Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

A-SIT

Seidlgasse 22 / 9, 1030 Wien
Tel.: (+43 1) 503 19 63–0
Fax: (+43 1) 503 19 63–66

Inffeldgasse 16a, 8010 Graz
Tel.: (+43 316) 873-5514
Fax: (+43 316) 873-5520

http://www.a-sit.at
E-Mail: office@a-sit.at

DVR: 1035461
ZVR: 948166612
UID: ATU60778947

ÜBERBLICK E-VOTING

Version 1.0 vom 22.05.2018
Alexander Marsalek – alexander.marsalek@a-sit.at
Bernd Prünster – bernd.pruenster@a-sit.at

A-SIT war im Bereich E-Voting aktiv, hat etwa in den Europaratsempfehlungen zu elektronischen Wahlen 2004 und der interministeriellen Arbeitsgruppe E-Voting 2004 den Bereich technische Sicherheit mitgeprägt und Bescheinigungen zur ÖH-Wahl 2009 ausgestellt. Die seinerzeitige technologische Basis hat sich jedoch verändert, etwa durch die Omnipräsenz von Mobiltechnologien, dem Erfolg der Handy-Signatur, dem Wegfall von Java-Applets oder auch durch neue Technologien wie der *Blockchain. Des Weiteren hat sich auch der internationale rechtliche Rahmen durch neue Europaratsempfehlungen zu E-Voting (Rec(2017)5) verändert und nationale Entwicklungen wie die Entscheidung des österreichischen Verfassungsgerichtshofs (VfGH) zur ÖH-Wahl sind ebenfalls zu berücksichtigen. Dieses Dokument präsentiert, aufbauend auf den zuvor genannten international und national gegebenen Grundlagen, einen Technologieüberblick unter Berücksichtigung aktueller technologischer Entwicklungen. Des Weiteren werden insbesondere für Österreich realistische Möglichkeiten aufgezeigt, wie die Ergänzung von Briefwahl mit elektronischen Methoden möglich wäre.*

Inhaltsverzeichnis

Inhaltsverzeichnis 1
1. Einleitung 2
2. Hintergrund und Historisches 2
2.1. Wahlphasendefinition im Rahmen von OASIS EML 2
2.2. Europaratsempfehlungen zum Thema E-Voting 3
2.3. ÖH-Wahl 2009 3
2.4. E-Voting-Konzept EVITA 4
2.5. E-Voting außerhalb Österreichs 6
2.5.1. Elektronisches Distanzwahlsystem in Estland 6
2.5.2. E-Voting in der Schweiz 7
3. Anforderungen an Wahlprozesse 8
3.1. Rechtlich-Organisatorisches 8
3.2. Technische Voraussetzungen 9
3.3. Bedingungen an Internetverfügbarkeit 10
4. Allgemeine Technische Konzepte und Modelle 10
4.1. Traditionelles Wahlverfahren in elektronischer Form 11
4.2. Anonyme Kommunikationskanäle 11
4.3. Wahlverfahren auf Basis blinder Signaturverfahren 12
4.4. Wahlverfahren auf Basis von homomorpher Verschlüsselung und Zero-Knowledge Proofs 13
4.5. Secret Sharing und Schwellwert-Kryptosysteme 14
4.6. Blockchain-basierte Wahlverfahren 14
4.6.1. Voting mit Rechenleistung 15
4.6.2. Voting mit Guthaben 15
4.6.3. Voting mit „Voting"-Token 15
5. Sicherheit von Endgeräten 16
6. Fazit 17
Referenzen 17

© A-SIT, Partner für Sicherheitsfragen

1. Einleitung

Im Rahmen dieser Studie sollen technische Möglichkeiten zur Durchführung geheimer elektronischer Distanzwahlen in Österreich analysiert werden. Im Fokus steht dabei eine potentielle Umsetzung des aktiven Wahlrechts, bzw. des Vorgangs der Stimmabgabe, sowie alle vor- und nachbereitenden Prozesse. Zwar war A-SIT bereits im Bereich E-Voting aktiv und hat etwa in den Europaratsempfehlungen zu elektronischen Wahlen 2004 [1] und der interministeriellen Arbeitsgruppe E-Voting 2004 den Bereich technische Sicherheit mitgeprägt und Bescheinigungen zur ÖH-Wahl 2009 ausgestellt, allerdings haben sich die technischen Gegebenheiten seither maßgeblich verändert. Besonders relevant sind in diesem Zusammenhang die hohe Verbreitung von leistungsfähigen Mobilgeräten (Smartphones), der gleichzeitige Wegfall von Java-Applets[1], sowie Entwicklungen im Blockchain-Umfeld, welche teilweise auch im Bereich E-Voting als Hoffnungsträger gehandelt werden. Der Fokus dieser Studie liegt dabei auf geheimen Wahlen und der Analyse von Möglichkeiten, diese in Form elektronischer Distanzwahlen in Österreich umzusetzen. Kein Schwerpunkt dieses Dokuments ist E-Partizipation, wie z.B. die elektronische Unterstützung von Volksbegehren, da (zumindest innerösterreichisch) die technischen, sowie auch die gesetzlichen Möglichkeiten und teilweise auch konkrete, gesetzlich geregelte Umsetzungen gegeben sind (siehe auch Volksbegehrengesetz 2018 [2]). Beispielsweise können Unterstützungserklärungen sowie Stimmen für Volksbegehren in Österreich bereits über das Internet (nach Identifikation mittels Bürgerkarte oder Handy-Signatur) abgegeben werden.
Nachfolgend werden zuerst Hintergründe, bestehende und in der Vergangenheit eingesetzte Verfahren, sowie E-Voting außerhalb Österreichs beleuchtet, um eine Einordnung technischer Konzepte und Verfahren zu erleichtern. Anschließend werden allgemeine Anforderungen an die Durchführung demokratischer Wahlen in Österreich unabhängig von technischen Möglichkeiten diskutiert. Aufbauend darauf wird ein Überblick über technische Konzepte, welche diese Anforderungen erfüllen könnten, gegeben.

2. Hintergrund und Historisches

In Österreich wurden bereits elektronische Distanzwahlen durchgeführt. Beispielsweise kam 2009 im Rahmen der ÖH-Wahl E-Voting zum Einsatz [3]. Die Umsetzung der elektronischen Distanzwahl wurde in diesem Fall vielfach kritisiert und tatsächlich wurde die entsprechende E-Voting-Verordnung vom Verfassungsgerichtshof für gesetzeswidrig erklärt [4]. Allerdings wurde dabei nicht die technische Umsetzung oder E-Voting an sich in Frage gestellt. Vielmehr wurden organisatorische Versäumnisse festgehalten. Beispielsweise wurde konkret bemängelt, dass nicht klar geregelt ist, wie die Wahlkommission ihren Pflichten nachkommen soll, bzw. dass die eingesetzten Prozesse insbesondere in der Nachwahlphase eine unabhängige Überprüfung des Wahlergebnisses nicht zufriedenstellend durchführen lassen (siehe Abschnitt 2.3). Daher ist bei eventuellen zukünftigen Konzepten auf größtmögliche Transparenz und klare organisatorische Vorgaben zu achten. Des Weiteren können Zweifel am Zustandekommen von Wahlergebnissen mit kryptografischen Verfahren (siehe Abschnitt 4) ausgeräumt werden, da Methoden existieren, die den Einbezug jeder einzelnen Stimme in ein Wahlergebnis mathematisch beweisbar machen. Nachfolgend werden weitere Details zu früheren Bemühungen, Konzepten, Vorarbeiteten und Erkenntnissen behandelt.

2.1. Wahlphasendefinition im Rahmen von OASIS EML

Ein internationaler Standard für Abwicklung elektronischer Wahlprozesse ist die auf XML basierende *OASIS Election Markup Language* (EML) [5]. Diese Spezifikation definiert elektronische Wahlprozesse gesetzes- und technologieunabhängig und ist daher bezüglich konkreter Abläufe bewusst abstrakt gehalten. Im Speziellen werden keine Anforderungen an die Kommunikation zwischen Wahlbehörde und Wahlberechtigten gestellt. OASIS EML umfasst sowohl alle Elemente der Vorwahlphase, der Stimmabgabe, als auch der Nachwahlphase. Dabei sind sowohl Personen-, bzw. Parteiwahlen als auch Referenda, wie z.B. Volksabstimmungen berücksichtigt.
Folgende Prozesse werden der Vorwahlphase zugeordnet:

[1] Im Rahmen der ÖH-Wahl wurden Java-Applets eingesetzt.

- Nominierung von Kandidaten, bzw. Optionen im Fall eines Referendums, bzw. eines Entscheids, oder einer Volksabstimmung
- Registrierung von Wahlberechtigten; dabei spielt die zweifelsfreie Identifizierung von Personen eine besondere Rolle, um deren Wahlberechtigung zu ermitteln. Das Ergebnis dieses Prozesses ist ein Wählerverzeichnis, welches an einem zuvor festgelegten Zeitpunkt am Ende der Vorwahlphase eingefroren wird. Wahlberechtigt sind jene Personen, welche in das Wählerverzeichnis aufgenommen wurden.

Der Wahlphase ist als einzige Aktivität die Stimmabgabe zugeordnet. EML sieht explizit eine Entscheidung des Wählers, bzw. der Wählerin vor, ob eine Stimmabgabe im Rahmen traditioneller Präsenzwahl, postalischer Distanzwahl, oder elektronischer Verfahren stattfinden soll. Die technischen Details des Prozesses sind nicht definiert. Im Fall eines Wahlzwangs ist noch im Rahmen der Wahlphase ein Prozess vorgesehen, um die Gründe für eine nicht erfolgte Stimmabgabe zu eruieren.

Die Nachwahlphase orientiert sich stark an traditionellen (Präsenz-)Wahlverfahren und definiert die folgenden Aktivitäten:

- Ein Wahl-Report-Prozedere, welches Stimmauszählung und Analyse der Ergebnisse beinhaltet. Eine Neuauszählung entspricht einem erneuten Durchlauf des Prozederes.
- Ein Audit, im Rahmen dessen das Zustandekommen des Wahlergebnisses nachvollzogen werden können muss. Im Zuge eines Audits muss auch eine Neuauszählung möglich sein.

OASIS EML ist hier angeführt, da dieser internationale Standard eine Basis der Empfehlungen des Europarats zu E-Voting, war. Wenngleich abstrakter als der technische Standard formuliert und allgemeine Anforderungen und Verpflichtungen definierend, ergänzen sich die Europarats-Empfehlungen und OASIS EML und werden im folgenden Abschnitt zusammengefasst.

