Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

„Sichere“ E-Voting-Systeme

Eric Dubuis

Image courtesy of IT Security Journal

Research Institute for Security in the Information Society

Sicherheit? (1)

SUISSE MONDE SPORTS FAITS DIVERS PEOPLE LOISIRS SOCIÉTÉ ÉCONOMIE A

Web Hard-/Software Jeux Images

Un citoyen a pu voter deux fois

INTERNET — Le système de vote électronique a permis à un électeur de voter à double ce week-end. La Chancellerie fédérale se veut rassurante, mais pour le Parti pirate, ce couac décrédibilise l'e-voting.

Par Simon Koch. Mis à jour le 12.03.2012

33 Commentaires

Recommander 9

Sicherheit? (2)

NATIONAL POST

News | Canada | Graphics | World

NEWS

Cyber attack on NDP leadership vote involved more than 10,000 computers

National Post Staff | Mar 27, 2012 12:07 PM ET | Last Updated: Mar 27, 2012 1:44 PM ET

Sicherheit? (3)

inside-it.ch

ictjobs.ch | Newsletter

Montag, 22.7.2013 / 12:22 0

Sicherheitslücke in Genfer E-Voting-Software demonstriert

Malware könnte Stimmen auf den PCs von Abstimmenden ändern, ohne dass diese etwas mitkriegen.

Wie die 'SonntagsZeitung' berichtet, hat der Genfer Sicherheitsexperte Sebastien Andrivet eine Sicherheitslücke in der E-Voting-Software gefunden, die im Kanton Genf verwendet wird. Die Schwachstelle

Vertrauen?

Misstrauen gegenüber E-Voting wächst

Für Christoph Blocher zeigt die NSA-Debatte, dass die Risiken beim elektronischen Abstimmen zu gross sind. Mit dieser Ansicht ist er nicht allein. Die Hälfte der staatspolitischen Kommission will einen vorläufigen Stopp.

Iwan Städler

«Es gibt nichts Gefährlicheres in einer Demokratie, als wenn man das Vertrauen in Abstimmungen untergräbt», mahnt Christoph Blocher. Genau dies geschehe nun mit der vom Bundesrat geplanten Einführung des E-Votings. Die NSA-Affäre zeige, wie gefährlich das elektronische Übermitteln und Speichern von Daten sei, kritisiert der SVP-Vizepräsident in einem Interview mit der «Schweiz am Sonntag». Elektronische Abstimmungen könnten manipuliert und das Stimmgeheimnis könnte kaum gewährleistet werden.

Wenn das Virus abstimmt

Nicht nur der 73-jährige Konservative, der mit Computern seine liebe Mühe hat, hegt Bedenken. Auch der 41-jährige Balthasar Glättli, der auf Twitter und Facebook aktiv ist, mahnt zur Vorsicht. Der grüne Nationalrat hat vor einem Monat eine Motion eingereicht, die den Bundesrat zum Stopp der E-Voting-Versuche zwingen will – bis das elektronische Abstimmen sicher ist. Ausnahmen möchte Glättli nur für Auslandschweizer in Ländern mit unzuverlässiger Postzustellung machen. Fast hätte die staatspolitische Kommission sein Anliegen letzte Woche in Form einer Kommissionsmotion übernommen. Laut Glättli fehlte dafür nur eine einzige Stimme. Rund die Hälfte der Kommissionsmitglieder hält die Sicherheitsbedenken also für gravierend. Grund dafür ist nebst der NSA-Affäre auch die Erkenntnis eines Genfer Hackers. Dieser hat im Sommer demonstriert, wie man aus einem Ja ein Nein machen kann, ohne dass es der Stimmende merkt.

Ein Mann rubbelt in Winterthur den E-Voting-Code auf. Foto: Keystone

Der Schwachpunkt beim E-Voting ist der Computer des Stimmbürgers. Er kann mit einem Virus infiziert sein oder beim Abstimmen auf eine falsche Website umgeleitet werden. Das weiss auch der Bund. Es gebe aber keine Hinweise auf tatsächlich erfolgte Manipulationen, relativiert die Bundeskanzlei. Sie hält daher an ihren Ausbauplänen fest und will das E-Voting – nebst der brieflichen Stimmabgabe und dem Gang zur Urne – als «dritten Kanal» etablieren.

Vor allem die Auslandschweizer sollen rasch davon profitieren – ein Grossteil bereits bei den Parlamentswahlen 2015. Später möchte der Bund alle Schweizer Stimmberechtigten vom heimischen Computer aus wählen und abstimmen lassen. Schliesslich soll auch das elektronische Sammeln von Unterschriften für Initiativen und Referenden ermöglicht werden.

