In: Zimmermann, Harald H.; Schramm, Volker (Hg.): Knowledge Management und Kommunikationssysteme, Workflow Management, Multimedia, Knowledge Transfer. Proceedings des 6. Internationalen Symposiums für Informationswissenschaft (ISI 1998), Prag, 3. – 7. November 1998. Konstanz: UVK Verlagsgesellschaft mbH, 1998. S. 373 – 384

Elektronische Wahlverfahren als Beispiel angewandter Kryptographie

Christian Wolff, Leipzig

Institut für Informatik
Universität Leipzig
Augustusplatz 10/11
D-04107 Leipzig
wolff@informatik.uni-leipzig.de

Inhalt

1 Einleitung
1.1 Plausibilität elektronischer Wahlverfahren
1.2 Vergleichbare Ansätze
2 Sicherheit und Kryptographie
3 Elektronische Wahlen
3.1 Ablauf des Wahlverfahrens
3.2 Systemaufbau
3.3 Implementierung
4 Sicherheitsbewertung
5 Generalisierung für beliebige Entscheidungsverfahren
6 Fazit
7 Literatur

Zusammenfassung

Der Beitrag schildert die Durchführung von Wahlen mit Hilfe kryptographischer Verfahren anhand einer Fallstudie mit Anwendungsbereich im Verbandswesen. Ausgehend von Vorüberlegungen zur kommunikativen Plausibilität und den technischen Voraussetzungen der Verwendung kryptographischer Algorithmen wird der Prototyp eines Wahlinformationssystems vorgestellt. Der Ansatz modelliert ein der traditionellen Briefwahl analoges Verfahren mit Hilfe von allgemein verfügbaren Kommunikationsdiensten im Internet (e-mail, WorldWideWeb). Dabei werden – im Vorgriff auf nach dem deutschen Signaturgesetz zertifizierte digitale Signatu-

ren und Schlüssel – asymmetrische Schlüsselpaare nach dem RSA-Verfahren eingesetzt.

1 Einleitung

In diesem Aufsatz soll aufgezeigt werden, wie unter Einsatz angewandter Kryptographie Wahlverfahren elektronisch durchgeführt werden können. Die Untersuchung geht aus einer Pilotstudie für die *Gesellschaft für linguistische Datenverarbeitung* (GLDV) hervor, in der ein elektronisches Wahlverfahren realisiert und getestet wird (vgl. MIELKE & WOLFF 1998). In vielen Ländern werden derzeit rechtliche Rahmenbedingungen für den Einsatz kryptographischer Verfahren bzw. der digitalen Signatur geschaffen, so in Deutschland durch das Signaturgesetz (SigG) im Rahmen des Informations- und Kommunikationsdienstegesetz (IuKDG) und die Signaturverordnung (SigV, vgl. BIESER 1997, BIESER & KERSTEN 1998:87-108). Die nachfolgend geschilderte Implementierung eines elektronischen Wahlverfahrens soll zumindest prinzipiell mit dem Einsatz kryptographischer Verfahren im Sinne des SigG kompatibel sein.

1.1 Plausibilität elektronischer Wahlverfahren

Wahlverfahren spielen in Vereinen und Verbänden zur Umsetzung von Entscheidungsprozessen eine wichtige Rolle und werden üblicherweise im Briefwahlverfahren durchgeführt, was mit nicht unerheblichen Kosten und einem hohen organisatorischen Aufwand verbunden ist. Die Motivation für den Einsatz elektronischer Wahlverfahren ergibt sich für derartige Personenmehrheiten u.a. aus folgenden Merkmalen:

Ein räumlich verstreuter heterogener Wählerkreis, der ein Briefwahlverfahren erforderlich macht.
Der Zugang zum Internet und seinen Diensten (e-mail, WWW) und die Realisierung bzw. Nutzung elektronischer Kommunikationsformen ist mit geringem Kostenaufwand möglich.
Traditionelle Kommunikationsverfahren bei Wahlen sind zeit- und kostenintensiv.
Die Wahlbeteiligung bei Verbandswahlen ist in der Regel relativ niedrig; ihre Erhöhung ist im Sinne einer höheren Mitgliederpartizipation anzustreben.

Diese Beobachtungen können als Argumente für eine Verwendung elektronischer Wahlverfahren gelten; zu beachten ist aber, daß auch mittelfristig nicht davon auszugehen ist, daß *alle* Wahlberechtigten an elektronischen Wahlverfahren teilhaben können oder wollen. Das nachfolgend beschriebene Verfahren hat daher *ergänzenden Charakter* und könnte allenfalls langfristig auf eine Ablösung traditioneller Kommunikationsformen abzielen. Rechtliche und demokratietheoretische Erwägungen zum Einsatz solcher Verfahren als neuer Form der Operationalisierung von Entscheidungsprozessen bleiben hier ausgeblendet (vgl. aber MIELKE & WOLFF 1998:32ff).

