UNIVERSITÄT KOBLENZ · LANDAU

12. Deutscher IT-Sicherheitskongress
11.Mai 2011

Der neue Personalausweis zur Authentifizierung bei elektronischen Wahlen

Katharina Bräunlich,

Andreas Kasten

Universität Koblenz-Landau

{hupfi, andreas.kasten}@uni-koblenz.de

Überblick

- Einleitung
- Komponenten der Wahlanwendung
- Funktionen des nPa
- Ablauf der Wahl
- Bedrohungen
- Fazit

Zielsetzung

- Wählerauthentifizierung bei Internetwahlen mittels des neuen Peronalausweises (nPa)
  - kein vollständiges Wahlprotokoll
  - nur Wählerauthentifizierung
  - generische und Wahlprotokoll-unabhängige Lösung

Rahmenbedingungen (1/2)

- Internetwahl für parlamentarische Wahlen
- Internetwahl zusätzlich zur Präsenzwahl (statt Briefwahl)
  - Internetwahl zeitlich vor der Präsenzwahl
  - Internetwahl gleichzeitig zur Präsenzwahl

  → Beide Szenarien sollen möglich sein

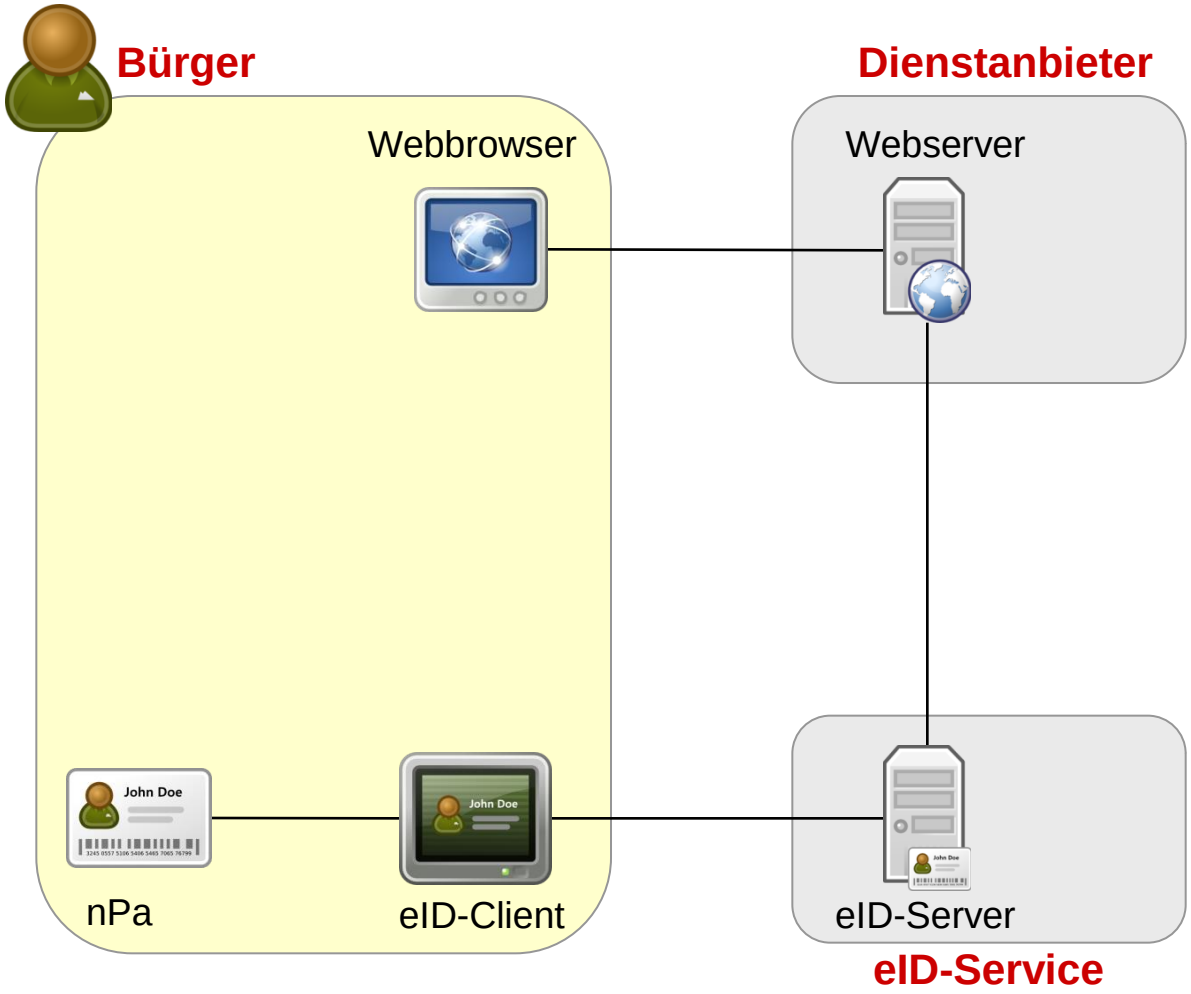
Rahmenbedingungen (2/2)

