Kryptographiebasierte Kommunikationsformen für Vereine und Verbände

Bettina Mielke
Juristische Fakultät
Universität Regensburg
bettina.mielke@jura.uni-regensburg.de

Christian Wolff
Institut für Informatik
Universität Leipzig
wolff@informatik.uni-leipzig.de

1 Einführung

Die Verfügbarkeit unterschiedlicher Kommunikationsformen innerhalb des Internet wirkt sich bereits seit einiger Zeit auch auf die Arbeit von Vereinen und Verbänden aus:

- Informationen über Verbandsaktivitäten werden über das WWW bereitgestellt.
- Mitglieder werden über elektronische Postverteiler per e-mail informiert oder
- können in Diskussionsforen über unterschiedliche Themengebiete mit Bezug zur Arbeit des Vereins oder Verbands durchführen.

In diesem Aufsatz wollen wir aufzeigen, wie unter Einsatz kryptographischer Verfahren weitere typische Kommunikationsformen (Meinungsbildungsprozesse, Umfragen, Wahlen) mit elektronischen Mitteln durchgeführt werden können und welche rechtlichen Rahmenbedingungen dabei zu beachten sind. Die Untersuchung geht dabei von der Situation der *Gesellschaft für linguistische Datenverarbeitung* (GLDV) als typischem Beispiel einer wissenschaftlichen Vereinigung aus.

1.1 Rahmenbedingungen elektronischer Kommunikationsformen

Der Ansatzpunkt für den Einsatz elektronischer Kommunikationsformen über das bereits oben angedeutete Maß hinaus ergibt sich für überregional (oder international) tätige Vereine und Verbände aus folgenden Merkmalen:

- Ein räumlich verstreuter heterogener Mitgliederkreis.
- Die Mitglieder haben zumeist Zugang zum Internet und seinen Diensten (e-mail, WWW) und die Realisierung bzw. Nutzung elektronischer

Kommunikationsformen ist mit geringem Kostenaufwand möglich, bei wissenschaftlichen Vereinigungen kann i. d. R. die technische Infrastruktur der Hochschulen genutzt werden.

- Traditionelle Kommunikationsverfahren bei Wahlen oder Abstimmungen sind zeit- und kostenintensiv.
- Gerade größere Verbände können über Mitgliederversammlungen nur einen Bruchteil der Mitglieder erreichten – im Fall der GLDV kann man annehmen, daß bei den Mitgliederversammlungen weniger als 20 % der Mitglieder anwesend sind. Es ist wünschenswert, aber mit traditionellen Mitteln zu aufwendig, *alle* Mitglieder eines Verbands in Meinungsbildungs- und Beschlußfassungsprozesse einzubinden.
- Mitgliederversammlungen finden – nicht zuletzt auch wegen des damit verbundenen Aufwands – in zeitlich relativ großen Abständen statt (im Fall der GLDV je nach Anbindung an unterschiedliche Fachtagungen bis zu 19 Monate). Zumindest für die satzungsgemäß der Mitgliederversammlung vorbehaltenen Entscheidungen zieht das eine nicht unbeachtliche Trägheit der Entscheidungsprozesse nach sich.

Zwar lassen sich aus diesen Beobachtungen Argumente für eine weitgehende Verwendung elektronischer Kommunikationsformen für zentrale Verbandsaufgaben wie Wahlen oder Abstimmungen ableiten; zu beachten ist jedoch, daß auch mittelfristig nicht davon ausgegangen werden kann, daß alle Mitglieder etwa an elektronischen Wahlverfahren teilhaben können oder wollen. Alle Realisierungsvorschläge müssen daher *ergänzenden Charakter* aufweisen, der erst langfristig auf eine Ablösung der traditionellen Kommunikationsmittel abzielt.

1.2 Sicherheitsrelevante Voraussetzungen elektronischer Kommunikation

Will man über rein informelle oder informative Dienste im Internet wie e-mail oder das WWW hinausgehen, stellt sich die Frage, wie wesentliche Sicherheitskriterien gewährleistet werden können. Zu ihnen gehören u. a.

- die Authentisierung (*authentication*) der Kommunikationspartner,
- die Vertraulichkeit (*confidentiality*) der Kommunikation, insbesondere die Gewährleistung der Anonymität von Wahlen und
- die Integrität (*integrity*) der kommunizierten Information.[1]

Neben diese zentralen Kriterien sicherer Kommunikation treten zusätzliche Faktoren, die bei der Operationalisierung kryptographischer Verfahren eine Rolle spielen, so etwa die Transparenz des Verfahrens und die Vertrauenswürdigkeit einer Anwendung.

1.3 Technische Umsetzung

Um die oben genannten Sicherheitskriterien erfüllen und eine rechtlich zulässige Alternative zu den traditionellen Kommunikationsformen anbieten zu können, bedarf es kryptographischer Verfahren, mit denen

- sich die Identität eines Kommunikationspartners feststellen läßt,
- Anonymität etwa bei geheimen Wahlen gewährleistet ist,
- Information so verschlüsselt werden kann, daß sie unbefugte Dritte nicht entziffern können.