2.2. Europaratsempfehlungen zum Thema E-Voting

In den vergangenen Jahren entwickelte der Europarat Empfehlungen zum Thema E-Voting. Aktuell sind diese als Empfehlung *CM/REC(2017)5* [6] verfügbar und verstehen sich als Neuevaluierung und Aktualisierung früherer Empfehlungen. Als Motivation, E-Voting voranzutreiben, werden unter anderem folgende Gründe genannt:

- Erleichterung der Stimmabgabe
- Ermöglichung von Distanzwahl
- Einfache Teilnahme an Wahlen für Wählberechtige, welche sich zum Zeitpunkt von Wahlen im Ausland aufhalten
- Erhöhte Barrierefreiheit
- Höhere Wahlbeteiligung durch die Verfügbarkeit alternativer Kanäle zur Stimmabgabe
- Anpassung des Wahlsystems an aktuelle gesellschaftliche und technologische Entwicklungen
- Langfristige Kostenreduktion
- Zuverlässige und schnellere Abwicklung der Nachwahlphase

Ganz allgemein werden als Grundvoraussetzungen an E-Voting-Systeme die Wahrung von demokratischen Grundrechten, sowie Sicherheit, Zuverlässigkeit und Transparenz genannt. Unter anderem sind die auch aus nationalen Gesetzen bekannten Standards für demokratische Wahlen detailliert beschrieben und daraus abgeleitete Voraussetzungen für E-Voting abgeleitet. Diese Anforderungen werden in Abschnitt 3 erneut aufgegriffen und im Kontext der österreichischen Gesetzeslage diskutiert. Zuvor werden jedoch Vorarbeiten zum Thema E-Voting in Österreich diskutiert.

2.3. ÖH-Wahl 2009

Vorangetrieben vom Bundesministerium für Wissenschaft und Forschung wurden in Österreich 2009 Internetwahlen im Rahmen der Wahl der Bundesvertretung der Österreichischen Hochschülerinnen-

und Hochschülerschaft („ÖH-Wahl“) pilotiert [3]. Mit der Durchführung wurde die Bundesrechenzentrum GmbH betraut [7]. Technisch-organisatorisch wurde die Wahrung des Wahlgeheimnisses über asymmetrische Kryptografie und entsprechenden Richtlinien betreffend der Verwaltung des kryptografischen Schlüsselmaterials gewährleistet [8]. Stimmen werden vom Wähler, bzw. der Wählerin mit dem öffentlichen Schlüssel der Wahlkommission verschlüsselt an die durchführende Behörde übertragen. Die zur Auszählung notwendige Entschlüsselung erforderte die Kooperation mehrerer Mitglieder der Wahlkommission (siehe Abschnitt 4.5). Dadurch konnten weder die Behörde noch einzelne Personen das Wahlgeheimnis verletzen. Die Identifikation von Wahlberechtigten wurde mittels Bürgerkarte umgesetzt. Wahlschluss für die elektronische Stimmabgabe war vier Tage vor Öffnung der Wahllokale. Generell war E-Voting im Rahmen der ÖH-Wahl 2009 „analog zu den Grundsätzen der Briefwahl ausgerichtet“ und „umfasst[te] neben mehreren Sicherheitsstufen auch ein System, dass sehbehinderten oder blinden Studierenden die Stimmabgabe per Computer ermöglicht“ [3].

Im Jahr 2011 wurde die ÖH-Wahl vom österreichischen Verfassungsgerichtshof (VfGH) im Wesentlichen auf Grund von Unzulänglichkeiten der Wahlordnung im Zusammenhang mit E-Voting aufgehoben [4]. Insbesondere wurden keine Bedenken bezüglich der technischen Umsetzung geäußert. Problematisch war die zum Zeitpunkt der ÖH-Wahl 2009 relevante Wahlordnung laut VfGH in folgenden Punkten:

- Der Wahlkommission sei zu großer Ermessensspielraum bei der Durchführung ihrer Aufgaben eingeräumt worden.
- Konkret sei nicht hinreichend geregelt gewesen, wie die Wahlkommission über Einsprüche wegen Verletzung der Bestimmungen über das Wahlverhalten bei elektronischer Stimmabgabe entscheiden soll.
- Der Quellcode der eingesetzten Wahlsysteme sei möglichst der Öffentlichkeit zugänglich zu machen und nicht wie im Falle der ÖH-Wahl 2009 lediglich der Wahlkommission und Beobachtern nach Unterzeichnung einer Verschwiegenheitserklärung zeitlich begrenzter Zugriff zu gewähren [8].
- Die ausgewählten Wahltage für die vorgezogene Stimmabgabe per E-Voting hätten den gesetzlichen Vorgaben des Hochschülerinnen- und Hochschülerschaftsgesetzes von 1998 [9] widersprochen.

Insgesamt ergibt sich aus diesem Erkenntnis vor allem die Notwendigkeit, E-Voting derart gesetzlich zu verankern, dass offene organisatorische Fragen im Zusammenhang mit elektronischer Stimmabgabe hinreichend geklärt sind. Konzepte für internetgestützte elektronische Distanzwahlen, welche den gesetzlichen Ansprüchen an demokratische Wahlen genügen, gibt es auf Basis unterschiedlichster technischer Ansätze. Ein solches Konzept wird nachfolgend vorgestellt.

2.4. E-Voting-Konzept EVITA

Im Jahr 2007 wurde das E-Voting-System *EVITA* im Rahmen einer Dissertation diskutiert [10], was auch teils in Kooperation mit A-SIT erfolgte. Dabei handelt es sich um ein umfassendes System, welches Empfehlungen für technische Eigenschaften, organisatorische Rahmenbedingungen, sowie Prozesse für die Durchführung elektronischer Distanzwahlen definiert. Da sich das Umfeld im vergangenen Jahrzehnt auf Grund diverser technischer Entwicklungen massiv verändert hat, und sich beispielsweise auch Nutzergewohnheiten hin zu Mobilgeräten verlagert haben [11], sind besonders die wählerseitigen Eigenschaften des Konzepts unter Berücksichtigung aktueller Umstände neu zu evaluieren. Andere, meist abstrakte Eigenschaften des EVITA-Systems, sowie insbesondere die Verwaltung kryptografischen Materials haben hingegen nach wie vor Gültigkeit.

EVITA beruht auf verpflichtender organisatorischer Trennung zwischen einer Wähler-Registrierungsstelle und der Wahlbehörde, sowie asymmetrischer kryptografischer Verfahren. Die Wahrung des Wahlgeheimnisses wird durch die Verwendung eines Hardware Security Module (HSM) sichergestellt. Ein Wahlvorgang wird wie folgt durchgeführt:

- Wählerinnen und Wähler identifizieren sich mittels eID gegenüber der Registrierungsstelle.

- Die Registrierungsstelle ist dafür zuständig, an Wählerinnen und Wähler, die ihre Stimme elektronisch abgeben möchten, Stimmzettel und eindeutige Wähler-IDs, bzw. Wahltoken auszustellen.
- Beides wird von der Registrierungsstelle signiert.
    - Die Wahltoken sind an sich anonym, da sie keinerlei personenbezogene Daten enthalten.
    - Prinzipbedingt kann die Registrierungsstelle jedoch eine Verknüpfung zwischen Wahltoken und Wählerin, bzw. Wähler herstellen.
    - Um geheime Wahlen sicherzustellen, darf die Registrierungsstelle folglich nie Zugang zu ausgefüllten Stimmzetteln erhalten.
- Wählerinnen und Wähler können die Authentizität der Stimmzettel und Token überprüfen, indem sie die Signatur der Registrierungsstelle verifizieren.
- Die Wählerin, bzw. der Wähler füllt den Stimmzettel aus und verschlüsselt diesen unter dem öffentlichen Schlüssel der Wahlbehörde.
- Optional kann eine blinde Signatur des Stimmzettels seitens der Registrierungsstelle angefordert werden.
- Die Wählerin, bzw. der Wähler signiert Stimmzettel und Token.
- Nach erfolgreicher eID-basierter Identifikation gegenüber der Wahlbehörde werden verschlüsselter Stimmzettel und Token übermittelt.
- Die Wahlbehörde überprüft Gültigkeit des Token (und optional die blinde Signatur des Stimmzettels) indem die Signatur der Registrierungsstelle verifiziert wird.
- Die Wahlbehörde überprüft die Zuordnung von Stimmzettel und Token zum Wähler, bzw. zur Wählerin mittels Signaturprüfung.
- Der Wähler, bzw. die Wählerin erhält eine Bestätigung, dass die Stimme erfasst wurde.
- Die Entschlüsselung der Stimmen erfolgt im Rahmen der Stimmauszählung innerhalb eines Hardware Security Module.

Ein schematischer Ablauf dieses Wahlvorgangs ist in Abbildung 1 dargestellt. Durch den Verzicht auf Verfahren wie z.B. homomorphe Verschlüsselung und anonyme Übertragungskanäle bei gleichzeitigem Einsatz eines HSMs ergeben sich weitere Anforderungen, deren Einhaltung jedoch insgesamt zu Vorteilen gegenüber kryptografisch komplexeren Wahlsystemen führen kann.
Besonders die Verwendung eines HSMs zur Stimmauszählung garantiert, dass keine Korrelation zwischen Wählerinnen und Wählern und deren Stimmen hergestellt werden kann. Das innerhalb des HSMs ausgeführte Programm, sowie das zur Entschlüsselung notwendige kryptografische Schlüsselmaterial ist durch vielschichtige Sicherheitsmechanismen vor Manipulationen geschützt. Des Weiteren kann dieses Schlüsselmaterial nicht ohne weiteres exportiert werden, bzw. nur für den Import in andere HSMs verschlüsselt übertragen werden. In jedem Fall ist es zu keinem Zeitpunkt, bzw. nur unter real nicht annehmbaren, hohem Kostenaufwand möglich, den zur Stimmentschlüsselung notwendigen kryptografischen Schlüssel zu exportieren.

Das EVITA-Konzept erfordert jedoch Vertrauen in die beteiligten Behörden, wie Registrierungsstelle und Wahlbehörde, ebenso wie Vertrauen in die organisatorischen Prozesse. Wählerinnen und Wähler müssen schlicht daran glauben, dass es zu keinem Datenaustausch zwischen Registrierungsstelle und Wahlbehörde kommt, und dass Stimmen tatsächlich nur im HSM direkt ausgezählt werden und nur ein Endergebnis, aber keine einzelnen, den Wählerinnen und Wählern zuordenbaren Stimmen veröffentlicht werden. Gesetzlich geregelte organisatorische Vorschiften und Prozesse, sowie die Veröffentlichung des Quellcodes eingesetzter Komponenten können diesen Glauben bestärken. Allgemein ist jedoch davon auszugehen, dass Bürgerinnen und Bürger keinem wie auch immer gearteten Wahlsystem vertrauen werden, wenn sie nicht daran glauben, dass der Staat die eigenen Gesetze befolgt.

