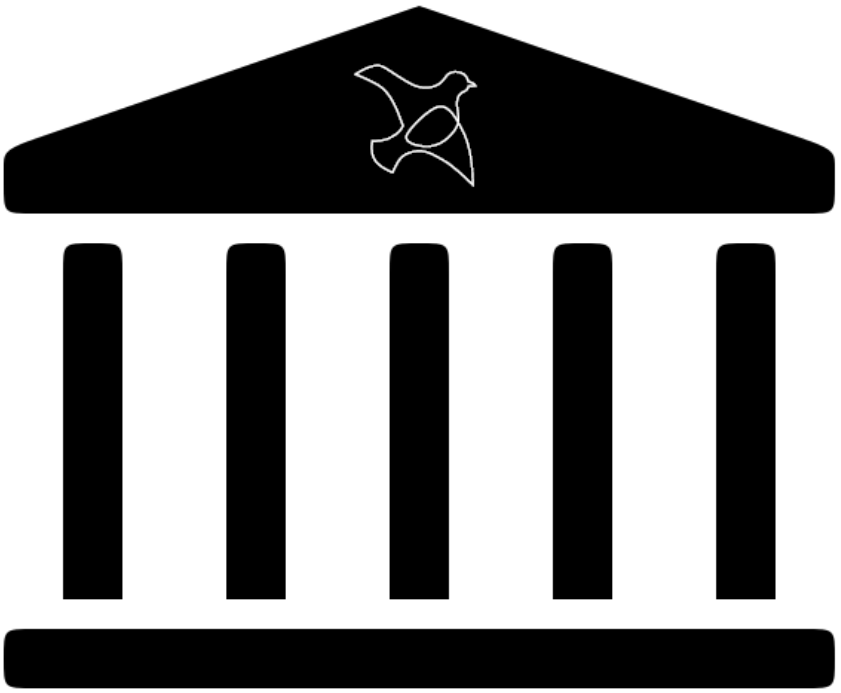
opn.vote

Demokratische Online-Abstimmungen



White Paper 04.2022

Joerg Mitzlaff, openPetition

1. Zielgruppe

Es sollen mit einfacher und allgemeinverständlicher Sprache alle Menschen erreicht werden, die an demokratischen Online-Abstimmungen teilnehmen möchten, sie organisieren oder über ihren zukünftigen Einsatz mitentscheiden.

Im Interesse der Lesbarkeit wird auf geschlechtsneutrale Formulierungen verzichtet.

2. Zusammenfassung

Vorgestellt wird opn.vote, ein Verfahren für demokratische Abstimmungen im Internet. Zunächst werden die Anforderungen an demokratische Online-Abstimmungen aufgezeigt und diskutiert. Im Anschluss werden existierende Ansätze aus der Praxis vorgestellt und bewertet. opn.vote arbeitet mit dem alternativen Verfahren der kryptografischen blinden Signatur. Es wird gezeigt, dass geheime Abstimmungen sichergestellt sind, ohne einer zentralen Instanz vertrauen zu müssen. Die Überprüfbarkeit der Abstimmung ist gewährleistet, da eine massenhafte Manipulation der Abstimmung aufgedeckt werden kann. Der Ausblick zeigt auf, wie für das Verfahren eine Manipulation selbst im Einzelfall ausgeschlossen werden kann.

3. Abstimmungen versus Wahlen

Bei Wahlen können sich die Wähler zwischen Personen und zwischen Parteien entscheiden, welche dann bis zur nächsten Wahl die Interessen des Wählers im Parlament vertreten sollen.

Bei Abstimmungen können sich die Teilnehmer direkt zwischen Gesetzentwürfen zu einem oder mehreren Themen entscheiden, die dann verbindlich vom Parlament umgesetzt werden müssen.

Das Verfahren und die Grundsätze, nach denen demokratische Abstimmungen und Wahlen geregelt sind, unterscheiden sich nicht. In diesem Sinne werden die Begriffe Abstimmungen und Wahlen hier synonym verwendet.

4. Anforderungen an demokratische Abstimmungen

Für Abstimmungen gelten die gleichen *demokratischen Grundsätze* wie für Wahlen[1]. Diese Grundsätze werden auch Wahlgrundsätze genannt.

Wahlbehinderung, Wahlfälschung und eine Duldung der Verletzung des Wahlgeheimnisses sind in Deutschland verboten (§§ 107 ff StGB) und werden sanktioniert.

4.1. Zugänglich

Jedem Wahlberechtigten muss die Wahl ermöglicht werden. Nicht Wahlberechtigte müssen von der Wahl ausgeschlossen sein.

Es gilt der Grundsatz der Allgemeinheit. Keine dem Wahlgebiet zugehörige, mündige Person ist von der Wahl ausgeschlossen.

Die genauen Kriterien für Wahlberechtigung legen die Organisatoren der Wahl fest.

4.2. Gleich

Jeder Wähler hat eine Wahlstimme. Die Stimme jedes Wählers zählt gleich viel bei der Ermittlung des Gesamtergebnisses.

Der Wähler hat das Recht, seine Wahlstimme nicht abzugeben.

Der Wähler hat das Recht, eine ungültige Stimme abzugeben.

4.3. Geheim

Jeder Wähler hat das Recht auf eine nicht öffentliche Stimmabgabe, bei der das Wahlgeheimnis auf Dauer gewahrt bleibt.

4.4. Unverfälscht

Abgegebene Stimmen sind unveränderlich und nicht löschbar.

Das Hinzufügen von zusätzlichen Stimmen ohne Stimmberechtigung muss ausgeschlossen sein.

Insbesondere muss das Hinzufügen von nicht abgegebenen Stimmen von Wahlberechtigten ausgeschlossen sein.

[1] https://de.wikipedia.org/wiki/Wahl

4.5. Überprüfbar

Jeder Wähler hat das Recht, die Einhaltung aller vorherigen Anforderungen zu prüfen.

Die Prüfung muss mit vertretbarem Aufwand und ohne Expertenwissen möglich und nachvollziehbar sein.

Eine mögliche Verletzung der Anforderungen an demokratische Abstimmungen muss erkennbar und beweisbar sein.

Damit ein möglicher Betrug bewiesen und sanktioniert werden kann, braucht es eine kritische Presse-Öffentlichkeit, die an der Veröffentlichung von Wahlbetrug interessiert ist und eine unabhängige Justiz.

4.5.1. Zugänglichkeit

Aktuell liegt die Kontrolle über Einwohnermelderegister und Wählerverzeichnis exklusiv beim Staat. Eine Überprüfung des Wählerverzeichnisses kann von jedem Bürger bei begründetem Verdacht auf Unrichtigkeit beantragt werden.

Im Interesse einer hohen demokratischen Legitimation des Wahlergebnisses durch eine hohe Wahlbeteiligung sollte der Wahlvorgang so einfach wie möglich gestaltet werden, ohne zeitliche, räumliche oder technische Restriktionen.

4.5.2. Geheimnis

Das Wahlverfahren muss die Trennung von Personen und Stimmzettel sicherstellen. Bei Wahlen vor Ort müssen Wahlkabinen aufgestellt sein und sie müssen benutzt werden. Bei Wahlen außerhalb des Wahllokals versichert die wählende Person an Eides statt, dass Sie die den Stimmzettel persönlich gezeichnet hat.