Bei kryptographischen Verfahren wird die zu übermittelnde Nachricht (der *Klartext, plain text*) mit Hilfe einer Umwandlungsvorschrift (des Kryptoalgorithmus) in *Geheimtext* (*cyphertext*) umgewandelt. Neben *symmetrischen* Verfahren, bei denen Sender wie Empfänger über denselben (geheimen) Schlüssel zur Verschlüsselung bzw. Entzifferung verfügen, haben sich in den letzten Jahren vor allen sog. *asymmetrische* Verfahren durchgesetzt, bei denen der Klartext mit Hilfe eines *öffentlichen* Schlüssels verschlüsselt und mit Hilfe eines *privaten* Schlüssels, der nur seinem Inhaber bekannt und durch eine Paßwortphrase o. ä. geschützt ist, entziffert werden kann.[2]

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 daß es *wie unterzeichnet* bei ihm eingetroffen ist, d. h. daß keine Modifikationen am Dokument vorgenommen worden sind. Dabei ist vorausgesetzt, daß der öffentliche Schlüssel in geeigneter Form publiziert worden ist (auf einem frei zugänglichen *key server* oder z. B. auch als ASCII-Text auf der Homepage des Schlüsselinhabers). Die Umsetzung solcher kryptographischer Techniken kann grundsätzlich über Standardsoftware (z. B. das für nicht-kommerzielle Zwecke frei erhältliche *Pretty Good Privacy – PGP*[3]) oder über proprietäre Eigenentwicklungen unter Verwendung kryptographischer *application programming interfaces* (APIs) erfolgen (s. u. Kap. 3).

1.4 Ansatzpunkte für kryptographische Verfahren

Für die Einführung kryptographischer Techniken lassen sich ausgehend von den bewährten traditionellen und elektronischen Kommunikationsformen im Vereins- und Verbandsleben im wesentlichen folgende Ansatzpunkte erkennen:

1) Durchführung von (Vorstands- und Beirats-) Wahlen mit elektronischen Mitteln.
2) Meinungsbildung und Beschlußfassung durch elektronische Kommunikation in Ergänzung der Rolle einer Mitgliederversammlung.
3) Einführung neuer Vereinsorgane durch Satzungsänderung, deren Funktionsweise ganz wesentlich vom Einsatz elektronischer Kommunikationsformen geprägt ist.

Im Mittelpunkt dieses Aufsatzes steht die rechtliche Bewertung elektronischer Vorstandswahlen vor dem Hintergrund des deutschen Vereinsrechts (Kap. 2) sowie ihre praktische Umsetzung und Implementierung (Kap. 3). Zu den Vorschlägen 2) und 3) erfolgen in Kap. 4 einige Hinweise.

2 Rechtliche Aspekte

2.1 Vereinsrechtliche Voraussetzungen

Die Verfassung eines rechtsfähigen Vereins wird gemäß § 25 BGB durch die gesetzlichen Vorschriften sowie durch die Satzung bestimmt. Hinsichtlich der gesetzlichen Vorschriften ist zu unterscheiden, ob es sich um zwingende oder um dispositive, d.h. durch die Satzung abänderbare, Vorschriften handelt. Aus § 40 BGB ergibt sich, welche der Vorschriften dispositiv sind und im Umkehrschluß daraus, welche Bestimmungen zwingender Bestandteil der Vereinsverfassung sind. Soweit die Satzung keine vom Gesetz abweichende Regelung trifft, sind die §§ 26 – 39 BGB und die nicht abänderbaren Vorschriften über die Auflösung des Vereins (§ 41 BGB) und über die Liquidation des Vereinsvermögens (§§ 47 – 52 BGB) Bestandteile der Verfassung jeden Vereins[4].

Die Verfassung eines Vereins wird weiter durch die Regelungen der Vereinssatzung festgelegt. Ihren Inhalt können die Gründer und später die Mitgliederversammlung durch Satzungsänderungsbeschluß im Rahmen der Privatautonomie frei gestalten.[5] Beim eingetragenen Verein stellen die §§ 57, 58 BGB die Mindesterfordernisse für den Satzungsinhalt auf. Hinsichtlich der hier zu besprechen-

den Vorschläge geben § 58 Nr. 3 und 4 BGB an, daß die Satzung Bestimmungen über die Bildung des Vorstands und die Voraussetzungen, unter denen die Mitgliederversammlung zu berufen ist, sowie über die Form der Berufung und die Beurkundung der Beschlüsse zu enthalten hat.

