eVoting mit der Adder-Implementation PiVote

präsentatiert von

Stefan Thöni
Simon Rupf

piratenpartei
www.piratenpartei.ch

Inhalt

- Wer wir sind – Themen
- Wer wir sind – Struktur
- Wer wir sind – Aktivitäten
- Warum eVoting?
- Problemzonen bei eVoting
- Adder Überblick
- PiVote – Unterschiede und Gründe
- Technik – Begriffe
- Technik – Annahmen
- Technik – Zertifikate & Authoritäten
- Technik – Abstimmen & Auszählen

Wer wir sind – Themen

- Piratenpartei Schweiz, gegründet 12. Juli 2009
- Themen
  - Privatsphäre und Datenschutz
  - Transparenz des Staatswesens
  - Zensur
  - Infrastrukturmonopole und Patente
  - Open Access
  - Befreiung unserer Kultur (Urheberrecht)
  - Mediale Gewalt und Jugendschutz

Wer wir sind – Struktur

- Piratenversammlung (PV)
- Vorstand
- Regionale Stammtische (Zürich, Winterthur)
- Arbeitsgruppen (Digitale Infrastruktur)
  - Teams (eVoting)

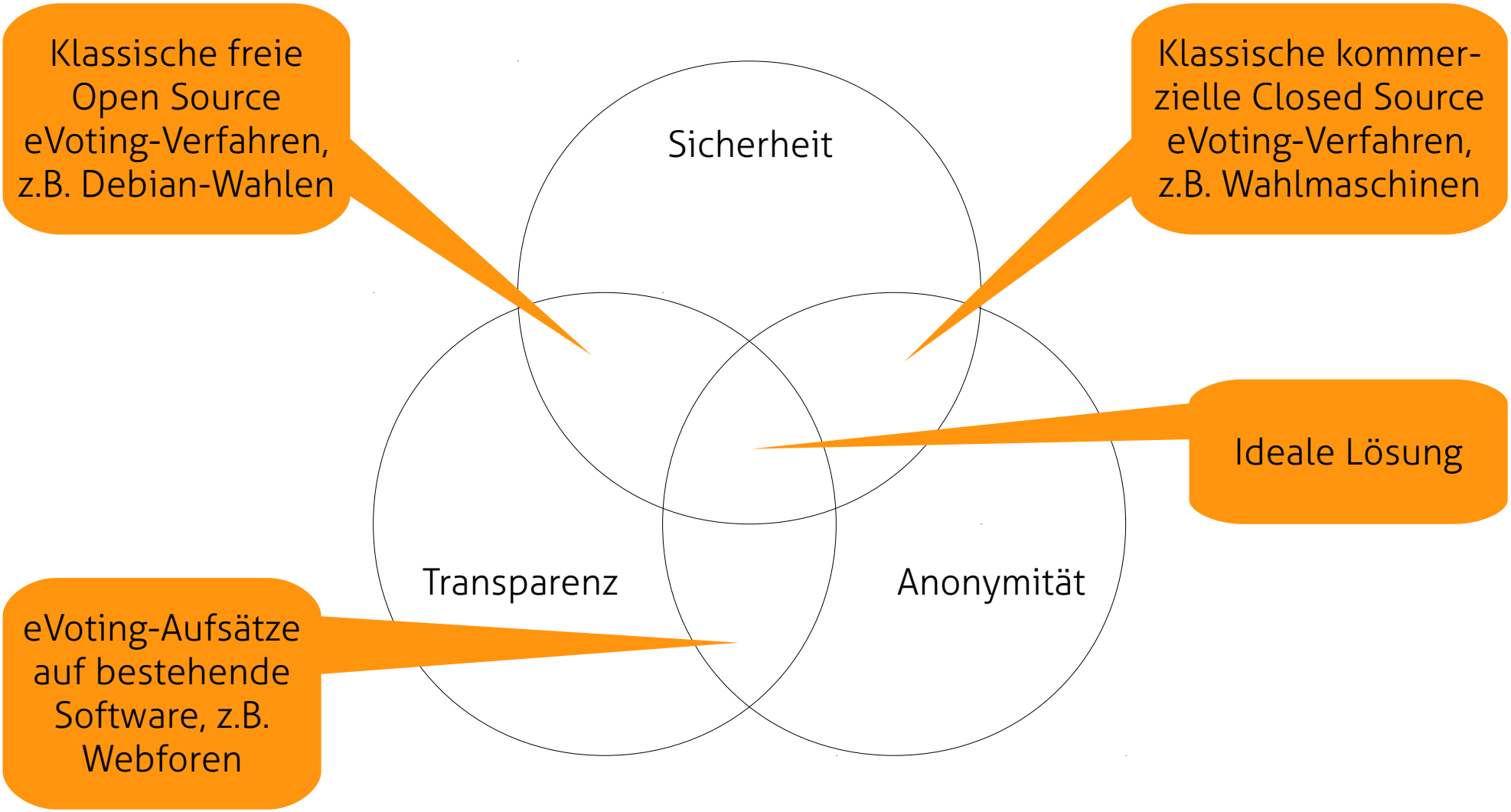
Wer wir sind – Aktivitäten

- Aktive Teilnahme an politischen Gremien
  - Grossratswahlen Kanton Bern
  - Gemeinderatswahlen Gemeinde Winterthur
  - Teilnahme an den nächsten Nationalratswahlen
- Aktivismus
  - Demo gegen Computerspieleverbot in Bern
  - AdACTA Day in Luzern
  - Vernehmlassung der BÜPF-Revision

Warum eVoting?