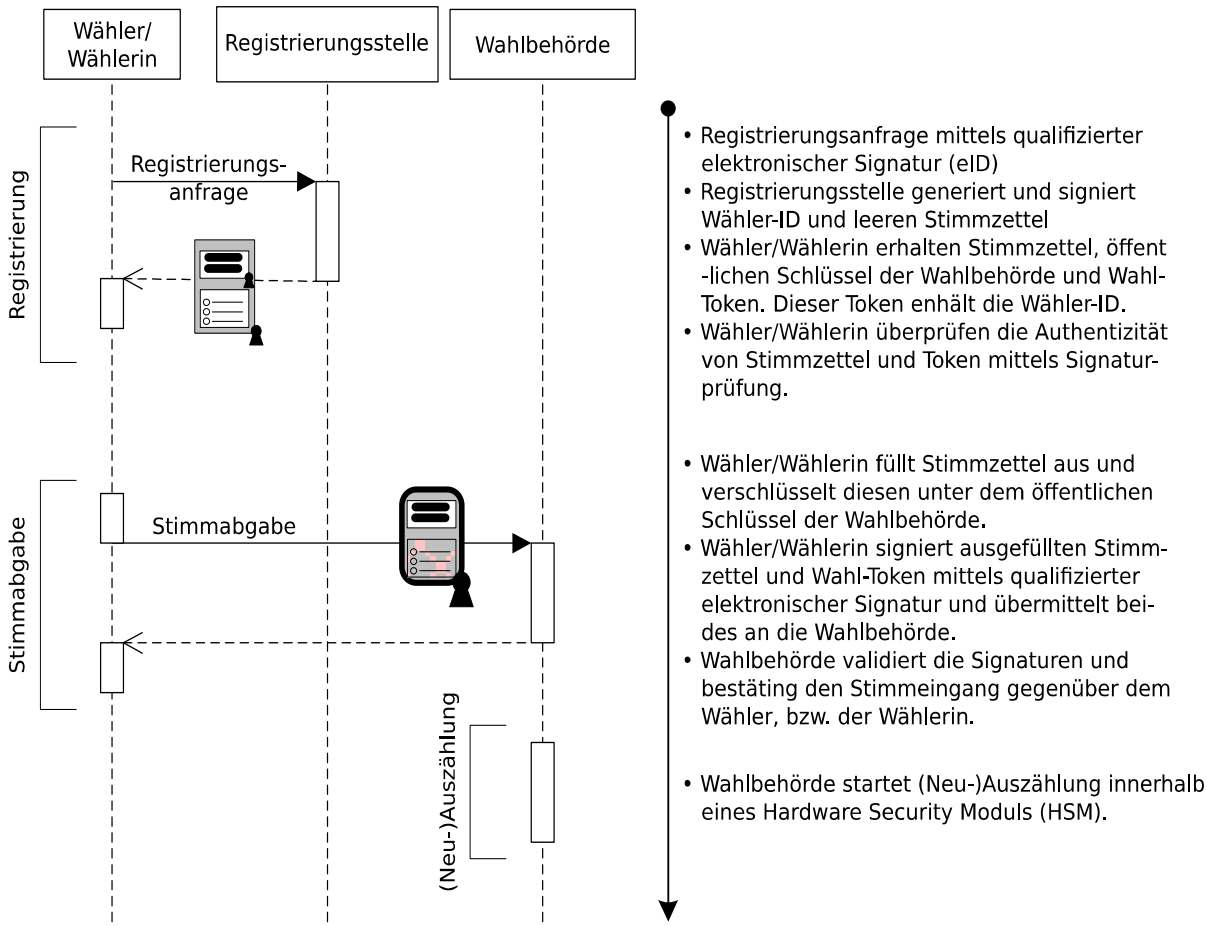

Abbildung 1: Wahlprozess im Rahmen von EVITA

Außerhalb Österreichs wurde bzw. wird E-Voting für demokratische Wahlen bereits flächendeckend eingesetzt. Details hierzu werden nachfolgend diskutiert.

2.5. E-Voting außerhalb Österreichs

Im Kontext von Internet-Voting wird die Umsetzung von E-Voting in Estland vielfach als Erfolgsgeschichte genannt. Was das Umfeld, bzw. die Vorbedingungen für E-Voting betrifft, gibt es durchaus Parallelen zwischen Österreich, bzw. den technischen Konzepten, welche im Rahmen der ÖH-Wahl 2009 eingesetzt wurden, und der Situation in Estland: Auch in Estland gibt es schon seit Jahren eID-Lösungen (ebenfalls auf Smartcard-Basis), welche eine Voraussetzung für die Identifikation im Rahmen vollelektronischer Distanzwahl darstellt [12]. Allerdings wurde E-Voting in Estland bereits um die Jahrtausendwende forciert und die gesetzlichen Vorgaben bestehen bereits seit 2002.
Die Schweiz hat ebenfalls eine langjährige Tradition im Bereich E-Partizipation und E-Voting. Beispielsweise wurde E-Voting bereits 1998 in den Kantonen Genf, Zürich und Neuchâtel pilotiert [13]. Auch in Ländern wie den Niederlanden [14] und Norwegen [15] wird, bzw. wurde E-Voting eingesetzt. Teils wurden aber Pilotprojekte auch nicht weiter verfolgt. Es wird nachfolgend zuerst auf die Umsetzung in Estland und anschließend auf elektronische Distanzwahlen in der Schweiz als zwei Beispiele eingegangen, in denen E-Voting mehrmals erfolgreich eingesetzt wurde.

2.5.1. Elektronisches Distanzwahlsystem in Estland

Das elektronische Distanzwahlsystem Estlands ähnelt in Grundzügen dem bereits in Abschnitt 2.4 beschreiben E-Voting-System EVITA. Zwar wurde das System 2014 erweitert, um Wählerinnen und Wählern die Möglichkeit einzuräumen, zu überprüfen, dass ihre Stimmen unverändert erfasst wurden. Konzeptionell ändert dies jedoch nichts an der grundlegenden Architektur [16].

Für die Stimmabgabe kommt eine so genannte *i-voting client application* (IVCA) zum Einsatz, welche auf den Endgeräten der Wählerinnen und Wähler betrieben wird. Diese ist an das *i-voting system* (IVS) angebunden, welches aus den folgenden Komponenten besteht:

- *Vote Forwarding Server* (VFS), welcher für Authentifizierung von Wählerinnen und Wählern, sowie für Auslieferung und Abnahme von Stimmzetteln zuständig ist
- *Vote Storing Server* (VSS), welcher für die Speicherung und Anonymisierung eingehender Stimmzettel verantwortlich ist.
- *Vote Counting Server* (VCS), welcher die Auszählung durchführt.

Das IVS verfügt über ein public/private key pair, dessen privater Teil in einem HSM gespeichert ist. Abgegebene Stimmen werden unter dem öffentlichen Teil dieses Schlüssels verschlüsselt, das resultierende Kryptogramm wird vom Wähler, bzw. der Wählerin signiert und anschließend an den VFS übertragen. Vor Wahlschluss können beliebig viele Stimme abgegeben werden. Gewertet wird jedoch nur die zuletzt abgegebene. Nach Wahlschluss wird die qualifizierte elektronische Signatur der Wähler entfernt und die dadurch anonymisierten Stimmen werden an den VCS übertragen. Eine Entschlüsselung der Stimmzettel ist nur möglich, wenn sich eine Mehrheit des nationalen estnischen Wahlkomitees gegenüber dem HSM (ähnlich eines Schwellwertkryptosystems, siehe Abschnitt 4.5) authentifiziert.
Verifizierbarkeit wurde wie folgt umgesetzt: Elektronische Stimmabgabe ist nur auf Desktop-Computern, bzw. Laptops vorgesehen. Zusätzlich zur Stimme wird ein vom Wähler, bzw. der Wählerin frei wählbarer Zufallswert als Teil der Stimme verschlüsselt. Nach Abgabe der Stimme wird dem Wähler, bzw. der Wählerin eine Stimmreferenz übermittelt. Auf Basis dieser Referenz kann die anonymisierte Stimme (bis zu drei Mal) abgerufen werden. Anschließend erzeugt der Wähler, bzw. die Wählerin von einem Mobilgerät aus erneut dieselbe Stimme, bezieht erneut den zuvor ausgewählten Zufallswert ein und verschlüsselt diese Daten. Deckt sich das resultierende Kryptogramm mit der an Hand der Referenz abgerufenen Stimme, so handelt es sich tatsächlich um die gleiche Stimme. Durch den Einbezug eines weiteren Geräts lässt sich (hinreichend) sicherstellen, dass es zu keiner Verfälschung der abgegebenen Stimme (z.B. durch Malware am Gerät, das für die Stimmabgabe benutzt wurde) gekommen ist.

2.5.2. E-Voting in der Schweiz

In der Schweiz kommt aktuell das in Teilen als Open-Source-Software veröffentlichte E-Voting-System *CHVote* in den Kantonen Basel-Stadt, Bern, Genf und Luzern als eines von zwei akkreditierten E-Voting Systemen zum Einsatz [17]. Abgesehen davon gab es schweizweit bereits mehr als 200 Einsätze elektronischer Distanzwahlsysteme um E-Voting zu evaluieren [18]. In der Schweiz wird E-Voting auch für Entscheide im Sinne der direkten Demokratie eingesetzt. Aus der offiziellen CHVote-Dokumentation geht hervor, dass die Sicherheit von E-Voting in der Schweiz nicht notwendigerweise auf kryptografischen Verfahren, sondern auf Prozessen beruht, welche weder HSMs noch komplexe Kryptosysteme voraussetzen [19]. So wird kritisches kryptografisches Schlüsselmaterial auf USB-Sticks oder CD-Roms gespeichert und von einem Polizeibeamten sicher verwahrt. Passwörter, welche benötigt werden um auf das für die Auszählung erforderliche Schüsselmaterial zuzugreifen, wird in Papierform in versiegelten Kuverts von einem Notar verwahrt. Die Auszählung erfolgt offline auf einem ebenfalls während der Wahlphase sicher verwahrten Laptops (in dieser Zeit ist der Laptop somit unzugänglich). Authentifikation und Wahrung des Wahlgeheimnisses wird ebenfalls durch strikt definierte Prozesse und weniger durch kryptografische Verfahren erreicht. Beispielsweise kommt keine qualifizierte elektronische Signatur im Rahmen eines Identitätsnachweises zum Einsatz. Stattdessen, identifiziert/authentifiziert sich ein Wähler, bzw. eine Wählerin mit einer einem Stimmrechtsausweis zu entnehmender Identifikationsnummer. Die Wahrung des Wahlgeheimnisses ist insofern garantiert, als dass Prozesse es verbieten, Stimme und personenbezogene Daten zusammenzuführen.
Der Umstand, dass sich Schweizer E-Voting-Systeme in vielen Punkten gravierend von anderen E-Voting-Systemen unterscheiden, wurde auch 2011 in einem Bericht der Berner Fachhochschule festgehalten [20]. Unter anderem wurde damals hervorgehoben, dass Schweizer Systeme technisch keine Verifizierbarkeit vom Wahlergebnissen zulassen. Dies deckt sich auch mit der aktuellen Beschreibung des Systems CHVote, welches lediglich eine Testurne und Teststimmen im Rahmen

einer Plausibilitätsprüfung vorsieht. Wenngleich keine technisch-kryptografische Sicherheit gegeben ist und Transparenz und Verifizierbarkeit technisch nicht umsetzbar sind, so ist die Akzeptanz vergangener und aktueller Schweizer E-Voting-Systeme ein Indikator dafür, dass sich Bürgerakzeptanz unabhängig von der technisch-kryptografischen Sicherheit eines Systems ausbilden kann.

Ein Vorteil der prozessbasierten Sicherheit und notarieller Beglaubigung gegenüber komplexer kryptografischer Verfahren ist, dass die Sicherheitsgarantien solcher Systeme auch vom Durchschnittsbürger und der Durchschnittsbürgerin ohne Spezialwissen aus den Bereichen Kryptografie, Informationssicherheit und Mathematik nachvollzogen werden können. Dies kann ebenfalls ein nicht zu vernachlässigender Erfolgs- oder Misserfolgsfaktor im Rahmen einer Einführung von E-Voting sein. Eine allgeimene Zusammenfassung von Anforderungen an Wahlprozesse findet sich im nachfolgenden Abschnitt.

