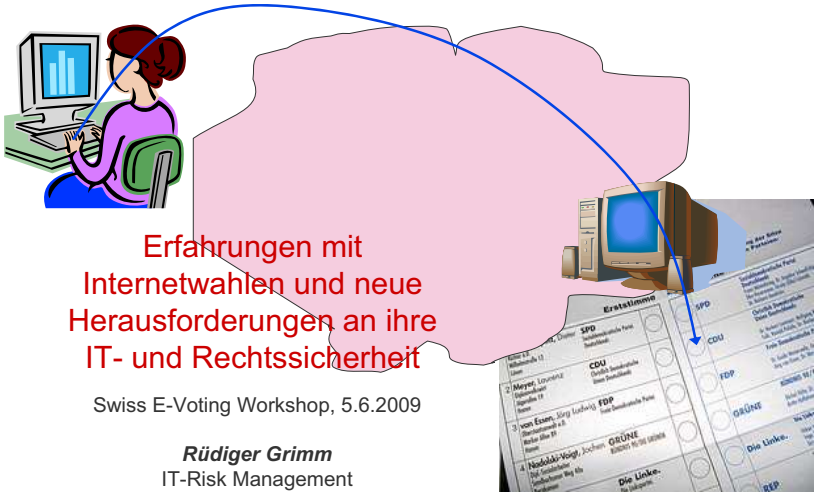


Erfahrungen mit Internetwahlen und neue Herausforderungen an ihre IT- und Rechtssicherheit

Swiss E-Voting Workshop, 5.6.2009

Rüdiger Grimm
IT-Risk Management
Universität Koblenz-Landau

Inhaltsübersicht

1. **Telekooperation im Internet**
   - Wahlen und andere Anwendungen
   - Algorithmische Ansätze
2. Interdisziplinärer Diskurs
   - Historie der GI-Wahlen
3. Requirements Engineering
   - Anforderungskataloge
   - Sicherheitsmodellierung
4. Nutzen
   - ... und Risiken
   - Offenheit
5. Was ist zu tun
   - Rechtsgemäße Gestaltung
   - KORA

E-Wahlgeräte und I-Wahlen

E-Wahlgeräte	Internet-Wahlen
– Präsenzwahl	– Alternative zur Briefwahl – Jederzeit und überall
– Wahlkabine+Urne als **ein** Terminal+Server	– Wahlkabine+Urne als **Internet Clients**+Server
– Einfache Bedienung	– Alltagsinstrument PC
– Einfache Auszählung	– Einfache Auszählung

Telekooperation

- Entfernte Kommunikationspartner
- Offenes Kommunikationsnetz
- Zielorientierte Kooperation
  - Verkaufen: Bücher, …
  - Bezahlen: C2C, Homebanking, …
  - Verabreden: Termine, Verträge, …
  - Planen: Reisen, Arbeitsabläufe u. -verteilung, …
  - Steuern: Arbeitsabläufe, Verkehrsflüsse, …

Telekooperation

- Verkaufen
  - Online Shopping
  - E-Bay
- Bezahlen
  - Homebanking
  - Paypal
- Verabreden
  - Doodle
  - Kaufvertrag
- Planen
  - Flug-, Bahntickets, Hotel, Mietwagen
  - Distributed Project Management
- Steuern
  - Network Management
  - Wide Area Traffic Control
  - Distributed Project Management

Die Entdeckung der Internet-Wahl

- David Chaum 1981/82/88/2004, v. a.
  - *Blind Signatures for Untraceable Payments. In Advances in Cryptology – Proceedings of CRYPTO '82.*
- Herausforderung für die Informatik:
  - Anonymität und Authentizität
- Algorithmische Ideen
- Prototypische Testwahlen

Algorithmische Ideen

- Blinde Signatur für doppelten Umschlag
- Aufgabenteilung zwischen Wahlliste und Urne
- Homomorphe Verschlüsselung für Einzelstimme und Stimmensummen
- Zero-Knowledge mit Zufallszahlen