- Gleiches Berechtigungszertifikat (BZ) für beide Wahlkanäle
  - eindeutige Restricted-ID für Präsenz- und Internetwahl
  - verhindert mehrfache Stimmabgabe über unterschiedliche Wahlkanäle
  - ermöglicht die Korrektur der digitalen Stimme
- Für jede Wahl neues BZ
  - ansonsten Erfassen von Wahltendenzen möglich

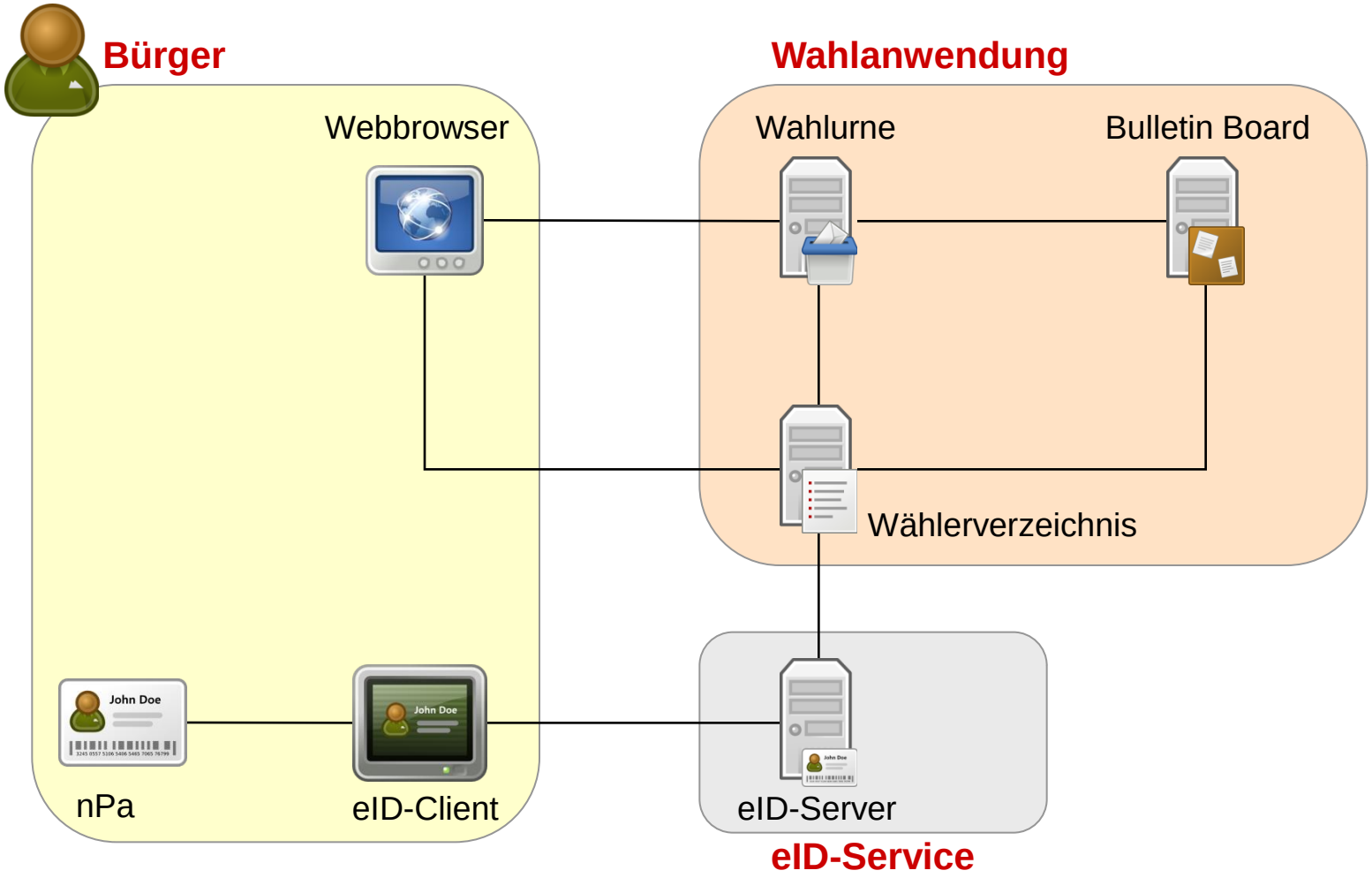
Überblick

- Einleitung
- Komponenten der Wahlanwendung
- Funktionen des nPa
- Ablauf der Wahl
- Bedrohungen
- Fazit

Komponenten bei eID



Komponenten der Wahlanwendung



Überblick

- Einleitung
- Komponenten der Wahlanwendung
- Funktionen des nPa
- Ablauf der Wahl
- Bedrohungen
- Fazit

Funktionen des nPa

- Altersverifikation
- Wohnortabfrage (Community-ID)