3. Anforderungen an Wahlprozesse

Als Basis für die Evaluierung technischer Umsetzungsmöglichkeiten für elektronische Distanzwahl werden die Grundsätze des österreichischen Wahlrechts [21], sowie das Bundesgesetz über die Wahl des Nationalrates (Nationalrats-Wahlordnung 1992 – NRWO) [22] herangezogen. Sowohl die rechtlich-organisatorischen Grundsätze als auch die technischen Anforderungen decken sich im Wesentlichen mit den entsprechenden Europaratsempfehlungen [6]. Ziel dieses Abschnitts ist nicht die gesamte österreichische Wahlordnung und die Europaratsempfehlungen wiederzugeben, sondern jene im Zusammenhang einer möglichen Umsetzung von elektronischen Distanzwahlen relevanten Aspekte zusammenzufassen, sodass die technische Erfüllbarkeit evaluiert werden kann.

3.1. Rechtlich-Organisatorisches

Prinzipiell müssen in Österreich laut geltender Gesetzeslage folgende Anforderungen an demokratische Wahlen erfüllt sein:

- **A1** Allgemeines Wahlrecht: Alle österreichischen Staatsbürgerinnen und Staatsbürger haben das Recht zu wählen, sobald das Wahlalter erreicht ist. Dieses Recht gilt unabhängig von Klasse, Geschlecht, Bildung, etc. Insbesondere muss dieses Recht auch unabhängig z.B. von technischer Kompetenz wahrnehmbar sein.
- **A2** Gleiches Wahlrecht: Jede Stimme hat den gleichen Einfluss auf das Wahlergebnis. Im speziellen darf es nicht möglich sein, eine Stimme mehrfach abzugeben, bzw. generell mehrfach zu Wählen.
- **A3** Unmittelbares Wahlrecht: Abgeordnete werden direkt gewählt. Delegative Demokratie (auch bekannt als *Liquid Democracy*[2]) und Wahlmännersysteme sind nicht erlaubt.
- **A4** Persönliches Wahlrecht: Wahlberechtigte müssen ihre Stimme „persönlich vor einer Wahlbehörde oder vor einem mit der Abwicklung der Wahl betrauten Staatsorgan“ [21] abgeben, bzw. im Falle einer Briefwahl ist eine eidesstattliche Erklärung unterzeichnen, die besagt, dass die Stimme persönlich, unbeobachtet und unbeeinflusst abgegeben wurde.
- **A5** Geheimes Wahlrecht: Wählerinnen und Wählern wird garantiert, dass ihre Stimme unbeobachtet abgegeben werden kann und zu keinem Zeitpunkt zuordenbar, bzw. nachvollziehbar ist.
- **A6** Freies Wahlrecht: „Wählerinnen und Wähler dürfen völlig frei entscheiden und sollen keinesfalls durch Zwang oder Druck in ihrer Wahl beeinträchtigt werden“ [21].

Diese Grundsätze sind im Rahmen persönlicher Wahlen verhältnismäßig einfach umsetzbar. Gleiches Wahlrecht (A2) bedeutet auch, dass alle Wahlberechtigten genau eine Stimme abgeben können. Dadurch, dass Stimmzettel (auch im Sinne geheimer Wahlen (A5)) kuvertiert abgegeben werden, ist eine diesbezügliche Garantie bei der Wahrnehmung des persönlichen Wahlrechts durch Wahlbeisitzer gewahrt: Spätestens bei der Auszählung würden Wahlkuverts, welche mehr als einen Stimmzettel enthalten, zu ungültigen Stimmen führen.

[2] https://wiki.p2pfoundation.net/Liquid_Democracy

Da für eine Stimmabgabe mittels Briefwahl dieselben, nicht zuordenbaren Stimmzettel und Wahlkuverts verwendet werden, können auch hier dieselben Garantien erreicht werden. Wenn gewährleistet werden kann, dass auch im Rahmen elektronischer Distanzwahlen pro Wählerin, bzw. pro Wähler nur ein Stimmzettel ausgestellt werden kann, dieser auch nur einmal abgegeben werden kann, und die Stimme keiner, bzw. keinem Wahlberechtigen zuordenbar ist, kann die aktuelle Praxis für Briefwahlen auch als Anhaltspunkt für elektronische Distanzwahlen herangezogen werden. Nachfolgend werden die technischen Voraussetzungen für die Umsetzung von E-Voting im Sinne demokratischer Wahlen diskutiert.

3.2. Technische Voraussetzungen

Ausgehend von den geltenden Grundsätzen für demokratische Wahlen ergeben sich eine Reihe von technischen Bedingungen, die (unabhängig von der konkreten Umsetzung) erfüllt sein müssen, um gesetzeskonforme elektronische Distanzwahlen zu ermöglichen. Diese technischen Anforderungen lauten wie folgt:

- **T1** Hochqualitative elektronische Identität (eID): Wahlberechtigte müssen sich im Rahmen einer elektronischen Stimmabgabe auch elektronisch identifizieren können. Diese Identifikation muss gesetzlich geregelt sein und gleichwertig mit einer persönlichen Identifikation im Rahmen persönlicher Stimmabgabe (A4) sein.
- **T2** Qualifizierte elektronische Signatur: Einhergehend mit elektronischer Identifikation, muss auch die Möglichkeit einer qualifizierten elektronischen Signatur gegeben sein. Diese Notwendigkeit ergibt sich allerspätestens, wenn in Anlehnung an die Briefwahl eine Eidesstattliche Erklärung unterzeichnet werden soll, in der der Wähler, bzw. die Wählerin festhält, dass die Stimme im Geheimen (A5) und freien Willens (A6) abgegeben wurde. Tatsächlich wird eID in Österreich mit qualifizierter Signatur kombiniert. Bei T1 und T2 handelt es sich somit genau genommen um gesetzliche Rahmenbedingungen und weniger um technische Machbarkeit.
- **T3** Zuordenbarkeit: Ebenso wie im Rahmen persönlicher Wahl oder Briefwahl muss feststellbar sein, welcher Wähler, bzw. welche Wählerin eine (elektronische) Stimme abgegeben hat.
- **T4** Einmaligkeit: Jede abgegebene Stimme, darf nur einmal in gültiger Form vorliegen, bzw. jede Wählerin und jeder Wähler darf nur eine in die Auszählung eingehende Stimme abgeben.
- **T5** Garantierter Stimmeingang / Individuelle Verifizierbarkeit: Abgesehen von obligaten Anforderungen an Transportsicherheit, wie z.B. Vertraulichkeit und Integrität, muss die Wahlbehörde auch garantieren, dass eine auf elektronischem Weg abgegebene Stimme eingegangen ist und in die Auszählung einbezogen wird. Einhergehend mit T4 könnte ein Stimmeingang auch für den Wähler, bzw. die Wählerin verifizierbar sein. Die Erfüllung dieser Voraussetzung stellt somit einen objektiven Fortschritt gegenüber der Briefwahl dar.
- **T6** Quittierungsfreiheit: Analog zur Urnenwahl soll im Sinne der Wahrung des Wahlgeheimnisses niemand (einschließlich den Wählerinnen und Wählern) nachweisen können, wie eine Wählerin, bzw. ein Wähler abgestimmt hat.
- **T7** Allgemeine Verifizierbarkeit: Genau wie im Rahmen traditioneller Wahlen muss auch das Zustandekommen des Wahlergebnisses beim Einsatz von E-Voting allgemein nachvollziehbar und verifizierbar sein.
- **T8** Anonymität: Abgegebene Stimmen dürfen dem Wähler, bzw. der Wählerin zu keinem Zeitpunkt zuordenbar sein, um geheime Wahlen (A5) zu garantieren.

T1 kann ebenfalls als Grundvoraussetzung angesehen werden, um Mehrfachstimmen auszuschließen und damit gleiches Wahlrecht (A2) zu garantieren. Im Rahmen konventioneller Wahlprozesse kann durch strenge Vorschriften ohne Weiteres garniert werden, dass die Identität von Wählerinnen und Wählern bei der Stimmabgabe verifiziert wird, die Stimmabgabe selbst geheim erfolgt, und die spätere Auszählung keine Rückschlüsse auf was Wahlverhalten einzelner zulässt. Durch die streng geregelte Ausstellung von Wahlkarten wird auch im Falle einer Briefwahl sichergestellt, dass jeder und jede Wahlberechtige über exakt eine Stimme verfügt. Versucht man diese Prozesse auf elektronische Distanzwahlen umzulegen, ergeben sich aus den Anforderungen T3 bis T8 jedoch scheinbar Widersprüche. Anforderungen T1 und T2 sind hingegen in Österreich über Bürgerkarte und Handy-Signatur (und auch europaweit grenzübergreifend im Rahmen der

eIDAS-Verordnung [23]) bereits erfüllt. Indirekt ist auch eine breite Akzeptanz, bzw. Nutzung von eID-Verfahren in der Bevölkerung eine Grundvoraussetzung, damit elektronische Distanzwahlen auch breitenwirksam umgesetzt werden können; auch das ist in Österreich der Fall.
Auf technischer Ebene sind jedoch auch die gemeinsame Erfüllung von Zuordenbarkeit, Anonymität, Einmaligkeit, individueller und allgemeiner Verifizierbarkeit gelöst. Die verbleibenden offenen Fragen sind in diesem Zusammenhang von den konkreten Anforderungen an Wahlprozesse und vom technologischen Umfeld bzw. der Infrastruktur abhängig.
Die Anforderungen T3 bis T8 sind jedoch aus demokratischer Sicht als besonders kritisch einzustufen: Eine Grundvoraussetzung für die breite Anerkennung eines Wahlergebnisses und Vertrauen in das demokratische System ist Transparenz und Akzeptanz des Wahlprozesses seitens der Bevölkerung. Besonders bei technisch komplexen Verfahren kann dies schwer zu bewältigen sein. In jedem Fall muss ausreichend Vertrauensarbeit geleistet werden und die dafür benötigten Ressourcen, bzw. die Frage nach der prinzipiellen Lösbarkeit dieser Aufgabe muss bei der Wahl eines elektronischen Distanzwahlverfahrens ebenso berücksichtigt werden. Vorab sind jedoch Anforderungen elektronischer Distanzwahlverfahren an die Infrastruktur und das Umfeld zu klären.

3.3. Bedingungen an Internetverfügbarkeit

Eine flächendeckende elektronische Wahl auch im Sinne einer Präsenzwahl erfordert ausfallsichere Internetverbindungen in Wahllokalen. Im Kontext des aktuellen Distanzwahlsystems der Briefwahl gibt es hingegen keinerlei derartige technische Anforderungen. Beispielsweise kann eine im Rahmen einer Briefwahl beantragte Wahlkarte laut Nationalratswahlordnung [22] auch im Wahllokal abgegeben werden, bzw. die Stimme auch im Rahmen einer Präsenzwahl abgegeben werden. Insbesondere kann unter bestimmten Voraussetzungen auch ein neuer Stimmzettel ausgehändigt werden, wenn der im Rahmen der Briefwahl beantragte nicht mehr (sehr wohl aber das verschließbare Kuvert noch) zur Verfügung. In jedem Fall kann auch nach Beantragung einer Wahlkarte für eine Distanzwahl mittels Briefwahl noch eine Präsenzwahl unter den gleichen Voraussetzungen wie einer regulären Präsenzwahl erfolgen, sofern sichergestellt werden kann, dass die Stimme der Wählerin, bzw. des Wählers noch nicht per Briefwahl abgegeben wurde. Dieser Nachweis ist durch Vorlage des Briefwahlkuverts zweifelsfrei möglich. Ein derartiges Verfahren lässt sich nur dann ohne weiteres auf elektronische Distanzwahlverfahren umlegen, wenn auch in Wahllokalen eine ausfallsichere Internetverbindung zu Verfügung steht. Diese ist notwendig, um in Echtzeit nachprüfen zu können, ob eine Stimme bereits abgegeben wurde.