1.2 Vergleichbare Ansätze

Auch andere Fachgesellschaften bereiten derzeit elektronische Wahlverfahren vor oder haben sie bereits umgesetzt. Die *Association for Computing Machinery*

(ACM) hat 1998 eine Satzungsänderung durchgeführt, die den Einsatz elektronischer Wahlverfahren ermöglicht. Die *IEEE Computer Society* hat bereits ein elektronisches Wahlverfahren für ihre Verbandswahlen implementiert (http://computer.org/election). Die wichtigsten Merkmale dieses Verfahrens sind:

Verteilung eines Zugangsschlüssels (Kontrollnummer, *ballot control number*) auf den (gedruckten) Wahlunterlagen.
Realisierung der Wahlanwendung und der Durchführung der Wahl durch einen externen Dienstleister (ICE Interactive Certified Elections, http://www.ice-ballot.com).
Zugang zu einem WWW-Formular (Stimmzettel) mit Hilfe von Mitgliedsnummer und Kontrollnummer.
Versenden des Wahlzettels über das WWW (ohne Verschlüsselung).
Rückmeldung des Wahlzettels per e-mail (ohne Verschlüsselung).

Dieses Verfahren basiert auf einem kommerziellen Softwarepaket und setzt lediglich eine Zugangskontrolle zur Identifizierung des Wahlberechtigten ein; die Daten werden dabei mehrfach unverschlüsselt zwischen Wähler und Wahlurne bzw. Wahlamt hin- und hergesendet. Als Alternativen stehen die Wahl per Brief oder Fax zur Verfügung.

Auch für die elektronische Umsetzung politischer Wahlen entstehen derzeit erste Anwendungen. So wurde an der Universität Osnabrück ein Wahllokal für einen virtuellen Bundestagswahlkreis 329 eingerichtet, in dem man nach Zuteilung einer Wahlberechtigung eine Probeabstimmung zur Bundestagswahl 1998 durchführen kann. Der Ansatz versucht, das Briefwahlverfahren zu modellieren, verzichtet aber auf Verschlüsselungsverfahren (vgl. OTTEN 1998).

2 Sicherheit und Kryptographie

Für die Realisierung eines anonymen Wahlverfahrens mit elektronischen Mitteln spielen Aspekte der Sicherheit elektronischer Kommunikation eine zentrale Rolle. Dazu gehören u.a.

die Identifizierung (*authentification*) der Kommunikationspartner (Feststellung der Wahlberechtigung),
die Vertraulichkeit (*confidentiality*) der Kommunikation, insbesondere die Gewährleistung der Anonymität von Wahlen und
die Integrität (*integrity*) der kommunizierten Information (vgl. RANNENBERG, MÜLLER & PFITZMANN 1997:22f; SUN MICROSYSTEMS 1998).

Weitere Faktoren, die bei der Operationalisierung kryptographischer Verfahren Bedeutung haben, sind die *Transparenz* des Verfahrens und die *Vertrauenswürdigkeit* einer Anwendung. Die letzteren Kriterien dürften für die breite Durchsetzung kryptographiebasierter Kommunikation besonders wichtig sein, da nur durch sie hinreichende Benutzerakzeptanz zu erreichen ist. Zur Gewährleistung dieser Leistungsmerkmale dienen kryptographische Verfahren. Dabei ist zwischen unterschiedlichen Klassen kryptographischer Algorithmen (v.a. symmetrische und asymmetrische Kryptographie), ihrer softwaretechnischen Umsetzung in einem

Dienst oder Protokoll (digitale Signatur, sicheres Kommunikationsprotokoll, digitales Zertifikat, Datenverschlüsselung) und den angestrebten Schutzzielen zu unterscheiden.