- Pseudonym (Restricted-ID)
  - keine statische ID
  - für jeden Dienstanbieter unterschiedlich
  - identifiziert einen Bürger für einen Dienstanbieter eindeutig
  - erlaubt keine Rückschlüsse über die Identität des Bürgers

Überprüfung der Wahlberechtigung

- Besitz des nPa

  → deutsche Staatsbürgerschaft

- Altersverifikation

  → Volljährigkeit

Ermittlung des Wahlkreises

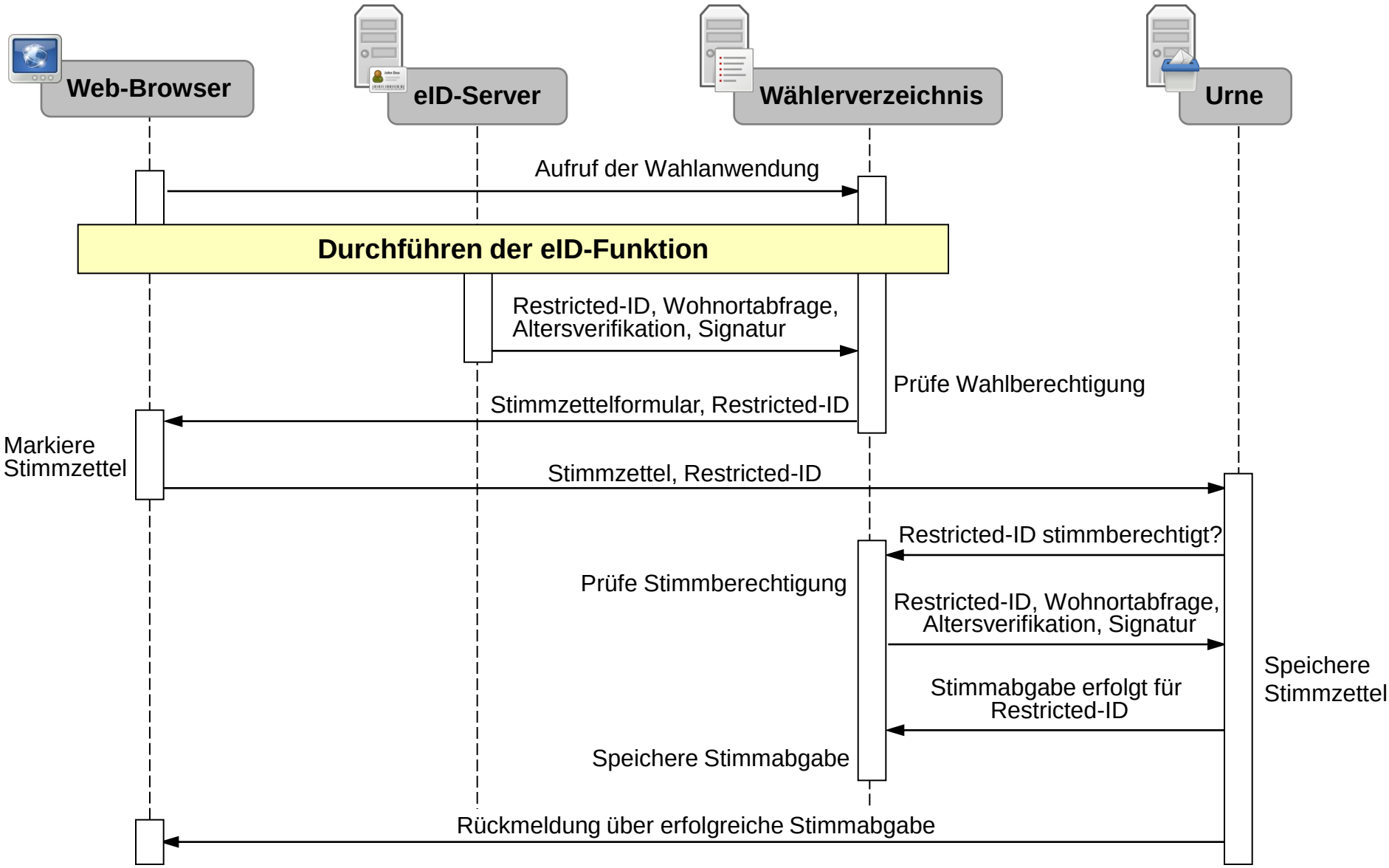
- Verwendung der Community-ID
- Problem:
  - Community-ID kann nicht direkt ausgelesen werden
- Lösung:
  - Übermittlung von Community-ID des Wahlkreises an Wähler mit Wahlbenachrichtigung
  - Eingabe von Community-ID des Wahlkreises durch Wähler
  - Abgleich mit Community-ID auf nPa