Ein alternativ gangbarer Weg wäre, den elektronischen Wahlschluss einige (wenige) Tage vor dem eigentlichen Wahlschluss festzulegen, damit in allen Wahllokalen ein Wählerverzeichnis vorliegt, in der erfolgte elektronisch Stimmabgabe ersichtlich ist, etwa analog des abgeschlossenen Wählerverzeichnisses mit der Anmerkung „Wahlkarte“. Zwar ergibt sich dadurch eine scheinbare Ungleichbehandlung der Wählerinnen und Wähler, welche E-Voting in Anspruch genommen haben, gegenüber dem Rest der Wählerschaft. Allerdings ist dies auch aktuell im Rahmen der Briefwahl der Fall und stellt daher keine Einschränkung dar. Im Gegenteil: Ein vorgezogener E-Voting-Wahlschluss muss nur so weit vorgezogen werden, bis aktuelle Wählerlisten in Wahllokalen verfügbar sind. Unabhängig davon hat es in der Vergangenheit in Österreich bereits mehrfach die Möglichkeit vorgezogener Stimmabgaben gegeben [24] [25]. Dabei ist es unerheblich, ob die Stimmabgabe im Wahllokal selbst ebenso auf elektronischem Weg erfolgt, oder nicht, da keine Echtzeitüberprüfung, ob bereits eine Stimme abgegeben wurde, notwendig ist.

Bewusst unabhängig davon werden nachfolgend technische Verfahren vorgestellt, welche eine geheime elektronische Distanzwahl im Sinne demokratischer Wahlen unter der Berücksichtigung der Anforderungen A1 bis A6 prinzipiell ermöglichen. Die konkreten Rahmenbedingungen, sowie bestehende und frühere elektronische Wahlsysteme werden hingegen in Abschnitt 2 diskutiert.

4. Allgemeine Technische Konzepte und Modelle

Prinzipiell können technische Verfahren zur Durchführung elektronischer Distanzwahlen an Hand ihrer Merkmale (in unterschiedlichen Dimensionen) klassifiziert werden. Diese Verfahrensklassen und Ihre Eignung im Sinne demokratischer Wahlen werden im Rahmen dieses Abschnitts diskutiert.

Auch wenn derartige Verfahren an sich keine hochaktuellen Entwicklungen darstellen, so sind diese mittlerweile praxisrelevant. Dies lässt sich einerseits auf signifikant effizientere Umsetzungen bestehender Verfahren zurückführen. Andererseits hat auch die Rechenleistung von Endgeräten erhöht, wodurch zuvor nur theoretisch interessante Konzepte praktisch nutzbar wurden.

Die Nennung eines technischen Ansatzes dient einem Überblick, eine Darstellung hier ist aber nicht als besondere Eignung in der österreichischen Infrastruktur zu verstehen. Es sollen vielmehr bekannte und aktuelle Konzepte als Anregung für mögliche Umsetzungen liefern.

4.1. Traditionelles Wahlverfahren in elektronischer Form

Ein Ansatz, elektronische Distanzwahlen umzusetzen, ist die traditionelle Präsenzwahl oder auch die Briefwahl sozusagen zu digitalisieren und die grundlegenden Prozesse de-facto unverändert beizubehalten. Die technischen Hürden dafür sind gering, besonders in Hinblick auf allgemein verfügbare eID- und qualifizierte elektronische Signaturlösungen. Wollte man Präsenzwahl in elektronischer Form umsetzen, ist ein Äquivalent zum Kuvert entsprechend abzubilden (wofür sich Verschlüsselung eignet) und der Vorgang selbst ist derart transparent zu gestalten, dass Wahlbeisitzer weiterhin ihre Aufgabe erfüllen können.
Letzteres ist im Falle elektronischer Distanzwahlen nicht notwendig und es existiert mit der Briefwahl auch das gesetzliche Rahmenwerk, welches Distanzwahlen an sich ermöglicht. Ein klarer Vorteil von elektronischer Distanzwahl gegenüber dem aktuellen Briefwahlsystem ist, dass allen Wählerinnen und Wählern der Stimmeingang bestätigt werden kann. Ohne den Einsatz kryptografischer Methoden, welche z.B. die Wahrung des Wahlgeheimnisses sicherstellen, erfordert ein solches Verfahren jedoch vollkommenes Vertrauen in die durchführenden Organe. Allerdings gibt es technische Lösungen, die entsprechende Eigenschaften und Sicherheitsniveaus garantieren können. Die Frage nach der Akzeptanz solcher Verfahren, die typischerweise nur von Personen mit einschlägigem Fachwissen nachvollzogen werden können, lässt sich jedoch nicht beantworten. Rein technisch ermöglicht der Einsatz moderner kryptografischer Konzepte und Verfahren die Erfüllung aller allgemeinen und (nahezu) aller technischen Voraussetzungen an geheime, demokratische Wahlen. Daher können die Voraussetzungen an eine „Digitalisierung der Briefwahl“ als erfüllt betrachtet werden. Vielen relevanten Verfahren ist gemein, dass sie zumindest an einem Punkt der Wahlphase anonyme Kommunikationskanäle erfordern. Daher wird dieser Aspekt vorab diskutiert.

4.2. Anonyme Kommunikationskanäle

(Wie auch immer geartete) elektronische Stimmzettel, die an sich keine auf den Wähler oder die Wählerin zurückzuführenden Merkmale enthalten, müssen, je nach Verfahren, tatsächlich anonym übermittelt werden können. Andernfalls können an Hand von Verbindungsdaten potentiell Rückschlüsse auf das Stimmverhalten von Individuen gezogen werden. Typischerweise wird dies durch den Einsatz von *Mix-Netzen* [26] oder –Kaskaden, bzw. *Onion Routing* erreicht. Dabei handelt es sich um ein Routing-Verfahren, das anonyme Kommunikation mathematisch/kryptografisch garantiert. Dafür wird der Routing-Pfad durch ein Netz aus so genannten *Mixen* vor dem Versenden der Nachricht vom Sender definiert. Jeder dieser Mixe verfügt über ein public/private key pair, dessen öffentlicher Schlüssel allgemein bekannt, bzw. abrufbar ist. Vor dem Versenden einer Nachricht wird die Nachricht in umgekehrter Folge entlang der Routing-Pfads mit den öffentlichen Schlüsseln der Mixe entlang dieses Pfades verschlüsselt (siehe Abbildung 2).

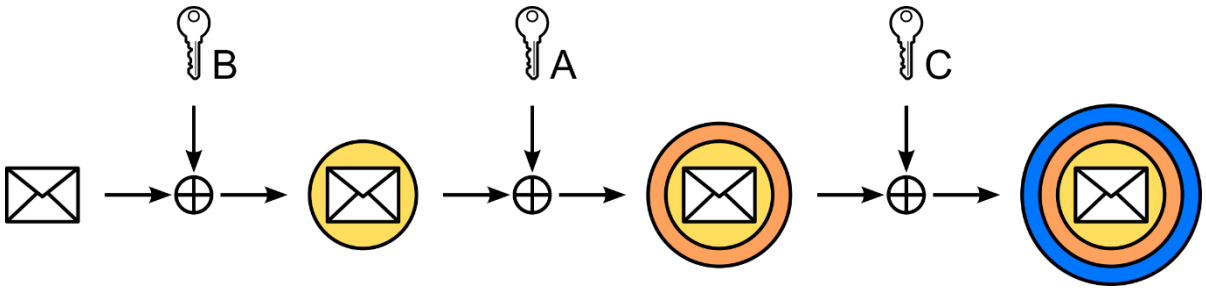

Abbildung 2:Verschlüsselung einer Nachricht vor dem Senden in ein Mix-Netz

Geht eine Nachricht an einem Mix ein, kann dieser sie nur entschlüsseln, wenn sie auch mit dem diesem Mix zugehörigen öffentlichen Schlüssel verschlüsselt wurde. Außerdem tritt (abgesehen vom letzten Abschnitt des Routingpfads, bzw. am endgültigen Empfänger angekommen) nur eine weitere Verschlüsselungsschicht, sowie die Information über den nächsten Mix entlang des Pfades zu Tage. Dadurch kann die Nachricht zwar weitergeleitet werden, jedoch nur vom endgültigen Empfänger gelesen werden. Folglich weiß jeder Mix entlang des Pfades lediglich über den vorhergehenden und nachfolgenden Abschnitt im Routingpfad Bescheid (siehe Abbildung 3). Auf Grund dieser mehrlagigen Verschlüsselung, welche strukturell an eine Zwiebel erinnert und Schritt für Schritt schichtweise entfernt wird, bezeichnet man diese Routingverfahren auch als Onion Routing.

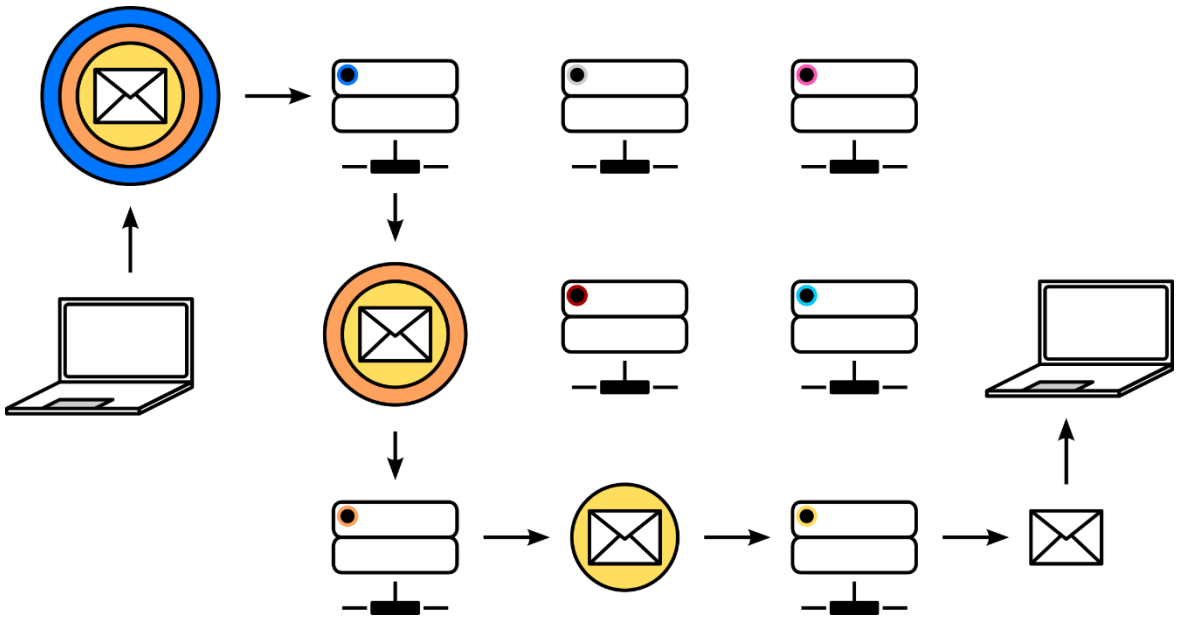

Abbildung 3: Weg einer Nachricht durch ein Mix-Netz

Der Inhalt der Nachricht ist ausschließlich Absender und Empfänger bekannt. Die Absenderidentität bleibt hingegen selbst dem Empfänger verborgen, da es technische Möglichkeiten gibt, eine anonyme, nicht nachverfolgbare Absenderadresse (*untraceable return address*) zu generieren. Eine ausführlichere Zusammenfassung über Mix-Netze kann in einer früheren A-SIT-Studie zum Thema Spurenverwischung im Internet [27] nachgelesen werden.
Was bleibt ist die Frage, wer ein solches Mix-Netz betreibt, bzw. inwieweit dem Betreiber das notwenige Vertrauen entgegengebracht wird, dass dieser den Netzwerkverkehr nicht über die Korrelation von eingehenden und ausgehenden Nachrichten deanonymisiert. Technisch kann dies nicht verhindert werden, wenn alle Mixe von einer einzigen Institution betreiben werden. Eine mögliche Gegenmaßnahme wäre, ein Mix-Netz über mehrere unabhängige Betreiber zu verteilen, die kein Interesse, bzw. keine Möglichkeit zur Kooperation haben, um Netzwerkverkehr zu deanonymisieren.

