

Anonyme Online-Wahlen

Lösungsansätze für die Realisierung von Online-Wahlen

Markus Ullmann, Frank Koob, Harald Kelter

In diesem Beitrag werden die Sicherheitsziele für politische Wahlen und bestehende Lösungsansätze für die Realisierung von Online-Wahlen gegenübergestellt und Problembereiche aufgezeigt. Basierend hierauf wird ein Realisierungskonzept für Online-Wahllokale skizziert.¹



Dipl.-Ing. Markus Ullmann

Referatsleiter im Bundesamt für Sicherheit i.d. Informationstechnik (BSI)

Arbeitsschwerpunkt: Sicherheitsmodelle und -Methodik

E-Mail: markus.ullmann@bsi.bund.de



Dipl.-Math. Frank Koob

Mitarbeiter des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Arbeitsschwerpunkt: Formale Methoden und Analyse von Sicherheitsprotokollen

E-Mail: frank.koob@bsi.bund.de



Dipl.-Ing. (FH) Harald Kelter

Mitarbeiter des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Arbeitsschwerpunkt: Kommunikationssicherheit und Sicherheitstrends

E-Mail: harald.kelter@bsi.bund.de

Einleitung

Das Thema Online-Wahlen erfreut sich zur Zeit im Zuge der Diskussion um e-government einer großen Beliebtheit. Weltweit gibt es Initiativen und Forschungsprojekte, die das Wählen über das Internet oder Handys ermöglichen wollen. In Estland ist beispielsweise die erste politische Online-Wahl für das Jahr 2003 angekündigt.

Wahlvorgänge spielen aber nicht nur eine Rolle in der politischen Meinungsbildung. Gewählt wird in unterschiedlichsten Institutionen, wie Aktiengesellschaften, Vereinen, politischen Parteien, Hochschulen. Die folgenden Betrachtungen konzentrieren sich auf politische Wahlen in Deutschland.

Zunächst soll der Begriff der Online-Wahl für die weitere Diskussion präzisiert werden: Unter Online-Wahlen wird hier die Möglichkeit verstanden, sich von jedem beliebigen Ort mittels entsprechender technischer Geräte (PCs, Handys) an Wahlvorgängen zu beteiligen.

Von Online-Wahlen versprechen sich sowohl die Wähler als auch die Wahlverantwortlichen Vorteile. Aus Sicht des Wählers ist es höchst wünschenswert, den Wahlvorgang von zu Hause oder, wenn er unterwegs ist, kurzerhand von seinem Handy von jedem Ort aus durchzuführen. Damit könnte er selbst an Wahltagen ein Höchstmaß an Mobilität aufrechterhalten.

Wahlverantwortliche erwarten von Online-Wahlen eine vereinfachte und beschleunigte Auszählung der Stimmen mit dem Ziel, das Wahlergebnis bereits unmittelbar nach der Wahl verkünden zu können. Langfristig wird prognostiziert, dass durch Online-Wahlen bei der Vorbereitung und Durchführung erhebliche Kosteneinsparungen gegenüber den heutigen Verfahren erzielt werden können.

Hinzu kommt das Problem, ausreichend Wahlhelfer für die Durchführung von Wahlen zu finden. Auch hier wird eine Entspannung erhofft, da durch eine zunehmende technische Unterstützung von Wahlvorgängen Wahlhelfer eingespart werden könnten.

1 Anforderungen

An politische Wahlen werden sehr hohe Anforderungen gestellt, die sich aus Artikel 38 des Grundgesetzes ableiten. Diese definieren die globalen Sicherheitsziele, die jedes Wahlverfahren erfüllen muss. Im Einzelnen sind dies:

- **Allgemeine Wahl:** Jeder Wahlberechtigte muss wählen können.
- **Unmittelbare Wahl:** Jedes abgegebene Votum wirkt sich unmittelbar auf das zu wählende Gremium aus.
- **Freie Wahl:** Es darf keinen Druck auf die Entscheidung vor oder während der Wahl und keinen Nachteil durch die Entscheidung nach der Wahl geben.
- **Gleiche Wahl:** Jedes gültige abgegebene Votum hat den gleichen Wert.
- **Geheime Wahl:** Die Entscheidung des Wählers darf nie auf ihn zurückgeführt werden können.