Das Grundprinzip der Kryptographie in ihrer klassischen Anwendung als Datenverschlüsselung ist dabei die Umwandlung einer zu übermittelnden Nachricht (*Klartext, plain text*, hier: der ausgefüllte Stimmzettel) mit Hilfe eines Kryptoalgorithmus in *Geheimtext* (*cyphertext*), der an den Empfänger gesendet und von ihm entschlüsselt werden kann. Neben *symmetrischen* Verfahren, bei denen Sender wie Empfänger über *denselben* Schlüssel zur Verschlüsselung bzw. Entzifferung verfügen, haben sich *asymmetrische* Verfahren durchgesetzt, bei denen der Sender den Klartext mit Hilfe des *öffentlichen* Schlüssels des Empfängers verschlüsselt. Der Empfänger kann die verschlüsselte Nachricht mit Hilfe seines *privaten* Schlüssels, der nur ihm bekannt und durch eine Paßwortphrase o.ä. geschützt ist, entziffern (Prinzip der *public key cryptography,* vgl. SALOMAA 1990:55ff, WOBST 1997:136ff). Auf der Basis *asymmetrischer* Verfahren lassen sich auch *digitale Signaturen*, das elektronische Pendant zur eigenhändigen Unterschrift, realisieren: Der Unterzeichner signiert ein Dokument mit Hilfe seines privaten Schlüssels. Unter Zuhilfenahme des öffentlichen Schlüssels kann der Empfänger verifizieren, daß ein Dokument von einem bestimmten Sender stammt und es *wie unterzeichnet* bei ihm eingetroffen ist (vgl. BIESER & KERSTEN 1998:20ff). Die Möglichkeit, einen Schlüssel zur Verschlüsselung von Daten problemlos veröffentlichen zu können, ohne die Sicherheit geschützter Daten zu kompromittieren, spielt auch bei dem hier erörterten Wahlsystem eine wesentliche Rolle.

3 Elektronische Wahlen

Das nachfolgend beschriebene Verfahren stellt die elektronische Umsetzung einer geheimen und anonymen Wahl auf der Basis einer Kombination symmetrischer *und* asymmetrischer Kryptographie dar. Dabei soll der Einsatz der kryptographischen Verfahren folgende Schutzziele gewährleisten:

Die *Anonymität* des Wählers, d.h. bei der Auszählung der Stimmzettel darf kein Hinweis auf die Identität des Wählers mehr vorhanden sein.
Die *Identifizierbarkeit* des Wählers, wofür eine digitale Signatur oder die Entschlüsselung mit Hilfe eines einem Wähler zugeordneten privaten Schlüssels zum Nachweis der Wahlberechtigung benötigt wird (Funktion des Wahlscheins bei der Briefwahl).
Die *Vertraulichkeit* nach außen, d.h. die ausgefüllten Stimmzettel müssen so versendet werden, daß kein Außenstehender von ihrem Inhalt Kenntnis erlangen kann und die
Sicherheit gegenüber Eingriffen unbefugter Dritter z.B. durch Schlüsselmißbrauch.

Die Realisierung eines solchen Verfahrens setzt voraus, daß

innerhalb der die Wahl durchführenden Vereinigung (Institution, Verein, Verband) die elektronische Wahlmöglichkeit durch geeignete Vereinbarungen (Satzungsänderung, Aufnahme der Möglichkeit einer elektronischen Wahl in eine Wahlordnung etc.) sanktioniert ist (rechtliche Voraussetzung),

die an der elektronischen Wahl teilnehmenden Wähler über e-Mail und WWW-Anschluß verfügen (technische Voraussetzung) und
für alle anderen Wähler ein geeignetes „traditionelles“ Wahlverfahren zur Verfügung steht (Prinzip der parallelen Durchführung).

3.1 Ablauf des Wahlverfahrens

Aus einer Mitgliederdatenbank generiert das elektronische Wahlamt für jeden Wähler ein Schlüsselpaar. Die Schlüssel tragen einen impliziten Zeitstempel und sind nur für je eine Wahl gültig. Das Wahlamt fungiert dabei als Zertifizierungsstelle (vgl. BIESER 1997:402ff), d.h. es gewährleistet die Überprüfung von Schlüsseln und Signaturen auf ihre Gültigkeit. Bei der Verwendung von Schlüsselpaaren im Sinne des SigG würde diese Aufgabe von einem externen Dienstleister übernommen (*trust center*, vgl. BIESER & KERSTEN 1998:49ff), worauf hier aus Gründen der frühzeitigen Anwendbarkeit des Verfahrens verzichtet wird.

Der Wähler erhält seinen öffentlichen Schlüssel per e-mail zugesandt, während der private Schlüssel in der Datenbank des Wahlamts verbleibt. Zusätzlich generiert die Wahlsoftware auf der Clientseite mit einem symmetrischen Verfahren einen Schlüssel (Sitzungsschlüssel), mit dem nur der Wahlzettel verschlüsselt wird. Es kommt also in Analogie zur Briefwahl ein zweistufiges Verfahren zum Einsatz:

Der Wähler füllt den Wahlzettel aus, die Wahlsoftware verschlüsselt ihn mit Hilfe des symmetrischen Sitzungsschlüssels, ohne daß der Benutzer eingreifen müßte.
Der verschlüsselte Wahlzettel wird zusammen mit dem symmetrischen Sitzungsschlüssel nochmals mit dem wählerbezogenen öffentlichen Schlüssel verschlüsselt. Der öffentliche Schlüssel trägt damit die Funktion des legitimierenden Wahlscheins und dient der Identifizierung des Wählers.

