to cast the vote can be protected against influence that can modify the vote.*
>
> *33. Residual information holding the voter's decision or the display of the voter's choice shall be destroyed after the vote has been cast. In the case of remote e-voting, the voter shall be provided with information on how to delete, where that is possible, from the device used to cast the vote.*
>
> *34. The e-voting system shall at first ensure that a user who tries to vote is eligible to vote. The e-voting system shall authenticate the voter and shall ensure that only the appropriate number of votes per voter is cast and stored in the electronic ballot box.*

Der Term „sealed" ist ein Kompromiss, um bei Wahlmaschinen in Wahllokalen nicht notwendigerweise Verschlüsselung vorzusehen. Für Distanzwahlverfahren geben die ER Empfehlungen explizit Verschlüsselung vor (Teil der rechtlichen Vorgaben der ER Empfehlungen: „*If stored or communicated outside controlled environments, the votes shall be encrypted.*").

> *35. The e-voting system shall ensure that the voter's choice is accurately represented in the vote and that the sealed vote enters the electronic ballot box.*
>
> *36. After the end of the e-voting period, no voters shall be allowed to gain access to the e-voting system. However the acceptance of electronic votes into the electronic ballot box shall remain open for a sufficient period of time to allow for any delays in the passing of messages over the e-voting channel.*

Sicherheitsanforderungen in der Auszählung

> *37. The integrity of data communicated from the voting stage (e.g. votes, voters registers, lists of candidates) shall be maintained. Data-origin authentication shall be carried out.*

Die Empfehlungen definieren für alle Daten, die von eine Phase in eine andere kommuniziert werden, dass die Integrität sichergestellt und die Datenquelle authentifiziert werden soll. Zur Sicherstellung der Datenintegrität kann auf verschiedene, gängige und standardisierte Verfahren zurückgegriffen werden, die auf kryptographischen Verfahren basieren. Zur Authentifizierung des Ursprungs sind elektronische Signaturen das Mittel der Wahl, damit wird auch die Integrität der Daten gewährleistet.

> *38. The counting process shall accurately count the votes. The counting of votes shall be reproducible.*
>
> *39. The e-voting system shall maintain the availability and integrity of the electronic ballot box and the output of the counting process as long as required.*

Das Wahlergebnis muss innerhalb der durch das österreichische Wahlrecht auferlegten Fristen reproduzierbar sein. Neuauszählungen müssen auf Verlangen möglich sein. Daher sind alle dafür notwendigen Komponenten und Daten zu sichern.

Audit - Prüfung

Allgemeines

40. An audit system shall be designed and implemented as part of the e-voting system. Audit facilities shall be present on different levels of the system: logical, application, and technical.

41. End-to-end auditing of an e-voting system shall include recording, providing monitoring facilities, providing verification facilities. Audit systems with the features set out in sections II – V below shall therefore be used to meet these requirements.

Aufzeichnung

42. An audit system shall be open, comprehensive, and actively report on potential issues and threats.

43. An audit system shall record times, events and actions, including:
- *a.) all voting related information, including number of eligible voters, number of votes cast, number of invalid votes, counts and recounts.*
- *b.) any attacks on the operation of the e-voting systems and its communications infrastructure;*
- *c.) system failures, and malfunctions and other aspects of system compromise.*

Beobachtung

44. An audit system shall provide the ability to oversee the election or referendum and to verify that the results and procedures are in accordance with the applicable legal provisions.

45. Disclosure of the audit information to unauthorised persons shall be prevented.

46. An audit system shall maintain voter anonymity at all times.

Überprüfbarkeit

47. An audit system shall provide the ability to cross check and verify the correct operation of the e-voting system and the accuracy of the result, detecting voter fraud and proving all counted votes are authentic and all votes have been counted.

48. An audit system shall provide the ability to verify that an e-election or e-referendum has complied with the applicable legal provisions, the aim being to verify that the results are an accurate representation of the authentic votes.

Weitere Anforderungen an das Audit

49. An audit system shall be protected against attacks which may corrupt, alter or lose records in the audit system.

50. Member states shall take adequate steps to ensure that the confidentiality of any information obtained by any person while carrying out auditing functions is guaranteed.

Zertifizierung

51. Member states shall introduce certification processes that allow for any ICT (Information and Communication Technology) component to be tested and certified as being in conformity with the technical requirements described in this Recommendation.

52. In order to enhance international co-operation and avoid duplication of work, member states shall consider whether their respective agencies shall join, if they have not done so already, relevant international mutual recognition arrangements such as the European Co-operation for Accreditation (EA), the International Laboratory Accreditation Cooperation (ILAC) and the International Accreditation Forum (IAF) and other bodies of a similar nature.

Österreich nimmt an den erwähnten Gremien teil (BMWA). Zusätzlich wären mit einer Erstellung von Common Criteria Schutzprofilen für E-Voting Komponenten eine Zertifizierung unter dem Common Criteria Mutual Recognition Agreement möglich.