Mit der NSA-Affäre sinkt nun aber das Vertrauen in die elektronische Datenübermittlung – auch bei Blochers Parteikollege Lukas Reimann. Für den St. Galler SVP-Nationalrat ist ohnehin klar: «Innerhalb der Schweiz gibt es schlicht keinen Grund für E-Voting.» Auslandschweizern möchte er dagegen die Option offen halten – sobald sie sicher ist.

Reimann hat Glättlis Vorstoss zusammen mit 31 weiteren Nationalrätinnen und Nationalräten unterschrieben. Konkret verlangt die Motion, dass alle E-Voter überprüfen können, ob ihre Stimmabgabe korrekt angekommen ist. Dies ist technisch nicht ganz einfach, da gleichzeitig das Stimmgeheimnis gewahrt bleiben muss. Darüber hinaus wird ein Offenlegen des sogenannten Quellcodes der Programme verlangt. So könnte jedermann das System auf Schwachstellen und allfällige Hintertüren für Geheimdienste überprüfen.

Bevor weitere E-Voting-Versuche stattfänden, müssten diese Bedingungen erfüllt sein, so Glättli. «Ich bin nicht prinzipiell gegen das elektronische Abstimmen, aber die Sicherheit ist mir wichtiger als die Geschwindigkeit», betont der grüne Nationalrat. Denn das Vertrauen in korrekte Wahl- und Abstimmungsresultate sei zentral.

Ist Papier wirklich besser?

«Wer garantiert denn, dass die alte Methode mit den Abstimmungszetteln manipuliersicher ist», kontert CVP-Ständerat Filippo Lombardi, der auch im Vorstand der Auslandschweizer-Organisation sitzt. SP-Vizepräsidentin Jacqueline Fehr hält die Missbrauchsgefahr beim E-Voting ebenfalls für nicht grösser als beim Papier. Die Sensibilität für die Sicherheit sei mit der Geheimdienstdebatte bestimmt nochmals gestiegen. «Aber wir sollten nicht in die Steinzeit zurückkehren und die Projekte abbrechen», so Fehr. Vielmehr müsse man die Sicherheit weiter verbessern.

Diesen Weg will auch die Bundeskanzlei beschreiten und auf Systeme setzen, bei denen die Stimmenden verifizieren können, ob ihr Ja wirklich als Ja gezählt worden ist.

NSA-Affäre

Politiker wollen Snowden befragen

Die Schweiz will zusammen mit 21 anderen Ländern in der UNO eine Resolution gegen Internetspionage und Überwachung einbringen. Dies berichtet die «SonntagsZeitung». Gefordert werden Massnahmen gegen die Überwachung von Privatpersonen besonders im Ausland sowie gegen das Eindringen in Datenspeicher, das Persönlichkeitsrechte verletzt. Parlamentarier wollen zudem eine Anhörung des NSA-Whistleblowers Edward Snowden erwirken. «Am besten wäre, die Geheimdienst-Aufsicht GPDel lädt Snowden in die Schweiz ein. Zweitbeste Lösung wäre eine Befragung in Moskau», sagt Daniel Vischer (Grüne, ZH). Auch SVP-Nationalräte unterstützen eine Anhörung Snowdens, während Carlo Sommaruga (SP, GE) Snowden in Moskau besuchen will («Bund» vom Samstag). *(bzr)*

Montag, 4. November 2013 – Der Bund

Zitat

also für gravierend. Grund dafür ist nebst der NSA-Affäre auch die Erkenntnis eines Genfer Hackers. Dieser hat im Sommer demonstriert, wie man aus einem Ja ein Nein machen kann, ohne dass es der Stimmende merkt.

Der Schwachpunkt beim E-Voting ist der Computer des Stimmbürgers. Er

Inhalt

1. Einleitung
2. Warum E-Voting?
3. Sichere E-Voting-Systeme → Vertrauen
4. Lösungsansatz
5. Offene Probleme
6. Fragen / Diskussion