Die Wahlsoftware sendet den so entstandenen Geheimtext an das Wahlamt. Es stellt zunächst anhand der verfügbaren privaten Schlüssel fest, ob der Wahlzettel von einem stimmberechtigten Wähler stammt. Anschließend legt es den verbleibenden, mit dem symmetrischen verschlüsselten Wahlzettel samt symmetrischem Schlüssel in die (elektronische) Wahlurne. Damit ist die Anonymität der Wahl bei gleichzeitiger Überprüfung der Wahlberechtigung gewährleistet. Nach Ablauf der Wahlfrist können alle eingegangenen anonymisierten und verschlüsselten Wahlzettel entschlüsselt und ausgezählt werden.

3.2 Systemaufbau

Aus der Schilderung des Wahlablaufs ergibt sich, daß zur Implementierung drei Softwarekomponenten erforderlich sind:

Das Modul für die Generierung und Verwaltung der Schlüsselpaare („Zertifizierungsstelle“) das auch die Identitätsüberprüfung und Anonymisierung eingehender Wahlbriefe übernimmt („Wahlamt“),
die eigentliche Wahlsoftware, ein WWW-Client, realisiert als Java-Applet („Wahlkabine“ mit „Stimmzettel“ (ein Java-Formular), der auch einen Container für den öffentlichen Schlüssel des Wählers enthält) und

das Modul zur Entschlüsselung der Wahlscheine, das auch Auswertungsausgaben übernehmen kann („Wahlurne“).

Die konzeptuelle Trennung von „Wahlamt“ und „Wahlurne“ soll das Vertrauen der Wähler in das Verfahren erhöhen, da es den Aspekt der Anonymität der Wahl betont – ist der Stimmzettel in der Wahlurne, so ist kein Bezug zu einem bestimmten Wähler mehr vorhanden. Die Zuordnung zwischen den Verfahrensschritten und den Softwaremodulen sieht wie folgt aus:

Arbeitsschritt	*Modul*
Generieren wählerbezogener Schlüsselpaare	*Wahlamt*
Verteilen der öffentlichen Schlüssel per e-mail an die Wähler	*Wahlamt*
Ausfüllen, und symmetrisches wie asymmetrisches Verschlüsseln des Wahlzettels	*Wahlkabine*
Abschicken an den Wahlserver/Wahlamt	*Wahlkabine*
Verifikation der Wahlberechtigung (1. Entschlüsselung), Füllen der Wahlurne; Markieren des Schlüsselpaars als verbraucht	*Wahlamt*
Entschlüsseln der Stimmzettel (2. Entschlüsselung)	*Wahlurne/Auswertungsmodul*
Auswertung der Stimmzettel, Ergebnisaufbereitung	*Wahlurne/Auswertungsmodul*

Tab. 1: Zuordnung Arbeitsschritt - Modul

Die erste Entschlüsselung macht die Auswahl des passenden privaten Schlüssels aus dem Wählerverzeichnis erforderlich. Bei den zunächst erwarteten überschaubaren Teilnehmerzahlen ist dies durch systematisches Durchprobieren der Schlüssel möglich, wobei als Selektionsindikator ein nicht-informationstragendes Erkennungsmerkmal zur Eingrenzung des Schlüsselraums in der Datenbank mitgesendet werden kann. Bei späterer Verwendung von amtlich zertifizierten Schlüsseln entfällt das Problem, da an die Stelle der Datenbankabfrage zur Auswahl des passenden Schlüssels die Verifikation der digitalen Signatur des Wählers beim externen *trust center* tritt.

3.3 Implementierung

Grundsätzlich ließe sich diese Architektur mit Hilfe kryptographischer Standardsoftware realisieren. Dies hat aber organisatorische Nachteile, da dabei hohe Voraussetzungen an die beim Wähler vorhandene technische Infrastruktur gestellt werden (z.B. Installation von Softwarepaketen wie *Pretty Good Privacy* oder *Privacy Enhanced Mail - PEM,* vgl. IANNAMICO 1997; SCHNEIER 1996:664ff; WOBST 1997:275ff.) und Automatisierungs- wie Generalisierungspotentiale ungenutzt bleiben müssen. Um den Preis eines höheren Entwicklungsaufwands wird hier versucht, Benutzerfreundlichkeit durch ein einheitliches Interface mit wenigen Interaktionsschritten zu erreichen: Dem Benutzer steht für die Wahl der Stimmzettel als Java-Applet zur Verfügung, den er in einen Browser laden und ausfüllen kann. Der einzige unter ergonomischen Aspekten problematische Verfahrensschritt ist die Übertragung des öffentlichen Schlüssels in den Wahlclient (Wechsel des Kommunikationsverfahrens von e-mail zum WWW).