Was sollte man als erstes tun, wenn man über neue Arten des Wählens nachdenkt? Zunächst muss man sich die entsprechenden Rechtsvorschriften anschauen und prüfen, welche Anforderungen sich daraus im Einzelnen herleiten aber auch, an welchen Stellen Änderungen oder Ergänzungen notwendig sind. Die relevanten Rechtsvorschriften sind das Bundeswahlgesetz, die Bundeswahlordnung, aber auch die Verordnung über den Einsatz von Wahlgeräten und die Richtlinie für die Bauart von Wahlgeräten. Ergebnis dieser Prüfung sollten sowohl die zu erfüllenden Sicherheitsanforderungen als auch die eventuell notwendigen Änderungen an den Rechtsvorschriften sein.

¹ Der Beitrag gibt ausschließlich die persönliche Meinung der Autoren wieder.

Im Folgenden wird auf die zu erfüllenden Sicherheitsanforderungen näher eingegangen. Aus diesen müssen sich die oben genannten globalen Sicherheitsziele ableiten lassen. Um bei politischen Wahlen seine Stimme online abzugeben, müssen mindestens folgende organisatorische und technische Anforderungen erfüllt werden.

Geheime Wahl

Der Grundsatz der geheimen Wahl hat Verfassungsrang. Er besagt, dass unbekannt bleiben muss, welche Wahlentscheidung der Wähler getroffen hat. Das Wahlgeheimnis ist für den einzelnen Wähler obligatorisch und unverzichtbar, d.h. er darf nicht nur, er muss geheim wählen. Dieser Grundsatz dient nicht nur dem Schutz des einzelnen Wählers sondern auch dem öffentlichen Interesse an einem – auf der kollektiven freien Willensentscheidung des Wahlvolkes beruhenden – Wahlergebnis als demokratische Legitimation staatlichen Handelns.

Die geheime Wahl erfordert eine technische Gestaltung des Wahlvorganges, die es unmöglich macht, die Wahlentscheidung eines Wählers zu erkennen oder zu rekonstruieren. Das bedeutet, dass das Wahlverhalten jedes Wählers auch nach der Stimmabgabe dauerhaft geheim bleiben muss. Dabei meint dauerhaft wirklich unbegrenzt. Dies ist eine sehr hohe Anforderung an eine technische Umsetzung, da eine zeitlich uneingeschränkte Sicherheitsaussage über z.B. heute eingesetzte Verschlüsselungsverfahren nicht möglich ist.

Freie Wahl

Der Grundsatz der geheimen Wahl ist eng verknüpft mit demjenigen der freien Wahl. Dieser meint die Ausübung des aktiven Wahlrechts ohne physischen Zwang oder psychischen Druck. Dies ist nur dann gewährleistet, wenn der Wähler davon ausgehen kann, dass seine Wahlentscheidung dauerhaft unbekannt bleibt. Dieser Umstand schützt die freie Wahlentscheidung des Wählers gegenüber Drohungen und Versprechungen für sein Stimmverhalten.

Gleichheit der Wahl

Dieser verfassungsrechtliche Wahlrechtsgrundsatz bedeutet, dass alle Wähler mit der Stimme, die sie abgeben, den gleichen Einfluss auf das Wahlergebnis haben. Die Stimme jedes Wählers muss den gleichen Zählwert haben. In diesem Zusammenhang gilt es zu verhindern, dass ein Wähler seine Stimme mehrfach abgibt oder die Stimme eines Wählers bei der Ergebnisfeststellung mehrfach gezählt wird. Es muss also insbe-

sondere sichergestellt werden, dass Mehrfachabgaben des gleichen Votums erkannt und ausgeschlossen werden können.

