Abschlussbericht zum Projekt

# voteremote: Online-Wahlen außerhalb von Wahllokalen

Teilvorhaben

## Sicherheitsanalyse

Technische Universität Darmstadt

| Zuwendungsempfänger: | Förderkennzeichen: |
|---|---|
| **Technische Universität Darmstadt**<br>**Fachbereich Informatik**<br>**Fachgebiet**<br>**Theoretische Informatik** | **01 MS 06 002** |
| Verbundvorhaben:<br>**voteremote:**<br>**Online-Wahlen außerhalb von Wahllokalen**<br><br>Teilvorhaben:<br>**Sicherheitsanalyse** | |
| Laufzeit des Vorhabens:<br>**01.04.2006-31.10.2008** | Berichtszeitraum:<br>**01.04.2006 - 31.10.2008** |


Ausführende Stelle: Technische Universität Darmstadt
Fachbereich Informatik
Fachgebiet Theoretische Informatik
Hochschulstr. 10
64289 Darmstadt
Tel. 06151 / 16 - 5541
Fax. 06151 / 16 - 6036
Mail: langer@cdc.informatik.tu-darmstadt.de
axel@cdc.informatik.tu-darmstadt.de

Autoren: Lucie Langer
Axel Schmidt



Das diesem Bericht zu Grunde liegende Forschungsvorhaben wurde mit Mitteln des Bundesministeriums für Wirtschaft und Technologie unter dem Förderkennzeichen 01 MS 06 002 gefördert. Die Verantwortung für den Inhalt dieser Arbeit liegt bei den Autoren.

# Inhaltsverzeichnis

**1 Kurzdarstellung** **1**
1.1 Aufgabenstellung . . . . . 1
1.2 Voraussetzungen . . . . . 2
1.3 Planung und Ablauf . . . . . 3
1.4 Stand in Wissenschaft und Technik . . . . . 4
1.5 Zusammenarbeit mit anderen Stellen . . . . . 5

**2 Eingehende Darstellung** **7**
2.1 Verwendung der Zuwendung und erzieltes Ergebnis . . . . . 7
2.2 Notwendigkeit und Angemessenheit der geleisteten Arbeit . . . . . 29
2.3 Verwertbarkeit der Ergebnisse . . . . . 29
2.4 Fortschritt bei anderen Stellen . . . . . 30
2.5 Veröffentlichung der Ergebnisse . . . . . 31

# 1 Kurzdarstellung

## 1.1 Aufgabenstellung

Im Verbundvorhaben *voteremote: Online-Wahlen außerhalb von Wahllokalen* sollte ein Wahlsystem geschaffen werden, mit dem nicht-parlamentarische elektronische Wahlen technisch sicher unter Einhaltung rechtlicher Anforderungen in der Praxis durchgeführt werden können. Das Teilvorhaben *Sicherheitsanalyse* hatte zum Ziel, sicherheitsrelevante Grundlagen des Wahlsystems zu erarbeiten sowie kryptographische Primitive für dessen Umsetzung in die Praxis bereitzustellen. Zur Untersuchung der Notwendigkeit einer Änderung der Gesetzeslage und daraus resultierenden Entwicklung eines Gesetzentwurfs für elektronische Wahlen wurde ein Unterauftrag an die Universität Kassel (Prof. Roßnagel) vergeben.

Ein wichtiges Arbeitsziel des Forschungsvorhabens, insbesondere in wissenschaftlicher Hinsicht, war die Analyse von Sicherheitskriterien. An eine Remotewahl müssen hohe Sicherheitsanforderungen gestellt werden: Beispielsweise muss verifizierbar sein, dass sowohl der Wahlklient als auch die dahinter stehende Serveranbindung sowie deren Verbindungswege frei von Viren, Trojanern oder sonstiger Malware ist. Dies sicherzustellen kann jedoch nur in der Verantwortung des Wählers liegen. Aufgabe des Betreibers des Wahlsystems ist es dagegen, Wege für die Nachvollziehbarkeit und Verifizierbarkeit der Korrektheit des Wahlsystems zu finden. Gewonnene Analysen und Resultate sowie Lösungswege wurden als wissenschaftliches Arbeitsziel dieses Vorhabens gewertet. Es erschein dabei als wichtig, diese nach außen zu kommunizieren, um den Diskurs bei nationalen und internationalen Experten anzukurbeln. Die Schlussfolgerungen waren eine wichtige Grundlage für die im Anschluss an das Projekt anstehenden Prüfungs- und Zertifizierungsvorhaben, da damit gleichzeitig die Grundlagen für ein Protection Profile und ein Security Target gegeben wurden.

Das technische Hauptarbeitsziel des Projekts voteremote war die Entwicklung eines Prototypen, der für verschiedene Wahlszenarien von Remotewahlen (z.B. Betriebsratswahl vom Arbeitsplatz über das Intranet, Sozialwahl vom heimischen PC über das Internet, etc.) anwendbar ist. Dieser Prototyp sollte innerhalb des Forschungsvorhabens bereits die notwendigen Tests durchlaufen haben, so dass im Anschluss an das Projekt direkt mit der Produktentwicklung begonnen werden kann. Zugehörig zu dieser Systementwicklung war die Erschließung einer passenden Serveranbindung, wofür im Vorfeld Untersuchungen zum Nutzerverhalten von Wählern vonnöten waren, um besonders hinsichtlich des Belastungsverhaltens während Peakzeiten verlässliches Datenmaterial zu gewinnen, das entsprechend umgesetzt werden kann. Hierzu gewonnene Erkenntnisse wurden als unerlässlich für die einsatzspezifische Konfiguration des Systems angesehen, um entsprechend unterschiedliche Wahlkonfigurationen ökonomisch sinnvoll ausrichten zu können.

Auch die Schaffung der Grundlagen von Gesetzesänderungen für elektronische Wahlen und deren letztliche Umsetzung floss als wissenschaftliches Arbeitsziel in das Forschungsvorhaben mit ein. Voraussetzung für Gesetzesänderungen, die vornehmlich im außerparlamentarischen Bereich angestrebt werden sollten, war die Definition der Anforderungen, die sich aus den einzelnen Gesetzen und Wahlordnungen ergeben sowie die technische Umsetzung dieser. Geplant war, die Resultate in die laufende juristische Debatte der Fachwelt zum Thema elektronische Wahlen miteinzubeziehen.

## 1.2 Voraussetzungen

Der Antragsteller und seine Arbeitsgruppe waren für das Teilvorhaben „Sicherheitsanalyse“ im Besonderen qualifiziert durch erhebliche Vorarbeiten im Bereich der Kryptographie und ihrer Anwendungen. Es wurden in der Vergangenheit neue kryptographische Primitive gefunden, Beiträge zur innovativen elliptische Kurven Kryptographie geleistet und viele kryptoanalytische Resultate erzielt. Die untersuchten kryptographischen Primitive spielen bei der Realisierung von elektronischen Wahlsystemen eine zentrale Rolle. Die Ergebnisse sind in die Open Source Kryptosoftware FlexiProvider eingeflossen.

In jüngerer Zeit haben der Antragsteller und seine Arbeitsgruppe im Bereich neuer kryptographischer Systeme auf Basis von Codierungstheorie, Multivariater Quadratischer Systeme und Gittertheorie im Kontext des Post Quantum Computer Szenarios gearbeitet. Hier sind erste Resultate für Post-Quantum Voting Verfahren erzielt worden.

Im Bereich der Anwendungen arbeitete der Antragsteller und seine Arbeitsgruppe im Projekt SicAri mit, das die Realisierung einer performanten und leicht zu konfigurierenden Sicherheitsplattform für eine ubiquitäre sichere Internetnutzung zum Ziel hat. Dies sind Grundlagen für sichere und performante Wahlsysteme.

Darüber hinaus hat der Antragsteller umfangreiche Forschung im Bereich der Public Key Infrastrukturen betrieben, die als zentraler Baustein moderner E-Voting Syteme betrachet werden müssen. Im BMWi Projekt FairPay hat der Antragsteller flexible Public Key Infrastrukturen für elektronische Zahlungssysteme und andere Anwendungen konstruiert, die es ermöglichen, unsichere kryptographische Systeme schnell auszutauschen. Die daraus entstandene Software FlexiTrust und FlexiProvider werden unter anderem in der deutschen Wurzelinstanz für digitale Signaturen bei der Bundesnetzagentur und zur Absicherung der neuen Bundesreisepässe eingesetzt.

Die Probleme der elektronischen Bezahlsysteme und der elektronischen Wahlsysteme sind miteinander verwandt. Der Antragsteller und seine Arbeitsgruppe haben im iVote Projekt mitgewirkt und ein neues Konzept für iVote entwickelt. Es wurden unter Einbeziehung moderner Technologien im Bereich der Netzwerk-

kommunikation und Kryptographie alternative E-Voting Systeme untersucht und eine Weiterentwicklung des Verfahrens vorgeschlagen.

## 1.3 Planung und Ablauf

Gegenstand des Teilvorhabens „Sicherheitsanalyse“ war die Klärung der Sicherheitsziele für voteremote, die Mitwirkung an der Konzeption von voteremote und der Nachweis, dass voteremote die geforderten Sicherheitsziele tatsächlich erreicht. Außerdem sollten in diesem Teilvorhaben die notwendigen kryptographischen Grundfunktionen für voteremote identifiziert und in optimierter Form bereitgestellt werden.

Erster Schritt dazu war die Identifikation der im voteremote-Verfahren beteiligten Player einschließlich ihrer Fähigkeiten, der Sicherheitsannahmen und der Sicherheitsziele für voteremote. Player sind zum Beispiel Wähler und elektronisches schwarzes Brett. Ein Beispiel für eine Sicherheitsannahme könnte lauten: Es steht eine vertrauenswürdige Public Key Infrastruktur (PKI) zur Verfügung. Insbesondere wurden Annahmen über die Sicherheit der verwendeten Wahlclients und Netzwerke formuliert. Die Sicherheitsannahmen wurden so formuliert, dass sie - auch mit Hilfe von nicht-technischen Maßnahmen wie Sozialkontrolle - nachweislich realisiert werden können.

Das voteremote-Verfahren soll vom Arbeitsplatz aus über Intranet oder Internet angewendet werden können sowie vom heimischen PC aus über das Internet. Die genauen Anwendungsszenarien sollten im Rahmen einer Anforderungsanalyse geklärt werden. Die Sicherheitsziele sollten daraufhin für diese Anwendungsszenarien beschrieben werden.

Im nächsten Schritt wurden existierende Remotewahlprotokolle und Wahlklienten analysiert im Hinblick auf Initialisierungsphase, Registrierungsphase, Wahlphase und Auszählphase. Geklärt wurde dabei, welche Elemente dieser Protokolle und Clienten in Hinblick auf die gefundenen Sicherheitsziele verwendet werden können und welche Elemente neu spezifiziert werden müssen. Besondere Beachtung wurde den verwendeten kryptographischen Primitiven und den darin verwendeten Parametern gewidmet.

Als nächstes sollte die Spezifikation und Implementierung des Prototypen von voteremote in Kooperation mit den anderen Projektteilnehmern erstellt werden. Diese Beschreibung sollte auch mögliche Fehler und die Reaktionen des Wahlprotokolls enthalten. Die Beschreibung wurde in einer Form vorgenommen, die einer Evaluierung nach Common Criteria zugänglich ist. Mögliche Varianten wurden im Hinblick auf Effizienz- und Sicherheitsaspekte verglichen. Die Planung sah vor, Standardverfahren wie TLS und IP/Sec nach Möglichkeit zu verwenden. Aufgabe des Teilvorhabens war es dabei insbesondere, dafür zu sorgen, dass Spezifikation und Implementierung durchgängig die gefundenen Sicherheitsziele berücksichtigen.

In dieser Phase wurden auch geeignete kryptographische Primitive sowie die notwendigen Parameter spezifiziert und hocheffiziente Implementierungen der Primitive im Rahmen des FlexiProviders bereitgestellt.

Nach erfolgreicher Spezifikation sollte im Teilvorhaben der Nachweis geführt werden, dass voteremote unter den getroffenen Sicherheitsannahmen die spezifizierten Sicherheitsziele tatsächlich erreicht. Ziel war dabei auch, die Nachweise so weit wie möglich allgemeinverständlich zu formulieren, um sie auf diese Weise auch Nicht-Technikern zugänglich zu machen und dadurch die Akzeptanz des Wahlsystems beim Anwender zu erhöhen.

## 1.4 Stand in Wissenschaft und Technik

Wahlen sind ein zentrales Instrument demokatrischer Entscheidungsprozesse. Die Teilnahme sollte daher für den Wähler so bequem wie möglich realisierbar sein, was eine starke Motivation für elektronische Wahlen über das Internet darstellt.

Elektronische Wahlen müssen aber gleichzeitig mindestens so sicher wie traditionelle Wahlen sein. Viele Länder experimentieren mit elektronischen Wahlen, zum Beispiel die Schweiz (Genf, Neuchatel, Zürich) [N. 03, Opp02, Sch02], Großbritannien (St.Albans, Sheffield, Liverpool) [Loc02] und die Niederlande [The02, Inv02]. Die Europäische Union hat eine Spezialistengruppe eingesetzt, die Empfehlungen für rechtliche, operative und technische Standards für elektronische Wahlen entwickeln soll [Cou03].

Laut §1 Abs.1 des Bundeswahlgesetzes sollen Wahlen allgemein, unmittelbar, frei, gleich und geheim sein. In [VH04] wurde versucht, diese gesetzlichen Prinzipien auf elektronische Wahlen zu übertragen. In der wissenschaftlichen Gemeinschaft besteht generell Übereinstimmung darin, dass e-Voting Systeme die folgenden Anforderungen erfüllen sollen (siehe z.B. [Rie98]):

1. Exaktheit
    - Ein gültiges Votum kann nicht geändert werden.
    - Alle gültigen Voten werden gezählt.
    - Ungültige Voten werden nicht gezählt.
2. Demokratie:
    - Nur berechtigte Wähler können wählen.
    - Jeder Wähler gibt nur ein Votum ab.
3. Geheimhaltung:

- Anonymität: Es ist nicht möglich ein Votum mit dem Wähler zu assoziieren der es abgegeben hat.
- Quittungsfreiheit: Kein Wähler kann beweisen, dass er ein bestimmtes Votum abgegeben hat.
- Unzwingbarkeit: Ein Wähler kann nicht gezwungen werden, ein bestimmtes Votum abzugeben.
- Fairness: Alle Voten bleiben bis zum Ende der Wahl geheim.

4. Verifizierbarkeit:
   - Universell: Jeder kann verifizieren, dass alle gültigen Stimmen gezählt wurden.
   - Individuell: Jeder Wähler kann verifizieren, dass seine gültige Stimme gezählt wurde.

Unterschiedliche Realisierungen von elektronischen Wahlen sind möglich. Elektronische Wahlen lassen sich mit homomorphen Verschlüsselungsverfahren, mit Mix Nets und mit blinden Signaturen oder einer Kombination dieser Techniken realisieren. Welche Technik verwendet wird, hängt von den Anforderungen ab. Um dies zu beurteilen, müssen sowohl das Anwendungsszenario und dessen Sicherheitsziele, als auch Aspekte der erforderlichen Effizienz in Betracht gezogen werden.

## 1.5 Zusammenarbeit mit anderen Stellen

T-Systems war während des Projektvorhabens voteremote neben der Projektleitung insbesondere zuständig für die Entwicklung der Software für das Wahlsystem sowie Forschungsaufgaben, soweit sie nicht in den Zuständigkeitsbereich der Technische Universität Darmstadt fielen. Insbesondere im Bereich der Common Criteria Evaluierung des Wahlsystems arbeitete die Technische Universität Darmstadt eng mit T-Systems zusammen. Die intensive Zusammenarbeit und die Kommunikation mit T-Systems waren stets reibungslos und produktiv.

Als neuer Projektpartner wurde während der Projektlaufzeit das Team um Prof. Roßnagel von der Universität Kassel für eine Kooperation hinzugezogen. Die vorrangigen Aufgaben der Universität Kassel waren die Überprüfung der Konformität des entwickelten Wahlsystems mit den bestehenden gesetzlichen Grundlagen sowie der Entwurf eines neuen gesetzlichen Regelungsrahmens für elektronische Wahlen mit Wahldiensteanbieter.