Wahlbezirke dürfen nicht zu klein sein, damit genügend Stimmzettel in der Wahlurne eine persönliche Zuordnung unmöglich machen.

4.5.3. Unverfälschtheit

Unveränderlichkeit der Stimme

Wahlbeobachter müssen bei der Auszählung sicherstellen, dass Stimmzettel nicht ungültig oder gültig gemacht werden.

Kein Löschen von Stimmen, Kein Hinzufügen von Stimmen, Kein Hinzufügen von nicht abgegebenen Stimmen

Stimmzettel und Wahlscheine und Urnen sind leicht zu fälschen.

Der Wahlvorstand und Wahlbeobachter müssen sicherstellen, dass Wahlscheine mit dem Wählerverzeichnis abgeglichen werden und jeder nur einmal wählt.

Der Wahlvorstand und Wahlbeobachter müssen sicherstellen, dass Wahlurnen vor dem Verschließen leer sind, dass Wahlurnen bis zur Auszählung dauerhaft beaufsichtigt sind, dass nur registrierte Wahlurnen ausgezählt werden, dass jeder Stimmzettel richtig gezählt wird, dass die Auszählungsergebnisse aus jedem Wahlbezirk richtig weitergegeben werden und dass die Summe der Ergebnisse aus den Wahlbezirken stimmt.

4.6. Unbeeinflusst

In Deutschland dürfen Zwischenstände der Wahl am Wahltag z.B. durch Befragung beim Verlassen des Wahllokals nicht veröffentlicht werden (§ 32 Absatz 2 Bundeswahlgesetz). Wähler sollen nicht durch die Entscheidungen anderer Wähler beeinflusst werden. Eine Missachtung des Verbots wird sanktioniert.

Es ist in Deutschland nicht verboten, seine eigene Stimmabgabe zu veröffentlichen.

4.7. Frei

Eine Beeinflussung der Wahl durch Wählerbestechung ist in Deutschland verboten (§ 108b, 108c StGB) und wird sanktioniert.

Eine Beeinflussung der Wahl durch Nötigung, Druck, Zwang oder Erpressung ist in Deutschland verboten (§ 108 StGB) und wird sanktioniert.

5. Anforderungen an Online-Abstimmungen

Online-Abstimmungen müssen genauso einfach und sicher sein wie Online-Shopping oder Online-Banking.

5.1. Freie Endgeräte

Online-Abstimmungen setzen die Kontrolle über die eigenen Endgeräte und Betriebssysteme voraus. Es dürfen keine Anwendungen auf einem Gerät zwangsweise installiert sein, ohne die Möglichkeit der Deinstallation, sei es von einem autoritären Staat oder einem Unternehmen.

Teilnehmer einer Online-Abstimmung brauchen Medienkompetenz, um mit hoher Wahrscheinlichkeit sagen zu können, dass ihre Netzanbindung und ihr Gerät nicht durch eine Schadsoftware kontrolliert werden.

Staatstrojaner dürfen nicht zugelassen werden. Betriebssysteme müssen Root-Rechte erlauben können.

Anwendungen in einem Abstimmungsverfahren müssen dem Teilnehmer ein klares Verständnis davon geben, welche Abstimmungsschritte von dem eigenen Gerät kontrolliert werden und welche Schritte auf der Abstimmungsplattform laufen.

5.2. Freies Internet

Teilnehmern einer Online-Abstimmung muss es möglich gemacht werden, ihre Kommunikation mit der Abstimmungsplattform durch Dienste wie VPN, Tor oder Proxy-Server verschleiern zu können.

Die Abstimmungsplattform darf nicht unter Zuhilfenahme des Internet-Providers eine verwendete IP-Adresse echten Personen zuordnen können.

5.3. Niederschwellig

Der demokratische Grundsatz der Zugänglichkeit muss es den Menschen so einfach wie möglich machen, an einer Online-Abstimmung teilzunehmen. Alle gängigen Endgeräte (Laptop, Tablet, Smartphone), Betriebssysteme (Windows, macOS, Linux) und Browser (Chrome, Firefox, Safari, Edge) müssen unterstützt werden.

Die Webseiten müssen übersichtlich sein, gut lesbar und in leichter Sprache verfügbar sein, selbsterklärend auf die nächsten möglichen Schritte hinweisen, insbesondere auch im Fehlerfall.

Der Abstimmungsvorgang sollte so wenig wie möglich zeitlich unterbrochen werden müssen.

Der Abstimmungsvorgang sollte so wenig wie möglich mit Medienbrüchen arbeiten und mit nur einem Gerät auskommen.

5.4. Unterbrechungsresistent

Der Abstimmungsvorgang muss jederzeit unterbrochen werden können, ohne die Stimmberechtigung oder die abgegebene Stimme zu verlieren.

5.5. Kostenlos

Nach dem demokratischen Grundsatz der Zugänglichkeit dürfen Menschen ohne finanzielle Mittel nicht von Abstimmungen ausgeschlossen werden.

Die Kosten der Organisation und des Ablaufs einer Abstimmung werden durch die Gemeinschaft über Spenden oder Steuern getragen.

Der demokratische Grundsatz der Überprüfbarkeit erfordert von ausreichend vielen Teilnehmern eine zeitliche Investition für eine Abstimmung, um die Korrektheit der Abstimmung sicherstellen zu können.

5.6. Skalierbar

Der Ressourcenverbrauch steigt pro Teilnehmer auf der Abstimmungsplattform nicht mehr als linear an.

Die finanziellen Kosten pro Teilnehmer sinken mit steigender Anzahl der Teilnehmer gegen Null.

5.7. Freie Software

Mit der Veröffentlichung des Quellcodes der Abstimmungssoftware müssen unabhängige Dritte überprüfen können, ob das Abstimmungsverfahren korrekt implementiert wurde.

Abstimmungssoftware für verbindliche Abstimmungen erfordert ausführliche, öffentliche Schwachstellentests.

6. Erwartungen an demokratische Online-Abstimmungen

Bei der Vielzahl der Anforderungen gibt es nicht das eine richtige Abstimmungsverfahren, das alle Anforderungen erfüllt.

Die Erwartungen an das Verfahren und die technischen Möglichkeiten entwickeln sich weiter. Die Debatte um das bestmögliche

Abstimmungsverfahren sollte in einer funktionierenden Demokratie kontinuierlich geführt werden.

6.1. Komfort versus Kontrolle

Ist der Aufwand für die Kontrolle des Verfahrens zu hoch, ist der demokratische Grundsatz der Zugänglichkeit verletzt.

Reichen die Möglichkeiten der Kontrolle nicht aus, ist der demokratische Grundsatz der Überprüfbarkeit verletzt.

Je nachdem wie sehr die Teilnehmer den Organisatoren der Abstimmung bzw. der ausführenden Plattform vertrauen, steigt oder fällt das Bedürfnis nach Kontrolle.

Die Teilnehmer möchten selbst darüber entscheiden können, wie viel Komfort und wie viel Kontrolle gewünscht ist.