- Sehr früh: neue Funktionalitäten, darunter
  - Komplexitätsreduktion (Panaschieren & Co)
  - Wählen+Informieren
  - E2E-Verifiability
  - Wahlbeobachtung

Inhaltsübersicht

1. Telekooperation im Internet
   - Wahlen und andere Anwendungen
   - Algorithmische Ansätze
2. **Interdisziplinärer Diskurs**
   - Historie der GI-Wahlen
3. Requirements Engineering
   - Anforderungskataloge
   - Sicherheitsmodellierung
4. Nutzen
   - ... und Risiken
   - Offenheit
5. Was ist zu tun
   - Rechtsgemäße Gestaltung
   - KORA

E-Wahlen sind nicht nur …

- … nicht nur Mathematik (Algorithmen) und Technik (Programmierung)
- sondern auch
  - Politische Kultur
  - Konfliktlösung
  - Beherrschbarkeit durch Menschen
  - Offenheit gegenüber den Wählern
- Recht + Informatik + Wirklichkeit
- Organisation + Technik + Akzeptanz

E-Wahlen erfordern …

- … einen interdisziplinären Diskurs
  - der Wissenschaften,
  - ihrer technischen Umsetzung
  - und ihrer Anwendungsumgebung
- In der CC-Sprache:
  - *Functional Requirements*
  - *Assurance*
  - *Trust Model of the Environment*

EU und De längst unterwegs

- Wahlen in Deutschland seit 1998:
  http://www.isl.uni-passau.de/isl-home/forschungsthemen/evoting.html
- EU Erfahrung mit politischen Online-Wahlen in
  - *Real/Pilot*: Estland, Schweiz, Niederlande (Auslandsbürger)
  - *Tests*: Österreich, Portugal, Spanien, Frankreich, Deutschland, Großbritannien
- Qualitätskriterien:
  - US Arizona Primaries 2001: Quality Criteria
  - OASIS 2005: Election Markup Language
  - Council of Europe (2004): Legal, operational and technical standards for e-voting
  - CC PP der GI/BSI/PTB/BFDI u.v.a.

Online-Wahlen in Deutschland

- Ab 1999 Feldversuche, Schattenwahlen
  - Campus Oldenburg (iVote, Otten, 1999)
  - Betriebsrat Brandenburg (2000)
  - Landrat Marburg-Biedenkopf (Diplomarbeit, 2001)
- Dez 2003: Erste elektronische Vereinswahlen der Initiative D 21
- Okt-Dez 2004-2008: Gesellschaft für Informatik
  - Fünfmal Präsidiums- und Vorstandswahl online reibungslos
  - März-April 2007: Erste Fachgruppensprecherwahl GI-FG ECOM
  - Ab 2008: Normalbetrieb in GI
- Herbst 2007: DFG-Gutachterwahl
- Jan 2008: Juniorwahl – Übungswahl zum Hessischen Landtag

GI – Gesellschaft für Informatik in Deutschland

- Dez 2003: Erste elektronische Vereinswahlen der Initiative D 21
  - GI Geschäftsführung, Cornelia Winter: „Das können wir auch!“
- Frühjahr 2004: Diskussion in Vorstand und Präsidium
  - Juni 2004: Positive Entscheidung
- Anforderungen:
  - Einfache Handhabung
  - „So sicher wie Briefwahl“
  - Entscheidung für Micromata/Polyas mit User-Id und PIN
- Juli 2004: Einsetzen eines Expertenteams
- Spätsommer 2004: Weiterentwicklung Software und Bedienbarkeit
- 2004-2007: Gültige Wahlen, aber Testbetrieb
- Ende 2007: Übernahme in Normalbetrieb

Jan 2008: „Juniorwahl“ in Hessen

Wahlbeteiligung GI 2004-2007

- ca. 20.000 Wahlberechtigte
- Briefwahlen 1999-2004
  - 10-17%
- GI Präsidium (und Vorstand, 2005)
  - Okt-Dez 2004: 4.926 Stimmen / 24,2%
  - Okt-Dez 2005: 4.112 Stimmen / 20,5%
  - Okt-Dez 2006: 4.070 Stimmen / 20,2%
  - Okt-Dez 2007: 3.603 Stimmen / 18,0%
- GI FG ECOM 2007
  - 2004: 17 (200) / 8%
  - 2007: 64 (232) / 28%