Bei der Implementierung stehen folgende Aspekte im Mittelpunkt:

Für den im Umgang mit kryptographischen Verfahren unerfahrenen Benutzer steht ein einfaches Interface zur Verfügung, die Wahl muß mit wenigen Interaktionsschritten durchführbar sein (vgl. Abb. 1).
Da bei einem heterogenen Benutzerkreis keine klare Aussage über die beim Wähler vorhandene technische Infrastruktur zu treffen ist (Rechnerplattform, Browser), werden plattformübergreifende und weit verbreitete Dienste, Standards und Sprachen verwendet (e-mail, WWW/HTML, Java).
Eine weitgehende Prozeßautomatisierung soll den Arbeitsaufwand im Vergleich mit traditionellen Wahlverfahren minimieren (Schlüsselgenerierung und –verteilung, Entschlüsselung der Wahlscheine, Auswertung).
Sichere Kryptographie verlangt nach einem Höchstmaß an Transparenz. Deshalb kommen nur kryptographische Verfahren zum Einsatz, deren Algorithmen öffentlich einsehbar sind und für die verläßliche Einschätzungen ihrer Sicherheit existieren (RSA, IDEA).
Die eigentliche Wahlinformation wird auf der Basis einer XML-DTD im Klartext kodiert, so daß eine (auch gedruckte) Speicherung der anonymisierten Wahlscheine für die spätere Überprüfung möglich ist. Sie kann auch der Dokumentation der Wahlentscheidung für den Wähler dienen (vgl. Abb. 2).
Die modulare Struktur soll die Generalisierbarkeit der Anwendung sicherstellen.

Die Softwaremodule werden in Java implementiert (der WWW-Client als Java-Applet, die anderen Module als Java *Applications*), da so die Integration ins WWW erreicht werden kann. Zudem verfügt Java über ein generisches kryptographisches API, die *Java Cryptography Architecture* (JCA, vgl. LI GONG 1998). Dieses API modelliert auf einer abstrakten Ebene die benötigten kryptographischen Verfahren (Schlüsselerzeugung, Datenstrukturen für private und öffentliche Schlüssel, Implementierung der eigentlichen Verschlüsselungsalgorithmen). In dieses API kann die konkrete Implementierung der einzelnen Algorithmen (z.B. RSA, DSA, IDEA) eines *provider* eingehängt werden. Sun stellt zwar mit den *Java Cryptography Extensions* (JCE) einen *provider* mit den benötigten Algorithmen bereit; aufgrund der U.S.-amerikanischen Exportrestriktionen dürfen die *JCE* als eigentlich verschlüsselungsrelevanter Teil der *JCA* nicht aus den USA exportiert werden, da nach amerikanischen Recht Datenverschlüsselungsverfahren als *Waffen* gelten (vgl. SCHNEIER 1996:691ff, WOBST 1996:275ff, 307ff). Deshalb wird auf die Reimplementierung der *Java JCA* und der *JCE* der TU Graz zurückgegriffen (vgl. PLATZER 1998). Bei der Schlüsselerzeugung und der Auswertung kommt zudem das *Java Database Connectivity*-API (JDBC) zum Einsatz (Brücke zur Wählerdatenbank).

Die Klartextverschlüsselung des Stimmzettels verwendet den *International Data Encryption Standard* (*IDEA*), das derzeit wohl mächtigste kryptographische Verfahren (vgl. SCHNEIER 1996:370ff; WOBST 1997:182ff.). Die asymmetrische Verschlüsselung des Stimmzettels sowie der IDEA-Schlüssel werden mit dem öffentlichen Schlüssel des Wählers verschlüsselt. Für die Generierung der Schlüsselpaare des asymmetrischen Verfahrens verwendet der Client den *RSA*-Algorithmus, das erste vollständige und am weitesten verbreitete asymmetrische kryptographi-

sche Verfahren (vgl. SALOMAA 1990:125-157, SCHNEIER 1996:531ff, WOBST 1997:143ff.). Ein Wechsel auf andere kryptographische Verfahren (z.B. von IDEA zu DES oder Triple-DES) ist aufgrund des hohen Abstraktionsgrads der in der JCA enthaltenen Klassen problemlos möglich – es muß nur jeweils ein Provider-Paket mit den benötigten Algorithmen zur Verfügung stehen.

Die Entscheidung, das Verfahren mit Hilfe asymmetrischer Kryptographie zu realisieren und Alternativen wie den Einsatz kryptographisch sicherer Übertragungs*protokolle* (z.B. S/MIME, Secure Socket Layers oder S-HHTP, vgl. GARFINKEL & SPAFFORD 1997:120ff) zu vernachlässigen, beruht auf dem Ziel einer konzeptuellen Nähe zum zukünftigen Einsatz digitaler Signaturen im Sinne der deutschen Signaturgesetzgebung.