Stimmabgabe durch Wahlberechtigte

Im Bundeswahlgesetz wird der Kreis der Wahlberechtigten bei Bundestagswahlen festgelegt. Bei der Durchführung der Wahl muss es insbesondere möglich sein zu überprüfen, dass derjenige, der ein Votum abgibt, auch wahlberechtigt ist. Und natürlich darf bei dieser Überprüfung die Wahlentscheidung nicht erkennbar sein.

Manipulationssicherheit

Es muss sichergestellt werden, dass sowohl das Wählervotum als auch die von Wählerorganen ermittelten Wahlergebnisse sowohl bei der Übertragung als auch bei der anschließenden Speicherung nicht verändert werden können und vor fälschenden Einflüssen sicher sind.

Verfügbarkeit und Funktionsfähigkeit

Eine Wahl ist an dem dafür festgesetzten Tag durchzuführen. Deshalb muss das Wahlsystem an dem Tag der Wahl sowohl verfügbar als auch funktionsfähig sein. Dies muss man insbesondere in Anbetracht der in der Vergangenheit immer häufiger vorkommenden DoS-Attacken beachten.

Die genannten Sicherheitsanforderungen sollen nur einen Eindruck vermitteln, mit welcher Art von Anforderungen man es zu tun hat. Ein Anspruch auf Vollständigkeit wird von Seiten der Autoren nicht erhoben.

2 Diskutierte Ansätze

Im Folgenden werden einige häufig diskutierte Ansätze zur Durchführung von Online-Wahlen im Hinblick auf die Erfüllung der genannten Sicherheitsanforderungen untersucht (siehe auch [SCHN1996]).

2.1 Einsatz asymmetrischer Kryptographie

Das einfachste denkbare Protokoll zur Realisierung eines elektronischen Wahlvorganges basiert auf der Verwendung asymmetrischer Kryptographie. Dabei chiffriert jeder Wähler sein Votum mit dem öffentlichen Schlüssel des Wahllokals und sendet diesem anschließend die erzeugte Nachricht. Das Wahllokal kann mit Hilfe seines privaten Schlüssels die Nachricht dechif-

frieren und die abgegebene Stimme auszählen.

Auf den ersten Blick gewährleistet dieses Verfahren, dass ein Votum während der Übertragung nicht manipuliert werden kann und einem unberechtigten Dritten nicht bekannt wird. Berücksichtigt man aber die geringe Menge der möglichen zu übertragenden chiffrierten Wahlzettel, ist die geheime Wahl nicht gewährleistet.

Außerdem versagt es bei der Authentisierung des Wählers: Das Wahllokal ist nicht in der Lage festzustellen, von wem es ein Votum erhalten hat. Damit ist mehrfaches Wählen ohne Probleme möglich. Allerdings lässt sich dieses Verfahren verbessern.

2.2 Verwendung einer digitalen Signatur

Ergänzt man das oben beschriebene Verfahren um eine digitale Signatur, können zusätzliche Sicherheitsanforderungen erfüllt werden:

- Ein Wähler signiert sein Votum mit seinem privaten Schlüssel.
- Das signierte Votum wird vom Wähler mit dem öffentlichen Schlüssel des Wahllokals chiffriert.
- Der Wähler sendet das signierte und chiffrierte Votum an das Wahllokal.
- Das Wahllokal entschlüsselt die Nachricht mit seinem privaten Schlüssel.
- Das Wahllokal überprüft die Unterschrift des entschlüsselten Dokuments und zählt die Stimme.

Durch das Einführen der digitalen Signatur wird die Authentisierung des Wählers möglich. Ebenfalls ergibt sich bei diesem Verfahren eine Möglichkeit zur Erkennung einer Mehrfachwahl. Dazu muss das Wahllokal lediglich festhalten, ob ein Wahlberechtigter schon gewählt hat oder nicht.

Gleichzeitig wird bei Einsatz dieses Wahlprotokolls allerdings eine neue Instanz erforderlich: Damit das Wahllokal einen Wähler authentisieren und die Tatsache seiner Stimmabgabe dokumentieren kann, muss es Zugriff auf ein Wählerverzeichnis haben. Innerhalb dieses Wählerverzeichnisses sind alle berechtigten Wähler sowie ihre zugehörigen öffentlichen Schlüssel aufgeführt.