Nach der Rechtsprechung des Bundesgerichtshofs müssen darüber hinaus „die das Vereinsleben bestimmenden Grundentscheidungen" in der Satzung enthalten sein.[6] Da eine Satzungsänderung nur durch Mehrheitsbeschluß und Eintragung in das Vereinsregister vorgenommen werden kann, genießt der Inhalt der Satzung einen gewissen „Bestandsschutz"[7], der zum Schutz der Minderheit und der einzelnen Mitglieder führt.[8] Um diese Schutzfunktion zu gewährleisten, müssen die satzungsmäßigen Regelungen eine hinreichende Regelungsdichte aufweisen.[9] Während die Grundsatzentscheidungen in der Satzung festzulegen sind, können Einzelheiten einer näheren Regelung vorbehalten sein; sie können in nachrangigen Ordnungen, etwa Verfahrensordnungen für Vereinsgerichte, Benutzungsordnungen für Vereinsanlagen[10] oder wie in unserem Fall der Wahlordnung ausgestaltet sein. Solche nachrangigen Ordnungen müssen von dem in der Vereinsverfassung für zuständig erklärten Organ aufgrund einer Ermächtigung erlassen sein und dürfen nicht gegen die Satzung verstoßen.[11]

Insofern ist also bei allen die Organisation eines Vereins betreffenden Regelungen zu fragen, ob eine entsprechende Bestimmung gegen zwingendes Recht verstößt, ob sie einer Bestimmung in der Satzung widerspricht und schließlich ob sie als eine das Vereinsleben bestimmende Grundsatzentscheidung in die Satzung aufzunehmen ist oder auch in einer nachrangigen Neben- oder Vereinsordnung geregelt werden darf.

2.2 Stellung digitaler Signaturen nach dem Signaturgesetz

Das Signaturgesetz (SigG, = Artikel 3 des Informations- und Kommunikationsdienstegesetz, IuKDG) regelt den Einsatz digitaler Signaturen als gesetzlich geregeltem Sicherheitsstandard. Es sind mit der Einführung digitaler Signaturen aber keine Rechtsfolgen verbunden.[12] GEIS bezeichnet das SigG als „gesetzgeberischen Torso"[13], da es die Signatur eben *nicht* dem Schriftformerfordernis des BGB oder der Privaturkunde des § 416 ZPO gleichstellt. Im konkreten Fall bedeutet dies, daß nicht davon auszugehen ist, daß elektronische Kommunikationsformen unter Einsatz kryptographischer Algorithmen ohne weiteres *gesetzlich vorgeschriebenen* schriftlichen Verfahren äquivalent sind oder diese verdrängen können. Im Vereinsrecht spielt dieser Gesichtspunkt jedoch nur eine untergeordnete Rolle, da fast alle Bereiche durch die Satzung frei ausgestaltet werden können (s. o.).[14]

2.3 Durchführung von Vorstandswahlen

Wie die Wahl des Vorstands zu erfolgen hat, ist gesetzlich nicht zwingend festgelegt. § 27 Abs. 1 BGB bestimmt, daß die Bestellung des Vorstandes durch Beschluß der Mitgliederversammlung erfolgt, falls die Satzung nichts anderes vorschreibt (§ 40 BGB).[15] Die Satzung der GLDV trifft hier jedoch eine andere Bestimmung: Gemäß § 19 der Satzung der GLDV wird die „Wahl des Vorstands und des Beirats als Briefwahl [...] durchgeführt". Zum genauen Ablauf der Briefwahl äußert sich die Satzung nicht. In Satz 4 von § 19 der Satzung heißt es nur: „Alles Nähere regelt die Wahlordnung". In der Wahlordnung ist zum technischen Ablauf lediglich ausgeführt, daß „in Briefwahl geheim gewählt" wird. Eine nähere Bestimmung des Begriffs *Briefwahl* erfolgt nicht – weder in der Satzung, noch in der Wahlordnung.

Da die Satzung auf Dauer angelegte Regeln für eine Vereinigung mit wechselndem Mitgliederbestand schafft, ist sie nach zutreffender Ansicht aus sich heraus auszulegen, d. h. die Auslegung kann sich nicht an dem Willen oder den Interessen der Gründer orientieren.[16] In erster Linie ist somit neben Sinn und Zweck der Regelung[17] der Wortlaut maßgebend, und zwar „in einem durch den allgemeinen Sprachgebrauch, evtl. auch durch die Fachsprache in bestimmten Lebensbereichen festgelegten Sinn"[18]. Bei der Auslegung des Begriffs *Briefwahl* wird man sich an anderen Bestimmungen, die eine Briefwahl vorsehen, orientieren können. So regeln z. B. § 36 Bundeswahlgesetz i. V. m. §§ 66, 74 f. Bundeswahlordnung die Briefwahl. Wesentliches Element dieser Bestimmungen ist, daß der Wähler dem Wahlleiter in einem verschlossenen Wahlbriefumschlag seinen Wahlschein und in einem besonderen verschlossenen Umschlag seinen Stimmzettel übersendet. Damit ist gewährleistet, daß der abgegebene Stimmzettel von einem berechtigten Wähler stammt und die Stimmabgabe selbst anonym erfolgt. Diese wesentlichen Bestandteile, wie im nachfolgenden Abschnitt beschrieben, lassen sich durch elektronische Verfahren sicherstellen. Eine Wahl in Form einer „traditionellen" Briefwahl ist also nicht notwendig, um diesen beiden Anforderungen gerecht zu werden. Da die Satzung den Ablauf der Briefwahl der Wahlordnung überläßt, könnte eine Änderung der Wahlordnung ausreichen. In sie wäre etwa einzufügen, daß die Briefwahl *auch* elektronisch durchgeführt werden kann. Selbstverständlich müssen dabei Mitglieder, die keinen Internetzugang haben, die Möglichkeit haben, sich weiterhin durch „traditionelle" Briefwahl zu beteiligen. Dies gebietet bereits der ungeschriebene Rechtsgrundsatz der Gleichbehandlung der Mitglieder.[19] Ob zusätzlich eine Änderung der Satzung notwendig ist, hängt im wesentlichen davon ab, ob man diese Bestimmung als für das Vereinsleben so

wesentliche Grundentscheidung ansieht, daß sie einer satzungsmäßigen Festlegung bedarf.