Pseudonymisierung der Wahl

- Verwendung der Restricted-ID
  - ist direkt an den nPa gebunden
  - ist für jeden Wähler eindeutig
  - erlaubt keine Rückschlüsse auf die Identität des Wählers
- Verwendung als *Sitzungsnummer*
  - Restricted-ID wird bei jeder Transaktion mit übermittelt
  - Jede Transaktion ist genau einem Wähler zuordenbar

Überblick

- Einleitung
- Komponenten der Wahlanwendung
- Funktionen des nPa
- Ablauf der Wahl
- Bedrohungen
- Fazit


Web-Browser
eID-Server
Wählerverzeichnis
Urne
Aufruf der Wahlanwendung
Durchführen der eID-Funktion
Restricted-ID, Wohnortabfrage, Altersverifikation, Signatur
Prüfe Wahlberechtigung
Stimmzettelformular, Restricted-ID
Markiere Stimmzettel
Stimmzettel, Restricted-ID
Restricted-ID stimmberechtigt?
Prüfe Stimmberechtigung
Restricted-ID, Wohnortabfrage, Altersverifikation, Signatur
Speichere Stimmzettel
Stimmabgabe erfolgt für Restricted-ID
Speichere Stimmabgabe
Rückmeldung über erfolgreiche Stimmabgabe

Überblick

- Einleitung
- Komponenten der Wahlanwendung
- Funktionen des nPa
- Ablauf der Wahl
- Bedrohungen
- Fazit

Bedrohungen der Wählerauthentifizierung

- Stimmabgabe durch Nicht-Wahlberechtigte
- Mehrfache Stimmabgabe durch Wähler
- Verweigerung des Stimmrechts
- Hinzufügen/Löschen von Stimmen

Angriffspunkte

- nPa
- eID-Server
- Urne
- Wählerverzeichnis
- Bulletin Board

Realisierbarkeit der Bedrohungen (1/2)

- Stimmabgabe durch Nicht-Wahlberechtigte 
  - Manipulation oder Fälschen des nPa 
  - Fälschen der Signatur des eID-Servers 
- Mehrfache Stimmabgabe durch Wähler 
  - mit einem nPa 
  - mit mehreren nPa 
- Verweigerung des Stimmrechts 

Realisierbarkeit der Bedrohungen (2/2)

- Hinzufügen/Löschen von Stimmen durch
  - Urne 
  - Wählerverzeichnis 
  - Urne und Wählerverzeichnis 

Überblick

- Einleitung
- Komponenten der Wahlanwendung
- Funktionen des nPa
- Ablauf der Wahl
- Bedrohungen
- Fazit

Fazit

- Konzept für Wählerauthentifizierung bei Internetwahlen mittels nPa
- Generisch, d.h. um beliebiges Wahlprotokoll erweiterbar
- Sicherheit hängt maßgeblich von Sicherheit des eID-Servers ab
- Manipulationsmöglichkeit nur wenn Urne und Wählerverzeichnis beide korrumpiert sind

Literaturverzeichnis

[Be87] Benaloh, J. D. C. (1987): *Verifiable secret-ballot elections*, Dissertation, Yale University, Department of Computer Science, Technical Report number 561.