Sicherheitsbegleitung der GI-Onlinewahlen

- „GI-Expertenkreis für GI- Wahlen“ seit 2004
- Prüfung des Polyas-Wahlsystems, seit März 2005, fortlaufend
  - Interaktion mit Micromata
  - Code-Review durch GI-Mitglieder
  - Penetrationstests, BSI Juni 2006, GI FG 2006/07
  - Penetrationstests durch GI-FG SIDAR angekündigt ab Dezember 2006
- „Anforderungen an internetbasierte Vereinswahlen“, Aug 2005
- Handreichungen für Wähler, Sep 2005/Okt 2006
- CC Protection Profile, Juni 2005 – Mai 2008
  - GI-Arbeitskreis „CC PP“
  - BSI, DFKI, GI, GI-ECOM, Beirat
- GI-Arbeitskreis Onlinewahlen weiter f. aktuelle Probleme

Inhaltsübersicht

1. Telekooperation im Internet
   - Wahlen und andere Anwendungen
   - Algorithmische Ansätze
2. Interdisziplinärer Diskurs
   - Historie der GI-Wahlen
3. **Requirements Engineering**
   - Anforderungskataloge
   - Sicherheitsmodellierung
4. Nutzen
   - ... und Risiken
   - Offenheit
5. Was ist zu tun
   - Rechtsgemäße Gestaltung
   - KORA

Es geht um mehr als Integrität und Anonymität

Vorbild Bundestagswahl (GG Art. 38):

- allgemein
- unmittelbar
- frei
- gleich
- geheim

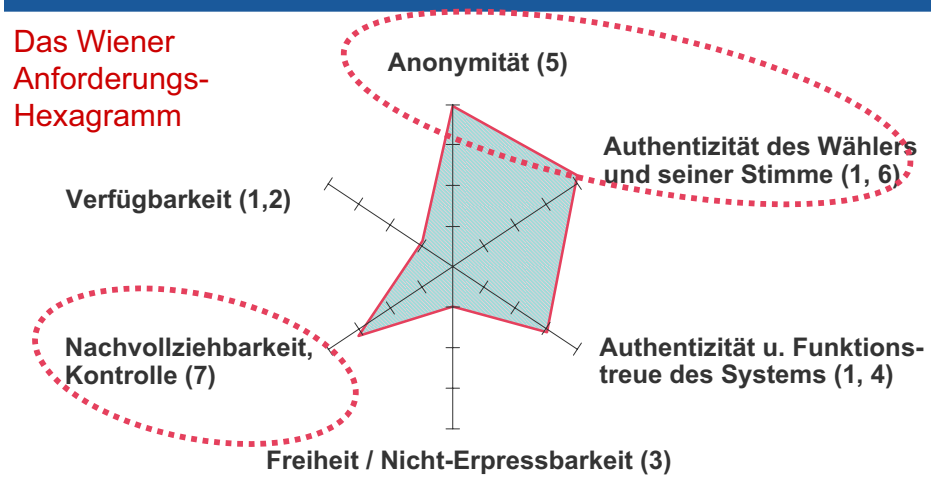
BRD, BVerG-Urteil vom 3.3.2009, GG Art. 38+Art. 20! :

- **Öffentliche Kontrolle**

Gesetzliche Anforderungen ⇒ IT Sicherheit

allgemein	**Zugang (1)**	Ausschluss
	Verfügbarkeit (2)	Sabotage/Ausfall
frei	**kein Einfluss (3)**	Stimmenkauf/Erpressung
gleich	**Funktionstreue des Systems (4)**	Manipulation d. Systems
geheim	**Anonymität Vertraulichkeit Nicht-Verknüpfb. (5)**	Aufdecken Wählerverhalten
(1)+(4)	**Fairness (6)**	Berechtigter ausgeschlossen Unberechtigter eingeschlossen Berechtigter mehr als 1x
Öffent-lichkeit	**Nachvollziehbarkeit Kontrolle (7)**	Unstimmigkeiten nicht nachvollziehbar