Zu den Grundentscheidungen zählen die Regelungen von Zweck und Mitteln des Vereins, von Voraussetzungen und Folgen der Mitgliedschaft, von Bildung, Bestellung und Wirkungskreis der Organe sowie von Sitz und Namen.[20] Die Abgrenzung zwischen den in die Satzung aufzunehmenden Grundentscheidungen und den außerhalb der Satzung in Nebenordnungen regelbaren Vereinsangelegenheiten ist im Einzelfall schwierig und umstritten.[21] Wenn man den Sinn der Satzungsvorschrift hinsichtlich der Briefwahl darin sieht, abweichend von der dispositiven Regelung des § 27 BGB und der in der Vereinspraxis gängigsten Art der Vorstandswahl[22] die Wahl des Vorstands ohne persönliche Anwesenheit auf der Mitgliederversammlung durchzuführen, muß man davon ausgehen, daß die nähere Ausgestaltung des technischen Ablaufs dieser Wahlmöglichkeit – ebenso wie bereits jetzt – der Wahlordnung überlassen werden kann. Dies gilt insbesondere dann, wenn die entscheidenden Anforderungen, die an eine Briefwahl zu stellen sind (vgl. oben) durch elektronische Mittel gewährleistet werden und die elektronische Wahl nur eine zusätzliche Möglichkeit der Stimmabgabe – neben der „traditionellen" Briefwahl – darstellt.

3 Elektronische Vorstandswahl

Das nachfolgend beschriebene Verfahren stellt die elektronische Umsetzung einer Vorstandswahl auf der Basis asymmetrischer Kryptographie dar. Es wird anschließend an voranstehende rechtliche Würdigung angenommen, daß

1) die elektronische Form durch Änderung der Wahlordnung (Beschluß der Mitgliederversammlung) sanktioniert ist,
2) die an der elektronischen Wahl teilnehmenden Mitglieder über e-mail und WWW-Anschluß verfügen und
3) für alle anderen Mitglieder weiterhin die schriftliche Wahlform zur Verfügung steht.

Für jedes Vereinsmitglied wird ein Schlüsselpaar generiert; der Verein fungiert dabei als eine Art Zertifizierungsstelle[23], wobei die Schlüssel ausschließlich für die verbandsinterne Kommunikation geeignet sind. Jedes Mitglied erhält den öffentlichen Schlüssel seines Schlüsselpaars per e-mail zugesandt. Mit dem Schlüssel kann der Wähler den Wahlschein verschlüsseln. Der Verein verwaltet die

privaten Schlüssel, um Nachrichten (hier: den Wahlschein) verifizieren zu können (*Authentisierung*). Zusätzlich generiert die Wahlsoftware mit Hilfe eines symmetrischen Verfahrens einen Schlüssel, mit dem der Wahlzettel *vor* der Verschlüsselung durch den Mitgliedsschlüssel verschlüsselt wird. Es kommt also in Analogie zur Briefwahl ein zweistufiges Verfahren zum Einsatz:

1) Das Mitglied füllt den Wahlzettel aus, die Wahlsoftware verschlüsselt ihn mit Hilfe des symmetrischen Schlüssels („Verbandsschlüssel"), ohne daß der Benutzer eingreifen müßte.
2) Der verschlüsselte Wahlzettel wird nochmals mit dem mitgliedsbezogenen öffentlichen Schlüssel verschlüsselt.

Die so entstandene Nachricht wird an den Wahlleiter gesandt. Dieser kann anhand der verfügbaren öffentlichen Schlüssel zunächst feststellen, daß der Wahlzettel von einem stimmberechtigten Mitglied stammt und den verbleibenden, mit dem Verbandsschlüssel verschlüsselten Wahlzettel in die (elektronische) Wahlurne geben. 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.

3.1 Implementierung

Wie bereits angedeutet, bieten sich im wesentlichen zwei Szenarien für die Implementierung des angedeuteten Verfahrens:

Szenario I - Einsatz von Standardsoftware
Setzt man ein geeignetes Kryptographiepaket (z. B. *Pretty Good Privacy*) bei allen Teilnehmern voraus, so könnte das Verfahren wie folgt ablaufen:

1. Generieren der Schlüsselpaare mit *PGP* durch den Verband
2. Verteilen der öffentlichen Schlüssel per e-mail an die Mitglieder
3. Verteilen des Wahlzettels als e-mail-Formular
4. Ausfüllen und (zweimaliges) Verschlüsseln des Wahlzettels mit *PGP*
5. Rücksenden per e-mail
6. Verifikation der Wahlberechtigung (1. Entschlüsselung)
7. Entschlüsseln der Wahlzettel durch den Wahlleiter (2. Entschlüsselung)
8. Auswertung