Im Einzelnen sollte dazu ein Wahldiensteanbieterkonzept erarbeitet und in exemplarischer Weise rechtlich am Beispiel von Betriebsratswahlen umgesetzt werden. Hierzu wurden verfassungs- und europarechtlichen Vorfragen behandelt, ein

Regelungskonzept erarbeitet und der Entwurf für ein Wahldiensteanbietergesetz einschließlich einer konkretisierenden Verordnung erstellt. Im weiteren Verlauf des Projekts arbeitete die Technische Universität Darmstadt hier eng mit der Universität Kassel zusammen, um insbesondere bei der Entwicklung der zum Wahldiensteanbietergesetz zugehörigen Verordnung technische Beratung zu leisten. Weiterhin wurde der Universität Kassel ein Entwurf zur Anpassung des Betriebsverfassungsgesetzes und der ersten Wahlordnung zum Betriebsverfassungsgesetz entwickelt und so die Umsetzbarkeit des Wahldiensteanbieterkonzeptes demonstriert. Weitere Fragen im Zusammenhang mit der Einführung von Gremienwahlen (wie das einfache Wahlverfahren nach dem Mehrheitswahlrecht; Delegiertenwahl nach dem Mitbestimmungsrecht, Sozialwahlen) wurden ergänzend betrachtet. Ein eigener Projektbericht der Universität Kassel befindet sich im Anhang.

Speziell für die Arbeit an der Verordnung zum Wahldiensteanbietergesetz wurde zur weiteren Unterstützung Herr Weinand vom BSI hinzugezogen. Auch diese Zusammenarbeit verlief sehr gut.

# 2 Eingehende Darstellung

## 2.1 Verwendung der Zuwendung und erzieltes Ergebnis

Im Folgenden werden die Arbeitspakete des Teilvorhabens Sicherheitsanalyse beschrieben, für dessen Bearbeitung die Zuwendung durch die Technische Universität Darmstadt empfangen wurde.

### AP 1.2.1.1: Identifikation der Player, Sicherheitsannahmen und Sicherheitsziele (4PM)

Gegenstand dieses Arbeitspaketes war die Klärung der Sicherheitsziele und Sicherheitsannahmen für voteremote. Insbesondere wurden Annahmen über die Sicherheit der verwendeten Wahlclients und Netzwerke formuliert. Die Sicherheitsannahmen wurden so formuliert, dass sie – auch mit Hilfe von nicht-technischen Maßnahmen wie Sozialkontrolle – nachweislich realisiert werden können. Ausgangspunkt für die Klärung der Sicherheitsziele war hierbei die Anforderungsanalyse. Die Sicherheitsziele entsprachen denjenigen, die im Allgemeinen für elektronische Wahlsysteme gefordert werden und die wir bereits in Abschnitt 1.4 beschrieben haben. Die Player des Wahlprotokolls sind der Wähler, der Bestätiger, das schwarze Brett (Bulletin Board), das Mix Net sowie der Auszähler. Die Sicherheitsannahmen sind folgende:

- Es steht eine vertrauenswürdige Public–Key–Infrastruktur (PKI) zur Verfügung und wird eingesetzt. Alle benutzten öffentlichen Schlüssel sind validiert. Eine Zertifizierungsstelle gibt entsprechende PKI–Zertifikate heraus. Das impliziert, dass alle Verschlüsselungen mit den richtigen öffentlichen Schlüsseln gemacht werden. Alle Parteien nehmen an der PKI teil. Die eingesetzte Kryptographie ist stark und praktisch nicht zu brechen.
- Zur Kommunikation wird ein Protokoll wie z.B. TCP/IP benutzt, welches das Ankommen der Nachrichten sicherstellt. Wir nehmen außerdem an, dass die Kommunikation durch ein Protokoll wie z.B. PKI–basiertes TLS [DA81] geschützt wird, welches die gegenseitige Authentisierung der Parteien und die Geheimhaltung der Kommunikation garantiert.
- Die Registrierungsphase verläuft korrekt.
- Der Wähler wird bei der Stimmabgabe nicht beobachtet und gibt seine Stimme insbesondere nicht unter Zwang ab.
- Bei der Stimmabgabe wird das Votum vom Endgerät des Wählers nicht verändert. Es wird genau das Votum erstellt, welches der jeweilige Wähler abgeben will.

- Der Wähler kann kein ungültiges Votum (d.h. falsche Struktur, ungültige Signatur, fehlerhafte Verschlüsselung) erzeugen. Er hat jedoch die Möglichkeit, sich aktiv von der Wahl zu enthalten, z.B. durch eine entsprechende Option auf dem Wahlzettel.
- Weder der Wähler noch irgendeine andere Partei hat die Möglichkeit, den zum Blenden des Votums benutzten Faktor zu sehen oder zu speichern. Der Wähler hat außerdem nicht die Möglichkeit, sein abgegebenes Votum unverschlüsselt auf seinem Endgerät zu speichern.
- Dem Wähler wird das für ihn auf dem schwarzen Brett veröffentlichte Votum innerhalb des Wahlvorgangs angezeigt.
- Dem schwarzen Brett wird wie folgt vertraut:
  - Es authentisiert die Abonnenten korrekt und autorisiert den Zugriff gemäß ihrer Rolle.
  - Es kann die Veröffentlichung von Informationen durch autorisierte Parteien nicht verweigern.
  - Es kann keine Informationen verändern oder löschen.
  - Es konspiriert nicht mit anderen Parteien.
- Das Mix–Net ist vertrauenswürdig in folgendem Sinne:
  - Es mischt korrekt.
  - Es gibt seinen privaten Schlüssel oder die benutzte Permutation nicht preis.
  - Es fügt keine Voti hinzu, tauscht diese aus oder verändert sie.
  - Es konspiriert nicht mit anderen Parteien.
- Die vertrauenswürdigen Parteien sind also:
  - Schwarzes Brett
  - Mix–Net
- Nicht notwendig vertrauenswürdig sind:
  - Wähler
  - Bestätiger
  - Auszähler

- Ein gültiges Votum ist eines, das
  - die korrekte Form hat,
  - vom Bestätiger signiert ist,
  - mit dem öffentlichen Schlüssel des Auszählers und des Mix–Netes in der korrekten Reihenfolge verschlüsselt ist und
  - auf dem schwarzen Brett veröffentlicht ist.

### AP 1.2.1.2: Analyse Vorhandener Remotewahlprotokolle und Wahlklienten (4PM)

In diesem Arbeitspaket wurden existierende Remotewahlprotokolle und Wahlklienten analysiert. Es wurde untersucht, welche Elemente dieser Protokolle und Klienten in Hinblick auf die im Arbeitspaket 1.2.1.1 gefundenen Sicherheitsziele für das Projekt voteremote verwendet werden können und ob gegebenenfalls Elemente neu spezifiziert werden müssen. Besondere Beachtung wurde den verwendeten kryptographischen Primitiven und den darin verwendeten Parametern gewidmet.

Tabelle 1 fasst unsere Ergebnisse zusammen. Sie beinhaltet organisatorische und technische Sicherheitsanforderungen verschiedener Wahlprotokolle und geeignete Maßnahmen. Kategorisiert wurde nach verschiedenen Familien von Anforderungen:

**Trusted components (Tr_Comp)** Vertrauenswürdige Komponenten

**Trusted communication (Tr_Comm)** Vertrauenswürdige Kommunikation

**Trusted storage and erasure (Tr_SE)** Vertrauenswürdiges Speichern und Löschen

**Trusted application of cryptography (Tr_AC)** Vertrauenswürdige Anwendung kryptographischer Verfahren

**Miscellaneous (Tr_Misc)** Verschiedenes

### AP 1.2.1.3: Entwicklung, Optimierung und Implementierung der notwendigen kryptographischen Primitive (18PM)

In dieser Phase wurden geeignete kryptographische Primitive spezifiziert und zum Teil auch Implementierungen der Primitive bereitgestellt. Konkret ging es dabei um digitale Signaturen, blinde Signaturverfahren, Bulletin Boards und Anonymisierungsmechanismen wie Mix Nets sowie sichere Kommunikationsprotokolle:

| **Requirement** | **Family** | **Protocol** | **Measures** |
|---|---|---|---|
| trustworthy administrator, trustworthy registration authority | Tr_Comp | [OMA+99], [LK02], [JCJ05] | legally binding contracts, non-disclosure agreements, dual-control |
| trustworthy time stamp server | Tr_Comp | [BFP+01] | secure operation, monitoring, partitioning-off |
| prevention of malicious collusion | Tr_Comp | [OMA+99] | logical or physical separation, restricted communication capabilities |
| anonymous channel | Tr_Comm | [OMA+99], [JCJ05] | secure mix net |
| untappable channel | Tr_Comm | [JCJ05] | physical separation, data exchange via read-only media, postal service |
| secure storage of private keys (server-side) | Tr_SE | [OMA+99], [JCJ05] | safety areas, physical access control, surveillance, reliable storage media |
| secure storage of blinding factor (client-side) | Tr_SE | [OMA+99], [BFP+01] | secure software design, tamper-resistant hardware |
| erasure of private credential share | Tr_SE | [JCJ05] | secure software design, file shredding |
| PKI | Tr_AC | [OMA+99], [BFP+01], [LK02], [JCJ05] | X.509 certificates, smartcards (e.g. electronic citizen cards), secure communication channels, secure hardware |
| delivery of voting equipment | Tr_Misc | [BFP+01], [LK02], [JCJ05] | electronic items are delivered via confidential and authenticated channel (TLS) or secured e-mail (S/MIME), hardware equipment requires logistics solution |

Tabelle 1: Security requirements and measures to satisfy them

**Blinde Signaturen** Dieses Verfahren stellt sicher, dass eine Nachricht signiert werden kann, ohne dabei jedoch lesbar zu sein (siehe [Cha82]). Zur Veranschaulichung kann man sich folgendes Szenario vorstellen: Der Empfänger deckt das zu unterschreibende Blatt mit Kohlepapier ab, steckt dieses in einen Briefumschlag und schickt diesen zum Signierer. Der Signierer unterschreibt den Briefumschlag und schickt ihn zurück an den Empfänger. Der Empfänger öffnet den Briefumschlag und entnimmt sein unterschriebenes Blatt. Erhält der Signierer das Blatt zu einem späteren Zeitpunkt, so kann er keine Aussage darüber treffen, wem er das Blatt unterschrieben hat. Blinde Signaturen werden im entwickelten Wahlsystem eingesetzt, um ein Votum durch Signatur des Validators als gültig (d.h. von einer wahlberechtigten Person abgegeben) zu bestätigen, ohne dabei jedoch den Inhalt des Votums einsehbar zu machen. Auf diese Weise bleibt das Wahlgeheimnis gewahrt. Durch die Blendung wird der Inhalt des Votums vom Wähler für den Validator unkenntlich gemacht, er kann dann lediglich die Wahlberechtigung des Wählers überprüfen. Die Blendung kann ausschließlich vom Wähler rückgängig gemacht werden.

**Bulletin Board** Es existiert ein öffentliches schwarzes Brett (Bulletin Board). Jeder kann die dort veröffentlichten Nachrichten lesen, aber nur autorisierte Parteien können Nachrichten dort ablegen. Weiterhin kann niemand einmal geschriebene Nachrichten löschen oder überschreiben.

**Mix Net** Ein Mix Net [Cha81] ist eine der Maßnahmen, die die Anonymität der Wahl gewährleisten. Es stellt sicher, dass die von den Wählern ausgehenden Nachrichten nicht mit denjenigen in Verbindung gebracht werden, die auf dem Bulletin Board eintreffen. Dies geschieht, indem eine Menge von Nachrichten empfangen und in randomisierter Reihenfolge weitergesendet wird.

**Public-Key Infrastruktur** Das Wahlsystem baut auf einer vertrauenswürdigen Public-Key-Infrastruktur (PKI) auf. Jede Instanz (Wähler, Validator, Mix Net, Auszähler) besitzt einen öffentlichen sowie einen privaten Schlüssel, wobei letzterer nur dem Besitzer bekannt ist. Alle benutzten öffentlichen Schlüssel sind durch ein Zertifikat an die Identität des Besitzers gebunden. Die Zertifikate werden von einer vertrauenswürdigen Instanz (dem Wahldiensteanbieter oder einem unabhängigen Betreiber einer PKI) ausgestellt.

**Sichere Kommunikation** Zur sicheren Kommunikation wird ein Protokoll wie z.B. TCP/IP benutzt, welches das Ankommen der Nachrichten sicherstellt. Wir nehmen außerdem an, dass die Kommunikation durch ein Protokoll wie z.B. PKI-

basiertes TLS geschützt wird, welches die gegenseitige Authentisierung der Parteien und die Geheimhaltung der Kommunikation garantiert.

Die Implementierung erfolgte in Form einer Erweiterung der bestehenden Kryptographie-Bibliothek FlexiProvider, welche ebenfalls an der Technischen Universität entwickelt worden ist. Implementiert wurde ein blindes Signaturverfahren auf der Basis von RSA. Für alle Verschlüsselungsverfahren des FlexiProviders aus den Providern FlexiCore, FlexiEC und FlexiPQC wurden außerdem Methoden für das Wrappen und Unwrappen von Schlüsseln beliebiger kryptographischer Verfahren eingebaut. Man spricht auch von umhüllen oder Wrappen, wenn man einen Schlüssel mit einem anderen Schlüssel chiffriert. Dies ist nötig, um beispielsweise geheime Schlüssel auch wirklich geheim zu halten. In diesem Zusammenhang wurden in den beiden Klassen `de.flexiprovider.common.api.AsymmetricCipherSpi` und `de.flexiprovider.common.api.BlockCipherSpi` die beiden Methoden `engineWrap()` und `engineUnwrap()` implementiert. Für die ausführliche Beschreibung der Implementierung verweisen wir an dieser Stelle auf die Seite `www.flexiprovider.de`, die sämtliche Dokumentationen in ihrem entsprechenden Kontext enthält, einschließlich der im Vorhaben implementierten Primitive.

### AP 1.2.1.4: Mitwirkung beim Entwurf des Wahlverfahrens (6PM)

Der Prototyp von voteremote wurde in Kooperation mit den anderen Projektteilnehmern spezifiziert. Nach Möglichkeit wurden Standardverfahren wie TLS und IPsec vorgesehen. Die Spezifikation umfasste die Initialisierungsphase, die Registrierungsphase, die Wahlphase und die Auszählphase.

Der folgende Abschnitt gibt einen Einblick in die Spezifikation des entwickelten Wahlsystems. Die Gliederung erfolgte entsprechend der einzelnen Phasen während des Ablaufs einer Wahl.

**Vorbereitungsphase.** Vor Beginn der Wahl wird ein Wählerverzeichnis T_Wähler angelegt, welches je nach Maßgabe der jeweiligen Wahlordnung veröffentlicht wird. Das Wählerverzeichnis liegt in elektronischer Form auf dem Bulletin Board. Es enthält für jeden Wahlberechtigten dessen Daten (Name, Adresse, digitales Zertifikat) sowie eine eindeutige Identifikationsnummer. Das Wählerverzeichnis ist vom Wahlvorstand signiert und damit authentisch sowie vor unberechtigter Veränderung geschützt. Vor Beginn der Wahl wird die Liste aller gültigen Wählerzertifikate schreibgeschützt an den Validator übertragen. Weiterhin existiert eine Liste T_Votum, in der während der Wahl unter der jeweiligen Identifikationsnummer des Wählers seine abgegebene Stimme verschlüsselt gespeichert wird. Die Kommunikation zwischen Wähler und Wahlsystem erfolgt über das Internet unter Verwendung des TLS-Verschlüsselungsprotokolls. Es bietet Identifikation und Authentifizie-

rung der Kommunikationspartner sowie Vertraulichkeit, Integrität und Authentizität der übermittelten Nachrichten. Weiterhin werden asymmetrische Verschlüsselungsverfahren eingesetzt, d.h. jede Einheit (wie Wähler, Mix Net, Auszähler) besitzt einen öffentlichen Schlüssel zum Verschlüsseln sowie einen privaten Schlüssel zum Entschlüsseln.