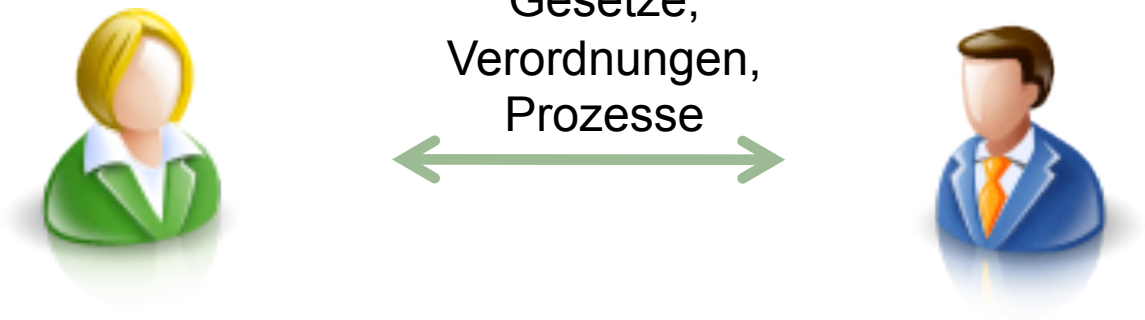
Einleitung

E-Banking – sehr vereinfacht

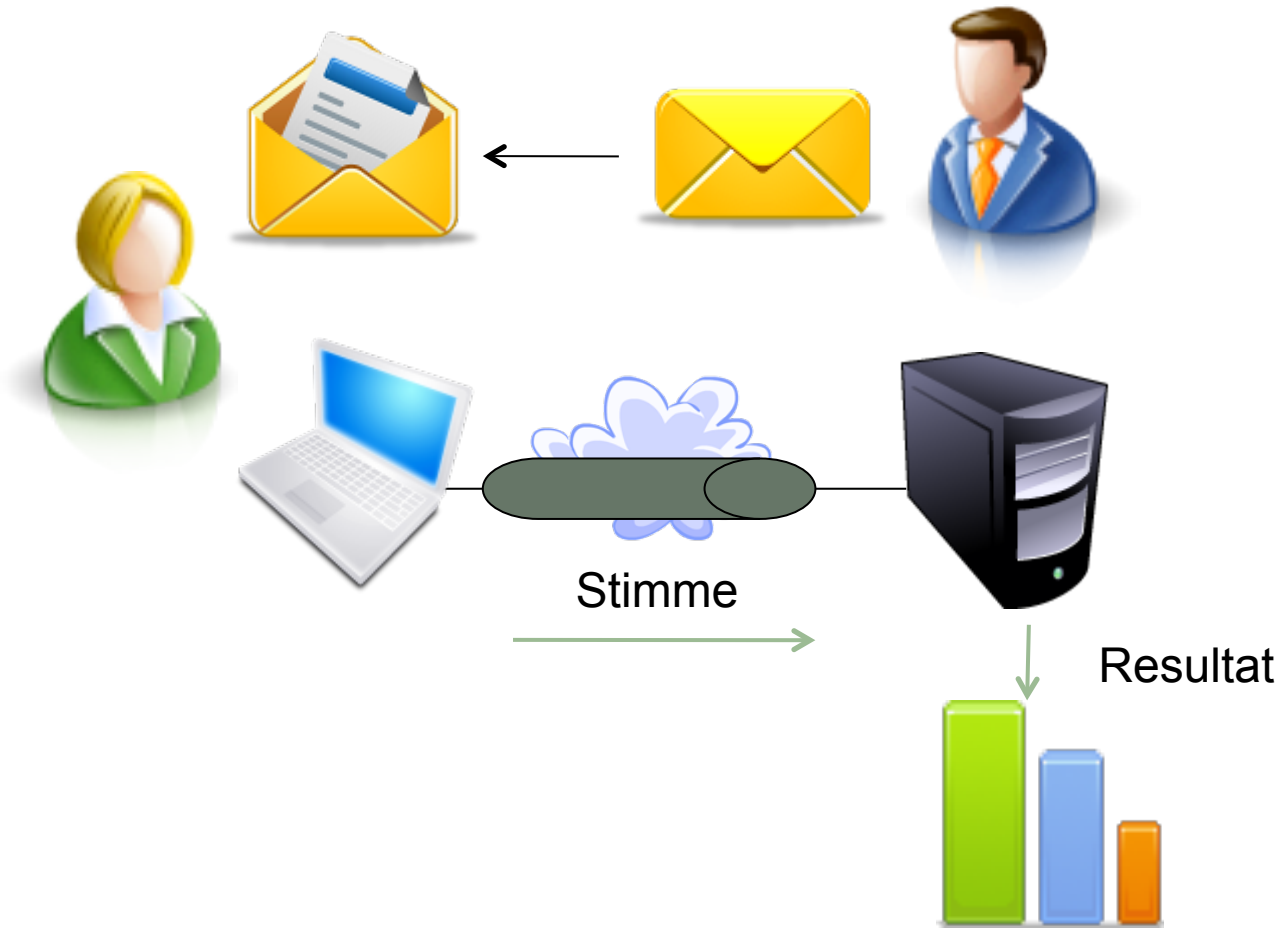
- Vertrag
- Bank kennt Kunde
- Dienste:
  - Bargeldbezug (Bancomat)
  - E-Banking (Internet)
- Die Kundin / der Kunde *verifiziert* am Ende der Abrechnungsperiode die Transaktionen

... und wie ist es bei E-Voting?