Das Wiener Anforderungs-Hexagramm



Nach Posser, Kofler, Krimmer, Unger (2004)

GI Anforderungskatalog

- GI-Anforderungen an Internetbasierte Vereinswahlen, 4.8.2005
- unter Verwendung von
  - PTB: Anforderungskatalog für Online-Wahlsysteme für nicht-parlamentarischen Wahlen 2004
  - Council of Europe: Recommendation of the Committee of Ministers to member states on legal, operational and technical standards for e-voting 2004
  - IEEE P 1583TM, Draft 5.0: Standard for the Evaluation of Voting Equipment 2005 (ongoing)
- Anwendung auf Polyas:
  - Micromata: Anforderungen an Internetbasierte Vereinswahlen, 10.6.2005

Anforderungskatalog (GI 2005)

A Allgemeine Anforderungen an Systementwicklung und Wahldurchführung
- Beschreibung, Analyse, Source-Code

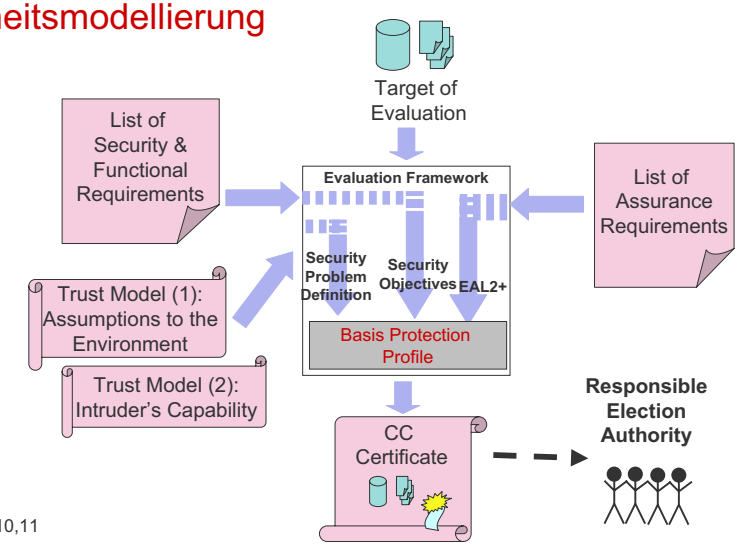
B Anforderungen an die Wahlserver
- Nachprüfbarkeit, 4-Augen-Prinzip, Aufgabenteilung

C Anforderungen an die Wahlsoftware
1. Funktionsanforderungen
2. Sicherheitsanforderungen
3. Besonders: Anonymisierung
4. Besonders: Schutz der Allgemeinheit und Gleichheit
5. Ergonomie

BSI / DFKI / GI CC Schutzprofil (GI 2008)

- Eine Wahl besteht aus drei Phasen:
  - Wahlvorbereitung,
  - Wahldurchführung inkl. der Stimmauszählung
  - und Archivierung des Online-Wahlsystems sowie der vom EVG erzeugten Daten, wie Stimmzettel und Protokolldaten
- EVG für die *Wahldurchführung* inkl. der *Stimmauszählung*
- „*Basissatz* von Sicherheitsanforderungen an Online-Wahlprodukte“
- Geeignet für Vereinswahlen (Trust Model prüfen!)
- PP-Zertifizierung Mai 2008

Sicherheitsmodellierung



Volkamer 2008,
+ IRIS-Folien #4,8,10,11

Inhaltsübersicht

1. Telekooperation im Internet
   - Wahlen und andere Anwendungen
   - Algorithmische Ansätze
2. Interdisziplinärer Diskurs
   - Historie der GI-Wahlen
3. Requirements Engineering
   - Anforderungskataloge
   - Sicherheitsmodellierung
4. **Nutzen**
   - ... und Risiken
   - Offenheit
5. Was ist zu tun
   - Rechtsgemäße Gestaltung
   - KORA