Dieses Szenario hat den wohl entscheidenden Nachteil, daß die Installation eines komplexen Softwarepakets nicht nur einen organisatorischen Zusatzaufwand darstellt, sondern auch eine zusätzliche Hemmschwelle darstellt, da sich jeder Einzelne in Bedienung und Funktionsweise einarbeiten muß. Demgegenüber versucht das nachfolgende Szenario – um den Preis eines höheren Entwicklungsaufwands – eine Lösung aufzuzeigen, die Benutzungsfreundlichkeit mit sehr wenigen notwendigen Interaktionsschritten zu verbinden sucht:

Szenario II – Webbasierte Eigenentwicklung

Bei dieser Lösung steht dem Nutzer für die Wahl ein Wahlzettel als Java™-Applet zur Verfügung, den er in einem Browser von der Verbands-WebSite laden, ausfüllen und versenden kann:

1. Generieren der Schlüssel mit Hilfe des *Java™ Cryptography-API*
2. Verteilen der öffentlichen Schlüssel per e-mail an die Wähler
3. Ausfüllen, (zweimaliges) Verschlüsseln und Signieren des Wahlzettels
4. Abschicken an den Vereins-Webserver
5. Verifikation der Wahlberechtigung (1. Entschlüsselung)
6. Entschlüsseln der Wahlzettel durch den Wahlleiter (2. Entschlüsselung)
7. Auswertung

Der Weg einer Eigenentwicklung hat den zusätzlichen Vorteil, daß sich auch die Schritte 5 – 7 weitgehend automatisieren lassen. Deshalb haben wir uns für dieses Szenario entschieden. Die Programmiersprache Java™ wird verwendet, da sie über ein geeignetes kryptographisches API verfügt, die *Java Cryptography Architecture* (JCA)[24], und gleichzeitig die Realisierung von *active contents* im WWW erlaubt. Die *JCA* gliedert sich in zwei Teile:

- Einen allgemein verfügbaren Teil, der ein plattform- und algorithmenneutrales Programmierinterface für die Entwicklung kryptographischer Anwendungen sowie Basisklassen für die Erstellung digitaler Signaturen und sog. *Message Digests* enthält und
- die sog. *Java Cryptography Extension* (JCE), die darüber hinaus Algorithmen für die Verschlüsselung von Daten bereitstellt.

Aufgrund der U.S.-amerikanischen Exportrestriktionen dürfen die Java™ *JCEs* von SUN nicht exportiert werden, da nach geltendem amerikanischen Recht (*Ex-*

port Control Act, Arms Export Control ACT etc.) Datenverschlüsselungsverfahren als *Waffen* (sic!) gelten.[25] Deshalb wird auf die Reimplementierung der Java™ *JCEs* der TU Graz zurückgegriffen.[26]

3.2 Die eingesetzten kryptographischen Algorithmen

Der Klartext, d.h. der eigentliche Stimmzettel wird mit einem symmetrischen Verfahren verschlüsselt. Hierbei kommt der *International Data Encryption Standard* (*IDEA*) zum Einsatz, das nach allgemeiner Ansicht derzeit mächtigste kryptographische Verfahren.[27] *IDEA* arbeitet als sog. Blockchiffrierverfahren auf der Basis der Mischung von Operationen unterschiedlicher algebraischer Gruppen, d. h. über je 64 Bit Klartext werden die Operationen XOR, Addition Modulo 2^{16} und Multiplikation Modulo $2^{16} + 1$ (eine Primzahl) eingesetzt. Der verschlüsselte Text sowie der für den Verschlüsselungsvorgang generierte Schlüssel von *IDEA* werden mit dem öffentlichen Schlüssel des Mitlieds verschlüsselt. Für die Generierung der Schlüsselpaare des asymmetrischen Verfahrens, mit denen der *IDEA*-Schlüssel und der Wahlschein verschlüsselt werden, verwenden wir den *RSA*-Algorithmus, der erste vollständige und heute am weitesten verbreitete asymmetrische Kryptographiealgortihmus.[28] Das Schlüsselpaar wird bei *RSA* mit Hilfe des Produkts zweier (sehr großer) Primzahlen gebildet. Die Sicherheit des Algorithmus beruht darauf, daß bisher kein einfaches Verfahren gefunden werden konnte, Zahlen dieser Größenordnung zu faktorisieren. *IDEA* ist durch ein europäisches Patent geschützt;[29] seine Verwendung für nicht-kommerzielle Zwecke ist aber freigestellt. *RSA* ist lediglich in den USA patentiert.[30]

3.3 Softwarekomponenten

Um das Verfahren wie dargelegt durchführen zu können, sind drei Softwarekomponenten erforderlich:

- Das Modul für die Generierung der Schlüsselpaare („Zertifizierungsstelle“; „Wahlamt“),
- die eigentliche Wahlsoftware, ein WWW-Client, realisiert als Java™-Applet: „Wahlkabine“ mit „Wahlschein“ (der öffentliche Schlüssel) und „Wahlzettel“ (das Java™-Formular) und
- das Modul zur Entschlüsselung der Wahlscheine, das auch Auswertungsausgaben übernehmen kann („Wahlurne“ und „Wahlleiter“).