6.2. Online versus Offline

Verfassungsrechtlich gilt das Leitbild der Urnenwahl. Die letzte Bundestagswahl 2017 hatte einen Briefwahlanteil von 28,6%. Verfassungsrechtler sehen Regulierungsbedarf, falls der Briefwahlanteil über 50% ansteigt[2]. Eine Online-Abstimmung muss sich in gleicher Weise verfassungsrechtlich legitimieren wie eine Briefwahl, da es sich auch hier nicht um eine Urnenwahl handelt.

6.3. Einzelfall versus Gesamtergebnis

Kein existierendes Wahlverfahren kann eine Verletzung eines Wahlgrundsatzes im Einzelfall verhindern. Es muss sichergestellt werden, dass ein massenhafter Missbrauch mit vertretbarem Aufwand immer aufgedeckt werden kann und bewiesen werden kann.

6.4. Sanktionierung versus Garantie

Die Grundsätze demokratischer Wahlen sind in Deutschland ein hohes Gut. Jede Verletzung wird sanktioniert. Ein technisches Verfahren muss nicht alle demokratischen Grundsätze direkt garantieren können, wenn die Verletzung eines Grundsatzes auch auf dem Rechtsweg verhindert werden kann. Je

---

[2] https://www.bundestag.de/resource/blob/829216/745dc4ea8d4b00624236bfa80449a9a3/WD-3-005-21-pdf-data.pdf

weniger die Rechtsstaatlichkeit in einem System gewährleistet ist, umso wichtiger wird die Sicherstellung der Grundsätze im technischen Verfahren.

7. Erwartungen an die Glaubwürdigkeit des Verfahren

2009 hat das Bundesverfassungsgericht den Einsatz von Wahlcomputern in Deutschland verboten mit der Begründung, dass „alle wesentlichen Schritte der Wahl einer öffentlichen Überprüfbarkeit unterliegen“[3].

Ohne jedes Vorwissen muss nachvollziehbar sein, warum eine Stimme geheim bleibt. Geheim heißt, dass keinen anderen Personen oder Institutionen vertraut werden muss, dass eine Stimme nicht doch einer Person zugeordnet werden kann. Online-Abstimmen muss so sicher sein wie in einem Wahllokal. Hier hat der Wähler die volle Kontrolle darüber, dass seine Stimme geheim bleibt.

Ohne jedes Vorwissen muss eine Stimme innerhalb von in wenigen **Minuten** überprüft werden können.

Mit einem guten mathematischen Verständnis muss das Abstimmungsverfahren und deren Prinzipien und Algorithmen innerhalb von **wenigen Stunden** verstanden werden.

Auf dem Stand eines Informatikstudenten im 3. Semester muss die Implementierung des Verfahrens anhand des offenen Quellcodes innerhalb von **wenigen Tagen** nachvollziehbar sein und dessen Korrektheit bestätigt werden können.

In Deutschland gibt es etwa 1 Mio. IT-Fachkräfte[4]. Wenn nur ein kleiner Anteil davon eine Überprüfung vornimmt, ist der demokratische Grundsatz der Überprüfbarkeit des Verfahrens gegeben.

Wenn es eines ausgewiesenen Expertenwissens bedarf, um ein Abstimmungsverfahren zu verstehen, ist der demokratische Grundsatz der Überprüfbarkeit nicht mehr gegeben.

Zertifizierungen sind für sich genommen noch keine Garantie für ein demokratisches Online-Verfahren, wenn die Kriterien, nach denen zertifiziert wird, nicht streng genug sind oder schlicht die falschen Kriterien sind. Die

[3] https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2009/bvg09-019.html

[4] https://statistik.arbeitsagentur.de/DE/Statischer-Content/Statistiken/Themen-im-Fokus/Berufe/Generische-Publikationen/Broschuere-Informatik.pdf

Kriterien, nach denen Zertifizierungsstellen Sicherheitszertifikate ausstellen und die Prüftiefe, müssen sich einer öffentlichen Begutachtung stellen.

8. Existierende Anwendungen

Das Bundesamt für Sicherheit in der Informationstechnik hat 2008 „Sicherheitsanforderungen an Online-Wahlprodukte definiert“[5]. Eine neue Version wird bis Ende 2022 in Aussicht gestellt[6]. Eine Technische Richtlinie „IT-sicherheitstechnische Anforderungen zur Durchführung einer elektronischen Wahl“ wird für das dritte Quartal 2022 erwartet[7].

Das Zentrum für sichere Informationstechnologie – Austria gibt einen guten Überblick zu existierenden Anwendungen und den zugrunde liegenden technischen Konzepten[8].

Der Europarat hat 2017 Standards für Online-Wahlen empfohlen[9].

Der Deutsche Bundestag hatte am 6. April 2022 zu einem öffentlichen Fachgespräch zum Thema „E-Voting – alternative Wahlformen und ihre Absicherung”[10] eingeladen. Das Büro für Technikfolgen-Abschätzung hat dazu ein Thesenpapier veröffentlicht[11].

8.1. Zero Knowledge Proof Verfahren

Existierende kommerzielle Anwendungen basieren im Wesentlichen auf komplexen Zero Knowledge Proof Verfahren.

Bei diesen kryptografischen Verfahren ist dem System bekannt, wer die Stimme abgegeben hat, der Stimmzettel selbst ist jedoch verschlüsselt. Die verschlüsselten Stimmzettel werden nun über mehrere Stufen gemischt und mit jeweils anderen Schlüsseln neu verschlüsselt, bis nicht mehr nachvollziehbar ist, von wem ein Stimmzettel stammt. (Mix network[12]). Über das komplexe Zero

[5] https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/Archiv/PP_0037.html

[6] https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Moderner-Staat/Online-Wahlen/Schutzprofile_Online-Wahlprodukte/schutzprofile_online-wahlprodukte_node.html

[7] https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Moderner-Staat/Online-Wahlen/Online-Wahlen_Wahlverantwortliche/online-wahlen_wahlverantwortliche_node.html

[8] https://technology.a-sit.at/ueberblick-e-voting/

[9] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680726f6f

[10] https://www.bundestag.de/dokumente/textarchiv/2022/kw14-pa-fachgespraech-bildung-882928

[11] https://www.tab-beim-bundestag.de/downloads/Veranstaltungen/Thesenpapier_E-Voting_2022.pdf

[12] https://en.wikipedia.org/wiki/Mix_network

Knowledge Proof Verfahren lässt sich beweisen, dass bei diesem Vorgang „nicht geschummelt wurde“. Die mathematische Theorie und die konkrete Software-Implementierung sind so komplex, dass nur wenige Experten das Funktionieren des Systems nachvollziehen bzw. widerlegen können. Es wird eine Überprüfbarkeit des Systems suggeriert, mit der Einschränkung, dass die Kosten für eine vollständige Überprüfung unermesslich hoch sind. Ein anderes Problem ist, dass die Schlüssel zum Entschlüsseln und neu Verschlüsseln meist auf einem zentralen Server liegen. Damit kann ein Administrator des Systems doch den Stimmzettel entschlüsseln. Ein Anbieter dieses Verfahrens in Deutschland ist Polyas[13]. International bekannt ist die spanische Firma Scytl[14], die den Intrusion Test ihrer Implementierung in der Schweiz nicht bestanden hat[15].