E-Voting – Bürger ↔ Verwaltung



E-Voting – vereinfacht



E-Voting – Angriffspunkte

- Eine Attacke ist dann erfolgreich, wenn ***niemand etwas merkt***…

E-Voting – als „Black Box“-System

Fragen:

- Wurde meine Stimme gezählt?
- Wurde richtig gezählt?
- Wurden nur berechtigte Stimmen gezählt?

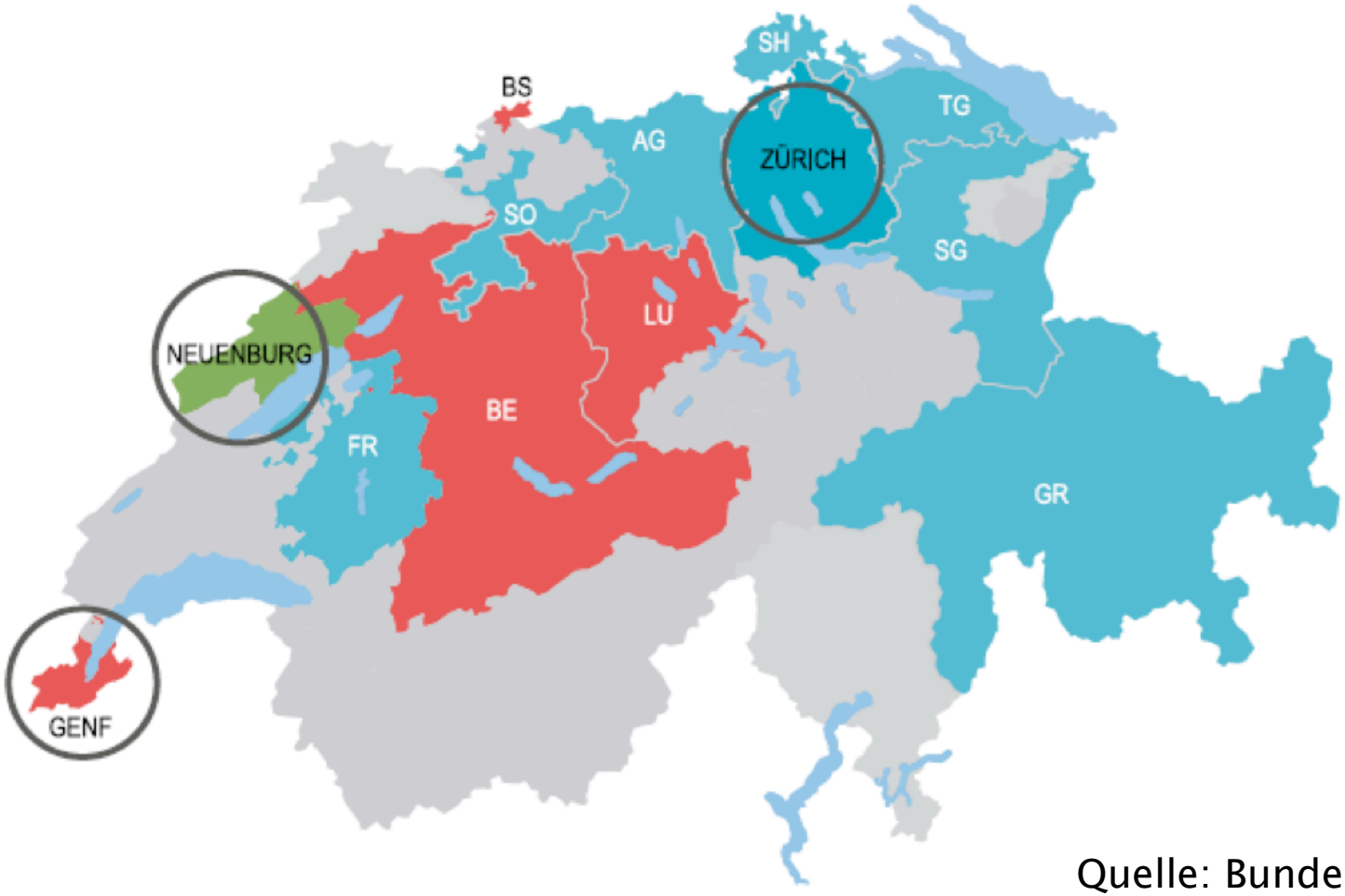
Warum E-Voting?