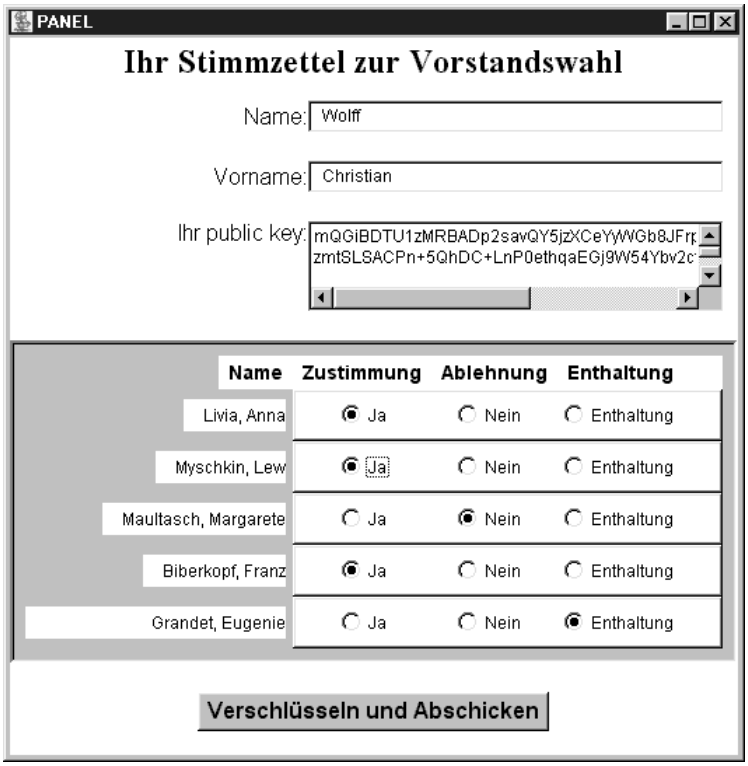

Abb. 1: Prototypische Realisierung von Wahlschein und Stimmzette

Bei der Implementierung stehen die folgenden Aspekte im Mittelpunkt:

1) Der Einsatz der Programmiersprache Java™ gewährleistet plattformübergreifende Verfügbarkeit.[31]
2) Sichere Kryptographie verlangt – auch um das Vertrauen der Benutzer zu gewinnen – nach einem Höchstmaß an Transparenz. Deshalb kommen nur kryptographische Verfahren zum Einsatz, deren Algorithmen öffentlich sind, und die bereits intensiver Kryptanalyse unterzogen wurden.
3) Alle Prozesse lassen sich weitgehend automatisieren, um den Arbeitsaufwand (des Wählers wie des Wahlleiters) im Vergleich zum traditionellen Wahlverfahren zu minimieren. Dabei wird zur Schlüsselgenerierung bzw.

-authentisierung auch auf eine Mitgliedsdatenbank zurückgegriffen.

4) Für den vielfach im Umgang mit kryptographischen Verfahren unerfahrenen Benutzer steht ein einfaches Interface zur Verfügung. Die wesentliche Hürde besteht aus dem Transfer der Schlüsseldaten aus dem e-mail-Viewer des Wählers in das entsprechende Textfeld des Wahlscheins.
5) Die modulare Struktur soll die Generalisierbarkeit der Anwendung sicherstellen. Dabei ist an eine automatische Generierung passender Wahlformulare für unterschiedliche Typen von Wahlen, Umfragen oder Erhebungen zu denken. Aufgrund der gegebenen formalen Beschreibbarkeit der abzufragenden Daten erscheint dies problemlos möglich.

Abb. 1 zeigt den Prototyp des Webclients mit einem hypothetischen Wahlzettel. Er sieht die Zustimmung, Ablehnung und Enthaltung als typische Wahlmöglichkeiten vor. Darüber hinaus kann im einzelnen auch *keine Stimmabgabe* erfolgen, wenn kein Radio Button angekreuzt ist.

4 Zur praktischen Umsetzung

Die entscheidenden Hindernisse auf dem Weg zum Einsatz kryptographiebasierter Kommunikationsverfahren liegen weniger auf dem Feld technischer Realisierbarkeit als vielmehr im Bereich der Organisation und der Logistik sowie der Akzeptanz durch den Benutzer. Im konkreten Einsatzgebiet – elektronische Vorstandswahlen der GLDV – bedeutet dies:

1) Das Verfahren wird den Mitgliedern frühzeitig vorgestellt und auf Mitgliederversammlungen diskutiert, ggf. modifiziert.
2) Vor dem eigentlichen Einsatz erfolgen Testläufe mit hypothetischen Daten, um technische und ergonomische Schwachstellen erkennen und beseitigen zu können.
3) Es wird nur parallel und in Ergänzung zum traditionellen papierbasierten Wahlverfahren eingesetzt; jedes Mitglied hat also die Möglichkeit, das für ihn einfachere Wahlverfahren zu verwenden.