Abb. 1 zeigt den Prototyp des Webclients mit einem hypothetischen Wahlzettel. Er sieht Zustimmung, Ablehnung und Enthaltung als typische Wahlmöglichkeiten vor. Darüber hinaus kann für jede Einzelentscheidung auch *keine Stimmabgabe* erfolgen, wenn kein *radio button* selektiert ist.

4 Sicherheitsbewertung

Der vergleichsweise aufwendige Einsatz kryptographischer Verfahren ist nur berechtigt, wenn die heterogenen Sicherheitsanforderungen erfüllt werden können. Auf der Ebene der Algorithmen scheint nach derzeitigem Stand gewährleistet zu sein, daß nur ein *brute force*-Angriff auf den Geheimtext Erfolgschancen hat und die Menge unterschiedlicher Schlüssel nicht vollständig durchgerechnet werden kann.

Durch die genau begrenzte Menge verschiedener Schlüsselpaare, ihren eingeschränkten Einsatzzweck („Einmalschlüssel“) und ihre limitierte zeitliche Gültigkeit erscheint zudem ausgeschlossen, daß gefälschte Schlüssel in diesem Verfahren untergeschoben werden können. Gleiches gilt für das *Unterschieben* eines gefälschten Geheimtextes bei der Versendung des verschlüsselten Stimmzettels an das Wahlamt, das *Abfangen* und *Vernichten* eines Stimmzettels ist allerdings denkbar. Weitergehend wäre zu fragen, wie gut das Wählerverzeichnis, d.h. die Datenbank des Wahlamts mit den privaten Schlüsseln gegen Angriffe von außen geschützt ist.