4.3. Wahlverfahren auf Basis blinder Signaturverfahren

So genannte *blinde Signaturverfahren* erlauben es, Daten zu signieren, ohne, dass diese eingesehen werden können. Nach dem Signaturvorgang, kann eine zuvor festgelegte Partei (typischerweise diejenige, die die Daten maskiert hat) diese demaskieren. Anschließend kann die Gültigkeit der Signatur auf Basis der nun im Klartext vorhandenen Daten überprüft werden. Nach der Demaskierung unterscheidet sich eine blinde Signatur somit (semantisch) nicht von herkömmlichen elektronischen Signaturverfahren. Erstmals vorgestellt wurden blinde Signaturverfahren 1983 von David Chaum [28]. Angelehnt an die in der Publikation enthaltene Beschreibung eines Wahlverfahrens auf Basis blinder Signaturen lässt sich ein elektronischer Distanzwahlprozess konzeptionell wie folgt umsetzen:

- Wahlberechtigte Personen geben ihre Stimme auf „elektronischen Stimmzetteln“ ab.
- Anschließend werden die ausgefüllten Stimmzettel maskiert.
- Wahlberechtigte signieren den maskierten Stimmzettel mittels elektronischer Signatur (nachdem die zu signierenden Daten Signatoren darstellbar sind, scheinen – unter Berücksichtigung dessen, dass die Stimme maskiert ist – qualifizierte Signaturen möglich).
- Die (unkenntlich gemachten), signierten Stimmzettel werden an die Wahlbehörde übermittelt.
- Die Wahlbehörde kann die Identität verifizieren, und somit protokollieren wer einer Stimme abgegeben hat, jedoch nicht wofür.
- Im nächsten Schritt wird die Signatur der Wählerinnen, bzw. der Wähler entfernt.
- Der (nach wie vor nicht lesbare) Stimmzettel wird von der Wahlbehörde (blind) signiert.
- Die blind signierten Stimmzettel werden an die Wählerinnen und Wähler zurückgesendet.
- Jeder Wähler und jede Wählerin demaskiert den erhaltenen blind signierten Stimmzettel.
- Abschließend übermittelt der Wähler, bzw. die Wählerin den eigenen (für jedermann lesbaren), von der Wahlbehörde nachweislich signierten, Stimmzettel über einen anonymen Kommunikationskanal (siehe Abschnitt 4.2) zurück an die Wahlbehörde.

Ein derartiges Verfahren erfüllt sowohl alle allgemeinen als auch alle technischen Voraussetzungen an elektronische Distanzwahlen. Behörden können an Hand qualifizierter elektronischer Signaturen sicherstellen, dass jeden authentifizierten Person nur ein Stimmzettel ausgehändigt wird, und durch die Speicherung der später im Klartext abgegebene Stimmen, doppelt abgegebene Stimmen filtern. Übertragungsfehler können auch durch erneute Übertragung von Stimmzetteln ausgeglichen werden (da doppelt abgegebene Stimmen gefiltert werden können). Außerdem gibt es keine technischen Einschränkungen bezüglich des Formats von Stimmzetteln und deren Auswertung. Es sind somit nicht nur ja/nein-Abstimmungen, oder Stimmen für vordefinierte Kandidatinnen und Kandidaten möglich, sondern auch Vorzugsstimmen, und theoretisch auch Freitextfelder umsetzbar. Die Auswertung von Stimmzetteln kann prinzipiell gleich erfolgen wie aktuell bei Urnenwahlen.

4.4. Wahlverfahren auf Basis von homomorpher Verschlüsselung und Zero-Knowledge Proofs

Einen weiteren Schritt in Richtung universell verifizierbarer Wahlprozesse ermöglicht homomorphe Verschlüsselung. Dabei handelt es sich um kryptografische Verfahren mit der Eigenschaft, dass bestimmte mathematische Operationen auf Kryptogrammen (anderen) mathematischen Operationen auf dem den Kryptogrammen zu Grunde liegenden Klartexten entsprechen. Derartige Abbildungen werden als Homomorphismus bezeichnet. Beispielsweise lassen sich mit Hilfe dieser Form von Kryptografie entsprechend verschlüsselte Daten addieren, ohne dass diese zuvor entschlüsselt werden müssen. Andere mathematische Operationen (z.B. Division) lassen sich hingegen (noch) nicht sinnvoll umsetzen. Da jedoch Wahlergebnisse typischerweise additiv zu Stande kommen, ist diese Limitierung nicht weiter relevant.
Im Wesentlichen können somit Stimmen verschlüsselt übermittelt und ausgezählt werden. Um sicher zu stellen, dass jeder und jede Wahlberechtigte nur eine Stimme abgibt, können im Zuge der Stimmabgabe eID-basierte Authentifizierungsmaßnahmen eingesetzt werden. Wenn hinter dem Authentifizierungsgateway anonyme Kommunikationskanäle zur Stimmübermittlung eingesetzt werden, ist auch Wähleranonymität gewährleistet. Nach Wahlschluss können alle verschlüsselten Stimmen veröffentlicht werden (dadurch wird keine Information über das individuelle Wahlverhalten bekannt), sodass Wählerinnen und Wähler verifizieren können, dass ihre Stimme gezählt wurde. Der Auszählungsprozess selbst ist ebenfalls transparent und somit für die Bevölkerung und beispielsweise auch für unabhängige Wahlbeobachter verifizierbar. Technisch erfolgt eine Auszählung indem die verschlüsselten Stimmen addiert und anschließend entschlüsselt werden. Um auch einen unbeeinflussten Ablauf dieses Schritts zu garantieren, werden so genannte *Secret-Sharing*-Verfahren eingesetzt, welche es erlauben, das zur Entschlüsselung notwendige Schlüsselmaterial unter mehreren Parteien zu verteilen. Details hierzu werden im nachfolgenden Abschnitt dargelegt.
Technisch ergibt sich im Rahmen eines derartigen Wahlprozesses die Notwenigkeit, sicherzustellen, dass es sich bei den verschlüsselt abgegeben Stimmen tatsächlich um semantisch gültige Stimmen handelt. Dies kann mittels sogenannter *Zero-Knowledge Proofs* sichergestellt werden. Dabei handelt

es sich um Verfahren, mit deren Hilfe bewiesen werden kann, dass (verschlüsselte) Daten tatsächlich Teil einer definierten Domäne sind, ohne dass bekannt wird, um welche Daten es sich konkret handelt. Damit kann sichergestellt werden, dass eine verschlüsselte Stimme tatsächlich für eine der zur Wahl stehenden Parteien abgegeben wurde.

4.5. Secret Sharing und Schwellwert-Kryptosysteme

So genannte *Secret-Sharing*-Verfahren basieren (wie der Name vermuten lässt) auf der Aufteilung eines Geheimnisses, wie beispielswiese eines zur Entschlüsselung geheimer Informationen notwenigen Schlüssels, auf mehrere Parteien [29] [30]. Typischerweise müssen *n* aus *m* Parteien kooperieren, um das Geheimnis wiederherzustellen, bzw. einen entsprechend verschlüsselten Text entschlüsseln zu können. Aus diesem Grund werden diese Art von Kryptosystemen auch *Schwellwert-Kryptosysteme* genannt. Nachdem jede Partei nur einen Teil des Geheimnisses kennt, und keine einzelne Parte das ganze Geheimnis, ist ein Entschlüsseln auf Eigeninitiative einzelner Parteien nicht möglich.
Dieses Prinzip kann ihm Rahmen elektronischer Wahlen vielseitig eingesetzt werden. Zum einen kann, wie im vorigen Abschnitt erwähnt, sichergestellt werden, dass zuvor verschlüsselte Stimmen erst im Rahmen der Auszählung unter Beisitz mehrerer Parteien (in diesem Fall eventuell Angehöriger unterschiedlicher politischer Parteien) entschlüsselt werden. Typischerweise kommen solche Verfahren im Rahmen asymmetrischer Kryptosysteme zum Einsatz. Daher können Wählerinnen und Wähler ihre Stimmen verschlüsseln und trotzdem sichergehen, dass diese erst nach Wahlschluss ausgewertet werden. Zusammenfassend können Schwellwert-Kryptosysteme den Schutz des Wahlgeheimnisses erhöhen, da keine im Wahlprozess beteiligte Instanz selbständig in der Lage ist, beispielsweise Stimmzettel zu entschlüsselt. In Kombination mit entsprechend definierten Prozessen ergibt sich dadurch ein hohes Maß an Sicherheit, ohne dass dabei die Nachvollziehbarkeit des Wahlprozesses beeinträchtigt wird. Es kann im Gegenteil sogar die Transparenz erhöht werden, wenn nachvollzogen werden kann, welche Parteien ihren Teil eines aufgeteilten kryptografischen Schlüssels bereitgestellt haben, um beispielsweise Stimmen auszuzählen.

4.6. Blockchain-basierte Wahlverfahren

Die Blockchain, auch als *Distributes Ledger Technology* (DLT) bekannt, ist die Basis vieler sogenannter Kryptowährungen, wie beispielsweise *Bitcoin*[3]. Die Blockchain ist dabei ein dezentral erstelltes, zentrales, sequentielles Transaktionsregister. Über unterschiedliche (dezentrale) Konsensverfahren wird bestimmt, welcher Teilnehmer eines Blockchain-basierten Netzwerks einen Eintrag in dieses Register vornehmen darf, bzw. wer einen Block, welcher kryptografisch an den aktuellen Stand der Blockchain gebunden ist, an diese anhängen darf. Ein Beispiel für ein solchesKonsensverfahren ist das im Rahmen von Bitcoin eingesetzte *Proof-of-Work*-Protokoll. Dabei müssen Teilnehmer, die darauf abzielen, Blöcke zu erstellen, ein kryptografisches Rätsel lösen. Die Lösung zu finden ist (analog zu Sudoku) schwierig, eine Verifikation eines korrekten Ergebnisses jedoch leicht. Dieser Vorgang wird (in Anlehnung an das Schürfen von Gold) als *Mining* und die ausführenden Teilnehmer entsprechend als *Miner* bezeichnet. Als Lohn für den (mittlerweile extrem rechenintensiven Aufwand) winkt demjenigen Teilnehmer, bzw. derjenigen Teilnehmerin, dem, bzw. der es gelingt vor allen anderen einen Block zu erzeugen, neues Kapital. Dieses wird im Rahmen einer so genannten *Coinbase*-Transaktion erzeugt. Zusätzlich werden an einen erfolgreichen Miner die Transaktionsgebühren aller in diesen Block aufgenommenen Transaktionen ausgeschüttet. Im Gegensatz zu Transaktionen im Rahmen traditioneller Zahlungsverfahren kommen keine personenbezogenen Daten, wie beispielsweise Kontonummern, sondern so genannte Adressen zum Einsatz, die jeder, bzw. jede frei und unreguliert generieren kann. Weitere Details zur Technologie können einer vorhergehenden A-SIT-Studie zum Thema [31] entnommen werden.