Was hat es gebracht? (GI-Wahlen)

- Zunächst wieder Erhöhung der Wahlbeteiligung
- Erstellung und Veröffentlichung eines ersten Anforderungskatalogs für elektronische Wahlen (Vorbildcharakter)
- Großes Interesse von Ministerien und Vereinen/Verbänden
- GI hat sich als Vorreiterin positioniert und Mut bewiesen
- Zusammenarbeit mit Micromata, BSI, DFKI, u.v.a.
- Fachleute tragen bei und tragen weiter
- Wiederbelebung der Diskussion ***auf der Basis einer realen Erfahrung und eines realen Systems***
- Vorbereitung des „Wahlalltags“ in den Fachbereichen und Fachgruppen der GI
- DFG übernimmt Modell

Nutzen für den Wähler (GI-Wahlen)

- Direkter Zugang zum Wahlvorgang
  - Jederzeit, überall
- Einfache Bedienbarkeit
- Schnelle, zuverlässige Auszählung
  - Klare Ergebnisdarstellung
  - Überprüfbarkeit der Integrität

Risiken für die Wähler (GI-Wahlen)

- Manipulation der Systeme
  - Open Source
  - Standardisierte Funktionen
  - Verteilte Herstellung
- Rückwirkendes Brechen der Krypto
  - Endgültige Trennung von Stimmen und Wählern
- Öffentlichkeitsprinzip nicht einfach genug
  - Sourcecode-Analyse als Expertenaufgabe
  - Kontrollfunktionen für Jedermann

Öffentliche Kontrolle (GI-Wahlen)

- GI-Wahlen als Briefwahl
  - Keine öffentliche Stimmabgabe
  - Keine öffentliche Stimmauszählung
- GI-Wahl als Internet-Wahl
  - Einladung zu Quellcode-Analysen
  - Einladung zu Penetrationstests
  - Auszählung unter Kontrolle von Informatikern und Juristen
  - Integritätskontrollen
  - Aufbewahrung der Wahlunterlagen
  - Dabei endgültige Trennung von Wählernamen und Stimmen

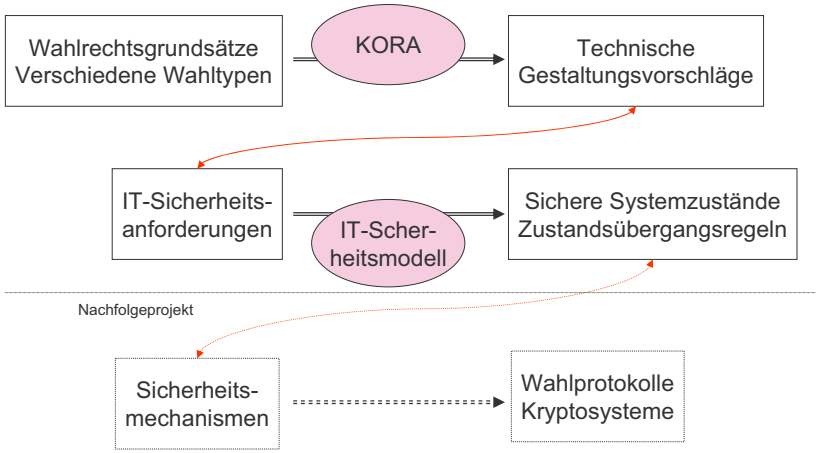
Inhaltsübersicht

1. Telekooperation im Internet
   - Wahlen und andere Anwendungen
   - Algorithmische Ansätze
2. Interdisziplinärer Diskurs
   - Historie der GI-Wahlen
3. Requirements Engineering
   - Anforderungskataloge
   - Sicherheitsmodellierung
4. Nutzen
   - ... und Risiken
   - Offenheit
5. **Was ist zu tun**
   - Rechtsgemäße Gestaltung
   - KORA

KORA – vom Recht zur Technik

- **Ko**nkretisierung **r**echtlicher **A**nforderungen zu technischen Gestaltungsvorschlägen für Informations- und Kommunikationssysteme
- Schrittweises, rückversicherndes Vorgehen
  (Roßnagel et al., 1992)
  1. Rechtsgrundsätze
  2. Rechtliche Kriterien
  3. Gestaltungsziele (*Security and Functional Requirements*)
  4. Gestaltungsvorschläge (*Specification*)
  5. Prototypische Implementierung
  6. Simulationstests

ModIWa – Modellierung von Internetwahlen
(Grimm, Roßnagel, DFG, 2009-2011)



Was ist nun zu tun?