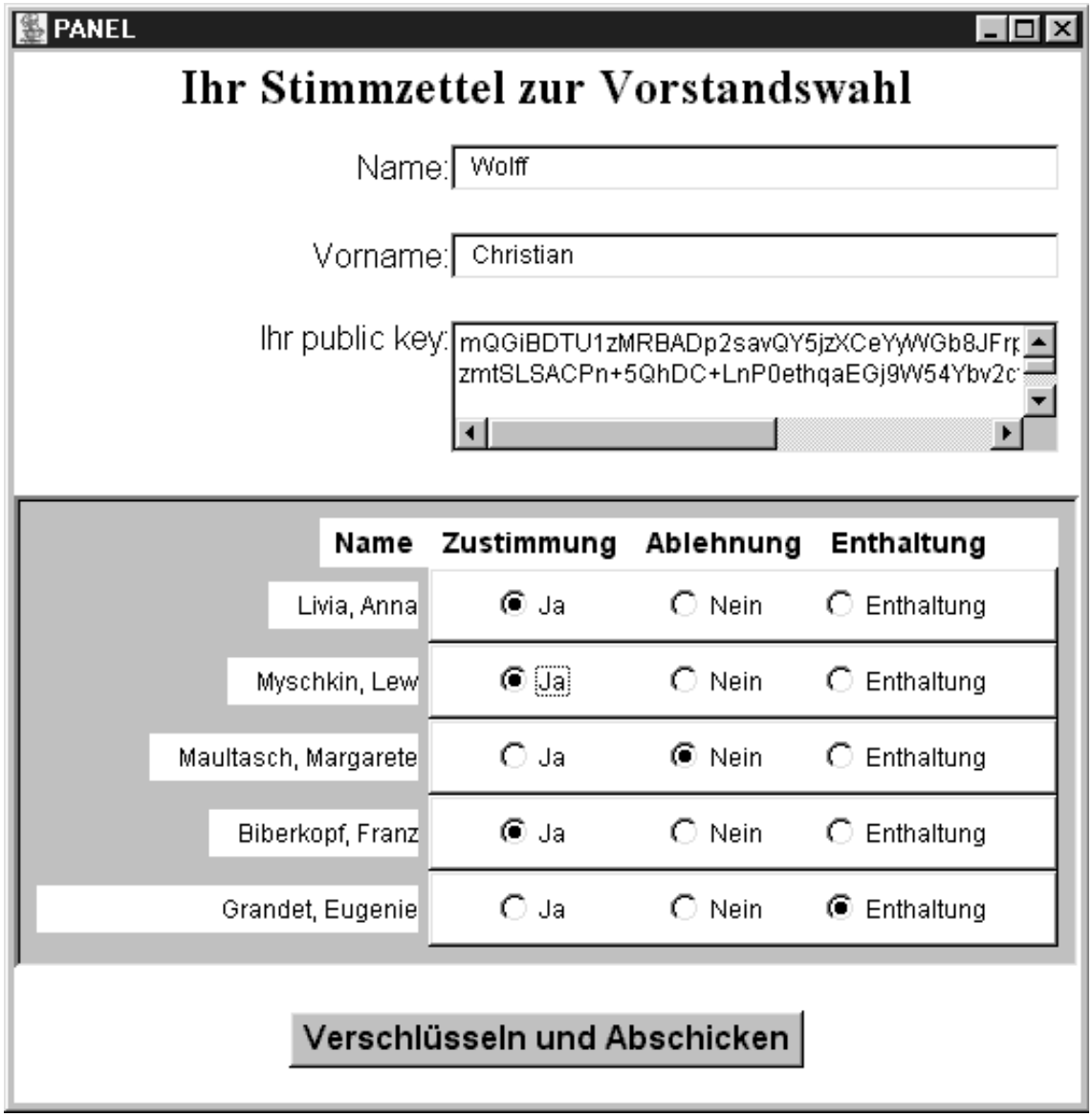

Abb. 1: Interface der „Wahlkabine“

Ein gravierender Schwachpunkt ist offensichtlich die Versendung der öffentlichen Schlüssel per e-mail an die Wähler, da diese im Internet abgefangen und von Unbefugten zur Wahl verwendet werden könnten. Im Extremfall könnte bei Abfangen *aller* öffentlichen Schlüssel mit jedem abgefangenen Schlüssel genau ein Wahlzettel ausgefüllt werden.

Im Rahmen des *gewählten Testszenarios* erscheint dieser Fall hinreichend unwahrscheinlich, so daß auf weitere, das Verfahren verkomplizierende, Sicherungsmaßnahmen verzichtet wird. Mit diesem Argument der geringen Wahrscheinlichkeit eines Angriffs steht aber das Gesamtkonzept in Frage. Wichtiger erscheint daher die Perspektive des mittelfristigen Übergangs zu amtlich beglaubigten Schlüsselpaaren, der diese Schwachstelle eliminiert.

5 Generalisierung für beliebige Entscheidungsverfahren

Ein Abstimmungsverfahren wie oben geschildert setzt sich aus einer Menge unterschiedlich strukturierter Auswahlentscheidungen zusammen. Geht man davon aus, daß dieser Verfahrens*ablauf* für unterschiedliche Verfahrens*inhalte* (Art und Anzahl der zu treffenden Entscheidungen) auf eine Vielzahl von Anwendungsfällen übertragbar ist, so wird offensichtlich, daß sich hinter der prototypischen Einzelanwendung ein großes Generalisierungspotential verbirgt. Mit Hilfe einer adäquaten Beschreibungssprache zur Spezifikation des Inhalts der Wahlzettel (oder allgemeiner: von Umfragen, Erhebungen etc.) wie einer XML-DTD (vgl. BRAY et al. 1997, LIGHT 1997) und einem geeigneten Parser läßt sich ein *Electronic Vote Management System* aufbauen, das nach Bedarf geeignete Wahlzettel generiert und im selben Format die Abstimmungsinhalte transportiert und auswertet. Dies ergibt einen weiteren Automatisierungsaspekt, nämlich die automatische Erstellung des Benutzerinterface für den Stimmzettel. Abb. 2 zeigt ein Beispiel eines XML-kodierten Stimmzettels, bei dem die Attribute des Elementes `DECISION` die Art der Entscheidung (`NAME`), ihren Typ (`TYPE`) und den Inhalt der Stimmabgabe (`SELECTION`) kodieren und automatisch generiert, geparst und ausgewertet werden können. Für den Aufbau des Interfaces sind allerdings weitere Elemente und Attribute erforderlich, die den Wertebereich einer Einzelentscheidung definieren oder eine Binnengliederung bzw. –gruppierung der Einzelentscheidungen festlegen.

```
        <VOTE>
         <DECISION   NAME='LIVIA, ANNA'
                TYPE='SELECTION'
                SELECTION='YES' />
         <DECISION   NAME='MYSCHKIN, LEW'
                TYPE='SELECTION'
                SELECTION='YES' />
         <DECISION   NAME='MAULTASCH, MARGARETE'
                TYPE='SELECTION'
                SELECTION='NO' />
         <DECISION   NAME='BIBERKOPF, FRANZ'
                TYPE='SELECTION'
                SELECTION='NO' />
         <DECISION   NAME='GRANDET, EUGENIE'
                TYPE='SELECTION'
                SELECTION='ABSTENTION' />
</VOTE>
```

Abb. 2: XML-kodierter Stimmzettel

6 Fazit

Das dargestellte Verfahren wird derzeit als Prototyp entwickelt; ein erster Test soll im Herbst 1998 stattfinden, bevor 1999 der erste Einsatz für eine elektronische Vorstandswahl erfolgen kann. Dabei werden die Akzeptanz und die Nutzungsbandbreite wichtige Untersuchungsgegenstände sein, die auch Aufschluß über die Plausibilität derartiger Verfahren für andere Einsatzzwecke geben können. Mittelfristig ist das Verfahren auf nach dem Signaturgesetz von einer amtlichen Zertifi-

zierungsstelle beglaubigte digitale Signaturen umzustellen. Auf diese Variante wurde hier zunächst verzichtet, da davon auszugehen ist, daß noch sehr wenige Wahlberechtigte über eine solche Signatur verfügen.