**Wahlphase.** Der Wähler initiiert eine TLS-Verbindung zum Wahlserver, um den Stimmzettel anzufordern. Dazu authentifiziert er sich mittels seines Zertifikats beim Wahlserver. Der Wahlserver überprüft die Wahlberechtigung des Wählers an Hand des Wählerverzeichnisses T_Wähler. Ist der Wähler nicht wahlberechtigt, befindet sich sein Zertifikat nicht in diesem Verzeichnis und die Anfrage zur Aushändigung des Stimmzettels wird abgelehnt. Dem Wähler wird dies durch eine entsprechende Fehlermitteilung angezeigt. Ist der Wähler dagegen wahlberechtigt, wird als nächstes an Hand der Identifikationsnummer des Wählers in der Liste T_Votum überprüft, ob er bereits eine Stimme abgegeben hat. Ist dies der Fall, so wird die Anfrage ebenfalls abgelehnt und der Wähler erhält den Hinweis, er habe bereits gewählt. Sofern der Wähler wahlberechtigt ist und noch kein Votum abgegeben hat, erhält er den Wahlzettel. Diesen füllt er aus und sendet ihn geblendet (d.h. ohne dass der Inhalt einsehbar ist) und signiert an den Validator. Der Validator prüft an Hand des Zertifikats des Wählers nochmals dessen Wahlberechtigung in seinem lokalen Auszug des Wählerverzeichnisses und verifiziert zusätzlich die Signatur des Wählers. Bei positiver Überprüfung trennt der Validator zunächst die Signatur des Wählers ab, um die Verbindung zum Wähler zu entfernen, und signiert das geblendete Votum anschließend selbst. Die Signatur des Validators zeichnet bis zum Ende der Wahl eine gültige, d.h. berechtigt und korrekt abgegebene Stimme aus. Der Validator schickt den von ihm blind signierten Stimmzettel an den Wähler zurück. Dieser überprüft die Signatur des Validators, entblendet des Stimmzettel und verschlüsselt ihn anschließend erst mit dem öffentlichen Schlüssel des Auszählers und hiernach mit dem öffentlichen Schlüssel des Mix Nets. Das doppelt chiffrierte Votum sendet der Wähler anschließend an den Wahlserver. Dieser erkennt die Identität des Wählers im Rahmen der TLS-Verbindung wieder an dessen Zertifikat, ermittelt aus der Liste T_Wähler die Identifikationsnummer des Wählers und legt das Votum schreibgeschützt unter dieser Nummer in der Liste T_Votum auf dem Bulletin Board ab. Die Konfiguration der Datenbank erlaubt darüber hinaus nicht, dass Einträge der Datenbanktabelle T_Votum gelöscht oder überschrieben werden oder dass ein Zwischenstand der Wahl abgerufen werden kann.

Sobald die Frist für die Stimmabgabe verstrichen ist, initiiert der Wahlvorstand das Mixen der Voten. Dabei werden die Stimmen so umgeordnet, dass

kein Zusammenhang zwischen Wähler und Votum hergestellt werden kann, insbesondere im Hinblick darauf, in welcher Reihenfolge die Stimmen abgegeben wurden. Aus der Liste T_Votum auf dem Bulletin Board holt das Mix Net die doppelt verschlüsselten Stimmen, und zwar nur diese ohne die Identifikationsnummern der Wähler. Das Mix Net entfernt die äußere Verschlüsselung der Stimmen. Nach diesem Vorgang sind die Stimmen noch immer mit dem Schlüssel des Auszählers verschlüsselt und damit vom Mix Net im Klartext nicht einsehbar. Das Mix Net mischt die Stimmen und legt sie danach wieder auf dem Bulletin Board ab. Die Liste der einfach verschlüsselten Stimmen ist schreibgeschützt und zu diesem Zeitpunkt nur vom Wahladministrator lesbar.

**Auszählphase.** Im nächsten Schritt initiiert der Wahlvorstand die Stimmauszählung. Der Auszähler holt die einfach verschlüsselten Stimmen vom Bulletin Board, entschlüsselt sie mit seinem privaten Schlüssel und prüft jeweils die Signatur des Validators. Dann berechnet er das Wahlergebnis. Dieses wird gemeinsam mit den offenen (d.h. unverschlüsselten) Stimmen sowie dem privaten Schlüssel des Auszählers auf dem Bulletin Board veröffentlicht. Der Bereich der einfach verschlüsselten Voten ist nun auch für die Öffentlichkeit zum Lesen freigegeben. Durch Entschlüsseln der einfach verschlüsselten Voten mit Hilfe des veröffentlichten privaten Auszählerschlüssels und anschließender Auszählung ist die Öffentlichkeit somit in der Lage, das Ergebnis der Stimmauszählung zu verifizieren.

### AP 1.2.1.5: Semiformale Spezifikation des Wahlverfahrens (8PM)

Innerhalb dieses Arbeitspaketes sollte das Wahlsystem ausgehend vom Entwurf an Hand semiformaler Verfahren spezifiziert werden: Mit Hilfe graphisch-formaler Beschreibungsformen wurden die ablaufenden Prozesse modelliert. Dabei soll sichergestellt werden, dass die Spezifikation durchgängig die gefundenen Sicherheitsziele berücksichtigt. Diese Spezifikation lieferte anschließend die Grundlage für eine korrekte Implementierung. Darüber hinaus diente sie dem Zweck, entsprechende Anforderungen, die im Rahmen der späteren Zertifizierung des Wahlverfahrens gestellt würden, zu erfüllen.

Im Folgenden beschreiben wir das spezifizierte Wahlprotokoll. Es verwendet folgende Notation:

| | |
|---|---|
| $E_L(m)$ | Verschlüsselung der Nachricht $m$ mit dem öffentlichen Schlüssel von $L$ |
| $S_T(m)$ | Signatur über die Nachricht $m$ mit dem privaten Schlüssel von $T$ |
| $B(m,r)$ | Funktion zum Blenden der Nachricht $m$ mit einer Zufallszahl $r$ |
| $UB(m,r)$ | Funktion zum Entblenden der Nachricht $m$, die mit $r$ geblendet wurde |
| $v$ | ein ausgefüllter Wahlzettel, auch Votum genannt |

### Wahlphase

Abbildung 1 zeigt die Wahlphase des Protokolls. Diese wird im folgenden Abschnitt genauer erläutert.

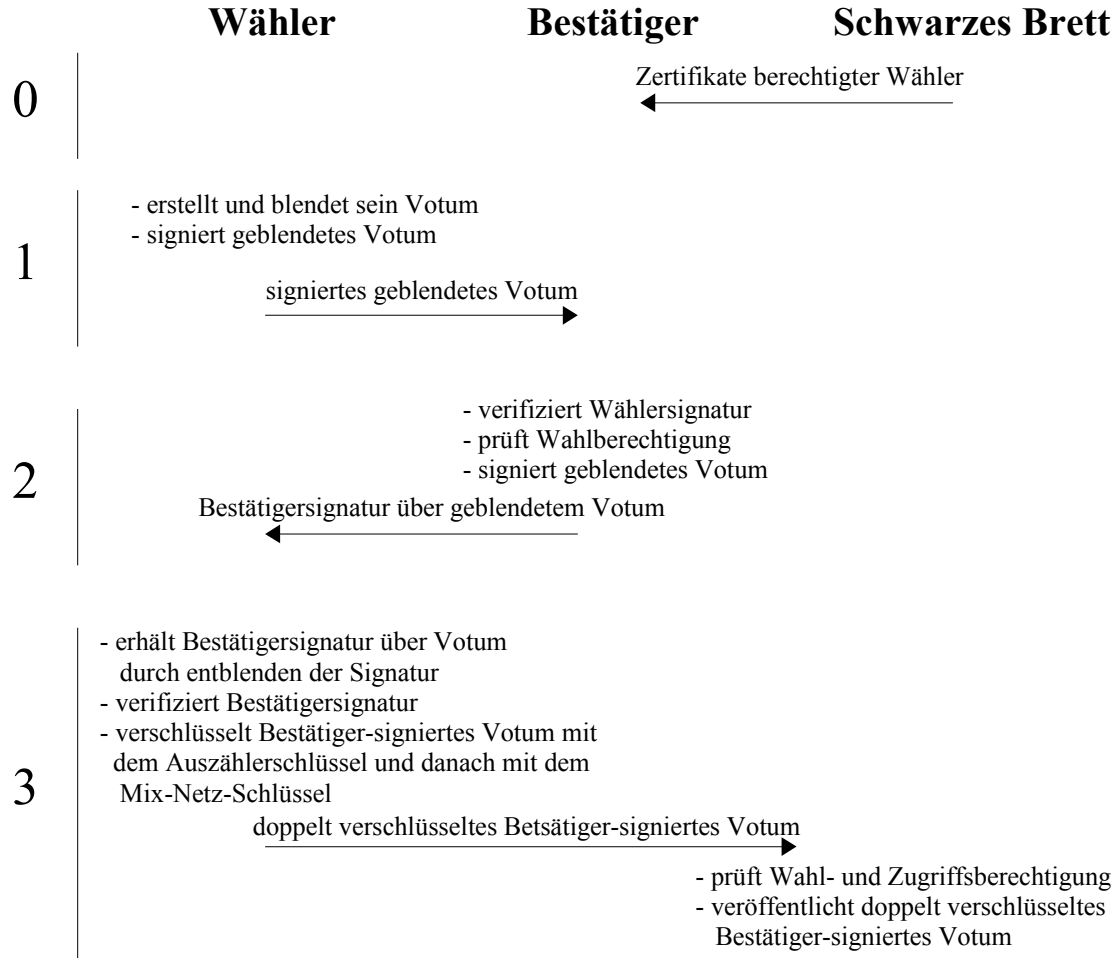


Abbildung 1: Die Wahlphase

**Stufe 0** Der Bestätiger holt die Liste der Zertifikate der berechtigten Wähler vom schwarzen Brett. Dies wird einmalig zu Beginn der Wahlphase gemacht.

Die folgenden Schritte 1-3 werden für jeden Wähler wiederholt.

**Stufe 1** Der Wähler fordert den Stimmzettel an und authentifiziert sich dazu mittels seines Zertifikats. Er erhält nur dann einen Stimmzettel, wenn er wahlberechtigt ist und noch keine Stimme abgegeben hat. Der Wähler generiert daraufhin sein Votum $v$. Dazu wird eine Zufallszahl $r$ erzeugt, mit welcher das Votum geblendet wird; d.h. es wird $x = B(v, r)$ berechnet. Dann wird $x$ vom Wähler signiert, und als $(x, S_{WAH}(x))$ zum Bestätiger geschickt.

**Stufe 2** Der Bestätiger verifiziert die Signatur des Wählers und prüft dessen Wahlberechtigung an Hand des Zertifikats. Dann signiert der Bestätiger $x$, also den geblendeten Stimmzettel ohne die Signatur des Wählers, und sendet $S_{BES}(x)$ zurück zum Wähler.

**Stufe 3** Nachdem der Wähler $S_{BES}(x)$ erhalten hat, entfernt er den Blendfaktor $r$ und erhält somit die Bestätigersignatur $S_{BES}(v)$, welche er anschließend verifiziert. Ist diese korrekt, so wird das Votum $v$ zusammen mit der Bestätigersignatur $S_{BES}(v)$ mit dem öffentlichen Schlüssel des Auszählers verschlüsselt, es wird also $E_{AUS}(v, S_{BES}(v))$ berechnet. Dann wird das Ergebnis mit dem öffentlichen Schlüssel des Mix–Netes verschlüsselt und das Ergebnis $E_{MIX}(E_{AUS}(v, S_{BES}(v))$ wird dem Wähler angezeigt. Wenn der Wähler berechtigt ist und noch kein Votum abgegeben hat, erlaubt das schwarze Brett ihm, $E_{MIX}(E_{AUS}(v, S_{BES}(v))$ zu veröffentlichen.

### Auszählphase

Abbildung 2 illustriert die Auszählphase des Protokolls, welche in diesem Abschnitt näher erklärt wird.

**Stufe 4** Nach der Wahlphase holt sich das Mix–Net die doppelt verschlüsselten Voti vom schwarzen Brett.

**Stufe 5** Das Mix–Net entfernt die äußere Verschlüsselung der Voti mit seinem privaten Schlüssel. Dann mischt es sie und sendet die neue Liste zurück zum schwarzen Brett. Zu diesem Zeitpunkt sind die Voti noch immer mit dem Auszählerschlüssel verschlüsselt.

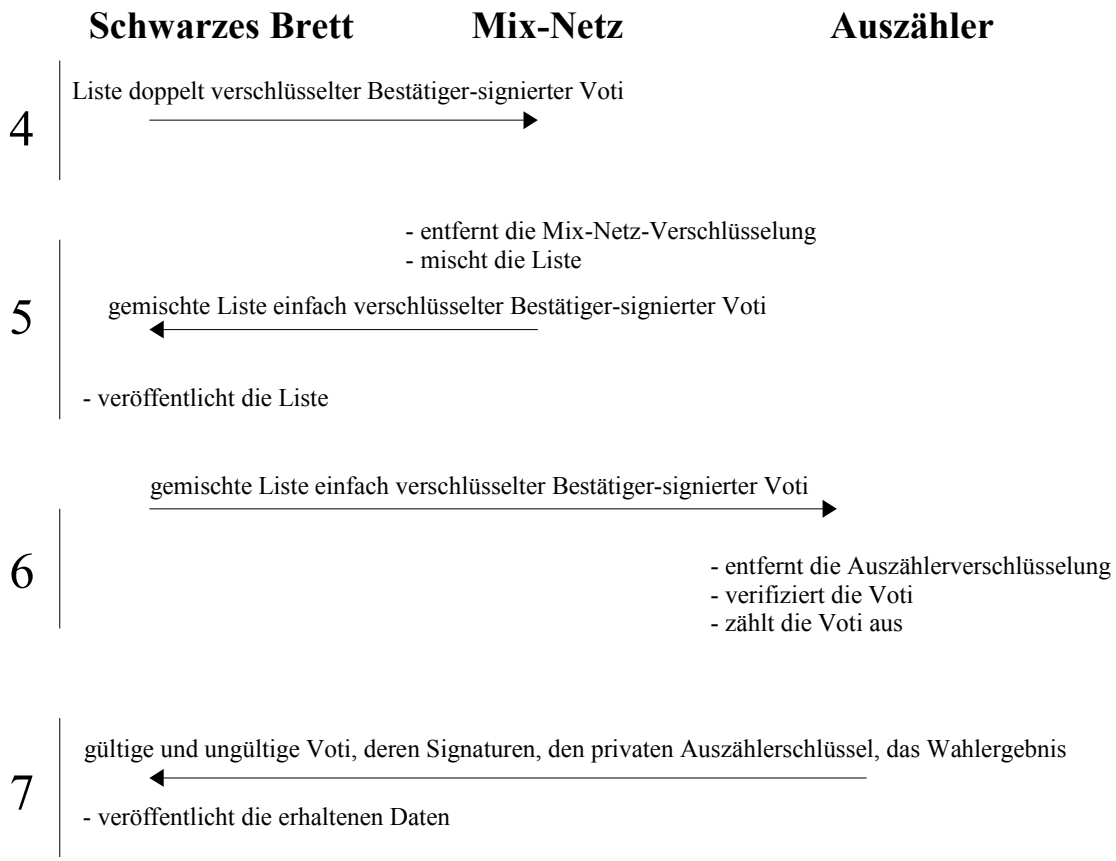


Abbildung 2: Die Auszählphase.

**Stufe 6** Der Auszähler holt sich die neue Liste vom schwarzen Brett und entschlüsselt die Voti. Er verifiziert die Bestätigersignaturen über den Voti und berechnet anschließend das Wahlergebnis.

**Stufe 7** Schließlich veröffentlicht der Auszähler alle Voti inklusiver ihrer Signaturen auf dem schwarzen Brett. Dort veröffentlicht er weiterhin seinen privaten Schlüssel und das Wahlergebnis.