Auf Grund der oftmals propagierten Nachvollziehbarkeit und Transparenz von Prozessen auf Blockchain-Basis gibt es vermehrt Überlegungen, Wahlen auf Blockchain-Basis durchzuführen. Bei

[3] https://www.bitcoin.org/

Blockchain-basierten Wahlverfahren können zumindest drei Varianten unterschieden werden. Im Folgenden werden diese Varianten kurz vorgestellt und deren Eignung für E-Voting im Sinne demokratischer Wahlen beurteilt.

4.6.1. Voting mit Rechenleistung

Diese Art von Voting kommt beispielsweise bei Abstimmungen zu *Bitcoin Improvement Proposals* (BIPs) zum Einsatz. Im Rahmen von BIPs wird (wie der Name vermuten lässt) über Weiterentwicklungen der Kryptowährung Bitcoin abgestimmt. Sobald ein BIP implementiert wurde, wird ein Abstimmungszeitraum definiert, beispielsweise 1000 Blöcke ab einem definierten Startblock. Ab diesem Startblock können alle Miner für ein BIP stimmen, indem Sie einen definierten Wert in die Coinbase Transaktion, die Teil jedes Blocks ist, aufnehmen. Nach dem Abstimmungszeitraum wird ermittelt, wie viele Blöcke den entsprechenden Wert enthalten und somit für ein BIP gestimmt haben. Beispielsweise erforderte das Bitcoin Improvement Proposal BIP 100 eine fünfundsiebzigprozentige Mehrheit [32].
Diese Art von Abstimmung ist in der Blockchain-Welt umstritten, da normale Anwender und Anwenderinnen mangels Rechenleistung nicht abstimmen können und Miner mit hohem Einfluss den Ausgang der Abstimmung potentiell im eigenen Interesse beeinflussen können. Entsprechend eignet sich das Konzept nicht für demokratische Wahlen, da weder allgemeines (A1) noch gleiches (A2) Wahlrecht gewährleistet werden kann. Des Weiteren kann üblicherweise nachvollzogen werden, wer wie abgestimmt hat, wodurch keine geheime (A5) Wahl möglich ist. Zusammenfassend haben Parteien mit hoher Mining-Leistung (diese sind öffentlich bekannt) den größten Einfluss auf den Ausgang von BIPs.

4.6.2. Voting mit Guthaben

Als Alternative zu Voting auf Basis von Mining-Leistung wurde Voting durch „Beweis von Besitz“ entwickelt, um die Meinung von Anwenderinnen und Anwendern zu erfassen. Teilnahmeberechtigt sind Nutzerinnen und Nutzer, die im Besitz von Kryptowährung sind. Ein Beispiel hierfür ist *Bitcoinocracy* [33]. Bei Bitcoinocracy kann jeder und jede, die einen (egal wie hohen oder niedrigen) Betrag *Bitcoin Cash*[4] besitzt, Abstimmungen erstellen bzw. an Abstimmungen teilnehmen. Die Teilnahme erfolgt durch Signieren eines Statements mit dem Präfix „I believe“ oder „I doubt“ und anschließender Übermittlung an Bitcoinocracy. Jede Stimme bekommt als Gewicht das Guthaben der zur Signatur gehörenden Adresse.
Diese Art der Abstimmung eignet sich schon allein deswegen nicht für demokratische Wahlen, da nicht alle Stimmen gleichberechtigt sind (A2).

4.6.3. Voting mit „Voting“-Token

Bei dieser Art von Voting müssen sich Wahlberechtigte anonym authentifizieren und erhalten anschließend Währungseinheiten oder Token für eine Abstimmung. In diesem Abschnitt wird von einer Tokenvergabe ausgegangen, bei der jeder Token genau einer Stimme entspricht. Nach dem Erhalt der Wahltoken hat jeder Wähler bzw. jede Wählerin einen anonymen Token. Jede zur Wahl stehende Kandidatin bzw. jeder zur Wahl stehender Kandidat generiert eine Adresse und veröffentlicht diese vor der Wahl. Anschließend wird ein Zeitraum definiert, in dem gewählt werden kann. Eine Stimme wird abgegeben, indem ein Wahltoken an die Adresse der jeweiligen Kandidatin bzw. des Kandidaten übermittelt wird. Nach Wahlschluss wird die Anzahl der Token jeder Kandidatin bzw. jedes Kandidaten ermittelt. Die Auszählung unterscheidet sich konzeptionell nicht von traditionellen Wahlen.
Durch den Authentifizierungsschritt kann sichergestellt werden, dass jeder, bzw. jede Wahlberechtigte exakt einen Token und somit eine Stimme erhält. Dadurch und durch die Eigenschaft der Blockchain *Double Spending*, also das doppelte Verwenden eines Token, bzw. einer Währungseinheit zu verhindern, kann gleiches Wahlrecht (A2) garantiert werden. Das allgemeine Wahlrecht (A1) kann bei öffentlichen Blockchains, wie sie von Kryprowährungen wie Bitcoin verwendet werden, nicht garantiert werden. Grund dafür ist der Blockerstellungsprozess: Durch die

[4] https://www.bitcoincash.org/

zunehmende Zentralisierung von Mining-Leistung könnten kooperierende Miner beispielsweise gezielt die Aufnahme einzelner Stimmen in die Blockchain verhindern. Dieser Angriff würde zwar auffallen, kann aber nicht effektiv verhindert werden. Ein Ausweg wäre die Verwendung einer privaten Blockchain, oder einer öffentlichen Blockchain mit hohem Dezentralisierungsgrad.
Im Fall einer privaten Blockchain lassen sich – sofern entsprechende organisatorisch Prozesse umgesetzt werden – alle allgemeinen Anforderungen an demokratische Wahlprozesse erfüllen: Durch die direkte Wahl einer Partei bzw. eines Kandidaten bleibt das unmittelbare Wahlrecht (A3) gewahrt. Die Erfüllung von persönlichem (A4) und freiem Wahlrecht (A6) sind ähnlich wie bei der Briefwahl zu bewerten. Auch das Wahlgeheimnis (A5) kann durch entsprechende Authentifizierungsmaßnahmen sichergestellt werden. Beispielsweise könnten der Authentifizierungsserver und der Token-Ausgabeserver von verschiedenen Institutionen betrieben werden. In diesem Fall wäre die Stimmabgabe anonym, solange nicht beide Betreiber miteinander kooperieren. Schließlich wird noch ein anonymer Kanal zur Stimmabgabe benötigt, um beispielsweise Korrelationsangriffe zu verhindern.

Was abgesehen von den im Rahmen dieses Dokuments vorgestellten Umsetzungsmöglichkeiten für E-Voting bleibt, ist die Frage der Gerätesicherheit. Um kritische IT-Infrastruktur ausfallsicher und weitestgehend unangreifbar zu betreiben, existieren Prozesse, welche sich auch direkt auf eventuelle E-Voting Infrastruktur anwenden lassen. Als kritische Angriffsfläche bleiben somit die Endgeräte, von denen aus abgestimmt wird. Details hierzu werden im nachfolgenden Abschnitt diskutiert.

5. Sicherheit von Endgeräten

Bisher wurden Konzepte vorgestellt, jedoch nicht konkrete Umsetzungsmöglichkeiten insbesondere unter Berücksichtigung von Endgerätesicherheit diskutiert. Konkret betrifft dies die der Bevölkerung zur Verfügung zu stellende Wahlsoftware: Auf klassischen Desktop-PCs und Laptops stellt sich die Frage nach Systemsicherheit, da durch Computerviren, Backdoors und Spyware infizierte Geräte Wahlmanipulationen und die Verletzung des Wahlgeheimnisses ermöglichen. Wenn klassische PCs und Laptops als Zugangsgeräte für E-Voting-Lösungen forciert werden, gibt es jedoch zumindest theoretisch Ansätze dieses Problem zu lösen: Beispielsweise könnten bootfähige CDs oder nicht beschreibbare, zertifizierte USB-Sticks mit Live-Betriebssystemen an die Bevölkerung verteilt werden, welche die notwendige Wahlsoftware enthalten. Dadurch kann der Einfluss im installierten Betriebssystem eventuell vorhandener Schadsoftware auf ein Minimum reduziert werden.
Tatsächlich sind solche Ansätze aktuell als wenig zukunftssicher und nicht im Sinne der Europaratsempfehlungen zum Thema E-Voting zu bewerten. Schließlich wird das Internet mittlerweile mehrheitlich von Mobilgeräten aus genutzt [34], welche (ebenso wie viele aktuelle Laptops) über kein optisches Laufwerk verfügen und auch kein Booten alternativer Betriebssysteme zulassen. Moderne Mobilgeräte bieten viele Sicherheitsfeatures, wie Secure Boot, Isolation von Applikationen und dadurch nur eingeschränkten Zugriff auf das Betriebssystem, sowie einen speziell geschützten Hardwarebereich zum Speichern und Verarbeiten von kritischen Informationen und kryptografischem Material. Theoretisch ergibt sich somit durch die vermehrte Nutzung von Mobilgeräten ein Sicherheitsvorteil gegenüber klassischen PCs, da Manipulationen auf Grund der vielfältigen Sicherheitsmaßnahmen erschwert werden müssten. Folglich sollte sich E-Voting auf Mobilgeräten noch sicherer umsetzen lassen. Tatsächlich haben Mobilgeräte jedoch vielfach das Problem, dass Updates und Sicherheitspatches – wenn überhaupt – nicht zeitnah ausgeliefert werden. Folglich ergibt sich eine neue Problematik betreffend Systemsicherheit, welche auf PCs de-facto ausgeschlossen, oder zumindest hinreichend behandelt werden kann. Weiters ist die in Österreich aktuell eingesetzte eID-Lösung mit Bürgerkarte und Handy-Signatur noch auf PC-Umgebungen ausgelegt. Für die Nutzung am mobilen Endgerät sind daher eID-Lösungen notwendig, wie sie in aktuellen österreichischen Aktivitäten zur neuen E-ID und mobilem E-Government ohnehin angedacht sind.

Ungeachtet der technischen Möglichkeiten und Maßnahmen ergeben sich bei allen denkbaren Wahlverfahren offene Fragen, die mit rein technischen Mitteln nicht lösbar sind. Diese können nur durch entsprechend implementierte (und im Weiteren auch gesetzlich geregelte) Prozesse zufriedenstellend gelöst werden. Das abschließende Fazit fasst die aktuelle Ausgangssituation auch

im Kontext dieser offenen Fragen zusammen und gibt einen Ausblick auf mögliche Umsetzungsmöglichkeiten.