Allerdings sind immer noch nicht alle Sicherheitsanforderungen erfüllt. Das Chiffrieren des signierten Votums durch den Wähler verhindert zwar, dass beim Abhören der Kommunikation zwischen Wähler und

Wahllokal das Votum bekannt wird, dem Wahllokal selbst ist die Zuordnung zwischen Wähler und Votum jedoch möglich.

Gesucht wird also eine Möglichkeit, einen Wähler zu authentisieren, seine Identität jedoch gegenüber dem Wahllokal nicht zu offenbaren.

2.3 Digitale Pseudonyme und das MIX-Modell

David Chaum hat 1981 in seiner Arbeit „Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms“ [CHAU1981] eine Möglichkeit zur anonymen Nutzung von Kommunikationsnetzen aufgezeigt.

Grundsätzlich geht es beim Einsatz des von ihm vorgeschlagenen MIX-Modells darum, dass zwei miteinander kommunizierende Instanzen, eben Sender und Empfänger, dies nicht direkt über das verwendete Kommunikationsmedium tun, sondern eine dritte Instanz gewissermaßen als Relais verwenden: den MIX.

Geht man im MIX-Modell davon aus, dass jede Kommunikationsinstanz im Besitz eines zu einem asymmetrischen Kryptosystem gehörenden Schlüsselpaares ist, wird eine vom Sender X zum Empfänger Y über den MIX M versendete Nachricht N in der folgenden Art und Weise durch den Sender X behandelt:

- Verschlüssele N mit dem öffentlichen Schlüssel von Y.
- Füge an das Ergebnis die Adresse des Empfängers Y an.
- Verschlüssele die erhaltene Zeichenkette mit dem öffentlichen Schlüssel von M.

Anschließend kann X die Nachricht versenden. Der MIX M entschlüsselt das erhaltene Paket mit seinem privaten Schlüssel, findet die Adresse des Empfängers vor und leitet das erhaltene Paket weiter an Y. Der Empfänger kann das erhaltene Paket nun mit seinem privaten Schlüssel entschlüsseln und die Nachricht lesen.

Tatsächlich werden von Chaum mehrere Verbesserungen des Verfahrens vorgeschlagen, wie das Verwenden von Füllbits als Maßnahme gegen Korrelationsangriffe und das Einführen einer History gegen Replay-Angriffe, grundsätzlich gibt die beschriebene Vorgehensweise jedoch die Funktionalität des MIX-Modells wieder. Erweitert man das Verfahren durch die Verwendung von MIX-Kaskaden oder MIX-Netzen, lässt sich die Sicherheit des Gesamtverfahrens sehr gut skalieren sowie eine Kompromittierung

der Kommunikation durch die Kompromittierung eines einzelnen MIX verhindern.

Als Anwendungsbeispiel des MIX-Modells formulierte Chaum sogenannte digitale Pseudonyme. Diese sollen es dem Empfänger einer anonym zugestellten Nachricht ermöglichen, sie eindeutig einem Sender zuzuordnen, ohne dass dessen wahre Identität aufgedeckt wird.

Das von Chaum eingeführte digitale Pseudonym ist dabei eigentlich lediglich der öffentliche Schlüssel eines Senders. Signiert der Sender eine Nachricht mit seinem privaten Schlüssel, kann die Signatur mit Hilfe des zugehörigen öffentlichen Schlüssels geprüft und somit der Urheber der Nachricht identifiziert werden. Eine dritte Instanz muss anhand von Daten über den Sender Entscheidungen über die Zertifizierung treffen.

Alle durch die Zertifizierungsinstanz akzeptierten Pseudonyme werden in Listen, ohne Zuordnung der wahren Identität und somit anonym, veröffentlicht.