8.2. Blockchain und Smart Contracts

Den Anspruch, einer zentralen Instanz nicht vertrauen zu müssen, erfüllen heutige produktive Systeme nicht. Dezentrale Systeme, wie sie mit Blockchains und Smart Contracts in der Wissenschaft diskutiert werden, sind noch zu komplex in der Anwendung und zu teuer in den Transaktionskosten. Damit die Dezentralität gewahrt bleibt, müssen Teilnehmer sich eine Wallet einer Krypto-Währung zulegen und in digitale Währung investieren, damit sie an einer Abstimmung teilnehmen können. Eine aktuelle Implementierung des Verfahrens ist snapshot[16].

9. opn.vote

opn.vote wird ein kostenloses Produkt der openPetition gGmbH für demokratische Online-Abstimmungen sein.

Die Idee zum Produkt entstand aus der Idee heraus, selbstorganisierte bundesweite Volksabstimmungen zu ermöglichen. Online-Abstimmungen werden dabei helfen, die Kosten für Papier, Druck, Porto und Rückporto und den hohen zeitlichen und personellen Aufwand für das Öffnen, Sortieren und Zählen der eingegangenen Stimmen deutlich zu senken.

---

[13] https://www.polyas.de/
[14] https://www.scytl.com/online-voting/invote/
[15] https://www.heise.de/newsticker/meldung/Brisanter-Krypto-Fehler-in-Schweizer-E-Voting-System-entdeckt-4337774.html
[16] https://snapshot.org/

Die demokratischen Grundsätze von Abstimmungen lassen sich in gleicher Weise auf das Unterschreiben von Online-Petitionen, Volksinitiativen und Volksbegehren anwenden. Auch hier müssen Zustimmungsquoren zu einem Anliegen überprüfbar sein, idealerweise unter Wahrung der Privatsphäre der Unterzeichner. Online-Eintragungen bei Volksinitiativen sind heute schon in Schleswig-Holstein möglich[17].

9.1. opn.vote Garantie

Demokratische Online-Abstimmungen sind mit bewussten Einschränkungen praktikabel nutzbar und bieten einen Mehrwert für unsere Beteiligungs-Demokratie. Der Zugang zur Abstimmung für alle Berechtigten ist gewährleistet, eine doppelte Stimmabgabe wird verhindert. Eine geheime Stimmabgabe kann garantiert werden. Eine Überprüfung der eigenen Stimme und der Summe aller Stimmen ist garantiert. Eine glaubhafte Überprüfung des Abstimmungsverfahrens kann gewährleistet werden. Die Abstimmungssoftware ist niederschwellig, unterbrechungsresistent, kostenlos, skalierbar und als offener Quellcode einsehbar.

9.2. opn.vote Einschränkungen

Beim Teilnehmer wird von einer schadsoftwarefreien Hard- und Software ausgegangen. Es wird angenommen, dass diese Voraussetzung für die meisten Teilnehmer erfüllt ist. Eine Verletzung der demokratischen Wahlgrundsätze im Einzelfall kann nicht ausgeschlossen werden.

Eine garantierte geheime Abstimmung erfordert eine weniger benutzerfreundliche Unterbrechung des Abstimmungsprozesses.

Die Abstimmung kann sabotiert werden, wenn die Abstimmungsplattform selbst kompromittiert wird. Eine Kompromittierung der Plattform kann nicht verhindert werden, sie kann jedoch durch Überprüfen des eigenen Stimmzettels und des Gesamtergebnisses aufgedeckt werden.

Die Veröffentlichung eines Zwischenstands der Abstimmung während des Abstimmungszeitraumes kann nicht ausgeschlossen werden, wenn die Organisatoren ihre eigene Abstimmung sabotieren oder die Abstimmungsplattform kompromittiert wurde.

[17] https://serviceportal.schleswig-holstein.de/Verwaltungsportal/Service/Entry/PARTIBUERG

Den Organisatoren der Abstimmung muss im Einzelfall vertraut werden, dass keine Stimmen dazu erfunden werden oder nicht abgegebene Stimmen selbst abgeben werden. Ein massenhafter Missbrauch kann durch nachträgliche statistische Stichprobenanalysen ausgeschlossen werden.

Die hier genannten Einschränkungen betreffen immer Einzelfälle, nie die Abstimmung als Ganzes. Auch bei einer physischen Wahl lässt sich ein Missbrauch im Einzelfall nicht verhindern. Es kommt darauf an, die Wahrscheinlichkeit des Missbrauchs weitestgehend zu reduzieren.

Das Kapitel 10 zeigt Wege auf, wie sich die hier genannten Einschränkungen weiter reduzieren lassen.

9.3. opn.vote Verfahren

Das opn.vote Verfahren basiert auf dem kryptografischen Verfahren der „Blinden Signatur“[18]. Hier ist dem System nicht bekannt, wer die Stimme abgegeben hat, der Stimmzettel muss deshalb bei der Abgabe der Stimme an der Online-Urne nicht verschlüsselt sein. Über eine Blinde Signatur, die das Abstimmungs-Register auf dem ausgefüllten Stimmzettel generiert, ist sichergestellt, dass nur registrierte Teilnehmer an der Abstimmung teilnehmen können und dass die Online-Urne nicht weiß, von wem der Stimmzettel abgegeben wurde.

Das hier verwendete Verfahren wendet die Blinde Signatur nicht auf den Stimmzettel an, sondern auf die Stimmberechtigung[1]. Damit lassen sich Registrierung und Abstimmung entkoppeln und eine Rückverfolgung des Teilnehmers ist selbst bei einer Kollaboration zwischen Register und Urne nicht mehr möglich.

Das Flussdiagramm im Anhang Kapitel 14 gibt eine Übersicht der Kommunikation zwischen den beteiligten Akteuren.

9.3.1. Stimmantrag

Mit dem Stimmantrag wird eine Stimmberechtigung bei den Organisatoren der Abstimmung beantragt. Die Organisatoren verwalten das Register aller Teilnehmer einer Abstimmung. Bei ABSTIMMUNG21 ist openPetition Mitorganisator und verwaltet das Register der Online-Stimmanträge.

[18] https://en.wikipedia.org/wiki/Blind_signature

Der Antrag enthält eine zufällig generierte Zeichenfolge (Token), die der Antragsteller bei sich erzeugt und die nur er persönlich kennt.

Der Antrag wird verschlüsselt an das Register verschickt, so wie bei einem versiegelten Briefumschlag mit dem Antragspapier, so dass der Antrag vom Register nicht eingesehen werden kann. Technisch wird der Antrag mit einem kryptografischen Schlüsselpaar[19] verschlüsselt, welches vorher ebenfalls beim Antragsteller erzeugt wurde.

Bevor der Antrag gesendet wird, müssen Token und Schlüsselpaar vom Antragsteller gespeichert werden. Nur so ist sichergestellt, dass eine später verloren gegangene Stimmberechtigung neu beantragt werden kann.

Zusätzlich zum Antrag muss sich der Antragsteller gegenüber dem Register mit seinem Namen und seiner Adresse als berechtigt ausweisen.