5 Fazit & Ausblick

"Good design starts with a threat model: what the system is to protect, from whom, and for how long."[32] Dieser Devise von Bruce SCHNEIER folgend sei gefragt, welche Sicherheitslücken und Angriffspunkte das vorgeschlagene Verfahren bietet: Der entscheidende Schwachpunkt ist wohl die einfache Versendung der öffentlichen Mitgliedsschlüssel per e-mail, da diese im Internet abgefangen werden könnten. Zwar ist ein mehrfaches Wirksamwerden einer Stimmabgabe mit demselben Schlüssel ausgeschlossen, aber es könnte ein Unbefugter dem berechtigten Mitglied die Stimme vorenthalten, indem er ohne Berechtigung das Stimmrecht ausübt und so das Wahlergebnis verfälscht. Im Rahmen des gewählten Testszenarios halten wir diesen Fall aber für hinreichend unwahrscheinlich, um auf weitere, das Verfahren verkomplizierende, Sicherungsmaßnahmen verzichten zu können.

Mittelfristig ist das Verfahren auf nach dem SigG von einer amtlichen Zertifizierungsstelle beglaubigte digitale Signaturen umzustellen. Auf diese Variante haben wir zunächst verzichtet, da wir davon ausgehen, daß nur sehr wenige Wahlberechtigte über eine derartige Signatur verfügen.

Die elektronische Wahl ist der am einfachsten zu formalisierende und automatisierende Kommunikationsprozeß im Verbandsleben. Wollte man z. B. eine Mitgliederversammlung elektronisch durchführen, so wäre einerseits eine wesentlich komplexere kommunikative Struktur zu modellieren (Einberufung, Tagesordnung, Eröffnung, Genehmigung der Tagesordnung, Anträge aus der Mitte der Mitgliederversammlung, Bericht und Diskussion, Abstimmung und Wahlen), was nur durch die Verwendung heterogener Software-Systeme denkbar erschiene (e-mail-Verteiler, Diskussionsforen, *electronic vote*, Videokonferenz). Andererseits ist es von vornherein fraglich, ob das ineinandergreifende Geflecht unterschiedlicher Rechte der Verbandsorgane und Mitglieder, das in einer Mitgliederversammlung zum Tragen kommt (Teilnahmerecht, Rederecht, Auskunftsrecht, Antragsrecht, Stimmrecht)[33] sich überhaupt mit elektronischen Mitteln modellieren läßt. Es erscheint daher sinnvoller, neben elektronischen Wahlen weitere rechnergestützte Kommunikationsformen als neue Vereinsorgane in die Satzung aufzunehmen. Auf diesem Weg könnten z.B. der Mitgliederversammlung vorbehaltene Entscheidungen auch auf elektronisch durchgeführte Diskussionen und Abstimmungen übertragen werden, ohne daß dies einer „virtuellen Mitgliederversammlung" gleichkäme.

Anmerkungen

[1]Vgl. RANNENBERG, MÜLLER & PFITZMANN 1997:22f; SUN MICROSYSTEMS 1997B:1.

[2]Zur Einführung in kryptographische Verfahren und die wichtigsten Algorithmen vgl. WOBST 1997, bes. 105ff, 136ff.

[3]Vgl. IANNAMICO 1997; SCHNEIER 1996:664ff; WOBST 1997:275ff.

[4]REICHERT & VAN LOOK 1995:Rdnr. 259.

[5]REICHERT & VAN LOOK 1995:Rdnr. 260.

[6]BGHZ 47, 172 (177) = NJW 1967, 1268 (1270); BGHZ 105, 306 (313 f.) = NJW 1989, 1724 (1725); zustimmend auch die herrschende Meinung in der Literatur: MÜNCHKOMM/*REUTER* § 25 Rdnr. 3; STAUDINGER/*WEICK* § 25 Rdnr. 3; REICHERT & VAN LOOK 1995:Rdnr. 262 mit weiteren Nachweisen sowie Rdnr. 315 ff.

[7]REICHERT & VAN LOOK 1995:Rdnr. 279.

[8]BGHZ 105, 306 (314) = NJW 1989, 1724 (1725); REICHERT & VAN LOOK 1995:Rdnr. 279; a. M.: MÜNCHKOMM/*REUTER* § 25 Rdnr. 6, der die Sicherung der Integration der Vereinsverfassung als Hauptzweck ansieht.

[9]REICHERT & VAN LOOK 1995:Rdnr. 263.

[10]STAUDINGER/*WEICK* § 25 Rdnr. 4.

[11]REICHERT & VAN LOOK 1995:Rdnr. 319.

[12]GEIS 1997:3000.

[13]GEIS 1997:3002.

[14]Nur ausnahmsweise sind zwingend Formvorschriften zu beachten, etwa gem. § 37 Abs. 1 BGB, nach dem der Antrag einer Minderheit auf Einberufung der Mitgliederversammlung „schriftlich unter Angabe des Zweckes und der Gründe“ zu stellen ist. Ebenso sind die Formvorschriften über die Bekanntmachung der Auflösung des Vereins oder der Entziehung der Rechtsfähigkeit (§ 50 BGB) zwingendes Recht.

[15]WALDNER & RÖSELER 1994:94, Rdnr. 130.

[16]REICHERT & VAN LOOK 1995:Rdnr. 301; STAUDINGER/*WEICK* § 25 Rdnr. 16.