### AP 1.2.1.6: Mitwirkung bei der Implementierung des Wahlverfahrens (6PM)

Dieses Arbeitspaket beinhaltete die Mitarbeit an der Implementierung des Wahlverfahrens. Diese umfasst die Realisierung aller Komponenten des Wahlprotokolls. Hierfür bildeten Entwurf und Spezifikation des Verfahrens die Grundlage. Gleichzeitig sollte die Implementierung sich an den definierten Sicherheitsanforderungen orientieren. Die Tätigkeit seitens der Technischen Universität Darmstadt belief sich dabei hauptsächlich auf Beratung der Entwickler beim Kooperationspartner T-Systems hinsichtlich der Umsetzung der Spezifikation und der Erfüllung der Sicherheitsanforderungen. Das Arbeitspaket wurde damit innerhalb der Laufzeit des Vorhabens erfolgreich abgeschlossen. Im Folgenden werden die zentralen Fragestellungen aufgeführt, bei welchen die Technische Universität Darmstadt im Rahmen des Vorhabens beratend tätig war.

#### A) Beratung zur Implementierung des Wahlprotokolls

**Warum wird die Wahlberechtigung laut Wahlprotokoll zweimal überprüft (durch Bestätiger und Voteserver)?** Die Wahlberechtigung wird bereits bei Anforderung des Stimmzettels überprüft. Jemand, der nicht im Wählerverzeichnis gespeichert ist, kann den Stimmzettel zur Wahl nicht erhalten, da seine Identität aufgrund des fehlenden Wählerzertifikates im Wählerverzeichnis unbekannt ist. Das Gleiche gilt für die Verbindung vom Wähler zum Bestätiger. Dieser erstellt keine blinde Signatur auf ein Votum, sofern die Identität des Wählers unbekannt ist, d.h. das Wählerzertifikat des Wahlberechtigten nicht in der Zertifikatsliste des Bestätigers vorliegt. Die Signatur des Bestätigers zeichnet eine gültige Stimme (im Sinne von korrekt abgegeben und nicht von irgendjemandem „untergeschoben“ oder manipuliert) aus und kann bis zum letzten Schritt (d.h. nach der Auszählung) verifiziert werden. Der Bestätiger ist außerdem ein verbreitetes Konzept im Hinblick auf das Vier-Augen-Prinzip: Er stellt eine zusätzliche Absicherung dar. Dies setzt aber eine entsprechende Rollentrennung voraus und wird ggf. hinfällig, wenn wie bei unserem Protokoll eine weitere Identitätsprüfung beim Voteserver stattfindet. Das Konzept würde im Prinzip auch ohne den Bestätiger funktionieren. Jedoch

ist die Gefahr der Manipulation des Voteservers höher. Der Bestätiger dient als zusätzliche Instanz um sicherzustellen, dass der Voteserver nicht manipuliert (z.B. Stimmen hinzufügt etc.).

**Wie wird die Rollentrennung zwischen Voteserver, Bestätiger und Mixnet sichergestellt?** Dies kann letztendlich nur durch eine logische Trennung der Komponenten erfolgen und liegt in der Verantwortung der Systemarchitektur des Systems. Sichergestellt muss sein, dass der Voteserver und der Bestätiger nicht zusammenarbeiten können.

**Was bedeutet bei der Auszählung „ungültige Stimme“? Technisch ungültig, weil z.B. die Wahlberechtigung nicht verifiziert werden konnte, oder inhaltlich ungültig, d.h. dass ungültig gewählt wurde?** Letzteres, da „technisch ungültig“ gar nicht möglich ist (laut Protokoll bzw. Software). Technisch ungültige Stimmen würden durch eine ungültige Signatur auffallen. Ein anderer Fall ist ausgeschlossen. Sofern die Nachricht intakt ist, lässt sie sich entschlüsseln. Sofern die Bestätigersignatur über das Votum gültig ist, ist das Votum (technisch gesehen) gültig.

**Für wen sind die einfach (d.h. nur mit dem Auszähler-Schlüssel) chiffrierten Stimmen auf dem Bulletin Board sichtbar?** Durch Entschlüsseln dieser Stimmen mit dem privaten Auszähler-Schlüssel, der am Schluss veröffentlicht wird, kann man sich von der korrekten Auszählung der Stimmen überzeugen. Die Sichtbarkeit des Datensatzes der einfach verschlüsselten Stimmen hängt also davon ab, wer alles in der Lage sein soll, die Auszählung zu verifizieren. Soll dies beispielsweise jedem Wähler möglich sein, so muss sichergestellt werden, dass die einfach verschlüsselte Stimme bei ihrer Erzeugung nicht ausgelesen werden kann, da man sonst einem Angreifer beweisen könnte, wie man gewählt hat. Denkbar wäre auch, den Datensatz der einfach verschlüsselten Stimmen nur für den Wahlvorstand einsehbar zu machen. Der Zugriff auf Datensätze des Schwarzen Brettes ist durch ein Rollen und Berechtigungskonzept geregelt. Hierin wird letztendlich gesteuert, wer zu welchem Zeitpunkt welche Daten lesen und/oder schreiben darf. Der Ansatz dieses Konzeptes ist außerst restriktiv, was bedeutet, dass nur sehr wenige Instanzen Daten auf das Schwarze Brett schreiben dürfen und dies auch noch in Abhänigkeit der jeweiligen Phase. Daten dürfen darüber hinaus nicht überschrieben oder gelöscht werden (für denn Fall, das Voten überschrieben werden dürfen - multiple cast). Demnach gibt es auch eine entsprechende Regelung für den lesenden zugriff auf die einfach verschlüsselten Voten. Diese sind nach dem Vorgang des Mixens (d.h. hier liegen die einfach verschlüsselten Voten das erste mal tatsächlich erst vor) zunächst nur über das Wahladministrationsprogramm

(Wahlvorstand) lesbar. Schreibenden Zugriff auf diese Tabelle hat wie gesagt nur der Mixer und auch nur in der Phase des Mixens. Nach dem Mixen ist diese Tabelle schreibgeschützt. Nachdem über die Wahladministration das Ergebnis ermittelt wurde (Entschlüsslung der Stimmen und Auszählung) und das Ergebnis nebst Auszählerschlüssel veröffentlicht wurde, kann der Bereich der einfach verschlüsselten Voten lesend für die Öffentlichkeit über eine separate Schnittstelle freigegeben werden.

**Ist die Verwendung der „multiple casting“ Technik im Protokoll sinnvoll?** Nein, das ist im Hinblick auf den geplanten Rahmen (Betriebs- und Sozialwahlen) nicht nötig.

**B) Beratung im Bereich der Technik**

**Bei welchem Schritt wird der Status des Wählers (hat gewählt bzw. hat nicht gewählt) geprüft? Wer kann diesen prüfen (Bestätiger oder Voteserver oder auch der Wähler selbst) und wie geschieht dies?** Der Ablauf ist folgender: Der Wähler initiiert über das Client-Applet eine authentische verschlüsselte TLS-Verbindung zum Voteserver. Für die client-seitige Authentisierung wird dabei das Zertifikat des Wählers verwendet, damit authentifiziert sich der Wähler gegenüber dem Voteserver. Dieser prüft an Hand der Wählerliste, ob der Wähler wahlberechtigt ist (in der Wählerliste ist neben der Identität des Wählers auch sein öffentliches Zertifikat abgelegt). Wenn ja, wird das Zertifikat akzeptiert und die Verbindung zugelassen. Somit kann die Verbindung nur bei bestehender Wahlberechtigung aufgebaut werden. Im positiven Fall prüft der Voteserver als nächstes den Wahlstatus. Hat der Wähler noch keine Stimme abgegeben, schickt ihm der Voteserver einen leeren Stimmzettel. Hat der Wähler bereits eine Stimme abgegeben, erhält er keinen neuen Stimmzettel und eine entsprechende Meldung. Der Wähler füllt nun den Stimmzettel aus und baut erneut eine TLS-Verbindung zum Bestätiger auf. Der Bestätiger selbst hat eine identische Liste mit Wählerzertifikaten, welche vor dem Starten der Wahl vom Bulletin Board auf den Bestätiger übertragen wird. Die Liste ist auf dem Bestätiger selbst als auch auf dem Bulletin Board mit dem Starten der Wahl schreibgeschützt. Der Bestätiger prüft bei einer Verbindungsanfrage eines Voteclienten erneut die Wahlberechtigung des Wählers über das Vorhandensein des entsprechenden Wählerzertifikates in der Liste von Zertifikaten. Im positiven Fall schickt der Wähler seinen Stimmzettel geblendet an den Bestätiger, der diesen signiert und zurück schickt. Kurz: Der Wahlstatus wir bei der Anmeldung des Wählers am Voteserver zur Wahl (Erlangung des Stimmzettels) geprüft. Nur dieser ist in der Lage den Wahlstatus des Wählers zu ermitteln. Der Bestätiger hat keinen Zugriff auf das Bulletin Board

und kann somit den Wahlstatus des Wählers nicht prüfen. Der Wähler kann seinen Wahlstatus prüfen, indem er einfach eine neue Verbindung zum Voteserver herstellt. Hat er noch nicht gewählt, erhält er einen Stimmzettel, hat er bereits gewählt, enthält er keinen Stimmzettel und eine entsprechende Meldung.

Der Wahlstatus wird technisch überprüft, indem in der Datenbank nach dem entsprechenden Eintrag der verschlüsselten Stimme mit passender Identität (ID) des Wählers gesucht wird.

**Wie wird die Identität des Wählers geprüft, wenn er seine Stimme an den Voteserver schickt?** Dies geschieht nur an Hand der TLS-Authentifikation. Die TLS-Verbindung verwendet client-seitig das Wählerzertifkat zur Authenfizierung. Somit ist eine Ende-zu-Ende-Sicherheit gewährleistet.

**Wäre eine Personalisierung durch Wählersignaturen hier besser?** Nein, da durch die Wählersignaturen eine unerwünschte Personalisierung der Stimmen geschaffen wird, die im Anschluss wieder entfernt werden muss, was unnötig kompliziert ist.

**Wie genau sehen die personalisierten Stimmen aus?** Die Stimmen sind verschlüsselt mit den Schlüsseln des Auszählers und des Mixnets, sie sind nicht vom Wähler signiert, aber vom Bestätiger. Der Voteserver erkennt die Identität des Wählers an Hand der authentischen TLS-Verbindung. Jeder Identität ist in der Wählerliste eine ID-Nummer eindeutig zugeordnet. Der Voteserver speichert die doppelt verschlüsselte Stimme des Wählers zusammen mit dessen ID-Nummer in einer Tabelle. (Die ID wird dabei aus der Wählerliste geholt.) Dadurch gibt es nur einen einzigen Schreibvorgang pro Wähler (für Stimme und Identität), wodurch Recovery-Probleme vermieden werden. Es gibt also am Ende eine Tabelle, in der in jeder Zeile eine ID-Nummer und die zugehörige Stimme stehen. Diese Tabelle wird vom Voteserver signiert.

**Ist der Datensatz der personalisierten Stimmen sicher genug (Zugriffsrechte, Fälschbarkeit)?** Der Wähler muss dem Voteserver vertrauen, dass er die Identität des Wählers und die Stimme korrekt notiert hat. Der Voteserver könnte hier betrügen. Wäre die Stimme hingegen vom Wähler signiert, könnte der Voteserver sie nicht fälschen. Hier greifen verschiedene Konzepte:

1. Stimmen können aufgrund des Zugriff- und Berechtigungskonzept nicht gelöscht werden. Dies bedeutet, das eingetragene Stimmen nicht gelöscht werden können.

2. Stimmen können nicht gefälscht werden: Es ist prinzipiell möglich, Stimmen im Stimmspeicher hinzuzufügen. Jedoch fehlt dann jeder Stimme die Bestätigersignatur. Beim Auszählen würde dieser Umstand bemerkt werden. Das gleiche gilt für die Änderung von Stimmen.

**Welche technischen und organisatorischen Maßnahmen rechtfertigen das Vertrauen in den Voteserver?** Technische Maßnahmen begleiten hier die organisatorischen. Letztendlich lässt sich dieses Vertrauensverhältnis nur durch eine Evaluierung/Zertifizierung erreichen. Technische Maßnahmen, die Sicherstellen, dass die eingesetzte Software tatsächlich die Software ist, die evaluiert wurde sind ebenfalls Bestandteil der Evaluierung/Zertifizierung. Somit ist sichergestellt, dass tatsächlich die zertifizierte Software betrieben wird. Des Weiteren wird durch das 4-Augen Prinzip mit dem Einsatz des Bestätigers ein großes Manipulationspotential verhindert.

**Wie genau sieht die Wählerliste aus, liegt sie im Klartext vor?** Die Wählerliste ist eine Tabelle, die die Identität jedes Wählers und eine zugehörige ID-Nummer enthält. Solange auf diese Tabelle kein unbefugter Lesezugriff (insbesondere durch die Wähler) möglich ist, könnten die Identitäten der Wähler im Klartext enthalten sein.

**Wie wird inhaltlich „ungültig“ gewählt? Kann man die Option „ungültig“ wirklich auswählen oder gar nichts ankreuzen?** Beides ist möglich, wobei ggf. (im Hinblick auf die Willensbekundung) im Fall eines leeren Stimmzettels der Wähler darauf hingewiesen werden sollte, dass er damit ungültig wählt, und er dieses bestätigen muss. Inhaltlich sind zwei Verfahren implementiert, um inhaltlich „ungültig“ zu wählen:

1. Mehrfachkreuzung (Auswahl von mehr Kandidaten als die Maximal zulässige Anzahl zur Auswahl) oder keine Auswahl von Kandidaten mit entsprechendem Hinweis, dass die Stimmauswahl ungültig ist.

2. Über einen separaten Button zum ungültig Wählen.

Das System kann entsprechend der Vorgaben für eins der beiden Verfahren konfiguriert werden.

**Was genau kann passieren, wenn jemand den Blendfaktor kennt?** Wenn jemand, der den Blendfaktor kennt, das signierte geblendete Votum abfängt, kann er dann den Stimmzettel einsehen und bricht somit das Wahlgeheimnis. Da er aber nicht sicher weiß, ob der Wähler diese Stimme auch abschickt, dient dies nicht als

Beweis, ob der Wähler wirklich so gewählt hat. Dazu müsste der Angreifer auch noch die zweite Verbindung vom Wähler zum Voteserver abhören. Hier wird das Votum aber randomisiert verschlüsselt übertragen, der Angreifer kann also nicht nachvollziehen, ob es sich noch um das Votum handelt, das er entblendet hat. Dazu müsste er die Randomisiserungsfaktoren der Verschlüsselung kennen, die nur das Applet des Wahlclients des Wählers kennt (und das auch nur temporär), der Angreifer müsste also das Applet hacken. Insgesamt dürfte der Aufwand als hoch einzustufen sein. Der Blendfaktor allein bringt hier wenig. Der Blendfaktor ist nur mit einem sehr erheblichen Aufwand und Expertenwissen zu erlangen.

**Wie wird Quittungsfreiheit sichergestellt?** Der Wähler hat theoretisch mit gewissem Aufwand seine vom Validator signierte Stimme im Klartext vorliegen. Dies beweist jedoch nicht, dass die Stimme auch so abgegeben und gezählt wurde: Die personalisierte verschlüsselte Stimme auf dem Bulletin Board kann nicht als Nachweis gelten, da die Verschlüsselung randomisiert ist, so dass nicht geprüft werden kann, welche Klartextstimme welcher verschlüsselten Stimme entspricht. Darüber hinaus ist die Ermittlung der Bestätigersignatur nicht trivial, da diese nicht zwischengespeichert wird. Diese lässt sich nur durch einen gezielten Angriff auf das Voteclientenprogramm ermitteln.

### AP 1.2.1.7: Nachweis der Erfüllung der Sicherheitsziele (10PM)

Nach erfolgreicher Spezifikation sollte in diesem Arbeitspaket der Nachweis geführt werden, dass das Wahlsystem voteremote unter den getroffenen Sicherheitsannahmen die spezifizierten Sicherheitsziele tatsächlich erreicht. Die Spezifikationen und Nachweise wurden so weit wie möglich allgemeinverständlich ausgeführt, um auch Nicht-Technikern zugänglich zu werden. Verwendet wurden Methoden aus den Common Criteria: Es wurde ein Security Target verfasst, welches Anforderungen an die Sicherheit und die Funktionalität des Wahlsystems formuliert und als Grundlage der Evaluierung und Zertifizierung dient.