- Schnellere Reaktionszeit um demokratisch legitimierte Entscheidungen zu Treffen als bei einer Vollversammlung (nur 1 – 2 mal im Jahr)
- Wichtige Entscheidungen nicht alleine der Exekutive überlassen
- Sicherheit, Transparenz & Anonymität (PV entscheidet derzeit durch Handheben)

Problemzonen bei eVoting



Sicherheit, Transparenz, Anonymität – Wähle 2…

Analog der Grundregel auf de.comp.security.firewall, gilt auch für eVoting:

---

eVoting ist nicht einfach eine Software,
eVoting ist ein Konzept,
Software nur ein Teil davon.

Adder Überblick

- *Sicherheit* durch «zero knowledge proofs»
- *Anonymität* durch homomorphe Verschlüsselung
- *Transparenz* durch Veröffentlichung aller (verschlüsselten) Stimmen um jedem Benutzer das nachrechnen des Resultats zu erlauben
- Server und Qt-Client in C++ (Linux), Webclient in PHP (GUI) und Java (clientseitige Kryptographie) implementiert

PiVote – Unterschiede und Gründe

- Beruht auf dem Paper zu Adder
- Mehrsprachigkeit GUIs & Abstimmungen
- Erlaubt komplexere Abstimmungen mit mehreren Fragen zum selben Thema
- Offenes Protokoll
- Server und Client in C# implementiert, Server läuft derzeit unter Linux, Client unter Linux, Mac (Mono) & Windows (.Net)

Technik – Begriffe

- Abstimmung – Zusammenhängende Fragestellung (auch mehrere) zu einem Thema
  z.B. «Wollt Ihr ein Glace essen?», «Falls ja, welche Sorte?»
- Option – Jede Fragestellung sollte zwei oder mehr vorgegebene Antworten besitzen, wenn immer möglich auch mit einer neutralen und «ungültigen» Option
  z.B. «Ja», «Nein», «Enthaltung» oder «Vanille», «Schoko», «Egal», «Andere»
- Person – Beliebige natürliche Person, welche berechtigt ist, an der Abstimmung teilzunehmen und ein Zertifikat besitzt
- Stimme – Die Antworten auf die Frage(n) einer Abstimmung von einer Person
- Zertifikat – Mittel um Personen während der Stimmabgabe eindeutig zu identifizieren und die Kommunikation zum Server zu signieren
- Zertifizierungsstelle – Organ, welches Zertifikatsanträge auf Gültigkeit prüft
- Adminstation – Organ, welches die Abstimmungen erstellt und verwaltet
- Authorität – Organ welche die Abstimmungen auszählt und Personen identifiziert

Technik – Annahmen

- Zufall existiert
- Diskrete Logarithmen sind schwer zu berechnen
- RSA, AES und SHA sind nach den jeweiligen Anforderungen sicher
- Der Computer jedes Wählers über dessen Stimme etwas ausgesagt wird, ist frei von Malware und der Client ist nicht manipuliert worden
- Die Zertifizierungsstelle stellt nur Zertifikate für stimmberechtigte Personen aus

Technik – Zertifikate & Authoritäten

π-Vote **Piratenpartei Schweiz**

Zertifizierungsanfrage

Nachname:	Muster
Vorname:	Max
Email Adresse:	max.muster@example.o
Id des Zertifikats:	95928451-662e-4afc-87
Fingerprint des Zert	a9 7f 36 7e 9c dd de 38 1d 40 0d 7e 6c f0 88 32

Datum	Datum	Datum	Datum
Unterschrift Anfragender	Unterschrift Erste Autorität	Unterschrift Zweite Autorität	Unterschrift Dritte Autorität

□ Akzeptiert
□ Verweigert, kein Pirat
□ Verweigert, hat ein gültiges Zertifik

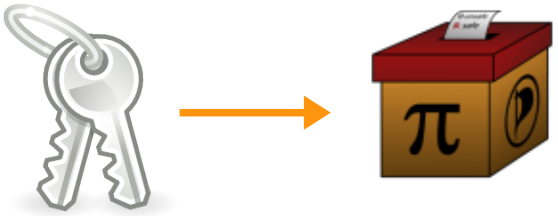
Datum

Unterschrift Zertifizierungsstelle

□ Widerrufen, vermutlich verloren
□ Widerrufen, vermutlich gestolen
□ Widerrufen, kein Pirat mehr

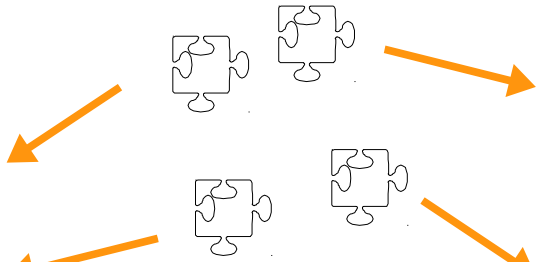
Datum

Unterschrift Zertifizierungsstelle



Öffentlicher Schlüssel

Erstellen einer neuen Abstimmung



Privater Schlüssel (verteilt)

Technik – Abstimmen & Auszählen