Literatur

[ARNOLD & GOSLING 1997]
ARNOLD, Ken; GOSLING, James: *The Java™ Programming Language,* Reading/MA et al.: Addison-Wesley, 1997[2].

[BIESER 1997]
BIESER, Wendelin: *Begründung und Überlegung zum Signaturgesetz*. In: MÜLLER & PFITZMANN (1997), S. 399-410.

[BIESER & KERSTEN]
BIESER, Wendelin; KERSTEN, Heinrich: *Chipkarte statt Füllfederhalter. Daten beweissicher "elektronisch unterschreiben" und zuverlässig schützen,* Heidelberg: Hüthig 1998.

[BRAY 1997]
BRAY, Tim et al.: *Extensible Markup Language*. In: World Wide Web Journal 2(4) (1997), S. 29-68).

[GARFINKEL & SPAFFORD 1997]
GARFINKEL, Simson; SPAFFORD, Gene: *Cryptography and the Web.* In: World Wide Web Journal 2(4) (1997), S. 113-126.

[IANNAMICO 1997]
IANNAMICO, Mike: *Pretty Good Privacy™. PGP for Personal Privacy, Version 5.0 for Windows® 95, Windows NT. User's Guide*. San Mateo/CA: Pretty Good Privacy, Inc., 1997.

[KHARE & RIFKIN 1997]
KHARE, Rohit; RIFKIN, Adam: *Weaving a Web of Trust.* In: World Wide Web Journal 2(4), 1997, 77-112.

[LIGHT 1997]
LIGHT, Richard: *Presenting XML*, Indianapolis/IN: Sams.net, 1997.

[MIELKE & WOLFF 1988]
MIELKE, Bettina; WOLFF, Christian: *Kryptographiebasierte Kommunikationsformen für Vereine und Verbände.* In: LDV-Forum 15(1) (1998), S. 29-44.

[MÜLLER & PFITZMANN 1997]
MÜLLER, Günter; PFITZMANN, Andreas (edd.): *Mehrseitige Sicherheit in der Kommunikationstechnik. Verfahren, Komponenten, Integration*, Bonn et al.: Addison-Wesley, 1997.

[OTTEN 1998]
OTTEN, Dieter: *Aufruf zur Wahl im virtuellen Internet-Wahlkreis* 329. Universität Osnabrück, FB Sozialwissenschaften, http://www.wahlkreis329.de/html/wahlaufruf.html, August 1998.

[PLATZER 1998]
PLATZER, Wolfgang: *The IAIK Java Cryptography Extension.* TU Graz, Institute for Applied Information Processing and Communications, http://jcewww.iaik.tu-graz.ac.at/IAIK_JCE/jce.htm, Juni 1998.

[RANNENBERG, MÜLLER & PFITZMANN]
RANNENBERG, Kai; MÜLLER, Günter; PFITZMANN, Andreas: *Sicherheit, insbesondere mehrseitige IT-Sicherheit.* In: MÜLLER & PFITZMANN (1997), 21-29.

[SALOMAA 1990]
SALOMAA, Arto: *Public-Key Cryptography*, Berlin et al.: Springer, 1990.

[SCHNEIER 1996]
SCHNEIER, Bruce: *Angewandte Kryptographie*. Bonn et al.: Addison-Wesley, 1996.

[LI GONG 1998]
Li Gong (1998): *Java™ Security Architecture (JDK1.2)*. Draft Document (Revision 0.9). Palo Alto/CA: Sun Microsystems, http://java.sun.com/products/jdk/1.2/docs/guide/security/spec/security-spec.doc.htm, Juni 1998.

[SUN MICROSYSTEMS 1998]
SUN MICROSYSTEMS: *Secure Computing with Java: Now and the Future. A White Paper*. Palo Alto/CA: Sun Microsystems, http://www.javasoft.com/ marketing/collateral/security.html, Juli 1998.

[WOBST 1997]
WOBST, Reinhard: *Abenteuer Kryptographie. Methoden, Risiken und Nutzen der Datenverschlüsselung.* Bonn et al.: Addison-Wesley, 1997.