Im Laufe des Verbundvorhabens änderten sich die Rahmenbedingungen insofern, als dass das BMI den Beschluss fasste, dass elektronische Wahlsysteme konform zum Schutzprofil von BSI/DFKI gestaltet werden müssen. Die Sicherheitsvorgaben (Security Target) für das im Projekt entwickelte Wahlsystem wurden dementsprechend an die Vorgaben des Schutzprofils angepasst. Dazu mussten sämtliche funktionalen Sicherheitsanforderungen und Vertrauenswürdigkeitsanforderungen, die im Schutzprofil definiert werden, auf die entsprechenden Anforderungen der Sicherheitsvorgaben übertragen werden und diese entsprechend angepasst werden.

Weiterhin stand die Frage im Raum, ob das Schutzprofil strict conformance oder demonstrable conformance für dazu konforme Sicherheitsvorgaben fordern

wird. Diese Entscheidung hatte maßgeblichen Einfluss auf die weitere Gestaltung der Sicherheitsvorgaben, da im letzteren Falle mehr Freiheitsgrade für die eigene Formulierung von Sicherheitsanforderungen existieren würden. Letztendlich erschien die Wahrscheinlichkeit für strict conformance jedoch als hoch, was eine sehr exakte Übereinstimmung der Sicherheitsvorgaben mit dem Schutzprofil und entsprechend detaillierte Überarbeitung nötig machte. Das Security Target wurde daher letztlich in Zusammenarbeit mit T-Systems finalisiert.

### AP 1.2.1.8: Abstimmung von Recht und Technik (3PM)

Im Laufe des Vorhabens wurde juristische Beratung durch Prof. Roßnagel von der Universität Kassel eingeholt. Gegenstand war hierbei die Überprüfung der Konformität des entwickelten Wahlsystems mit bestehenden rechtlichen Grundlagen sowie der Entwurf eines neuen gesetzlichen Rahmens für elektronische Wahlen mit Wahldiensteanbieter. Die juristische Prüfung des im Projekt entwickelten Wahlsystems hat neue Anforderungen hervorgebracht, insbesondere hinsichtlich der Nachprüfbarkeit der Wahl: Ein Wahlsystem soll die Möglichkeit bieten, den korrekten Ablauf des gesamten Wahlprozesses zu verifizieren. Das heißt, dass befugte Personen jeden Schritt des Wahlprotokolls überprüfen können, ohne dabei die übrigen Sicherheitsziele wie beispielsweise das Wahlgeheimnis zu gefährden.

Innerhalb dieses Arbeitspakets sollte das Wahlverfahren an die neuen rechtlichen Anforderungen technisch angepasst werden. Dazu gehörte insbesondere die Verifizierbarkeit der korrekten Funktionsweise einzelner Komponenten des Wahlsystems. Um eine weit reichende Verifizierbarkeit des Wahlsystems für die Wähler und/oder andere Beteiligte zu erreichen, muss nach Möglichkeit die Funktion aller relevanten Komponenten des Systems nachvollziehbar sein. So muss zum Beispiel überprüfbar sein, ob das Mix Net die Stimmzettel korrekt gemischt hat, das heißt insbesondere, ob die Eingangs- und die Ausgangsdaten des Mix- Nets inhaltlich identisch sind, also nicht verändert wurden. Nur so kann sichergestellt werden, dass keine Stimmzettel durch das Mix Net manipuliert, gelöscht oder hinzugefügt wurden. Die Verifizierbarkeit des Wahlsystems ist insbesondere im Sinne der Nachprüfbarkeit durchgeführter Wahlen wichtig. Hier wird in Abhängigkeit der jeweils geltenden rechtlichen Bestimmungen gefordert, dass bestimmte Wahldaten und Wahlprozesse langfristig nachvollzogen werden können. Eine technische Voraussetzung dafür ist, dass entsprechende Verifikationsmechanismen zur Verfügung stehen. Dieses Arbeitspaket, welches auch in engem Zusammenhang zu Arbeitspaket 1.2.1.11 stand, wurde erfolgreich bearbeitet.

### AP 1.2.1.9: Umsetzung der Anforderungen für Sozialwahlen (3PM)

Dieses Arbeitspaket ist entfallen und wurde durch ein anderes erstzt, siehe Arbeitspaket 1.2.1.10.

### AP 1.2.1.10: Realisierung gemischter Wahlen (2PM)

Gemeinsam mit Arbeitspaket 9 wurde dieses Arbeitspaket auf Antrag ersetzt durch das neue Arbeitspaket 1.2.1.12. Die Arbeitsschwerpunkte der Technische Universität Darmstadt haben sich im Laufe des Vorhabens inhaltlich verschoben. Die in Arbeitspaket 1.2.1.9 definierten Aufgaben wurden von Projektpartner T-Systems bearbeitet. Weiter hat sich heraus gestellt, dass die Aufgaben des Arbeitspakets 1.2.1.10 rein organisatorischer Art sind und somit nicht von der Technische Universität Darmstadt bearbeitet werden. Dahingegen wurde die Technische Universität Darmstadt stark in die technische Beratung und Ausgestaltung des Wahldiensteanbieter-Gesetzes und insbesondere der zugehörigen Verordnung einbezogen, die in Zusammenarbeit mit der Universität Kassel erarbeitet wurde.

### AP 1.2.1.11: Langzeitarchivierung (2PM)

Rechtlichen Anforderungen entsprechend müssen nach einer elektronischen Wahl die Daten langfristig archiviert werden. Hierdurch kann jederzeit transparent die ordnungsgemäße Durchführung der Wahl nachgewiesen werden. In diesem Zusammenhang sollte ein Konzept für die Langzeitarchivierung entwickelt und technisch realisiert werden.

Innerhalb dieses Arbeitspakets wurden zunächst die technischen Anforderungen hinsichtlich der Langzeitarchivierung von Wahldaten unter Berücksichtigung der rechtlichen Vorgaben spezifiziert. Durch die Archivierung von Wahldaten soll jederzeit transparent die ordnungsgemäße Durchführung der Wahl nachgewiesen werden können. Der Schutz des privaten Mix Net-Schlüssels ist hierbei maßgeblich für die Sicherstellung der Anonymität der Wahl. Die Archivierung dieses Merkmals ist kritisch, wenn gleichzeitig das Verzeichnis der doppelt verschlüsselten Stimmen aufbewahrt wird, da hier die Identität der Wähler mit den Stimmen verknüpft ist. Innerhalb des Arbeitspakets sollte ein Konzept entwickeln werden, wie die Archivierung der Wahldaten unter gleichzeitiger Wahrung der Anonymität möglich ist. Hierzu wurden drei verschiedene Möglichkeiten in Betracht gezogen. Diese verschiedenen Ansätze wurden diskutiert und auf ihre Vor- und Nachteile hin überprüft:

1. **Verifizierbares Mix Net bei gleichzeitiger Vernichtung des privaten Mix Net-Schlüssels.** Es muss nachgewiesen werden, dass die Ausgangsgröße der Eingangsgröße des Mixvorgangs entspricht. Wenn dies belegbar ist,

kann der private Schlüssel des Mixnets vernichtet werden. Die Anonymität wäre bei den archivierten Daten nicht mehr zu brechen, da der Mixvorgang nicht wiederholt werden kann. Dies behindert in gewisser Weise jedoch den Transparenznachweis im Nachhinein, da der gesamte Vorgang der Stimmberechnung inklusive Mixing nicht mehr möglich ist. Es mag aus rechtlicher Sicht genügen, wenn man die korrekte Funktionsweise des Mixers durch einen Zero Knowledge Proof nachweisen kann, aber für die Vertrauenswürdigkeit nach außen hin ist die Wiederholbarkeit einzelner Vorgänge (wie Mixen und Auszählen) entscheidend.

2. **Daten löschen, die eine nachträgliche Identifizierung ermöglichen.**

   - **Die ungemischten, doppelt verschlüsselten Voten werden ohne Wähler-IDs archiviert.** Der Nachteil liegt hier darin, dass die Vermerke zur Stimmberechtigung einzelner Wähler verloren gehen. Eine Möglichkeit, die individuelle Verifizierbarkeit dennoch zu gewährleisten, könnte wie folgt aussehen: Laut Protokoll wird dem Wähler seine doppelt verschlüsselte Stimme während des Wahlvorgangs angezeigt. Da randomisiert verschlüsselt wird, ist jedes Votum individuell, was dem Wähler einen Vergleich mit den doppelt verschlüsselten Voten auf dem Bulletin Board ermöglicht. Allerdings ist dann wieder die Quittungsfreiheit in Gefahr, falls ein Angreifer den privaten Mixer-Schlüssel erlangt.
   - **Das Wählerverzeichnis wird ohne die zugehörigen IDs archiviert.** Wenn jemand in Besitz des privaten Mixer-Schlüssels gelangt, kann er dann zwar das Votum inklusive der ID sehen, diese jedoch keinem konkreten Wähler mehr zuordnen. Problematisch an diesem Ansatz ist eventuell, dass bestimmte Rollen das Wählerverzeichnis inklusive der IDs während der Wahl auf dem Bulletin Board lesen können. Um dennoch die individuelle Verifizierbarkeit zu gewährleisten, wäre denkbar, dass jeder Wähler seine ID kennt und damit gezielt nachfragen kann. Das führt aber wieder zu anderen Problemen (z.B. dass ein Angreifer, der die Voten offengelegt hat, den Wähler zur Herausgabe seiner ID zwingen kann).

3. **Verteilung des privaten Mix Net-Schlüssels auf verschiedene Rollen bzw. Personen (Threshold Verschlüsselung).** Dadurch würde zwar die Rekonstruktion des privaten Schlüssels für Einzelpersonen erschwert (Zugang zu allen Schlüsselteilen erforderlich). Der Einsatz verteilter Architekturen wäre jedoch beim vorliegenden Wahlsystem unpassend, denn das Wahldiensteanbieter-Konzept beinhaltet ja gerade eine Zentralisierung und Bündelung (fast) aller sicherheitskritischen Aufgaben beim Wahldiensteanbieter. Es würde

daher wenig Sinn machen, etwas zu verteilen, das dann doch wieder unter einem Dach ist, zumal die Archivierung der Wahldaten vermutlich beim Wahldiensteanbieter stattfinden wird.

Ergebnis der Diskussion war eine Tendenz zum zweiten Vorschlag, was entsprechend im Wahlsystem umgesetzt wurde. Längerfristig ist – auch im Hinblick auf die Umsetzung von Wahlen mit größerer Tragweite – angedacht, die erste Lösung umzusetzen, da diese ein besonders hohes Maß an Verifizierbarkeit mit sich bringt.

### AP 1.2.1.12: Technische Ausgestaltung der Verordnung zum Wahldiensteanbieter-Gesetz (5PM)

Im Zuge der Entwicklung eines rechtlichen Regelungsrahmens für die Durchführung von elektronischen Wahlen und insbesondere der Erarbeitung von Regelungswerken für Wahldiensteanbieter war ein Wahldiensteanbieter-Gesetz einschließlich entsprechender Verordnung geplant. Ein Entwurf für ein solches Gesetz wurde im Laufe des Projekts von der Universität Kassel vorgelegt. Dazu musste anschließend eine passende Verordnung erstellt werden, welche auch technische Aspekte der Vorbereitung und Durchführung der Wahl durch den Wahldiensteanbieter beinhalten sollte. Die Verordnung sollte darüber hinaus voraussichtlich auch den Inhalt eines Sicherheitskonzepts für Wahldiensteanbieter festlegen, ähnlich wie die Signaturverordnung den Umfang des Sicherheitskonzepts von Zertifizierungsdiensteanbietern regelt. Zur Bearbeitung der Wahldiensteanbieter-Verordnung wurde ein Arbeitskreis gegründet, an dem die Technische Universität Darmstadt maßgeblich beteiligt war, indem sie die auftretenden technischen Fragen beantwortet und dadurch gleichzeitig die Inhalte des Sicherheitskonzepts mitgestaltet hat. Die zentrale Frage bei der Erstellung der Verordnung zum im Projektvorhaben entwickelten gesetzlichen Regelungswerk behandelte das Problem der Gestaltung eines Verfahrens zur Prüfung der technischen und organisatorischen Sicherheit von Wahlsystemen und Wahldiensteanbietern. Dazu wurde von der Technischen Universität Darmstadt ein Vertrauenskonzept entwickelt, das sich am deutschen Signaturgesetz und der Signaturverordnung orientiert. Das Verfahren verspricht ein sehr hohes Sicherheitsniveau. Es umfasst drei Maßnahmen, die im Folgenden vorgestellt werden.

**Gesetzlicher Rahmen.** Ein Gesetz und eine Verordnung legen die Sicherheitsanforderungen an elektronische Wahlen und Wahldiensteanbieter fest. Dies umfasst sowohl technische und organisatorische Sicherheitsanforderungen, Dokumentationspflichten als auch Angaben über eine vorgesehene Kontrollbehörde und das Akkreditierungsverfahren von Wahldiensteanbietern, das nachfolgend erläutert wird. Jeder Wahldiensteanbieter ist nach dem Gesetz verpflichtet, ein Sicherheitskonzept vorzulegen, in dem die Umsetzung technischer und organisatorischer Sicherheits-

anforderungen aufgezeigt wird. Dieses Sicherheitskonzept dient unter anderem als Grundlage für das Akkreditierungsverfahren eines Wahldiensteanbieters. Ein entsprechendes Wahldiensteanbietergesetz wird gegenwärtig im Rahmen des Projekts entwickelt. Die gesetzlichen Regelungen orientieren sich am deutschen Signaturgesetz und der Signaturverordnung.

**Kontrollbehörde.** Dem Signaturgesetz entsprechend, schlagen wir vor, dass die Qualifikation und Sicherheit des Wahldiensteanbieters hinsichtlich des gesetzlichen Rahmens von einer übergeordneten, unabhängigen Kontrollbehörde geprüft und überwacht wird. Die Kontrollbehörde prüft das Sicherheitskonzept des Wahldiensteanbieters, das die Umsetzung der Sicherheitsanforderungen aufzeigt. Wahldiensteanbieter sollten sich von der Behörde akkreditieren lassen. Die Akkreditierung dient als Nachweis der umfassend geprüften technischen und administrativen Sicherheit des Wahldiensteanbieters.

**Common Criteria Evaluation.** Die Common Criteria (CC) bilden einen internationalen Standard für die Kriterien der Bewertung und Zertifizierung der Sicherheit von Computersystemen im Hinblick auf Datensicherheit und Datenschutz. Eine Evaluation nach CC ist für Produkte, die gemäß Signaturgesetz bestätigt werden sollen, vorgeschrieben. Die CC Evaluation wird von einer vom BSI anerkannten Prüfstelle durchgeführt. Die vom Wahldiensteanbieter verwendete Software des Wahlsystems wird einer CC-Evaluation unterzogen und auf ihre Sicherheit hin überprüft. Andere für die Sicherheit der Wahltätigkeit relevante technische Komponenten, die beim Wahldiensteanbieter eingesetzt werden, werden ebenfalls nach CC evaluiert. Das Prüfungsergebnis wird dem BSI zur Bestätigung vorgelegt. Im positiven Falle erhält die geprüfte Software ein Zertifikat, das die Einhaltung aller Sicherheitanforderungen bestätigt. Für das im Projekt entwickelte Wahlsystem wird die Prüfstufe EAL3 angestrebt. Das für die CC-Evaluation zentrale Dokument, in dem die konkreten Sicherheitziele und -anforderungen der Software des Wahldiensteanbieters beschrieben werden, sind die CC-Sicherheitsvorgaben. Sollen viele Produkte für denselben Zweck evaluiert werden, kann als Grundlage für die CC-Evaluation ein CC-Schutzprofil für diesen Produkttyp erstellt werden. Das BSI hat aktuell in Zusammenarbeit mit dem DFKI ein CC-Schutzprofil fertiggestellt, welches einen Basissatz von Sicherheitsanforderungen an Online-Wahlsysteme enthält. Im Projekt wurden die CC-Sicherheitsvorgaben speziell für die eingesetzte Wahlsoftware konform zu diesem CC-Schutzprofil erstellt und anschließend evaluiert.

