Urabstimmungen mit PiVote

AG DI, Team e-Voting
Stefan Thöni
Thomas Bruderer
Simon Rupf

piratenpartei
www.piratenpartei.ch

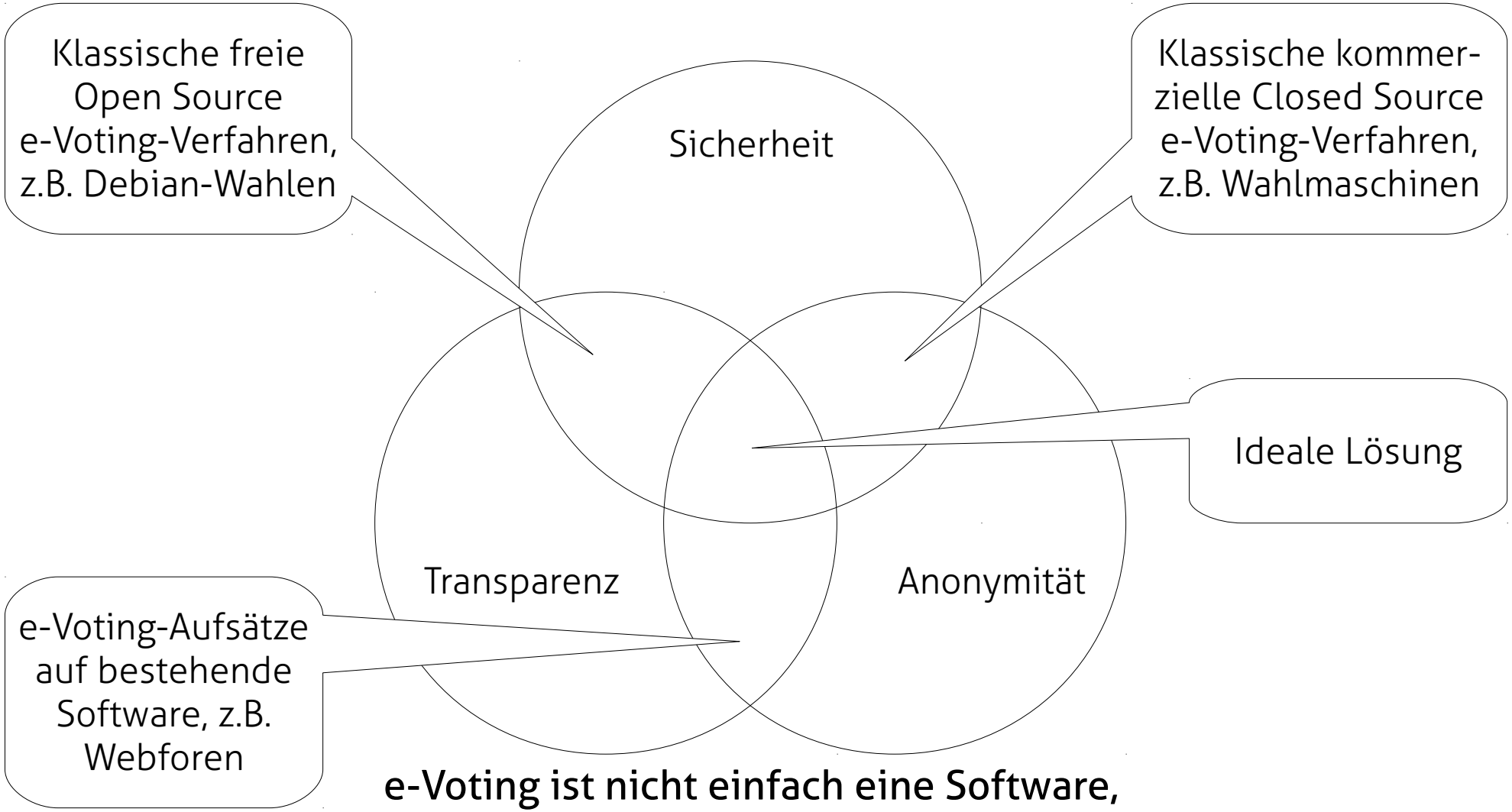
Inhalt

- Warum Urabstimmen mit PiVote?
- Problemzonen bei e-Voting
- PiVote – Überblick
- Technik – Annahmen
- Technik – Zertifikate & Authoritäten
- Technik – Abstimmen & Auszählen
- Glossar

Warum Urabstimmen mit PiVote?

- Schnellere Reaktionszeit um demokratisch legitimierte Entscheidungen zu treffen als bei Vollversammlungen (nur 1 – 2 mal im Jahr)
- Konsultationsmöglichkeit für den Vorstand
- Möglichkeit die Anzahl der Traktanden an der PV zu verringern
- Sicherheit, Transparenz & Anonymität

Problemzonen bei e-Voting



e-Voting ist nicht einfach eine Software,
e-Voting ist ein Konzept,
Software nur ein Teil davon.