- *Transparenz* und Vertrauen
- Öffentliche Kontrolle
- Stärkung des Wählers
- Neue Funktionen
- Wahlen, *Abstimmungen, Meinungsbildung*

- CC Schutzprofil abschließen, härten
- Zertifizierung mehrerer Systeme

- Rechtsgemäße Technikgestaltung
- Sicherheitsmodellierung

- Bauen, nutzen, lernen!

Das Öffentlichkeitsprinzip – Leitsätze des BVerfG-Urteils vom 3.3.2009

1. Der Grundsatz der Öffentlichkeit der Wahl aus Art. 38 in Verbindung mit Art. 20 Abs. 1 und Abs. 2 GG gebietet, dass alle wesentlichen Schritte der Wahl öffentlicher Überprüfbarkeit unterliegen, soweit nicht andere verfassungsrechtliche Belange eine Ausnahme rechtfertigen.

2. Beim Einsatz elektronischer Wahlgeräte müssen die wesentlichen **Schritte der Wahlhandlung und der Ergebnisermittlung** vom Bürger **zuverlässig und ohne besondere Sachkenntnis** überprüft werden können.

E2E Verifiability

- Receipt
  - Wähler erhalten Quittung
- Non-coercion
  - Quittung ist kein Beweis für den Inhalt
- Cast-as-intended
  - Wähler können feststellen, dass ihre Stimme berücksichtigt wurde
- Counted-as-cast
  - Wähler können feststellen, dass die Auszählung korrekt ist

Ben Adida and C. Andrew Neff (2006)

Zum Beispiel

- Bingo Voting (Deutschland)
- Prêt à Voter (UK)
- Punchscan (UK/US)
- ThreeBallot (Rivest, US)
- Voteremote (Deutschland, T-Systems)
- …

Vielen Dank!

Besuchen Sie uns in Koblenz

Abenteuer Informatik
25. Juni 2009

Schülerinfo-Tage
nach Verabredung

Multimedia-Kongress
4. Mai 2009
eGov-Day 2010

Literatur (1)

Grimm, Rüdiger; Reinhard, Kai; Winter, Cornelia; Witte, Jule: Erfahrungen mit Online-Wahlen für Vereinsgremien. In: Datenschutz und Datensicherheit (DuD) 2/2009, Februar 2009, Vieweg Verlag, Wiesbaden.

Richter, Dieter: Wahlgeräte in Deutschland: Eine Erwiderung. Informatikspektrum 30/6, Springer Berlin/Heidelberg, Dezember 2007, 440-443.

Volkamer, M.; und Krimmer, R.: Die Online-Wahl auf dem Weg zum Durchbruch. Informatikspektrum April 2006, S. 98-113.

Micromata: Polyas Online Voting Solutions – Online-Wahlen für Verbände und Vereine. Kassel, 2005 http://www.micromata.de/produkte/documents /polyas_broschuere_72dpi.pdf.

Posser, Kofler, Krimmer, Unger: Security Assets in E-Voting. In: Prosser, Krimmer (Eds.): Electronic Voting in Europe – Technology, Law, Politics and Society. Workshop of the ESF TED Programme, 7-9 July 2004, Bregenz. Lecture Notes in Informatics, P-47, GI, Bonn 2004, 171-180, figs. 2 and 3.

BVerfGE Urteil vom 3. März 2009, 2 BvC 3/07, 2 BvC 4/07.