Am Beispiel der Online-Wahl erklärt, würde der Einsatz eines digitalen Pseudonyms etwa folgendermaßen ablaufen:

Der Wähler (Sender) kann seine Stimme (Nachricht) mit seinem privaten Schlüssel signieren und zusammen mit seinem öffentlichen Schlüssel, dem digitalen Pseudonym, anonym über ein MIX-Netz zum Wahllokal schicken. Dort wird mit Hilfe der Liste der gültigen Pseudonyme geprüft, ob die Nachricht angenommen werden soll. Nach Anwenden des digitalen Pseudonyms auf die Nachricht kann die Stimme gezählt werden.

Obwohl dieses Verfahren im Hinblick auf die Erfüllung der Sicherheitsanforderungen deutlich mehr leistet als die beiden vorher diskutierten Verfahren, bleibt die Bewertung der Anonymisierung durch das MIX-Netz hinsichtlich der Dauerhaftigkeit der Trennung von Wähleridentität und Votum problematisch.

2.4 Blinde Signaturen

Ein weiterer Versuch, das Wählervotum vom Wähler zu trennen, ohne dabei die Möglichkeit der Authentifizierung zu verlieren, ist der Einsatz der ebenfalls von Chaum entwickelten blinden Signaturen [CHAU1982]. Sinn einer blinden Signatur ist es, sich ein Dokument von jemandem signieren zu lassen, ohne dass derjenige erkennen oder herausfinden kann, was er unterschreibt.

Blinde Signaturen verfolgen also das entgegengesetzte Ziel von digitalen Signaturen, bei denen es wesentlich ist, dass der Unterzeichner weiß, was er unterschreibt.

Wie das Verfahren funktioniert, sei an einem kurzen Beispiel erläutert. Dazu wird angenommen, dass die Signaturfunktion und die Multiplikation kommutativ sind. Ein Beispiel für eine solche Signaturfunktion ist eine auf dem RSA-Verfahren basierende Funktion.

Um ein Dokument blind signieren zu lassen, multipliziert der Ersteller das Dokument mit einer Zufallszahl, die er selber gewählt hat und die er geheim hält. Dieses damit unkenntlich gemachte Dokument lässt er nun vom Unterzeichner signieren. Da dieser den Blindfaktor nicht kennt, weiß er auch nicht, was er unterschreibt. Der Ersteller des Dokumentes kann auf Grund der Kommutativität den Blindfaktor wieder herausrechnen und erhält so das unterschriebene Originaldokument.

Ein Einsatzfeld blinder Signaturen sind Protokolle, die für Zahlungssysteme mit elektronischem Geld verwendet werden.² Ein bekanntes Beispiel für ein solches System ist DigiCash [DiCa1994]. Um es auch im Rahmen von Wahlprotokollen einzusetzen, muss man beachten, dass nicht nur ein Schritt des Protokolls, sondern das gesamte Protokoll Anonymität gewährleisten muss. Außerdem kommt hier zum Tragen, dass der Zeitraum, für den man Anonymität zu gewährleisten hat, unbegrenzt sein muss. Sicherheitsgarantien über derartige Zeiträume bekommt man jedoch beim Einsatz von Verschlüsselungsverfahren wie dem RSA-Verfahren im Allgemeinen nicht.³

3 Lösungsansatz

Nach den vorhergehenden Ausführungen kann der Schluss gezogen werden, dass keine Verfahren bekannt sind, die bei politischen Online-Wahlen den hohen Grad der Anonymität der Wahlvoten über einen unbegrenzten Zeitraum sicherstellen können. Die vielen weiteren Sicherheitsprobleme, denen man sich bei Online-Wahlen stellen muss, sollen an dieser Stelle nicht behandelt werden. Hierzu sei beispielhaft auf eine Untersuchung der amerikanischen *National*

² Zu blinden Signaturen siehe auch Petersen, DuD 7/1997, S. 410-417.

³ Zur Abschätzung der Sicherheit kryptographischer Verfahren siehe z.B. Lenstra/Verheul, DuD 3/2000, S. 166.

Foundation of Science [NFS2000] verwiesen.