Das Register identifiziert den Antragsteller entweder mit seinem elektronischen Personalausweis oder mit einem PIN-Brief an die Postadresse des Antragstellers.

9.3.2. Stimmberechtigung

Ist der Antragsteller erfolgreich identifiziert, prüft das Register die Berechtigung zur Teilnahme an der Abstimmung. Im Falle einer bundesweiten Volksabstimmung muss der Antragsteller wohnhaft in Deutschland sein.

Hat der Antragsteller noch keinen Stimmantrag vorher gestellt, wird der Antrag zur Teilnahme bewilligt. Das Register signiert den Antrag blind, so wie mit einem Prägedruckstempel durch den Umschlag hindurch auf das Antragspapier, also ohne den Antrag selbst gesehen zu haben. Technisch ist das der Vorgang der Blinden Signatur.

Der Antragsteller muss nun den noch immer verschlüsselten und nun signierten Antrag bei sich wieder entschlüsseln, so wie ein versiegelter Briefumschlag geöffnet wird. Der Antrag mit dem Prägestempel des Registers berechtigt zur Teilnahme an der Abstimmung. Technisch stellt das kryptografische Verfahren der Blinden Signatur sicher, dass die Signatur des Registers erhalten bleibt, wenn der signierte Antrag beim Antragsteller entschlüsselt wird.

Der Stimmberechtigte kann die Stimmberechtigung für eine spätere Stimmabgabe speichern oder sofort mit der Stimmabgabe fortfahren.

[19] https://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem

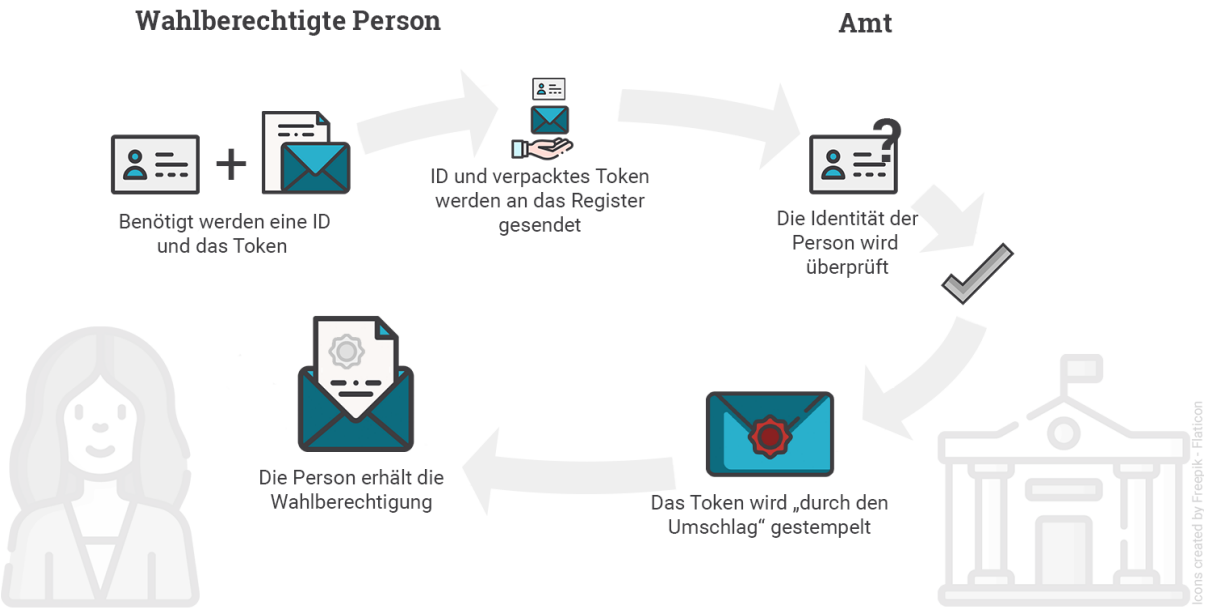


Abbildung 1: Blinde Signatur Verfahren für die Stimmberechtigung

9.3.3. Stimmabgabe

Die Stimmabgabe ist während des von den Organisatoren festgelegten Abstimmungszeitraums möglich. Stimmberechtigte melden sich mit ihrer Stimmberechtigung auf der Abstimmungsseite der Online-Urne an.

Die Urne prüft, ob die Signatur des Registers in der Stimmberechtigung valide ist und gibt im Erfolgsfall eine Seite mit dem Stimmzettel zurück. Der ausgefüllte und signierte Stimmzettel geht zurück an die Urne, wobei es möglich sein muss, ungültig abzustimmen. Die Urne sendet eine Quittung mit der Urnen-Signatur zurück an den Abstimmungsteilnehmer.

Der Teilnehmer überprüft bei sich, ob der quittierte Stimmzettel der eigenen Stimmabgabe entspricht.

Eine Abstimmung kann mehrmals wiederholt werden. Bei der Auszählung wird jeweils nur die letzte abgegebene Stimme pro Stimmberechtigung gezählt.

Wenn Stimmquittungen reproduzierbar fehlerhaft sind, muss die Abstimmung annulliert werden.

9.3.4. Abstimmungsergebnis

Nach Ende des Abstimmungszeitraums veröffentlicht das Register eine anonyme Liste aller Teilnehmer, deren Einträge nur für den jeweiligen Teilnehmer selbst lesbar sind (Hashfunktion).

Die Urne veröffentlicht die Stimmen aller abgegebenen Stimmzettel im Klartext, mit den Stimmberechtigungen der Teilnehmer.

Das Abstimmungsergebnis ergibt sich direkt aus den veröffentlichten Stimmen.

9.3.5. Überprüfung

Nach der Veröffentlichung des Abstimmungsergebnisses kann jeder Teilnehmer in der Liste der veröffentlichten Stimmen mit Hilfe seiner Stimmberechtigung überprüfen, ob seine Stimme richtig gezählt wurde.

Das Gesamtergebnis lässt sich einfach durch aufaddieren der veröffentlichten Einzelstimmen ermitteln und überprüfen.

Die Gültigkeit der Abstimmung kann überprüft werden, indem überprüft wird, dass Stimmberechtigungen nicht mehrfach vorkommen und dass alle Stimmberechtigungen eine valide Signatur des Registers haben.

9.3.6. Warum ist das Wahlgeheimnis geschützt, auch wenn das Wahlsystem kompromittiert ist?

Das Register kennt Name und Adresse des Teilnehmers. Das Register signiert einen Stimmantrag, den es selbst jedoch nicht sehen kann. Um den Stimmantrag sehen zu können, müsste es das kryptografische Verfahren (RSA-Verfahren) der Blinden Signatur brechen, was mit heutigen Rechnern nicht möglich ist[20].

Die Urne sieht den signierten Stimmantrag (Stimmberechtigung), der selbst keinen Rückschluss auf eine Person zulässt, da er nur die persönliche Zeichenfolge enthält, die sonst niemandem mitgeteilt wurde.

Auch wenn die Urne mit dem Register kollaboriert, weiß auch das Register nicht, wem es die persönliche Zeichenfolge zuordnen soll, weil es sie nicht gesehen haben kann.