PiVote – Überblick

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

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

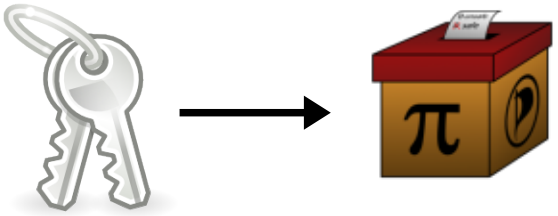
Datum

Unterschrift Zertifizierungsstelle

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

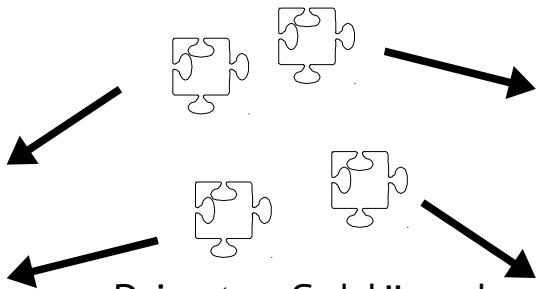
Datum

Unterschrift Zertifizierungsstelle



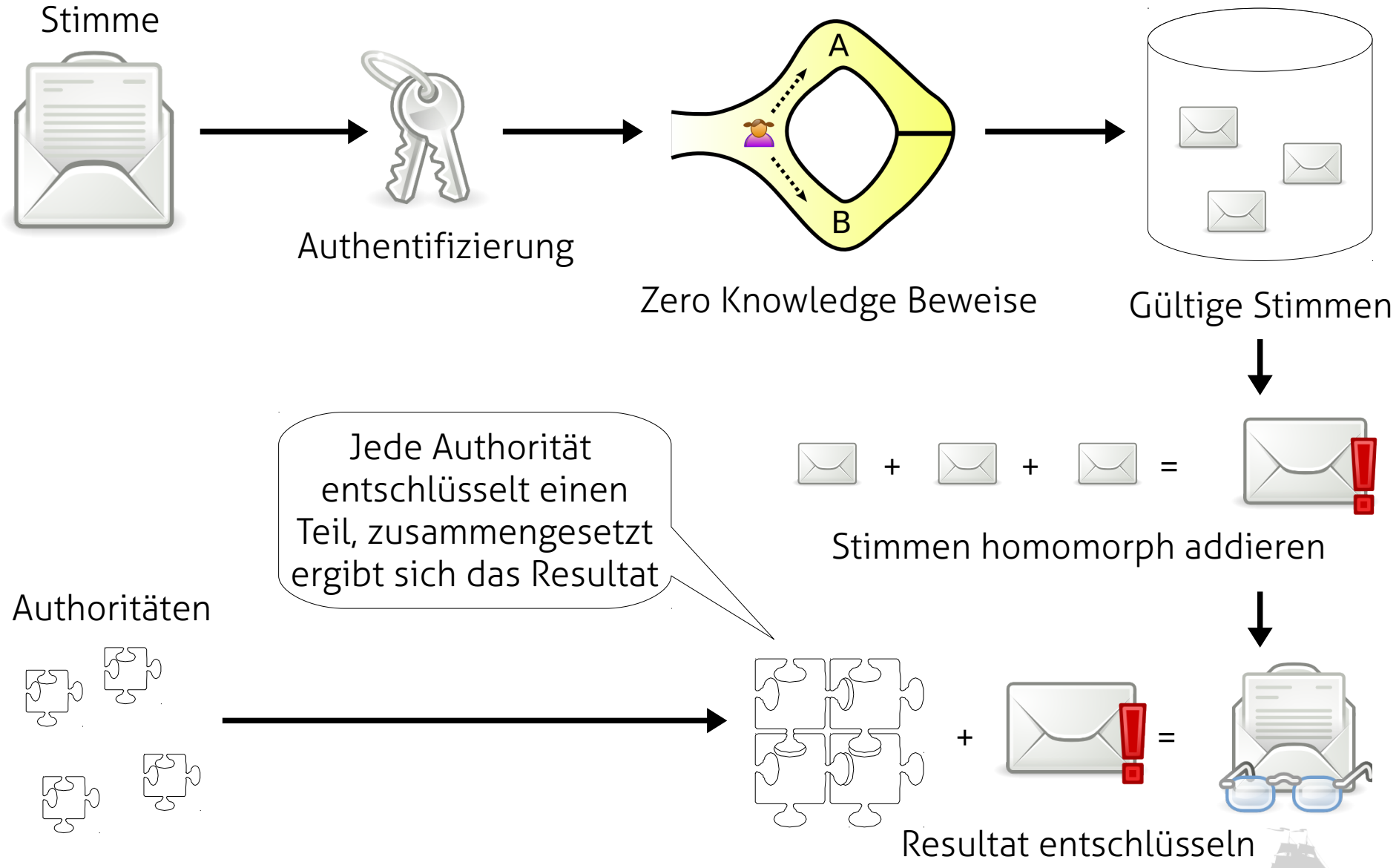
Öffentlicher Schlüssel

Erstellen einer neuen Abstimmung



Privater Schlüssel (verteilt)

Technik – Abstimmen & Auszählen



Glossar

- **Abstimmung** – Zusammenhängende Fragestellung (auch mehrere) zu einem Thema
  - «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
  - «Ja», «Nein», «Enthaltung»
  - «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