Vergleicht man die hier beschriebenen Lösungsansätze mit der heutigen Urnenwahl, so ist eine ungeheure technische Distanz augenfällig. Hinsichtlich einer aus Sicherheitssicht angemessenen Vorgehensweise erscheint deshalb eine stufenweise Einführung sinnvoll.

Wie aber könnte ein Lösungsansatz gerade unter dem Gesichtspunkt der hohen Anonymitätsforderung an das Wahlervotum aussehen? Hierbei verfolgen die Autoren den Ansatz einer technischen Umsetzung der bisherigen Urnenwahl. Zu diesem Zweck muss man sich den Wahlvorgang bei der Urnenwahl noch einmal detailliert vor Augen führen. Eine sicherheitstechnische Betrachtung ist in [UKS2001] zu finden.

Der erste Schritt bei der Entwicklung eines Lösungsansatzes für die Realisierung von Online-Wahlverfahren muss die Erstellung einer umfassenden Sicherheitskonzeption sein. Dabei ist der Ausgangspunkt eine Security-Policy, die das Sicherheitsverhalten abstrakt beschreibt. In weiteren Schritten werden dann Zug um Zug Mechanismen definiert, mit deren Hilfe das Sicherheitsverhalten umgesetzt werden kann. Dieses Vorgehen erlaubt eine beschleunigte Evaluierungsmöglichkeit einer entsprechenden technischen Wahlösung.

Basisbestandteile der Security-Policy sind passive Objekte, aktive Subjekte und Aktionen von Subjekten auf Objekten, mit deren Hilfe das Sicherheitsverhalten spezifiziert wird. Im Zuge der Verfeinerung werden neue Bedrohungen, die sich durch den Verfeinerungsprozess ergeben, erfasst und neue Sicherheitsanforderungen und Sicherheitsmaßnahmen zu ihrer Abwehr definiert.

Im Nachfolgenden wird dargestellt, wie dies exemplarisch aussehen könnte. Die Beschreibung ist dabei abgeleitet von der heutigen Urnenwahl. Betrachtet wird an dieser Stelle ein einzelnes Wahlbüro.

Die zu betrachtenden Objekte sind

- ◆ das Online-Wahllokal,
- ◆ der Wahlrechner,
- ◆ die Wahlurne,
- ◆ das elektronische Wählerverzeichnis,
- ◆ der Wahlschein und
- ◆ das Wahlervotum.

Als Subjekte werden

- ◆ der Wähler und
- ◆ der Wahlvorstand

unterschieden. Notwendige Aktionen sind:

- Identifikation prüfen
- Wahlberechtigung prüfen

- Wahlrechner für einen wahlkreisbezogenen Wahlvorgang freischalten
- Wahlvotum erzeugen
- Wahlvotum in die Wahlurne einwerfen
- Wähler im Wählerverzeichnis als gewählt markieren.

Die Beschreibung setzt voraus, dass das gesamte technische Wahlequipment in einer vertrauenswürdigen Umgebung (Online-Wahllokal) betrieben wird. Vertrauenswürdig bedeutet in diesem Zusammenhang, dass die Integrität einer als sicher geprüften technischen Wahleinrichtung und seiner Bestandteile zum Wahlbeginn und zur Laufzeit sichergestellt werden kann. Dies bedeutet beispielsweise, dass vor Inbetriebnahme der Wahlurne geprüft wird, ob diese leer ist. **Es bedeutet aber auch, dass der Wahlvorstand vertrauenswürdig ist und das gesamte Wahlsystem sicher bedienen kann.**

Die eigentliche Wahlvorgehensweise ist an den von der Urnenwahl gewohnten Ablauf angelehnt: Nachdem sich der Wähler gegenüber dem Wahlvorstand authentisiert hat, prüft dieser die Wahlberechtigung des Wählers. Liegt diese vor, wird für den Wähler der Wahlrechner frei geschaltet. Auf diesem findet er einen wahlkreisbezogenen Wahlschein vor. Nachdem er seinen Wahlvorgang abgeschlossen hat, wird die Wahlurne frei geschaltet und das Wahlvotum an die Wahlurne weitergeleitet. Ist dieser Prozess abgeschlossen, wird der Eintrag des Wählers in der Wahlliste als „gewählt“ markiert. Nach Ablauf des Zeitintervalls, innerhalb dessen die Wahl stattfindet, werden keine weiteren Wahlvorgänge mehr durchgeführt und die Wahlurne abschließend gesperrt und für die Auszählung freigegeben.