Teilnehmer werden darauf hingewiesen, wenn sie bei Stimmantrag und Stimmabgabe die selbe IP-Adressen verwenden mit einer Erklärung, wie sie ihre IP-Adresse ändern können. Damit ist eine Zuordnung von Stimmantrag zu Stimmabgabe über die IP-Adresse durch das System ausgeschlossen.

Die Urne gewährleistet nachvollziehbar, dass sie keine Cookies speichert und kein Cross-Site Tracking eingebaut hat, um nicht doch Rückschlüsse auf die

[20] http://geb.uni-giessen.de/geb/volltexte/2005/2267/pdf/FremdtChristine-2005-06-24.pdf

Identität des Teilnehmers durch Aktivitäten auf anderen Seiten treffen zu können.

Zukünftige Quantencomputer könnten heutige sichere blinde Signaturen brechen. Es ist zu erwarten, dass quantenkryptographisch sichere digitale Signaturverfahren heutige Signaturverfahren ablösen werden, um diese Gefahr zu kompensieren.

9.3.7. Warum ist die Überprüfbarkeit der abgegebenen Stimmen gesichert, auch wenn das Wahlsystem kompromittiert ist?

Für einen Angreifer gibt es keinen Anreiz die abgegebenen Stimmen im Wahlsystem zu manipulieren, da es ausreicht, wenn nur einer der Teilnehmer eine Abweichung zwischen veröffentlichter Stimme und der eigenen Stimmquittung nachweisen kann und die Wahl damit annulliert wäre.

Jeder Teilnehmer kann seine eigene Stimmabgabe überprüfen. Wenn genügend Teilnehmer ihre Stimme prüfen ist die statistische Wahrscheinlichkeit sehr hoch, dass eine Manipulation selbst im Einzelfall erkannt wird. Es wird eine Prüfquote von mindestens 50% angestrebt. Eine Manipulation von mindestens 1% der abgegebenen Stimmen würde dann statistisch bei jeder 2. Wahl nachgewiesen werden können.

Um die Wahl nicht sabotieren zu können, indem eine falsche Abweichung gemeldet wird, muss der Stimmzettel eine valide Signatur des Teilnehmers haben und die Stimmquittung eine valide Signatur der Urne haben.

Ein Auffüllen von abgegebenen Stimmen oder das Erfinden von Stimmen kann bei einem zentralen Register, das kompromittiert wurde, nicht verhindert werden. Dazu bedarf es eines dezentralen Registers (siehe Kapitel 10.4) oder einer „Gruppen-Registrierung“ (siehe Kapitel 10.5)

9.3.8. Warum ist das Verfahren der Blinden Signatur in produktiven Wahlsystemen kaum verbreitet?

Das Verfahren der Blinden Signatur ist aufwendiger als sich einfach mit seiner ID und seinem Passwort anzumelden. Es muss sichergestellt werden, dass Schlüsselpaar und die persönliche Zeichenfolge des Stimmantrags beim Teilnehmer gespeichert sind, bevor der Stimmantrag gestellt wird.

9.4. opn.vote Praxistest

opn.vote wird erstmals Anfang 2023 für die zweite deutschlandweite selbstorganisierte Online-Volksabstimmung des Vereins ABSTIMMUNG21 e.V.[21] eingesetzt.

Die Teilnehmer haben die Wahl zwischen einer Online-Abstimmung und einer Abstimmung per Brief. Eine doppelte Abstimmung per Brief und online ist ausgeschlossen. Bevor die Abstimmungsunterlagen versendet werden, erfolgt ein Adressabgleich mit den registrierten Teilnehmern zur Online-Abstimmung. Nach Versand der Abstimmungsunterlagen ist eine Teilnahme nur noch online möglich.

10. Ausblick

Es werden hier mögliche Erweiterungen des opn.vote Verfahrens vorgestellt, um die in Kapitel 9.2 genannten Einschränkungen aufzuheben.

Die Sicherstellung der Kontrolle über das eigene Gerät sowie die Verschleierung der IP-Adresse sind generelle Herausforderungen in der Nutzung des Internets und stehen nicht im Fokus von opn.vote.

10.1. Freiheit

Es sollte die Möglichkeit bestehen, eine Online-Abstimmung durch eine Abstimmung vor Ort am Wahltag zu überschreiben [2]. Damit könnten gekaufte Stimmen und Stimmen unter Zwang ausgeschlossen werden.

10.2. Robustheit

Die Möglichkeit der Sabotage der gesamten Abstimmung kann über dezentrale Abstimmungsurnen weiter reduziert werden.

Dezentrale Urnen mit einer dezentralen Stimmabgabe und Auszählung der Stimmen minimieren das Risiko der Sabotage auf jeweils eine dieser Urnen. Das Register merkt sich, bei welcher Urne ein Teilnehmer abgestimmt hat. Die Auswahl der Urne bestimmt ein externer Zufall[22]. Die Zufallswerte müssen revisionssicher veröffentlicht werden. Im Falle einer Sabotage muss nur für diese eine Urne eine Wiederholung der Abstimmung organisiert werden.

[21] https://abstimmung21.de/
[22] https://www.random.org/randomness/

Es braucht ein von den Organisatoren der Abstimmung unabhängiges Verfahren, um Urnen zu registrieren und zu betreiben.

Das Risiko einer vorherigen Veröffentlichung eines Zwischenergebnisses lässt sich reduzieren, wenn der gemeinsame Schlüssel zur Veröffentlichung der Ergebnisse unter allen Urnenbetreibern aufgeteilt wird.

10.3. Transparenz

Eine tägliche, inkrementelle Veröffentlichung der Listen der anonymisierten Registrierungen und der verschlüsselten Stimmabgaben verringert das Risiko einer nachträglichen Manipulation der Listen. Das IPFS[23] eignet sich hierfür als revisionssicheres Archiv. Vorherige Veröffentlichungen werden in der aktuellen Veröffentlichung referenziert. Die Veröffentlichungen werden von der Abstimmungsplattform signiert und mit einem Zeitstempel versehen, damit eine spätere Manipulation der Listen bewiesen werden kann.

Eine Veröffentlichung der Stimmabgaben in Echtzeit würde dem Teilnehmer zusätzlich die Sicherheit geben, dass seine Stimme unveränderlich eingegangen ist. Eine weitere Prüfung der Stimme nach der Abstimmung wäre dann entbehrlich.

10.4. Vertrauen

Die Abhängigkeit von der Vertrauenswürdigkeit des Registers lässt sich durch eine verteilte Registrierung reduzieren.

Für eine gültige Wahlberechtigung braucht es die Signaturen von einer Mindestanzahl von Registraren [3]. Registrare prüfen die Identität des Teilnehmers anhand eines Identifikationsausweises und signieren die Stimmberechtigung des Teilnehmers. Von welchen Registraren ein Teilnehmer überprüft wird, bestimmt ein externer Zufall. Die Zufallswerte müssen revisionssicher veröffentlicht werden. Es steht jedem frei, sich als Registrar zur Verfügung zu stellen.

10.5. Zugang

Die Abhängigkeit von einer zentralen staatlichen Instanz für die Ausgabe von Identifikationsausweisen lässt sich durch ein dezentrales Identifikationsverfahren reduzieren.