[BSI-03110] Bundesamt für Sicherheit in der Informationstechnik (2010): *Advanced Security Mechanisms for Machine Readable Travel Documents*, Technische Richtlinie TR-03110 (v 2.03)

[BSI-03130] Bundesamt für Sicherheit in der Informationstechnik (2010): *Technische Richtlinie eID-Server*, Technische Richtlinie TR-03130 (v 1.3)

[BSI-03130-C]Bundesamt für Sicherheit in der Informationstechnik (2010): *Infrastruktur des elektronischen Personalausweises -- Anforderungen an den Betrieb von eID-Servern*, Ergänzung zu TR-03130 (v 1.1)

[BSI-03127] Bundesamt für Sicherheit in der Informationstechnik (2010): *Architektur elektronischer Personalausweis und elektronischer Aufenthaltstitel*, Technische Richtlinie TR-03127 (v 1.11)

[BSI-CM] Bundesamt für Sicherheit in der Informationstechnik: *Common Criteria Protection Profile Cryptographic Modules, Security Level "Moderate",* BSI-CC-PP-0042, Version 1.01, 31. März 2008

[BVerfG09] BVerfG, 2 BvC 3/07 vom 3.3.2009, Absatz Nr. 119.

[BWG] *Bundeswahlgesetz*, in der Fassung der Bekanntmachung vom 23. Juli 1993 (BGBl. I S. 1288, 1594), das zuletzt durch die Bekanntmachung vom 5. August 2009 (BGBl. I S. 2687) geändert worden ist, http://www.gesetze-im-internet.de/bundesrecht/bwahlg/ gesamt.pdf [eingesehen am 01.09.2010]

[BWO] *Bundeswahlordnung*, in der Fassung der Bekanntmachung vom 19. April 2002 (BGBl. I S. 1376), zuletzt geändert durch Art. 1 der Zweiten Verordnung zur Änderung der Bundeswahlordnung und der Europawahlordnung vom 3. Dezember 2008 (BGBl. I S. 2378), http://www.bundeswahlleiter.de/de/ bundestagswahlen/ downloads/ rechtsgrundlagen/bundeswahlordnung.pdf [eingesehen am 01.09.2010]

Literaturverzeichnis

[CEN-SSCD] CEN/ISSS: *Protection Profile for Secure signature creation device – Part 2: Device with key generation,* BSI-CC-PP-0059, Version 1.03, 11. Dezember 2009

[Fu08] Furgel, I. (2008): *Common Criteria Protection Profile 'Electronic Identity Card (IDCard PP)'*, BSI-CC-PP-0061, Version 1.03, 15 Dezember 2009.

[JCJ05] Juels, A.; Catalano, D.; Jakobsson, M. : Coercion-resistant electronic elections. In WPES ’05: Proceedings of the 2005 ACM workshop on Privacy in the electronic society, pages 61–70 (ACM, 2005), http://eprint.iacr.org/2002/165.pdf.

[Kr02] Krimmer, R.: e-Voting.at: Elektronische Demokratie am Beispiel der österreichischen Hochschülerschaftswahlen. Working Paper 05/2002 des Instituts für Informationsverarbeitung und -wirtschaft, 2002.

[MHEA08] Meister, G.; Hühnlein, D.; Eichholz, J.; Araujo, R. (2008): *eVoting with the European Citizen Card*. BIOSIG 2008: 67-78

[ODIHR07] Office for Democratic Institutions and Human Rights: Republic of Estonia – Parliamentary Elections – OSCE/ODIHR Election Assessment Mission Report. Technical report, Organization for Security and Co-operation in Europe (2007)

[VV08] Volkamer, M.; Vogt, R. (2008): *Common Criteria Protection Profile for Basic Set of Security Requirements for Online Voting Products*, BSI-CC-PP-0037, Version 1.0, 18. April 2008.