6. Fazit

Elektronische Stimmabgabe über das Internet darf im Sinne breiter Einsetzbarkeit und Bürgerakzeptanz keine Anforderung nach speziellen Endgeräten oder spezieller Hardware, Fachwissen, oder Software stellen. Die aktuellen gesetzlichen Rahmenbedingungen in Österreich begünstigen eine Umsetzung elektronischer Distanzwahlen in Form einer „Digitalisierung" der Briefwahl, da sich die aktuellen Prozesse nahezu unverändert auf E-Voting übertragen lassen. Durch die allgemeine Verfügbarkeit von eID und qualifizierter elektronischer Signatur sind bereits jetzt einige wichtige Voraussetzungen für die flächendeckende Einführung von E-Voting erfüllt. Die Tatsache, dass E-Partizipation im Rahmen von Volksabstimmungen bereits umgesetzt ist, ist ein Indikator für die Eignung bestehender Systeme auch im Kontext von E-Voting.
Verfahren auf Blockchain-Basis sind besonders auf Grund der propagierten Transparenz für E-Partizipation geeignet. Allerdings lassen sich auch Teile des Blockchain-Konzepts aufgreifen um Transparenz im Rahmen geheimer demokratischer Wahlen zu gewährleisten. Eine kryptografische Verkettung von Schnappschüssen eines im Gange befindlichen Wahlprozesses und dessen (unter Umständen kontinuierliche) Veröffentlichung kann sowohl individuelle, als auch allgemeine Verifizierbarkeit ermöglichen. Ungeachtet dessen müssen (genau wie im Kontext anderer E-Voting-Konzepte) Prozesse und gesetzliche Rahmenbedingungen über die Zuständigkeiten aller beteiligten Organe definiert werden, um die Sinnhaftigkeit aller Teilaspekte des Gesamtkonzepts Blockchain bewerten zu können. In jedem Fall müssen Kosten und Nutzen, besonders was potentiellen organisatorischen Mehraufwand angeht, evaluiert werden.
Unabhängig von konzeptionellen Aspekten muss die Sicherheit von Wahlsoftware sowohl auf Desktop-Computern und –Betriebssystemen sowie Mobilgeräten und modernen Mobilbetriebssystemen evaluiert werden, um Wahlmanipulation (beispielsweise durch Schadsoftware) zu verhindern. Hier sind Lösungen sinnvoll, die möglichst keine oder wenig spezifische Anforderungen ans Endgerät stellen, etwa ohne spezifische Software auskommen und nur Funktionalität meistverwendeter und gängiger Browser verwenden.

Zusammenfassend müssen auf Grund der Entwicklungen der vergangenen Jahre E-Voting-Lösungen auf lange Sicht insbesondere von Mobilgeräten aus nutzbar sein, damit diese breit verwendbar und damit auch im Einklang mit den entsprechenden Europaratsempfehlungen sind. Der Ablauf von Wahlen muss auf abstrakter Ebene nicht verändert werden, da sich dieser konzeptionell nicht von traditionellen Präsenzwahlen unterscheidet. Die Voraussetzungen sind in Österreich, besonders was eine mögliche Digitalisierung der Briefwahl angeht, günstig. Eine zukunftssichere Lösung setzt jedoch eine eID-Lösung voraus, welche auch und gerade von Mobilgeräten aus nutzbar ist und trotzdem ein entsprechendes Sicherheitsniveau bietet. Mittelfristig kann die Ausrichtung auf Mobilgeräte jedoch entkoppelt von den Kernaufgaben betrachtet und entsprechende Umsetzungen können separat evaluiert werden, wodurch Aktivitäten im Bereich elektronischer Distanzwahl keine neuen technischen Hindernisse im Weg stehen.

Referenzen

[1] Coincil of Europe, „Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting," 30 09 2004. [Online]. Available: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805dbef8. [Zugriff am 20 04 2018].

[2] „Volksbegehrengesetz 2018 – VoBeG," Republik Österreich, [Online]. Available: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009719. [Zugriff am 16 02 2018].

[3] Bundesministerium für Wissenschaft und Forschung, „ÖH Wahlen beginnen planmäßig mit E-Voting Tagen," 17 05 2009. [Online]. Available:

https://www.ots.at/presseaussendung/OTS_20090517_OTS0013/oeh-wahlen-beginnen-planmaessig-mit-e-voting-tagen. [Zugriff am 28 03 2018].

[4] Österreichischer Verfassungsgerichtshof, „VfGH Erkenntnis V 85/11 ua," 13 12 2011. [Online]. Available: https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Vfgh&Dokumentnummer=JFT_09888787_11V00085_00. [Zugriff am 19 04 2018].

[5] OASIS Open, „Election Markup Language (EML) Specification Version 7.0," 11 09 2011. [Online]. Available: https://docs.oasis-open.org/election/eml/v7.0/eml-v7.0.html. [Zugriff am 12 04 2018].

[6] Council of Europe, „Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting," 14 06 2017. [Online]. Available: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680726f6f. [Zugriff am 19 04 2018].

[7] Republik Österreich, „Übertragung der Durchführung der elektronischen Wahlen (E-Voting) bei den Hochschülerinnen- und Hochschülerschaftswahlen 2009 an die Bundesrechenzentrum GmbH," 13 02 2009. [Online]. Available: https://ris.bka.gv.at/eli/bgbl/II/2009/38. [Zugriff am 19 04 2018].

[8] J. Hahn, „E-Voting bei ÖH-Wahlen 2009 (1171/AB)," 04 05 2009. [Online]. Available: https://www.parlament.gv.at/PAKT/VHG/XXIV/AB/AB_01171/index.shtml. [Zugriff am 19 04 2018].

[9] Republik Österreich, „Bundesgesetz über die Vertretung der Studierenden (Hochschülerinnen- und Hochschülerschaftsgesetz 1998 – HSG 1998)," 1998. [Online]. Available: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10010113. [Zugriff am 20 04 2018].

[10] T. G. Rössler, *Electronic Voting over the Internet – an E-Government Speciality,* Technische Universität Graz, 2007.

[11] Europäische Kommission, „Distribution of the number of mobile phones owned per household in Austria in 2015," 2015. [Online]. Available: https://www.statista.com/statistics/615609/number-of-mobile-phones-owned-per-household-in-austria/. [Zugriff am 20 04 2018].

[12] S. Heiberg, P. Laud und J. Willemson, „The Application of I-Voting for Estonian Parliamentary Elections of 2011," in *E-Voting and Identity*, Berlin, Springer, 2012, pp. 208-223.

[13] A. H. Trechsel, „E-voting and Electoral Participation," in *The Dynamics of Referendum Campaigns*, Palgrave Macmillan UK, 2007, pp. 159-182.

[14] B. Jacobs und W. Pieters, „Electronic Voting in the Netherlands: From Early Adoption to Early Abolishment," in *Foundations of Security Analysis and Design V*, Berlin, Springer, 2009, pp. 121-144.

[15] Kommunal- og regionaldepartementet, „Evaluering av e-valgforsøket i 2011," 13 06 2013. [Online]. Available: https://www.regjeringen.no/en/historical-archive/Stoltenbergs-2nd-Government/Ministry-of-Local-Government-and-Regiona/tema-og-redaksjonelt-innhold/kampanjesider/e-vote-trial/evaluations-of-the-e-voting-trials/evaluation-of-the-e-voting-trials-in-201/id684. [Zugriff am 20 04 2018].

[16] S. Heiberg und J. Willemson, „Verifiable internet voting in Estonia," in *6th International Conference on Electronic Voting: Verifying the Vote*, Lochau, IEEE, 2014.

[17] État de Genève - CHVote, „E-voting system - CHVote," [Online]. Available: https://republique-et-canton-de-geneve.github.io/chvote-1-0/index-en.html. [Zugriff am 19 04 2018].

[18] Bundeskanzlei BK, „Versuche mit E-Voting," 04 2018. [Online]. Available: https://www.bk.admin.ch/bk/de/home/politische-rechte/e-voting/versuchsuebersicht.html. [Zugriff am 19 04 2018].

[19] État de Genève - CHVote, „System Overview,“ 07 04 2017. [Online]. Available: https://github.com/republique-et-canton-de-geneve/chvote-1-0/blob/master/docs/system-overview.md. [Zugriff am 19 04 2018].

[20] E. Dubuis, R. Haenni, R. Koenig, S. Fischli und M. Schläpfer, „Konzept und Implikationen eines verifizierbaren Vote Électronique Systems,“ Berner Fachhochschule, Departement Technik und Informatik, Biel, 2012.

[21] „Grundsätze des Wahlrechts,“ Republik Österreich, Parlamentsdirektion, [Online]. Available: https://www.parlament.gv.at/PERK/PARL/DEM/GRUNDS/index.shtml. [Zugriff am 15 02 2018].

[22] „Bundesgesetz über die Wahl des Nationalrates (Nationalrats-Wahlordnung 1992 – NRWO),“ Republik Österreich, [Online]. Available: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001199. [Zugriff am 16 02 2018].

[23] „VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG“.

[24] Land Steiermark, „GRW - vorgezogene Stimmabgabe,“ [Online]. Available: http://www.verwaltung.steiermark.at/cms/beitrag/11684070/74836454/. [Zugriff am 20 04 2018].

[25] Land Kärnten, „Gesetz vom 2. Juli 1974 über die Wahl des Kärntner Landtages (Kärntner Landtagswahlordnung - K-LTWO),“ 2017. [Online]. Available: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=LrK&Gesetzesnummer=20000022. [Zugriff am 20 04 2018].

[26] D. L. Chaum, „Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms,“ in *Communications of the ACM*, New Yor, NY, USA, ACM, 1984, pp. 84-88.

[27] A. Marsalek, B. Prünster und D. Ziegler, „Spurenverwischung im Internet,“ 16 18 2017. [Online]. Available: https://technology.a-sit.at/spurenverwischung-im-internet/. [Zugriff am 22 03 2018].

[28] D. Chaum, „Blind Signatures for Untraceable Payments,“ in *Advances in Cryptology*, Boston, MA, Springer US, 1983, pp. 199-203.

[29] A. Shamir, „Hot to Share a Secret,“ *Communications of ACM,* pp. 612-613, 11 1979.

[30] G. Blakley, „Safeguarding Cryptographic Keys,“ in *Proceedings of Americian Federation of Information Processing Societies*, California, 1979, pp. 313-317.

[31] A. Marsalek und B. Prünster, „Technologieüberblick Blockchain,“ 24 10 2016. [Online]. Available: https://technology.a-sit.at/technologieueberblick-blockchain/. [Zugriff am 24 04 2018].

[32] J. Garzik, T. Harding und D. V. Johannsson, „Dynamic maximum block size by miner vote,“ [Online]. Available: https://github.com/jgarzik/bip100/blob/master/bip-0100.mediawiki. [Zugriff am 26 03 2018].

[33] Saint Bitts LLC, „Vote with your Bitcoin (BCH) signature — Bitcoinocracy,“ [Online]. Available: https://vote.bitcoin.com/. [Zugriff am 26 03 2018].

[34] StatCounter, „Mobile internet traffic as percentage of total web traffic in August 2017, by region,“ [Online]. Available: http://gs.statcounter.com/platform-market-share/desktop-mobile-tablet/worldwide/#monthly-201708-201708-bar. [Zugriff am 25 04 2018].