## 2.2 Notwendigkeit und Angemessenheit der geleisteten Arbeit

Die in der Vorhabensbeschreibung der Technischen Universität Darmstadt für das Projektvohaben voteremote formulierten Arbeitspakete 1.2.1.1 bis 1.2.1.7 wurden insbesondere durch die zusätzliche Arbeit durch technische Beratung seitens der Universität Kassel im Bereich des Entwurfs eines Regelungsrahmens für elektronische Wahlen mit Wahldiensteanbietern im Aufstockungsantrag um zusätzliche Arbeitspakete 1.2.1.8 bis 1.2.1.11 erweitert. Während der Projektlaufzeit zeigte sich, dass eine Umgestaltung dieser Arbeitspakete notwendig wurde, da sich die Arbeitsschwerpunkte der Technische Universität Darmstadt im Projektvorhaben voteremote inhaltlich verschoben. Die in Arbeitspaket 1.2.1.9 definierten Aufgaben wurden von Projektpartner T-Systems bearbeitet. Weiter stellte sich heraus, dass die Aufgaben des Arbeitspakets 1.2.1.10 rein organisatorischer Art waren und somit nicht von der Technischen Universität Darmstadt bearbeitet werden konnten.

Dahingegen wurde die Technische Universität Darmstadt stark in die technische Beratung und Ausgestaltung des Wahldiensteanbietergesetzes und insbesondere der zugehörigen Verordnung einbezogen, die in Zusammenarbeit mit der Universität Kassel erarbeitet wurde. Der Schwerpunkt des Arbeitsaufwands der Technische Universität Darmstadt entfiel damit auf diesen Bereich. Diese Situation bestand bis zum Ende der weiteren Projektlaufzeit fort. Diese Umgestaltung wurde mit Schreiben vom 02.09.2008 beim Projektträger beantragt und die Arbeitspakete 1.2.1.9 und 1.2.1.10 durch das neue Arbeitspaket 1.2.1.12 mit gleichem Arbeitsaufwand ersetzt. Der Gesamtarbeitsaufwand blieb somit unverändert.

Für die den Arbeitspaketen 1.2.1.1 bis 1.2.1.8 sowie 1.2.1.11 bis 1.2.1.12 entsprechend geleistete Arbeit gilt, dass sie zur Erreichung der Ziele des Projektvorhabens notwendig und angemessen war. Der tatsächliche Arbeitsaufwand entsprach den Angaben aus den entsprechenden Vorhabensbeschreibungen.

## 2.3 Verwertbarkeit der Ergebnisse

Das Forschungsvorhaben zielte darauf ab, die Lücke zwischen Theorie und Praxis im Hinblick auf elektronische Wahlverfahren zu schließen. Dieses Ziel wurde erreicht und bietet nach Abschluss des Forschungsvorhabens diverse Ansatzpunkte für eine erfolgversprechende Verwertbarkeit der Projektergebnisse.

Es wurde ein Wahlverfahren entwickelt, welches sicherheitstechnisch auf hohem Niveau ist und das gleichzeitig unter Verwendung von moderner Informationstechnologie effizient im Kontext gegenwärtiger IT-Architekturen einsetzbar ist. Das Wahlprotokoll bietet einen guten Ausgangspunkt für weitere Forschungsarbeit im Kontext sicherer Onlinewahlen. Es kann durch den Einbau von Verifikationsverfahren für die einzelnen Bausteine noch weiter verbessert werden und auf diese Weise

auch für Onlinewahlen einsetzbar werden, die höhere Sicherheitsanforderungen als die bisher betrachteten Wahlformen (Betriebsrats- und Sozialwahlen) haben. Damit wäre künftig auch denkbar, beispielsweise parlamentarische Wahlen online mit Hilfe neuerer Varianten des im Forschungsvorhaben entwickelten Wahlprotokolls durchzuführen. Dazu können auch die entstandenen formalen Modelle und experimentellen Erfahrungen beitragen. Das entwickelte Verfahren soll jedoch zunächst im nichtparlamentarischen Bereich eingesetzt und erprobt werden. Es ist geplant, das Onlinewahlverfahren bei den Sozialwahlen im Jahr 2017 einzusetzen.

Das im Rahmen des Forschungsvorhabens entwickelte Konzept des Wahldiensteanbieters bietet ein erhebliches Potential. Dies ist insbesondere darin begründet, dass dieser Ansatz mit einem überlegenen Sicherheits- und Vertrauenskonzept einhergeht. Dazu gehört auch ein rechtlicher Rahmen, der den Einsatz des Wahldiensteanbieters reguliert. Die künftige Umsetzbarkeit des Wahldiensteanbieterkonzeptes wird unter anderem auch durch einen entsprechenden Entwurf zur Anpassung des Betriebsverfassungsgesetzes und der ersten Wahlordnung zum Betriebsverfassungsgesetz gewährleistet. Weiterhin ist denkbar, das Konzept des Wahldiensteanbieters auch in Verbindung mit anderen Wahlverfahren einzusetzen, da diese beiden Aspekte unabhängig voneinander erforscht wurden.

## 2.4 Fortschritt bei anderen Stellen

Während des Projektvorhabens voteremote haben sich an verschiedenen anderen Stellen Entwicklungen im Bereich elektronischer Wahlen ergeben, die für das Projekt relevant waren oder aus Gründen der inhaltlichen Verwandtschaft zum Projekt hier erwähnt werden.

Während der Laufzeit des Projektvorhabens voteremote wurde durch das BSI das Common Criteria Schutzprofil für „Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte“ [Bun08] evaluiert und erfolgreich zertifiziert. Das Schutzprofil definiert einen Basissatz von Sicherheitsanforderungen, den jedes Online-Wahlprodukt zumindest erfüllen muss, um einige Arten von Vereinswahlen, Gremienwahlen, etwa in den Hochschulen, im Bildungs- und Forschungsbereich, und insbesondere nicht-politische Wahlen mit geringem Angriffspotential sicher auszuführen. Das betrachtete Online-Wahlprodukt ist in ein Phasenmodell für den Ablauf einer Wahl eingebettet. Eine Wahl wird in drei Phasen eingeteilt: Wahlvorbereitung, Wahldurchführung inkl. Stimmauszählung, Archivierung. Die Anforderungen an das zu evaluierende Produkt beziehen sich nur auf die Phase Wahldurchführung inkl. der Stimmauszählung. Anforderungen an den Übergang zu den angrenzenden Phasen werden in Sicherheitszielen für die Umgebung zum Ausdruck gebracht. Die Fertigstellung und Zertifizierung des genannten Schutzprofils hat die Arbeit im Projektvorhaben voteremote dahin gehend beeinflusst, dass das im Projekt entwickelte Wahlsystem schon zur Entwicklungszeit auf Kon-

formität zum Schutzprofil ausgerichtet wurde. Die sich anschließende Evaluierung des Wahlsystems und die damit einhergehende Erstellung der Common Criteria Sicherheitsvorgaben („Security Target“), welche als Grundlage für die Common Criteria Evaluierung dienen, wurde schon während des Projekts an das genannte Schutzprofil angepasst. Somit erfüllt das voteremote Wahlsystem nach erfolgreicher Zertifizierung als eines der ersten Onlinewahlsysteme die Anforderungen des genannten Schutzprofils des BSI, die voraussichtlich für alle Wahlsysteme dieser Art in Deutschland zur Pflicht erhoben werden.

Ein weitere relevanter Punkt ist das Wahlsystem „Polyas“ der Firma Micromata GmbH aus Kassel [Mic05]. Hierbei handelt es sich um eine Software zur Durchführung von Onlinewahlen für Organisationen, Vereine oder Unternehmen. Micromata beschäftigt sich auch mit den Anforderungen an die Rechtsverbindlichkeit. Der Wahlausrichter wird bei Einsatz von Polyas durch Micromata betreut und unterstützt. Darüber hinaus strebt Micromata eine Zertifizierung des Polyas Wahlsystems nach dem oben genannten Common Criteria Schutzprofil für „Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte“ an. Im Vergleich zu Polyas hebt sich das System des Projektvorhabens voteremote insbesondere durch das wesentlich umfangreichere Vertrauens- und Sicherheitskonzept ab. Durch die im Projektvorhaben neu geschaffenen gesetzlichen Grundlagen speziell für Wahldiensteanbieter sowie die dort geforderte Existenz einer Kontrollbehörde und insbesondere das in der zugehörigen Verordnung beschriebene Sicherheitskonzept, welches von gesetzeskonformen Wahldiensteanbietern vorgelegt werden muss, wird neben der technischen Sicherheit des eingesetzten Wahlsystems auch die organisatorische Sicherheit des Wahldiensteanbieters geprüft und überwacht und damit auch nachvollziehbar für den Wähler. Das Sicherheitsniveau einer Onlinewahl wird so signifikant verbessert.

## 2.5 Veröffentlichung der Ergebnisse

Die Ergebnisse des Vorhabens wurden auf einschlägigen Konferenzen im Bereich e-Voting und e-Government veröffentlicht. Darüber hinaus wurden zahlreiche Bachelorarbeiten sowie eine Diplomarbeit angefertigt. Es folgt eine Zusammenstellung aller Veröffentlichungen, die in Zusammenhang mit dem Vorhaben erfolgt sind:

#### Veröffentlichungen im Rahmen des Vorhabens


[Ber08] Bergner, Martin: *Minimale Voraussetzungen für blinde Signaturen.* Technische Universität Darmstadt, Bachelorarbeit, 2008

[Clo08] Clos, Johannes: *Secure Client Platforms for Remote Internet Voting*, Technische Universität Darmstadt, Diplomarbeit, 2008

[fle] *FlexiProvider*. – `http://www.flexiprovider.de/`

[GLOOT08] Gitter, Rotraud ; Langer, Lucie ; Okunick, Susanne ; Opitz-Talidou, Zoi: Long-term retention in e-voting – Legal requirements and technical implementation. In: Krimmer, Robert (Hrsg.): *3rd International Conference on Electronic Voting EVOTE08* Bd. 131, Gesellschaft für Informatik, 2008 (LNI), S. 109–123

[Kah07] Kahl, Benjamin: *Blinde Signaturen und Post-Quantum-Kryptographie*. Technische Universität Darmstadt, Bachelorarbeit, 2007

[Lan08] Langer, Lucie: Towards Legally Binding Online Elections in Germany. In: Remenyi, Dan (Hrsg.): *Proceedings of the 4th International Conference on eGovernment ICEG 2008*, Academic Conferences International, 2008, S. 247–254

[LS08] Langer, Lucie ; Schmidt, Axel: Onlinewahlen mit Wahldiensteanbieter – das Verbundprojekt voteremote. In: Parycek, Peter (Hrsg.) ; Prosser, Alexander (Hrsg.): *Tagungsband der EDem 2008 – Tagung für elektronische Demokratie* Bd. 239, OCG Verlag, 2008, S. 281–290

[LSA08] Langer, Lucie ; Schmidt, Axel ; Araujo, Roberto: A pervasively verifiable online voting scheme. In: Hegering, Heinz-Gerd (Hrsg.) ; Lehmann, Axel (Hrsg.) ; Ohlbach, Hans J. (Hrsg.) ; Scheideler, Christian (Hrsg.): *GI Jahrestagung (1)* Bd. 133, GI, 2008 (LNI). – ISBN 978–3–88579–227–7, S. 457–462

[LSB08] Langer, Lucie ; Schmidt, Axel ; Buchmann, Johannes: Secure an Practical Online Elections via Voting Service Provider. In: *Proceedings of the 4th International Conference on eGovernment ICEG 2008*, Academic Conferences International, 2008, S. 255–262

[Vel08] Veljanova, Veneta: *An Analysis of the Neff's Voter Verifiable Election Scheme*. Technische Universität Darmstadt, Bachelorarbeit, 2008

# Literatur


[BFP+01] Baudron, Olivier ; Fouque, Pierre-Alain ; Pointcheval, David ; Stern, Jacques ; Poupard, Guillaume: Practical Multi-Candidate Election System. In: *PODC*, 2001, S. 274–283

[Bun08] Bundesamt für Sicherheit in der Informationstechnik: *Schutzprofil Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte*. 2008

[Cha81] Chaum, David L.: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. In: *Communications of the ACM* 24 (1981), February, Nr. 2, 84–90. http://dx.doi.org/http://dx.doi.org/10.1145/358549.358563. – DOI http://dx.doi.org/10.1145/358549.358563. – ISSN 0001–0782

[Cha82] Chaum, David: Blind Signatures for Untraceable Payments. In: *CRYPTO*, 1982, S. 199–203

[Cou03] Council of Europe: *Multidisciplinary Ad Hoc Group of Specialists on legal, operational and technical standards for e-enabled voting (IP 1-S-EE),*. 2003

[DA81] Dierks, Tim ; Allen, Christopher: *The TLS Protocol*. IETF RFC 2246, January 1981. – http://www.ietf.org/rfc/rfc2246.txt

[Inv02] Invitation to Tender (Netherlands): *Remote Electronic Voting and Voting by Telephone Experiment*. 2002

[JCJ05] Juels, Ari ; Catalano, Dario ; Jakobsson, Markus: Coercion-Resistant Electronic Elections. In: Atluri, Vijay (Hrsg.) ; Vimercati, Sabrina De C. (Hrsg.) ; Dingledine, Roger (Hrsg.): *WPES*, ACM, 2005, 61–70

[LK02] Lee, Byoungcheon ; Kim, Kwangjo: Receipt–Free Electronic Voting Scheme with a Tamper–Resistant Randomizer. In: *Information Security and Cryptology — ICISC 2002: 5th International Conference*, 2002, S. 389–406. – http://link.springer.de/link/service/series/0558/bibs/2587/25870389.htm

[Loc02] Local Government Organisation (LGA): *The implementation of electronic voting in the UK - Research Summary*. 2002

[Mic05] MICROMATA: *Polyas Online Voting Solutions. Online-Wahlen für Verbände und Vereine.* Polyas Online Voting Solutions, 2005. – http://www.micromata.de/produkte/documents/polyas_broschuere_72dpi.pdf

[N. 03] N. BRAUN ET AL. ; PROSSER, A. (Hrsg.): *E-voting in der Schweiz, Deutschland und Österreich.* Collection of working papers of the e-Democracy/e-Voting workshop at IRIS 2003, 2003

[OMA+99] OHKUBO, Miyako ; MIURA, Fumiaki ; ABE, Masayuki ; FUJIOKA, Atsushi ; OKAMOTO, Tatsuaki: An Improvement on a Practical Secret Voting Scheme. In: MAMBO, Masahiro (Hrsg.) ; ZHENG, Yuliang (Hrsg.): *ISW* Bd. 1729, Springer, 1999 (Lecture Notes in Computer Science). – ISBN 3–540–66695–8, S. 225–234

[Opp02] OPPLINGER, R.: *Addressing the Secure Platform Problem for Remote Internet Voting in Geneva.* eSecurity Technologies, 2002

[Rie98] RIERA, Andreu: An Introduction to Electronic Voting Schemes / University of Barcelona. Version: October 1998. `http://pirdi.uab.es/document/pirdi9.ps`. 1998 (PIRDI 9-98). – Forschungsbericht

[Sch02] SCHWEIZER BUNDESBLATT NR. 5: Bericht über den Vote electronique vom 9. Januar 2002. In: *Chancen, Risiken und Machbarkeit elektronischer Ausübung politischer Rechte.* 2002

[The02] THE CHAIRMEN OF THE HOUSE OF REPRESENTATIVES OF THE STATES GENERAL (NETHERLANDS): *Remote Voting Project.* 2002

[VH04] VOLKAMER, Melanie ; HUTTER, Dieter: From Legal Principles to an Internet Voting System. In: *Electronic Voting in Europe*, 2004, S. 111–120

UNIKASSEL
VERSITÄT

Abschlussbericht zum Projekt

**voteremote:**

**Online-Wahlen außerhalb von Wahllokalen**

Teilvorhaben

**Sicherheitsanalyse**

Unterauftrag

**Rechtliche Bewertung**

Zuwendungsempfänger:

Technische Universität Darmstadt
Fachbereich Informatik
Fachgebiet
Theoretische Informatik

Förderkennzeichen:

01 MS 06 002

Verbundvorhaben:
**voteremote:**
**Online-Wahlen außerhalb von Wahllokalen**

Teilvorhaben:
**Sicherheitsanalyse**

Unterauftrag
**Rechtliche Bewertung**

Laufzeit des Unterauftrags: 1. Juli 2007 – 31.10.2008
Berichtszeitraum: 1. Juli 2007 – 31.10.2008

Unterauftragnehmer:

Universität Kassel
Projektgruppe verfassungsverträgliche Technikgestaltung (provet)
im Forschungszentrum für Informationstechnik-Gestaltung (ITeG)

Ausführende Stelle: Universität Kassel
Projektgruppe verfassungsverträgliche Technikgestaltung (provet)
im Forschungszentrum für Informationstechnik-Gestaltung (ITeG)
Wilhelmshöher Allee 64-66
34109 Kassel
Tel. 0561/804-609
Mail: a. rossnagel@uni-kassel.de

Autor: Prof. Dr. jur. Alexander Roßnagel

Das diesem Bericht zu Grunde liegende Forschungsvorhaben wurde mit Mitteln des Bundesministeriums für Wirtschaft und Technologie unter dem Förderkennzeichen 01 MS 06 002 gefördert. Die Verantwortung für den Inhalt dieser Arbeit liegt beim Autor.