[17]BGH NJW 1994, 51 [52].

[18]STAUDINGER/*WEICK* § 25 Rdnr. 16.

[19]Vgl. BGH NJW 1954, 953; BGHZ 47, 172 (177) = NJW 1967, 1268 (1270); BGHZ 47, 381 [386].

[20]MÜNCHKOMM/*REUTER* § 25 Rdnr. 3; vgl. auch REICHERT & VAN LOOK 1995:Rdnr. 263, 296.

[21]MÜNCHKOMM/*REUTER* § 25 Rdnr. 4 mit einer Auflistung der dazu ergangenen Rechtsprechung sowie der Ansicht in der Literatur; vgl. auch REICHERT & VAN LOOK 1995:Rdnr. 315.

[22]REICHERT & VAN LOOK 1995:Rdnr. 1227: „Im Regelfall wird der Vorstand in der Mitgliederversammlung gewählt.“

[23]Eine Zertifizierungsstelle im Sinne des SigG ist eine Behörde oder ein von einer Behörde beauftragtes Unternehmen, daß Signaturschlüssel und digitale Zertifikate generiert, ausgibt und verwaltet, d. h. zur Verfikation in einer Datenbank bereithält, vgl. BIESER 1997:402ff.

[24]Vgl. SUN MICROSYSTEMS 1997A.

[25]Dies gilt aber nicht für kryptographische Verfahren, die lediglich der Authentisierung dienen, also etwa digitale Signaturen, da sie die eigentliche Nachricht nicht verschlüsseln. Deshalb sind

die Algorithmen für digitale Signaturen frei verfügbar. Vgl. SCHNEIER 1996:691ff; WOBST 1996:275ff, 307ff.

[26]Vgl. PLATZER 1998.

[27]Vgl. SCHNEIER 1996:370ff; WOBST 1997:182ff.

[28]Der RSA-Algorithmus ist *vollständig*, da er sowohl für Verschlüsselung als auch für digitale Signaturen geeignet ist; RSA ist nach seinen Entwicklern RIVEST, SHAMIR und ADLEMAN benannt, vgl. SCHNEIER 1996:531ff; WOBST 1997:143ff.

[29]*IDEA*: Europ. Patent Nº 0482154 vom 30.6.1991.

[30]Vgl. WOBST 1997:154.

[31]Vgl. ARNOLD & GOSLING 1997.

[32]SCHNEIER 1997:3.

[33]Vgl. REICHERT & VAN LOOK 1995:Rdnr. 869ff, 880ff, 885ff, 890ff, 895ff.

Literatur

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

BIESER, Wendelin (1997). „Begründung und Überlegung zum Signaturgesetz." In: MÜLLER & PFITZMANN (1997), 399 – 410.

GARFINKEL, Simson; SPAFFORD, Gene (1997). „Cryptography and the Web." In: World Wide Web Journal 2(4) (1997), 113 – 126.

GEIS, Ivo (1997). „Die Digitale Signatur." In: Neue Juristische Wochenschrift 1997, 3000 – 3004.

IANNAMICO, Mike (1997). 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.

KHARE, Rohit; RIFKIN, Adam (1997). „Weaving a Web of Trust." In: World Wide Web Journal 2(4) (1997), 77 – 112.

MÜNCHKOMM/*REUTER*. Münchener Kommentar zum Bürgerlichen Gesetzbuch, Bd. 1, Allgemeiner Teil, 3. Auflage, München: Beck 1993, zit. als MÜNCHKOMM/*REUTER*.

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

PLATZER, Wolfgang (1998). The IAIK Java Cryptography Extension. TU Graz, Institute for Applied Information Processing and Communications. März 1998. http://jcewww.iaik.tu-graz.ac.at/IAIK_JCE/jce.htm . (22. Mai 1998).

RANNENBERG, Kai; MÜLLER, Günter; PFITZMANN, Andreas (1997). Sicherheit, insbesondere mehrseitige IT-Sicherheit. In: MÜLLER & PFITZMANN (1997), 2129.

REICHERT, Bernhard; VAN LOOK, Frank (1995). Handbuch des Vereins- und Verbandsrechts. Neuwied et al.: Luchterhand.

SCHNEIER, Bruce (1996). Angewandte Kryptographie. Bonn et al.: Addison-Wesley.

SCHNEIER, Bruce (1997). Why Cryptography Is Harder Than it Looks. Technical Report, Counterpane Systems Inc, Minneapolis.

SCHUSTER, Rolf; FÄRBER, Johannes; EBERL, Markus (1997). Digital Cash. Zahlungssysteme im Internet. Berlin et al.: Springer.

STAUDINGER/*WEICK*. J. v. STAUDINGERS Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, 13. Bearbeitung, Berlin: Sellier-de Gruyter 1995.

SUN MICROSYSTEMS Inc. (1997A). Java Security Architecture. October 1997.

SUN MICROSYSTEMS Inc. (1997B). Secure Computing with Java: Now and the Future. A White Paper. 1997. http://www.javasoft.com/marketing/collateral/security.html . (22. Mai 1997).

WALDNER, Wolfram; RÖSELER, Diana (1994[15]). Der eingetragene Verein. München: Beck.

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