[23] https://de.wikipedia.org/wiki/InterPlanetary_File_System

Es könnte ausreichen, wenn eine Person sich einmal im Jahr über ihre physische Präsenz zu einem bestimmten Zeitpunkt an einem bestimmten Ort als mündiger Bürger präsentiert und sich dort gegenseitig eine eindeutige Abstimmungsberechtigung ausstellt [4]. Da eine Person zu einem Zeitpunkt nur an einem Ort gleichzeitig sein kann ist sichergestellt, dass diese Person nur eine Stimmberechtigung erhält. Zudem ist sichergestellt, dass diese Person real existiert und keine Sockenpuppe[24] ist. Das setzt voraus, dass alle anderen Verpflichtungen zu diesem bestimmten Zeitpunkt dahinter zurückstehen. Es könnte verbunden werden mit einem/r großen (Mani-)Fest(-ation) der Demokratie.

11. Fazit

Die Frage, ob Online-Wahlen und Abstimmungen im Netz stattfinden sollen oder nicht, ist bereits entschieden. Die wissenschaftlichen Grundlagen und die technischen Voraussetzungen sind gegeben und sie werden bereits aktiv genutzt, sei es aus kommerziellen Interessen oder politisch motiviert. Mitunter helfen Sie autokratischen Staaten eine Wahl noch einfacher zu manipulieren[25] oder demokratischen Staaten sich als technisch fortschrittlich zu zeigen, ohne das Wahlgeheimnis garantieren zu können [5]. Schon jetzt wird mit hohen Erwartungen in die Entwicklung von E-Voting Systemen investiert, ohne ausreichende Transparenz, Evaluation und öffentlichen Diskurs[26].

Es ist an uns allen sicher zu stellen, dass Online-Entscheidungen im Netz zu demokratischen Online-Entscheidungen werden. Es braucht ein breites Wissen darum, wann eine Entscheidung im Netz demokratisch legitimiert ist.

Die vollautomatische, demokratische Online-Abstimmung wird es nicht geben.

Es braucht die Kontrolle des Verfahrens durch die teilnehmenden Menschen selbst. Es braucht weiterhin Menschen, die Online-Registrierung, -Stimmabgabe und -Stimmauswertung überprüfen.

Die Technik kann Wahlen und Abstimmungen in den digitalen Raum holen, die Wahlhelfer und Wahlbeobachter ersetzen kann sie nicht.

---

[24] https://de.wikipedia.org/wiki/Sockenpuppe_(Netzkultur)

[25] https://www.heise.de/news/Wahlen-in-Russland-Rufe-nach-Annullierung-der-Online-Ergebnisse-6196498.html

[26] https://www.digitale-gesellschaft.ch/2021/08/04/nach-20-jahren-gescheitertem-versuchsbetrieb-soll-an-e-voting-unbeirrt-festgehalten-werden-updates-stellungnahme/

12. Quellen

[1] O. &. D. A. Cetinkaya, „Pseudo-Voter Identity (PVID) Scheme for e-Voting Protocols," 2007. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4159926

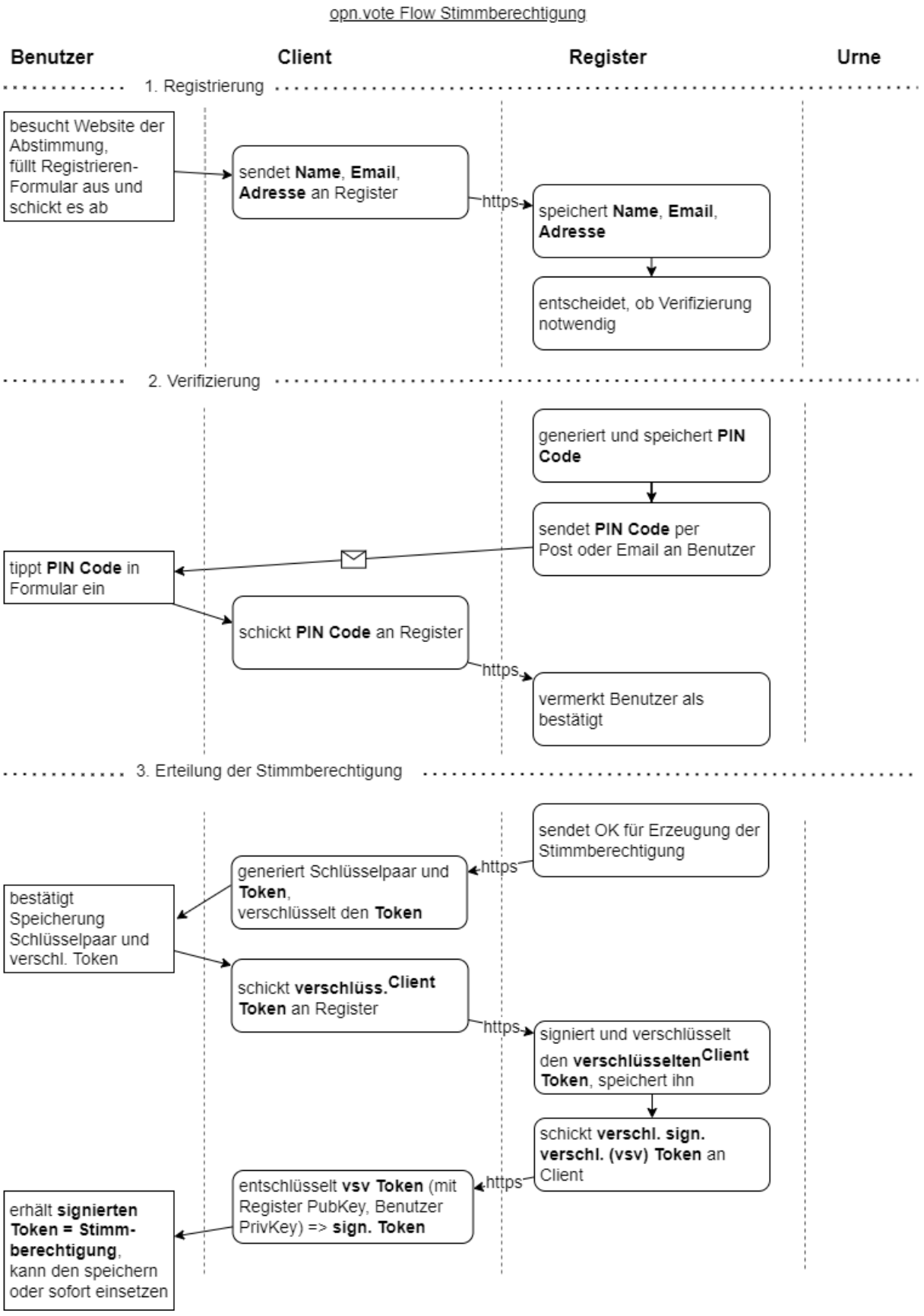
[2] R. K. R. F. S. &. D. E. Haenni, „TrustVote: A proposal for a hybrid e-voting system," 2009. [Online]. Available: https://www.researchgate.net/profile/Eric-Dubuis/publication/266046766_TrustVote_A_Proposal_for_a_Hybrid_E-Voting_System/links/573c306d08aea45ee841550d/TrustVote-A-Proposal-for-a-Hybrid-E-Voting-System.pdf