## Inhaltsverzeichnis


1 Kurzdarstellung 6

1.1 Aufgabenstellung . . . . . 6

1.2 Voraussetzungen . . . . . 6

1.3 Planung und Ablauf . . . . . 7

1.4 Stand in Wissenschaft und Technik . . . . . 7

1.5 Zusammenarbeit mit anderen Stellen . . . . . 8

2 Eingehende Darstellung 9

2.1 Verwendung der Zuwendung und erzieltes Ergebnis . . . . . 9

2.2 Notwendigkeit und Angemessenheit der geleisteten Arbeit . . . . . 14

2.3 Verwertbarkeit der Ergebnisse . . . . . 14

2.4 Fortschritt bei anderen Stellen . . . . . 15

2.5 Veröffentlichung der Ergebnisse . . . . . 15

# 1. Kurzdarstellung

## 1.1 Aufgabenstellung

Im Verbundvorhaben „voteremote: Online-Wahlen außerhalb von Wahllokalen“ sollte ein Wahlsystem geschaffen werden, mit dem nicht-parlamentarische elektronische Wahlen technisch sicher unter Einhaltung rechtlicher Anforderungen in der Praxis durchgeführt werden können. Das Teilvorhaben Sicherheitsanalyse hatte zum Ziel, sicherheitsrelevante Grundlagen des Wahlsystems zu erarbeiten sowie kryptographische Primitive für dessen Umsetzung in die Praxis bereitzustellen.

Zur Untersuchung der Konformität der für „voteremote“ gefundenen Lösung mit den rechtlichen Wahlgrundsätzen, zur Entwicklung eines Konzeptes für ein Wahldiensteanbietergesetz und zur Anpassung von Wahlvorschriften am Beispiel der Betriebsratswahlen wurden ein Unterauftrag an die Universität Kassel (Prof. Roßnagel) vergeben (Juli 2007 bis März 2008) und einmal verlängert (April 2008 bis Oktober 2008).

Für die Durchführung nichtparlamentarischer elektronischer Wahlen von beliebigen Endgeräten aus sollte ein Wahldiensteanbieter für die Wahlveranstalter die technische Durchführung der Wahlen übernehmen. Dieser sollte einschließlich seines Sicherheitskonzepts überprüft und akkreditiert werden. Statt bei jedem Wahlveranstalter immer wieder sicherstellen zu müssen, dass die Allgemeinheit, Freiheit, Gleichheit, Unmittelbarkeit, Vertraulichkeit und Sicherheit der Wahl auch bei elektronischer Durchführung gewährleistet ist, sollte es genügen, einen Wahldiensteanbieter in gewissen Abständen einmal zu überprüfen und zu akkreditieren, damit er seine Dienstleistung vielfach zur Anwendung bringen kann. Durch dieses Konzept entstanden zwei entscheidende Herausforderungen, für die praktikable Lösungen gefunden werden mussten:

- Der Wahldiensteanbieter ist eine Vertrauensinstanz, für die definiert werden muss, unter welchen Voraussetzungen ihr Vertrauen entgegengebracht werden kann und in welchem Verfahren die Vertrauenswürdigkeit überprüft und bestätigt werden kann. Der Wahldiensteanbieter setzt technische Komponenten ein und nutzt diese, um einen Wahlprozess durchzuführen. Sowohl für die technischen Komponenten als auch für den organisatorischen Prozess der elektronischen Wahl sind Voraussetzungen ausreichender Sicherheit zu bestimmen und Verfahren zu entwickeln, sie zu überprüfen und zu bestätigen. Für diese Herausforderungen ist ein geeigneter rechtlicher Rahmen zu konzipieren und ein Regelungsvorschlag zu entwickeln. Die jeweilige Wahlordnung kann dann Bezug auf das Wahldiensteanbietergesetz nehmen.

- Die bisherigen Wahlen sind an dem Informationsträger Papier orientiert. Zur Durchführung elektronischer Wahlen waren hinderliche wahlrechtliche Vorgaben zu identifizieren und funktionaläquivalente Alternativen zu diesen für elektronische Wahlen zu bestimmen. Aus diesen waren Vorschläge zur Änderung oder Ergänzung bestehender Wahlregelungen zu entwerfen.

## 1.2 Voraussetzungen

Der Unterauftragnehmer und seine Projektgruppe verfassungsverträgliche Technikgestaltung (provet) waren für den Unterauftrag im Besonderen qualifiziert. Sie hatten für die Bundesregierung bereits mehrere vergleichbare Projekte erfolgreich durchgeführt, in denen Konzepte zur Regelung sicherheitskritischer IT-Anwendungen zu entwerfen und in Entwürfe für gesetzliche Regelungen zu überführen waren. Beispiele hierfür sind:

- 1997 Entwurf des Signaturgesetzes und des Teledienstedatenschutzgesetzes für das Bundesministerium für Forschung und Technologie
- 2000 Entwurf eines Datenschutzauditgesetzes für das Bundesministerium für Wirtschaft und Arbeit
- 2001 Entwurf für eine Modernisierung des Datenschutzrechts für das Bundesministerium des Innern
- 2004 Machbarkeitsstudie für eine Digitalen Personalausweis für das Bundesministerium des Innern
- 2007 Entwurf der Regelungen für die Authentisierungsfunktion des elektronischen Personalausweises für das Bundesministerium des Innern
- 2008 Entwurf eines Gesetzes und einer Verordnung zur Einführung von Bürgerportalen für das Bundesministerium des Innern

Außerdem war der Unterauftragnehmer durch eine Vielzahl von Forschungsprojekten zu vergleichbaren Themenstellungen für die Durchführung des Unterauftrags qualifiziert.

## 1.3 Planung und Ablauf

Der Unterauftrag wurde in zwei Phasen durchgeführt. In der ersten Phase (Juli 2007 bis März 2008) wurden die verfassungs- und europarechtlichen Grundlagen untersucht, ein Konzept für ein Wahldiensteanbietergesetz entwickelt und ein Gesetzentwurf erarbeitet sowie die Wahlregelungen für Betriebsratswahlen untersucht und Vorschläge zu ihrer Änderung entworfen. Die Arbeiten zu den einzelnen Arbeitspaketen werden unter 2.1 näher dargestellt.

In der zweiten Phase (Verlängerung von April 2008 bis Oktober 2008) wurde eine Verordnung zum Wahldiensteanbietergesetz entworfen, in der die rechtlichen Anforderungen an die Durchführung von Onlinewahlen mit den technischen Konzepten zur Gewährleistung ausreichender Sicherheit und zur Zertifizierungen von Produkten und zur Akkreditierung der Wahldiensteanbieter (u.a. Protection Profile) näher abgestimmt wurden. Außerdem wurde die Untersuchung der Wahlregelungen auf Wahlen der Sozialversicherungsträger und auf gemischte Wahlen sowie die Erprobung neuer Wahlverfahren ausgeweitet.

Die Arbeiten erfolgten planmäßig.

## 1.4 Stand in Wissenschaft und Technik

Zu Internetwahlen gab es eine Reihe von rechtswissenschaftlichen Untersuchungen wie zum Beispiel:

*Bremke, N.,* Internetwahlen – Eine Analyse einer Wahlverfahrensänderung für das 21. Jahrhundert unter besonderer Berücksichtigung rechtlicher Anforderungen, LKV 2004, 102.

*Hanßmann,A.,* Möglichkeiten und Grenzen von Internetwahlen, Baden-Baden 2005.

*Holznagel, B. / Grünwald, A. / Hanßmann, A.* (Hrsg.), Elektronische Demokratie. Bürgerbeteiligung per Internet zwischen Wissenschaft und Praxis, München 2001.

*Karpen, U.,* Elektronische Wahlen?: Einige verfassungsrechtliche Fragen, Baden-Baden 2005.

*Khorrami, E.,* Bundestagswahlen per Internet. Zur rechtlichen und tatsächlichen Realisierbarkeit von Internetwahlen, Baden-Baden 2006.

*Rüß, O.-R.,* Wahlen im Internet – Wahlrechtsgrundsätze und Einsatz von digitaler Signaturen, MMR 2000, 73-76.

*Schönau, R.,* Elektronische Demokratie: Verfassungsrechtliche Zulässigkeit elektronischer Wahlen, Hamburg 2007.

*Will, M.,* Internetwahlen. Verfassungsrechtliche Möglichkeiten und Grenzen, Stuttgart u.a. Dresden 2002.

Zur konventionellen Durchführung von bisher geregelten Wahlen gab es Aufsatz- und Kommentarliteratur.

Auch zu den verfassungs- und europarechtlichen Grundlagen konnte auf Standardliteratur zurückgegriffen werden.

Zur eigentlichen Aufgabe des Unterauftrags, nämlich Regelungen zu Wahldiensteanbietern, deren Zulassung und Überprüfung, sowie zu Änderungen der Wahlvorschriften für Betriebsrats- und Sozialversicherungswahlen zu entwerfen, gab es jedoch keine Vorarbeiten. Hierzu musste wissenschaftliches Neuland betreten werden.

## 1.5 Zusammenarbeit mit anderen Stellen

Mit den anderen Beteiligten des Projekts „voteremote“ gab es eine intensive Zusammenarbeit.

Das betrifft zum einen T-Systems, nicht nur in der Funktion der Projektleitung, sondern auch als Entwickler von Software für das Wahlsystem sowie als potentieller Anbieter von Wahldienstleistungen. Schließlich konnte T-Systems auch seine Erfahrungen mit der Durchführung von Telemedienwahlen einbringen. Die intensive Zusammenarbeit und die Kommunikation mit T-Systems waren stets reibungslos und produktiv.

Eine enge Kooperation erfolgte vor allem mit dem Auftraggeber, der Technischen Universität Darmstadt, Fachgebiet Theoretische Informatik (Prof. Dr. Johannes Buchmann). Diese betraf vor allem die Aufgaben und das Sicherheitskonzept des

Wahldiensteanbieters und damit die Erarbeitung der Voraussetzungen für eine Akkreditierung von Wahldiensteanbietern.

Eine Abstimmung hinsichtlich der Anforderungen an Wahldiensteanbieter und die Anforderungen an Telemedienwahlen für die Wahl von Betriebsräten und die Vertretungen in Sozialversicherungsträgern erfolgte auch mit Vertreterinnen und Vertretern des Bundesministeriums für Arbeit und Soziales, des Bundesministeriums des Innern und des Bundesministeriums für Wirtschaft und Technologie.

Speziell für die Arbeit an der Verordnung zum Wahldiensteanbietergesetz wurde zur weiteren Unterstützung Herr Weinand vom BSI hinzugezogen. Auch diese Zusammenarbeit verlief sehr gut.

# 2. Eingehende Darstellung

## 2.1 Verwendung der Zuwendung und erzieltes Ergebnis

Die Zuwendung für die Durchführung des Unterauftrags wurde wie beantragt verausgabt. Die Arbeitspakete wurden in der Weise bearbeitet, wie sie jeweils im Antrag für die erste und die zweiten Phase beschrieben worden waren. Die wesentlichen Schritte und Ergebnisse werden im Folgenden dargestellt:

In der ersten Phase wurden die folgenden Arbeitspakete bearbeitet:

AP 1: Konzipierung eines Regelungsrahmens für Wahldiensteanbieter

Die Durchführung von Telemedienwahlen setzt aufwendige Investitionen in eine komplexe Technik und eine besondere Fachkompetenz für ihren Einsatz voraus. Dies spricht für die Förderung einer Professionalisierung der Online-Wahldienstleistungen: Einerseits kann die Auslagerung von Wahldiensten an spezialisierte Diensteanbieter die Qualität der angebotenen Dienste steigern. Andererseits kann eine staatliche Kontrolle der Erfüllung der gesetzlichen Anforderungen das Vertrauen der Wahlteilnehmer und der Öffentlichkeit an die Zuverlässigkeit von Telemedienwahlen und somit ihre Akzeptanz befestigen. Aus diesen Gründen erscheint als sinnvoll, die speziellen Anforderungen an die Durchführung von Telemedienwahlen in einem neuen Gesetz – unabhängig von den bereichsspezifischen Wahlordnungen – festzulegen, das sich auf das Angebot von Wahldiensten bezieht und den Wahlausrichtern die Möglichkeit eröffnet, die Durchführung von Telemedienwahlen auszulagern (Outsourcing)

Für dieses Gesetz wurde ein Regelungsrahmen konzipiert, der für die Wahldiensteanbieter – ähnlich wie für Zertifizierungsdiensteanbieter nach dem Signaturgesetz – eine Akkreditierung vorsieht. Außerdem wurden Vorschläge für die Zielsetzung des Gesetzes, die notwendigen Definitionen, die Pflichten des Wahldiensteanbieters, die Anforderungen an technische Komponenten und Prozesse, die materiellen und prozessualen Anforderungen an ihre Prüfung und Bestätigung sowie die Kontrolle über die Wahldiensteanbieter erarbeitet. Auch wurden Regelungen zur Unterrichtung der Wahlveranstalter und der Wählenden, zur Dokumentationspflicht, zum Datenschutz und zur Haftung konzipiert. Außerdem wurden Vorgaben zur Anerkennung von Prüf- und Bestätigungsstellen sowie von ausländischen Wahldiensteanbietern entworfen. Schließlich wurden Sanktionen und der Erlass einer spezifizierenden Verordnung vorgesehen.

Dieses Konzept wurde mit den anderen Projektpartnern und mit dem Bundesministerium für Arbeit und Soziales besprochen und es wurden alternative Lösungsmöglichkeiten erörtert.

AP 2: Überprüfung des Regelungskonzepts an europarechtlichen und verfassungsrechtlichen Vorgaben

Das Gesetz darf nicht gegen europarechtliche oder verfassungsrechtliche Vorgaben verstoßen. Daher wurde untersucht, ob es Hindernisse für die Umsetzung des Konzepts im europäischen Primär- und Sekundärrecht oder im Grundgesetz gibt.

Europarechtlich waren einerseits die Vereinbarkeit einer Reglementierung und Zulassung von Wahldiensteanbietern mit der Dienstleistungsfreiheit des Vertrags für die Europäische Gemeinschaft und der Dienstleistungsrichtlinie und andererseits die Möglichkeit eines Angebots der Dienstleistungen von Wahldiensteanbietern aus allen anderen Mitgliedstaaten von Interesse. Hierzu konnte festgestellt werden, dass die Akkreditierung der Wahldiensteanbieter eine Zusatzleistung für die Auszeichnung des Angebots von Wahldiensteanbietern und keine unzulässige Beschränkung und verbotene Zulassungsgenehmigung darstellt. Sie verstößt damit weder gegen die Dienstleistungsfreiheit noch gegen die Dienstleistungsrichtlinie. Für die Anerkennung von Wahldiensteanbietern aus allen anderen Mitgliedstaaten ist eine Regelung vorgesehen, die den europarechtlichen Vorgaben entspricht.

Verfassungsrechtlich wurde vor allem die Vereinbarkeit der vorgesehenen Anforderungen mit der Berufsfreiheit der Wahldiensteanbieter und der Prüf- und Bestätigungsstellen untersucht. Sowohl die Akkreditierung und die Anforderungen an die Wahldiensteanbieter als auch die Pflichten der akkreditierten Wahldiensteanbieter sind Regelungen der Berufsausübung, die durch vernünftige Erwägungen des Allgemeinwohls gerechtfertigt werden können. Das Gleiche gilt für die Anerkennung der Prüf- und Bestätigungsstellen. Außerdem wurde die Gesetzgebungskompetenz des Bundes und seine Verwaltungskompetenz als Aufsichtsbehörde untersucht und bejaht.