Abb. 1: Schematische Darstellung des Wahlvorgangs

Für die Gewährleistung der geheimen Wahl müssen bei einer elektronischen Umsetzung des Wahlvorgangs mindestens folgende Eigenschaften erfüllt sein:

- ◆ eine vollständige Trennung von Authentisierung und Wahlvotum
- ◆ eine genügend große Menge abgegebener Wahlvoten (wenn nur ein Wahlvotum erfasst wird, besteht keine Anonymität, weil das eine Wahlvotum und die eine Wähleridentifikation eindeutig zusammengeführt werden können)
- ◆ die Reihenfolge der abgegebenen Wahlvoten kann nicht hergeleitet werden.

4 Verfeinerung

Bereits durch die Unterscheidung von Wahlrechner und Wahlurne wird deutlich, dass man es hier mit zwei separaten und unabhängigen Prozessen, bzw. unabhängigen und getrennten Rechnersystemen zu tun hat. Dieses sehr einfache Modell kann nun in vielfältiger Hinsicht instantiiert bzw. verfeinert werden. Bei der obigen Beschreibung wurde bewusst offen gelassen, in welcher Form die Aktionen „Identifikation prüfen“ und „Wahlberechtigung prüfen“ ausgeführt werden. Für den Fall, dass der Wahlvorstand eine physische Person ist, kann dies – wie bisher bei der Urnenwahl – durch Prüfen der Identität anhand des Personalausweises und dem händischen Nachsehen in einer (elektronischen) Wählerliste erfolgen. Bei stärkerer Verbreitung der digitalen Signatur und Ausrüstung der Wähler mit persönlichem Equipment und privatem Signaturschlüssel zur Erzeugung der digitalen Signatur (z.B. Signatur - Smartcards) könnten die Aktionen 1. und 2. durch einen Wahlvorstand-Prozess ausgeführt werden. Hierbei ist aber unbedingt sicherzustellen, dass die Aktionenkette 1 bis 6 stringent für einen erfolgreichen Wahlvorgang durchlaufen werden muss.

Obiges Modell lässt bewusst vollständig offen, in welchem Online-Wahllokal ein Wähler wählen geht. Dabei ist die Beibehaltung des bisherigen Vorgehens, bei dem dem Wähler ein festes Wahllokal vorgegeben wird, bei Wahlen in Online-Wahllokalen nicht mehr zwingend erforderlich, weil über entsprechende Mechanismen sichergestellt werden kann, dass auch dann ein Wähler nur einmal ein Wahlvotum abgeben kann. Dies könnte für den Wähler einen echten Mehrwert bedeuten, da er dann sein Wahlvotum in jedem beliebigen Online-Wahllokal zur Wahlzeit abgeben könnte. Mit der Möglichkeit, in beliebigen Online-Wahllokalen das Wahlvotum abgeben zu können, gehen jedoch neue Sicherheitsbedrohungen einher. Einige sollen exemplarisch aufgezeigt werden:

- Zum Zeitpunkt der Durchführung der Urnenwahl muss die Möglichkeit zur Teilnahme an der Briefwahl bestehen (z.B. bei kurzfristiger Erkrankung). Hierdurch darf keine Mehrfachwahl möglich werden. Um diese Freiheit zu erhalten und gleichzeitig zu gewährleisten, dass ein Wähler nur eine Stimme abgeben kann, müssen die aktuellen Wählerverzeichnisse online zum Zeit-

punkt der Wahldurchführung für die Wahlvorstände der Online-Wahllokale zugreifbar sein.