Adida, B.; Neff, A.C.: Ballot Casting Assurance. In EVT '06, Proceedings of the First Usenix/ACCURATE Electronic Voting Technology Workshop, August 1st 2006, Vancouver, BC, Canada, 2006. http://www.usenix.org/events/evt06/tech/full_papers/adida/adida.pdf [13.5.2009]

Bohli, Jens-Matthias; Mueller-Quade, Joern; Roehrich, Stefan: Bingo Voting: Secure and coercion-free voting using a trusted random number generator. Cryptology ePrint Archive: Report 2007/162.

Hammer/Pordesch/Roßnagel, KORA – eine Methode zur Konkretisierung rechtlicher Anforderungen zu technischen Gestaltungsvorschlägen für Informations- und Kommunikationssysteme, Arbeitspapier 100, provet, Darmstadt, 1992.

Literatur (2)

BSI: Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte. Common Criteria Schutzprofil BSI-CC-PP-0037, Version 1.0. Autoren: Volkamer, Melanie, und Vogt, Roland. Antragsteller: GI. BSI-Zertifikat erteilt im Mai 2008. http://www.bsi.bund.de/zertifiz/zert/reporte/pp0037b.pdf.

CC/ISO (2006/2007): Common Criteria for IT Security Evaluation, 3 Parts , ISO/IEC 15408:2006. And Common Methodology for IT Security Evaluation, 1 Part . ISO/IEC 18045. Version 3.1; Release 1: Sep 2007; Release 2: Sep 2007. www.commoncriteriaportal.org and www.bsi.bund.de/cc/.

Gesellschaft für Informatik (GI, 2005): GI-Anforderungen an Internetbasierte Vereinswahlen („GI requirements for Internet based elections in non-governmental organisations"). 4. August 2005. www.gi-ev.de/fileadmin/redaktion/Wahlen/GI-Anforderungen_Vereinswahlen.pdf.

IEEE Standards Coordinating Committee 38 (SCC 38, 2005): Voting Standards. Project 1583 – Voting Equipment Standard; and Project 1622 – Electronic Data Interchange. http://grouper.ieee.org/groups/scc38/1583/index.htm.

Council of Europe (2004): Legal, operational and technical standards for e-voting. Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 and explanatory memorandum, Straßburg, 2004. https://wcd.coe.int/ViewDoc.jsp?id=778189

PTB (2004): Online-Wahlsysteme für nicht-parlamentarischen Wahlen: Anforderungskatalog. April 2004. http://www.berlin.ptb.de/8/85/LB8_5_2004_1AnfKat.pdf.

Literatur (3)

David Chaum (1981): Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Commununication of the ACM, 24(2):84–90, 1981.

David Chaum (1982): Blind Signatures for Untraceable Payments. In Advances in Cryptology – Proceedings of CRYPTO '82, pages 199–203, New York, 1982. Plenum Press.

David Chaum (1988): Elections with Unconditionally-Secret Ballots and Disruption Equivalent to Breaking RSA. In Advances in Cryptology – EUROCRYPT '88 – International Conference on the Theory and Application of CryptographicTechniques, volume 0330 of LNCS, pages 177–182, New York, 1988. Springer-Verlag.

David Chaum (2004). Secret-Ballot Receipts: True Voter-Verifiable Elections. In IEEE Security and Privacy, volume 2, pages 38–47, Los Alamitos, 2004. IEEE Computer Society.

P.Y.A. Ryan, T. Peacock (2005): Prêt à Voter: a Systems Perspective. Technical Report CS-TR 929, School of Computing Science, Newcastle University, 2005.

R. L. Rivest (2006): The ThreeBallot Voting Scheme. http://theory.csail.mit.edu/~rivest/Rivest-TheThreeBallotVotingSystem.pdf, September 2006.

S. Popoveniuc, B. Hosp (2006): An Introduction to Punchscan. IAVoSS Workshop on Trustworthy Elections (WOTE), June 2006, Cambridge, UK and VSRW 06, Washington, DC.

J.-M. Bohli; J. Mueller-Quade; S. Roehrich (2007): Bingo Voting: Secure and coercion-free voting using a trusted random number generator. Cryptology ePrint Archive: Report 2007/162.