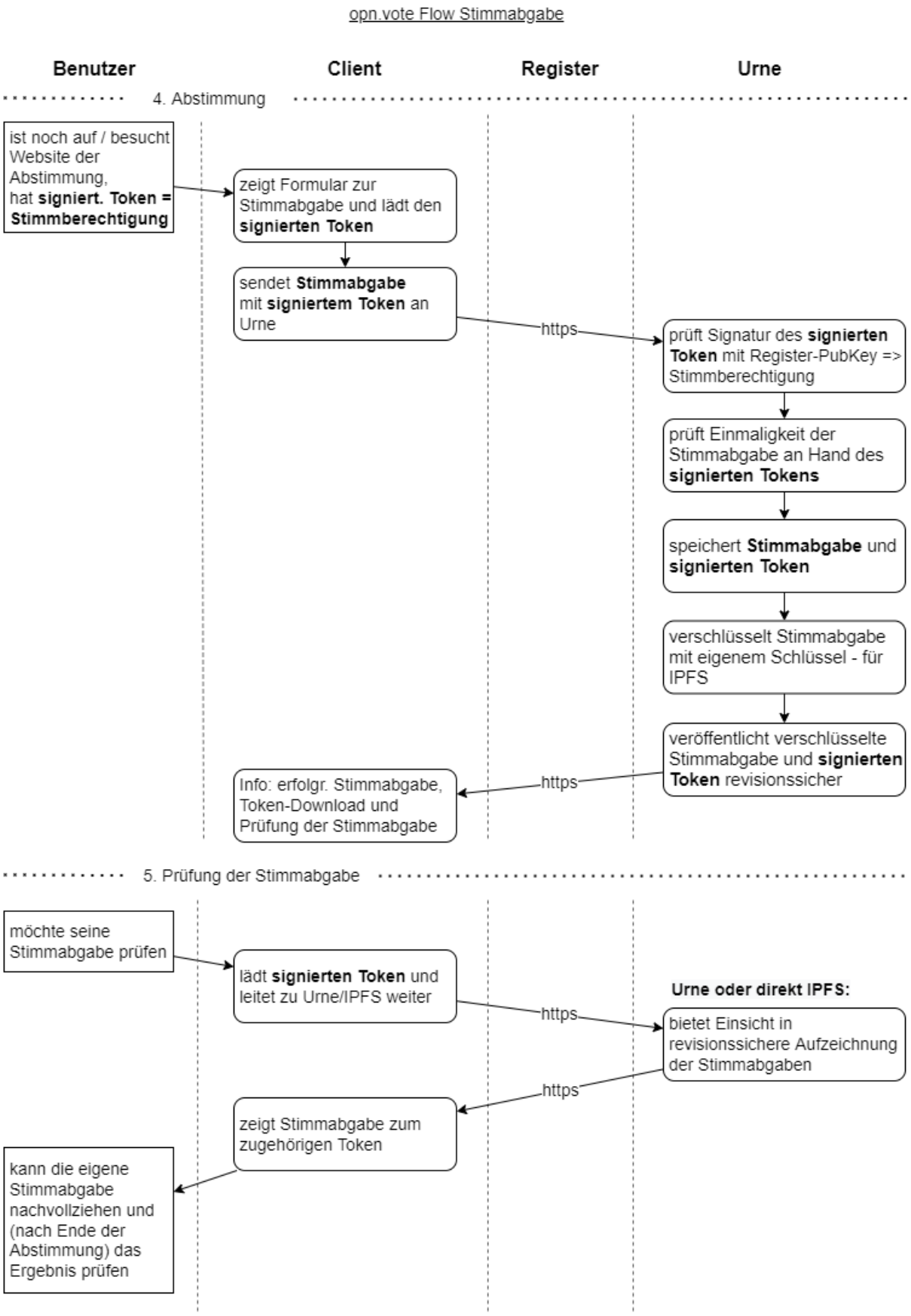
[3] R. E. D. E. &. H. R. Koenig, „Why Public Registration Boards are Required in E-Voting," 2010. [Online]. Available: https://dl.gi.de/handle/20.500.12116/19497

[4] B. Ford, „Identity and Personhood in Digital Democracy: Evaluating Inclusion, Equality, Security, and Privacy in Pseudonym Parties and Other Proofs of Personhood," 2020. [Online]. Available: https://arxiv.org/abs/2011.02412

[5] D. &. M. T. Clarke, „E-voting in Estonia," 2016. [Online]. Available: https://arxiv.org/pdf/1606.08654

13. ANHANG


opn.vote Flow Stimmberechtigung
Benutzer
Client
Register
Urne
1. Registrierung
besucht Website der Abstimmung, füllt Registrieren-Formular aus und schickt es ab
sendet Name, Email, Adresse an Register
https
speichert Name, Email, Adresse
entscheidet, ob Verifizierung notwendig
2. Verifizierung
generiert und speichert PIN Code
sendet PIN Code per Post oder Email an Benutzer
tippt PIN Code in Formular ein
schickt PIN Code an Register
https
vermerkt Benutzer als bestätigt
3. Erteilung der Stimmberechtigung
sendet OK für Erzeugung der Stimmberechtigung
https
generiert Schlüsselpaar und Token, verschlüsselt den Token
bestätigt Speicherung Schlüsselpaar und verschl. Token
schickt verschlüss.Client Token an Register
https
signiert und verschlüsselt den verschlüsseltenClient Token, speichert ihn
schickt verschl. sign. verschl. (vsv) Token an Client
https
entschlüsselt vsv Token (mit Register PubKey, Benutzer PrivKey) => sign. Token
erhält signierten Token = Stimm-berechtigung, kann den speichern oder sofort einsetzen


opn.vote Flow Stimmabgabe
Benutzer
Client
Register
Urne
4. Abstimmung
ist noch auf / besucht Website der Abstimmung, hat signiert. Token = Stimmberechtigung
zeigt Formular zur Stimmabgabe und lädt den signierten Token
sendet Stimmabgabe mit signiertem Token an Urne
https
prüft Signatur des signierten Token mit Register-PubKey => Stimmberechtigung
prüft Einmaligkeit der Stimmabgabe an Hand des signierten Tokens
speichert Stimmabgabe und signierten Token
verschlüsselt Stimmabgabe mit eigenem Schlüssel - für IPFS
veröffentlicht verschlüsselte Stimmabgabe und signierten Token revisionssicher
https
Info: erfolgr. Stimmabgabe, Token-Download und Prüfung der Stimmabgabe
5. Prüfung der Stimmabgabe
möchte seine Stimmabgabe prüfen
lädt signierten Token und leitet zu Urne/IPFS weiter
https
Urne oder direkt IPFS:
bietet Einsicht in revisionssichere Aufzeichnung der Stimmabgaben
https
zeigt Stimmabgabe zum zugehörigen Token
kann die eigene Stimmabgabe nachvollziehen und (nach Ende der Abstimmung) das Ergebnis prüfen

openPetition

info@openpetition.eu

www.openpetition.de

openPetition gGmbH

Werkstatt Digitale Demokratie

Am Friedrichshain 34, 10407 Berlin