- Die verteilten Wählerverzeichnisse könnten komplett gefälscht bzw. ihre Integrität verletzt sein. Deshalb muss die Integrität und die Authentizität der verteilten Online-Wählerverzeichnisse sichergestellt werden.
- Sollte ein großer Teil der Wahlberechtigten außerhalb ihres Heimatwahlbüros ihr Wahlvotum abgeben wollen, erfordert dies einen hohen Kommunikationsbedarf zur Klärung der Wahlberechtigung, was zu Verfügbarkeitsproblemen führen könnte. Deshalb muss eine Verteilungsstruktur der Online-Wählerverzeichnisse gewählt werden, die den Kommunikationsanfrageaufwand möglichst lokal hält.

5 Fazit

Ziel des Beitrags ist es, aufzeigen, dass sehr hohe Sicherheitsanforderungen an politische Wahlen über das Internet bestehen und man, gerade hinsichtlich der Anonymität, neue technische Lösungen finden muss. Deshalb wird vorgeschlagen, diese Art von Wahlen stufenweise umzusetzen, indem man in einem ersten Schritt Online-Wahllokale einführt. Ein entsprechendes Sicherheitskonzept wurde im Ansatz im Artikel vorgestellt, müsste aber noch weiter ausgearbeitet und einer genauen Analyse und Diskussion unterzogen werden.

Wird über die Einführung neuer Wahlsysteme nachgedacht, sollte auf jeden Fall frühzeitig die Öffentlichkeit mit einbezogen werden, denn Wahlen berühren die Grundwerte unserer Demokratie. Vertrauensbildende Maßnahmen bei den Wählern für technische Lösungen sind deshalb unbedingt notwendig, um das bestehende Vertrauen in politische Wahlen zu erhalten.

Insbesondere ist ein Vorgehen nach dem Motto „Erfahrung und Gewöhnung schafft Vertrauen“ bei der Einführung eines neuen Wahlverfahrens sehr gefährlich, weil Fehlschläge oder Sicherheitsmängel in Umfeld von politischen Wahlen sehr negative Auswirkungen haben werden. Als Beispiel dafür seien die letzten Präsidentschaftswahlen in Amerika genannt. Die Autoren regen deshalb ein sehr umsichtiges Vorgehen bei der Einführung eines neuen Wahlverfahrens an.

Ein Grundsatz sollte bei der Einführung eines neuen Wahlverfahrens aber immer er-

füllt sein: Nur wegen eines Gewinns an Bequemlichkeit darf im Umfeld politischer Wahlen ein sicheres Verfahren wie die Urnenwahl nicht durch ein Verfahren ersetzt werden, welches eine politische Wahl nicht im gleichen Maße sicher machen kann.

Allerdings: Ohne das Medium Internet auch zur Information und Kommunikation mit dem Bürger gerade im Zusammenhang mit politischen Fragestellungen zu nutzen, machen Online-Wahlen wenig Sinn. Ein ganzheitlicher Ansatz könnte möglicherweise der zunehmenden Politikverdrossenheit der Wähler entgegenwirken und damit eventuell eine Erhöhung der Wahlbeteiligung bewirken.

Literatur

- [CHAU1981] Chaum, D. L., *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms*, Communication of the ACM, Vol. 24, No. 2, Februar 1981, <http://world.std.com/~francl/crypto/chau-m-acm-1981.html>
- [CHAU1982] Chaum, David: *Blind Signatures for Untraceable Payments*. Proceedings of Crypto '82, Plenum Press, S. 199-203.
- [DiCa1994] *DigiCash – Numbers that are money, the ultimate electronic payment system for any application*, DigiCash 1994, http://www.eff.org/pub/Privacy/Digital_money/digicash.brochure
- [NSF2000] National Science Foundation, USA, 2000, http://www.internetpolicy.org/research/e_voting_report.pdf
- [SCHN1996] Schneier, B., *Angewandte Kryptographie: Protokolle, Algorithmen und Sourcecode in C*, Bonn, Addison-Wesley 1996
- [UKS2001] Ullmann, M., Koob, F., Schulz, F., *Online-Wahlen: Skizze einer Security Policy*, Tagungsband 7. Deutscher IT-Sicherheitskongress, SecuMedia Verlag, 2001