Das AP 2 führt somit zu dem Ergebnis, dass die Umsetzung des in AP 1 erarbeiteten Konzepts weder gegen Europarecht noch gegen Verfassungsrecht verstößt.

AP 3: Erarbeitung eines Entwurfs eines Gesetzes für Wahldiensteanbieter

Auf der Grundlage des Regelungskonzepts und der europarechtlichen und verfassungsrechtlichen Prüfung wurden ein Entwurf für ein Wahldiensteanbietergesetz sowie ein Entwurf für eine allgemeine Begründung und eine besondere Begründung der einzelnen Vorschriften erarbeitet. Außerdem wurde eine Rechtsverordnung zur Konkretisierung bestimmter Anforderungen konzipiert. Die Entwürfe wurden mit den Projektpartnern und Vertreterinnen und Vertretern des Bundesministeriums für Arbeit und Soziales, des Bundesministeriums des Innern und des Bundesministeriums für Wirtschaft und Technologie ausführlich erörtert.

AP 4: Identifizierung und Bewertung von hinderlichen Wahlbestimmungen des geltenden Rechts

In Absprache mit dem Bundesministerium für Arbeit und Soziales wurden am Beispiel der Wahlen zum Betriebsrat die Bestimmungen für die Durchführung der Wahlen analysiert und dahin gehend bewertet, inwieweit sie der Durchführung elektronischer Wahlen entgegenstehen. Zuerst wurde festgestellt, dass die allgemeinen Wahlrechtsgrundsätze wei8tgehend auch für die Betriebsratwahlen gelten und bei Umstellung auf Telemedienwahlen zu beachten sind. Für die Regelungen zur Vorbereitung und Einleitung der Wahl, zur eigentlichen Wahlphase, zur Stimmauszählung und zur Bekanntgabe des Ergebnisses sowie zur Dokumentation des gesamten Wahlverfahrens wurde untersucht, welche Zielsetzung sie verfolgen und wie diese Zielsetzung – soweit sinnvoll – funktionaläquivalent in elektronischen Wahlen erreicht werden kann.

Ein besonderer Anpassungsbedarf in der Wahlordnung wurde vor allem für die Vorgaben in §§ 11 und 12 zur Ausgestaltung und zum Einsatz von Stimmzetteln und zu sonstigen Vorkehrungen, die zur Gewährleistung der Wahlrechtsgrundsätze bei der Ausübung des aktiven Wahlrechts zu treffen sind, identifiziert. Außerdem wurde vorgeschlagen in einer neuen Vorschrift für die öffentliche Stimmauszählung bei der Telemedienwahl folgende Regelungen vorzusehen: Bei der Telemedienwahl kann der Wahlvorstand beschließen, dass die öffentliche Stimmauszählung durch die Auszählung in Anwesenheit von Mitgliedern des Wahlvorstandes ersetzt wird, die selbst fachkundig sind oder sich von Sachverständigen ihrer Wahl begleiten lassen. Um jederzeit eine öffentliche Nachvollziehbarkeit der Ergebnisfindung zu gewährleisten, müssen die wesentlichen Schritte der Stimmauszählung so dokumentiert werden, dass die Auszählung nachträglich von jedem Betriebsangehörigen wiederholt werden kann. Die Vorschrift des § 16 WO zur Wahlniederschrift, in der das Ergebnis und die wesentlichen Schritte der Wahl dokumentiert werden, muss ebenfalls ergänzt werden.

Die Vorschriften zur Einreichung von Vorschlagslisten, Bekanntgabe der Wählerliste und des Wahlausschreibens sowie die Bekanntgabe des Wahlergebnisses enthalten entweder schon die Möglichkeit elektronischen Handelns oder sind so generisch gefasst, dass sie auch auf Telemedienwahlen Anwendung finden können.

Aus der Untersuchung der Wahlvorschriften konnten außerdem mehrere Gestaltungsanforderungen für eine Wahl mit „voteremote“ sowie Regelungsanforderungen für das Wahldiensteanbietergesetz abgeleitet werden.

AP 5: Konzipierung eines Regelungsrahmens für elektronische Wahlen

Zusammen mit den Untersuchungen in AP 4 wurde ein Regelungsrahmen konzipiert, der Vorschläge enthält, wie geltende Bestimmungen zu streichen, zu ändern oder zu ersetzen sind und welche neue Regelungen erforderlich sind, um den Spezifika von Telemedienwahlen gerecht zu werden. Diese Regelungen wurden – soweit möglich – technikneutral konzipiert, um auch für den Fall, dass andere Konzepte elektronischer Wahlen als „voteremote“ genutzt werden sollen, nicht für jedes neue Konzept eine Änderung der Wahlbestimmungen erforderlich ist.

AP 6: Überprüfung des Regelungskonzepts an verfassungsrechtlichen Vorgaben und Einpassung in den umgebenden einfachrechtlichen Regelungsrahmen

Sowohl die praktische Durchführung einer Betriebsratswahl als Telemedienwahl als auch die vorgesehenen Anpassungen der Wahlordnung für solche Wahlen wurden daraufhin überprüft, ob sie mit den zu beachtenden Wahlgrundsätzen vereinbar sind. Auch wurde darauf geachtet, dass die neuen oder veränderten Regelungen in den Regelungsrahmen der Wahlordnung passten. Die Wahlgrundsätze konnten eingehalten und die geänderten und neuen Regelungen in die Wahlordnung eingepasst werden.

AP 7: Erarbeitung eines Entwurfs eines Gesetzes zur Einführung elektronischer Wahlen

Auf der Grundlage mehrerer Gespräche mit dem Bundesministerium für Arbeit und Soziales wurde beschlossen, im Betriebsverfassungsgesetz selbst nur die Ergänzung des § 18 um einen neuen Absatz 2 vorzuschlagen. Nach dieser neuen Vorschrift kann der Wahlvorstand im Einvernehmen mit dem Arbeitgeber beschließen, die Betriebsratswahl als Telemedienwahl von einem akkreditierten Wahldiensteanbieter im Sinne des § 3

Absatz 1 des Wahldiensteanbietergesetzes durchführen zu lassen. Die Möglichkeit zur Stimmabgabe im Wahlraum muss erhalten bleiben, wenn die Möglichkeit der Telemedienwahl nicht allen Wählern gewährleistet ist. Diese Vorschrift wurde mit dem Wahldiensteanbietergesetz zum Entwurf für ein Artikelgesetz verbunden und in dem Gesetzentwurf auch begründet.

Außerdem wurde ein Entwurf zur Änderung der Wahlordnung zum Betriebsverfassungsgesetz samt Begründung erarbeitet, der nach § 27 WO einen neuen fünften Abschnitt: „Ergänzende Vorschriften bei Telemedienwahlen“ mit den neuen Paragraphen 28 bis 35 in die Wahlordnung einfügt.

In der zweiten Phase (April 2008 bis Oktober 2008 wurden die folgenden Arbeitspakete bearbeitet:

AP 1: Konzipierung und Überprüfung eines Regelungsrahmens für gemischt durchgeführte Wahlen

Sowohl für Betriebsrats- als auch für Sozialwahlen wurde vorgeschlagen, die Telemedienwahlen nicht als einzige Wahlform zuzulassen, sondern ersatzweise auch die Präsenzwahl oder die Briefwahl zu ermöglichen. Auch in anderen Bereichen dürfte in der Praxis der Wechsel von der Papierwahl zur Onlinewahl vielfach nicht abrupt, sondern schrittweise erfolgen. Dies setzt ein Konzept für einen Regelungsrahmen und Regelungsvorschläge für gemischte Wahlen (Papierwahlen und Onlinewahlen) voraus, bei denen die Wähler entscheiden können, ob sie mit Stimmzettel im Wahllokal oder online am Rechner abstimmen wollen. Eine solche Wahl stellt besondere Anforderungen an die Konsistenz der Wahldurchführung und des Wahlergebnisses. Ein Konzept und Regelungsvorschläge wurden erarbeitet.

AP 2: Untersuchung des Änderungsbedarfs und Vorschläge für Änderungen des Wahlrechts bei der Einführung von nicht-parlamentarischen Telemedienwahlen am Beispiel der Sozialwahlen

Nachdem in der ersten Phase in Absprache mit dem Bundesministerium für Arbeit und Soziales eine Beschränkung der Untersuchung auf Telemedienwahlen zur Wahl des Betriebsrats erfolgte, wurde in diesem Arbeitspaket am Beispiel der Sozialwahlen der Blick auf weitere nichtparlamentarische Wahlen erweitert. Diese verursachen andere Änderungs- und Anpassungsbedarfe. So unterscheiden sich Sozialwahlen beispielsweise von betrieblichen Wahlen maßgeblich dadurch, dass ein größerer Wählerkreis aus unterschiedlichen Lebenszusammenhängen eingebunden werden muss, die Nutzung von Informations- und Kommunikationstechnik dementsprechend nicht in einem betrieblichen, sondern in einem heterogenen Umfeld erfolgt und dass Brief- und nicht Präsenzwahl die Regel darstellt. Ferner können Sozialwahlen nicht von einzelnen Trägern privatautonom organisiert werden. Am Beispiel von Sozialwahlen wurden diese Unterschiede bearbeitet und untersucht, wie für Sozialwahlen die Wahlrechtsgrundsätze auch bei der Durchführung von Telemedienwahlen eingehalten werden können.

AP 3: Untersuchung und Entwurf einer Erprobungsklausel am Beispiel der Durchführung von Telemedienwahlen bei Sozialversicherungsträgern

Für die Sozialwahlen 2011 war geplant gewesen, die Wahlen zu drei Sozialversicherungsträgern in Hamburg probeweise als Telemedienwahlen durchzuführen. Hierfür sollte ein Regelungsvorschlag für eine Erprobungsklausel erarbeitet werden. Sollen Telemedienwahlen in bestimmten Bereichen tatsächlich in absehbarer Zeit durchgeführt werden, ohne dass der Gesetzgeber sich zu einer vollständigen Änderung des Wahlrechts entschließen kann, sind Erprobungsklauseln erforderlich. Im Arbeitspaket wurde untersucht, was für eine solche Erprobungsklausel zu beachten und wie diese zu gestalten ist. Der Plan zur Erprobung einer Telemedienwahl in Hamburg wurde jedoch leider nicht weiter verfolgt.

AP 4: Untersuchung und Abstimmung der in der Wahldiensteanbieterverordnung enthaltenen technischen Details

Im Mai 2008 hat das Bundesamt für Sicherheit in der Informationstechnik das Common Criteria Schutzprofil „Basissatz von Sicherheitsanforderungen an Onlinewahlprodukte“ als BSI-PP-0037 verabschiedet. Die Konkretisierung der rechtlichen Anforderungen an die Durchführung von Telemedienwahlen musste daher mit den technischen Konzepten zur Gewährleistung ausreichender Sicherheit und zur Zertifizierungen von Produkten und zur Akkreditierung der Wahldiensteanbieter abgestimmt werden. Zu diesem Zweck fanden mehrere Besprechungen zwischen T-Systems, der Technischen Universität Darmstadt, der Universität Kassel und dem Bundesamt für Sicherheit in der Informationstechnik, vertreten durch Herrn Weinand, statt, in denen immer wieder überarbeitete Entwürfe einer Wahldiensteanbieterverordnung erörtert wurde. Ergebnis dieses Arbeitspakets ist der Vorschlag einer Wahldiensteanbieterverordnung samt amtlicher Begründung.

AP 5: Schlussbericht

Als Ergebnisse des Unterauftrags liegen vollständige Entwürfe für ein Wahldiensteanbietergesetz und eine Wahldiensteanbieterverordnung mit jeweils einer amtlichen Begründung. Außerdem wurden die in 2.5 genannten Publikationen veröffentlicht. Derzeit wird zusätzlich eine Buchpublikation über die Untersuchungen und Ergebnisse der Arbeitspakete aus beiden Phasen erstellt und in Kürze beim Verlag eingereicht.

## 2.2 Notwendigkeit und Angemessenheit der geleisteten Arbeit

Die durchgeführten Arbeitspakete entsprechen den jeweils vereinbarten Unteraufträgen.

## 2.3 Verwertbarkeit der Ergebnisse

Die Entwürfe für ein Wahldiensteanbietergesetz und eine Wahldiensteanbieterverordnung mit jeweils einer amtlichen Begründung können von den zuständigen Bundesministerien unmittelbar für die Vorbereitung und Durchführung eines Gesetzgebungsprozesses übernommen werden.

Die Untersuchungen zur rechts- und verfassungskonformen Durchführung von Telemedienwahlen im nicht-parlamentarischen Bereichen können sowohl von den Entwicklern von Telemedienwahlsystemen für ihre Konzeption und Gestaltung ebenso berücksichtigt werden wie von Wahldiensteanbietern für die Durchführung von Telemedienwahlen.

## 2.4 Fortschritte bei anderen Stellen

Während der Durchführung des Unterauftrags voteremote haben sich an verschiedenen anderen Stellen Entwicklungen im Bereich elektronischer Wahlen ergeben, die für das Projekt relevant waren oder hier erwähnt werden.

Während der Laufzeit des Projekts "voteremote" wurde durch das BSI das Common Criteria Schutzprofil für einen "Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte" evaluiert und erfolgreich zertifiziert.

Während der Laufzeit des Projekts führte die Deutsche Forschungsgemeinschaft mit dem Telemediensystem Polyas des Unternehmens Micromata in Kassel die Telemedienwahlen zu den Fachkollegien durch (ca. 1.500 Wahlvorschläge und ca. 90.000 Wahlberechtigte). Prof. Roßnagel fungierte als Beauftragter des Senats der DFG für diese Wahlen.

Nach Abschluss der Arbeiten hat das Bundesverfassungsgericht am 3. März 2009 die Verwendung von Nedap-Wahlgeräten bei Wahlen zum Deutschen Bundestag für unzulässig erklärt. Dies betrifft die Arbeiten im Projekt „voteremote" nicht unmittelbar, weil es weder um Wahlgeräte noch Bundestagswahlen ging. Doch hat das Bundesverfassungsgericht den Wahlgrundsatz der Öffentlichkeit in einer bis dahin nicht mehrheitlich diskutierten Weise konkretisiert. Diese aus den Staatszielbestimmungen der Demokratie, der Republik und des Rechtsstaats abgeleiteten Vorgaben gelten nicht für Wahlen in privaten Körperschaften und haben auch nur beschränkte Geltung von Wahlen zum Betriebsrat oder zu Vertretungen der Selbstverwaltung in Sozialversicherungsträgern. Hier hat der Gesetzgeber einen großen Entscheidungsspielraum, der ihm auch erlaubt die im Unterauftrag entwickelten Vorschläge umzusetzen. Zur Einschätzung des Urteils s. den Aufsatz Buchmann, Johannes/Roßnagel, Alexander: Das Bundesverfassungsgericht und Telemedienwahlen – Zu den Auswirkungen des Urteils des Bundesverfassungsgerichts zu elektronischen Wahlgeräten für die Durchführung von „Internetwahlen" in nicht-politischen Bereichen.

## 2.5 Veröffentlichung der Ergebnisse

Ergebnisse des Unterauftrags wurden oder werden in folgenden Veröffentlichungen publiziert:

Gitter, Rotraud/Langer, Lucie/Okunick, Susanne/Opitz-Talidou, Zoi: Long-term retention in e-voting – Legal requirements and technical implementation, in: Krimmer, Robert (Hrsg.): 3rd International Conference on Electronic Voting EVOTE08 Bd. 131, Gesellschaft für Informatik, 2008 (LNI), S. 109–123.

Roßnagel, Alexander/ Gitter, Rotraud/Opitz-Talidou, Zoi: Telemedienwahlen in Vereinen, Multimedia und Recht 2009, i.E.

Buchmann, Johannes/Roßnagel, Alexander: Das Bundesverfassungsgericht und Telemedienwahlen – Zu den Auswirkungen des Urteils des Bundesverfassungsgerichts zu elektronischen Wahlgeräten für die Durchführung von „Internetwahlen" in nicht-politischen Bereichen, Juristenzeitung 2009, i.V.

Roßnagel, Alexander/ Gitter, Rotraud/Opitz-Talidou, Zoi: Telemedienwahlen – Der rechtlicheRahmen für Wahldiensteanbieter im nicht-politischen Bereich, Buchmanuskript i.V.