Warum braucht es E-Voting?

Quelle: swissinfo.ch

- Auslandschweizer (Gesetz)
- Höhere Wahlbeteiligung (Generation Y)
- Bessere Effizienz, geringere Kosten
- *Generalversammlung von juristischen Personen*

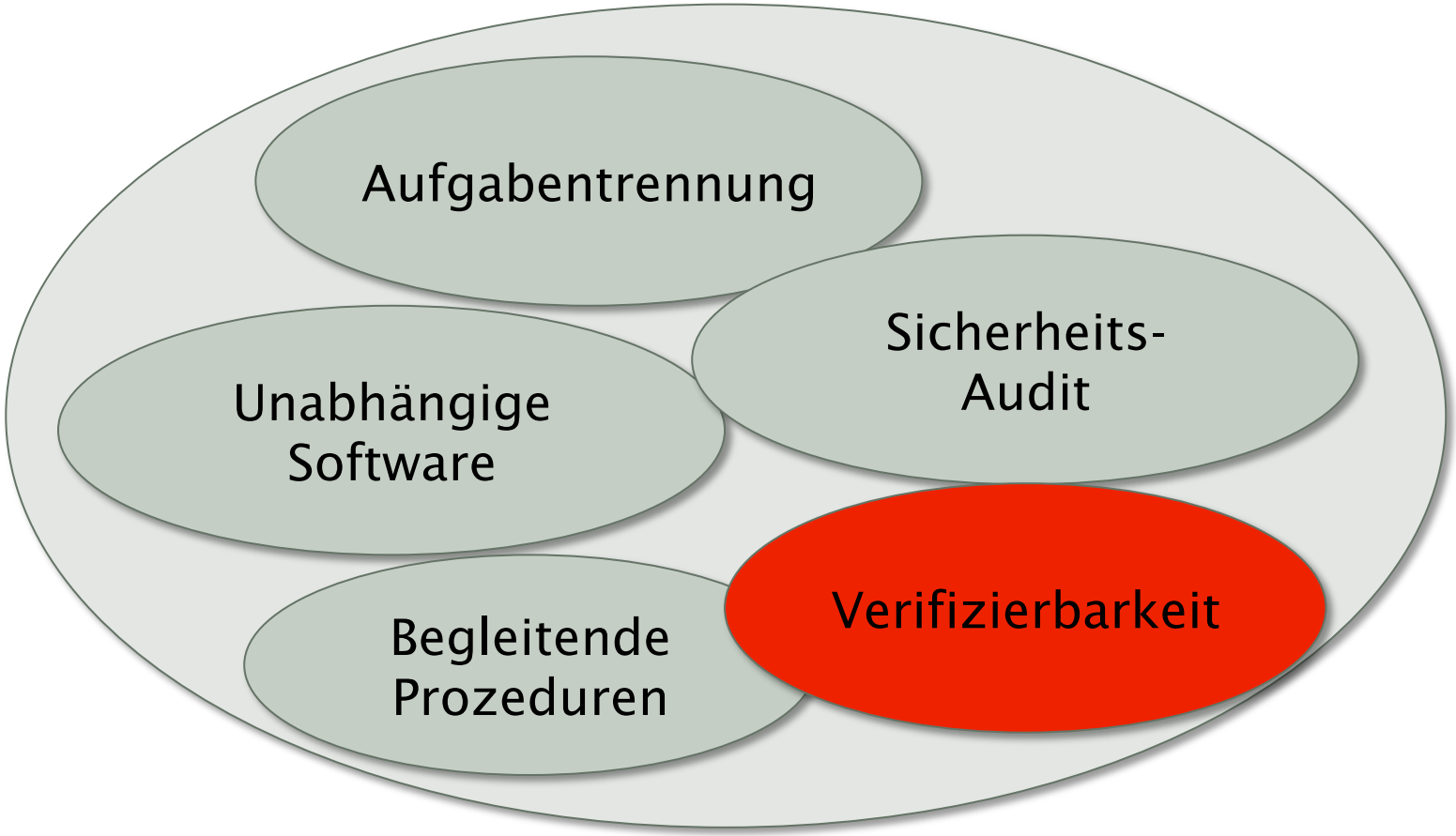
E-Voting in der Schweiz



Quelle: Bundeskanzlei

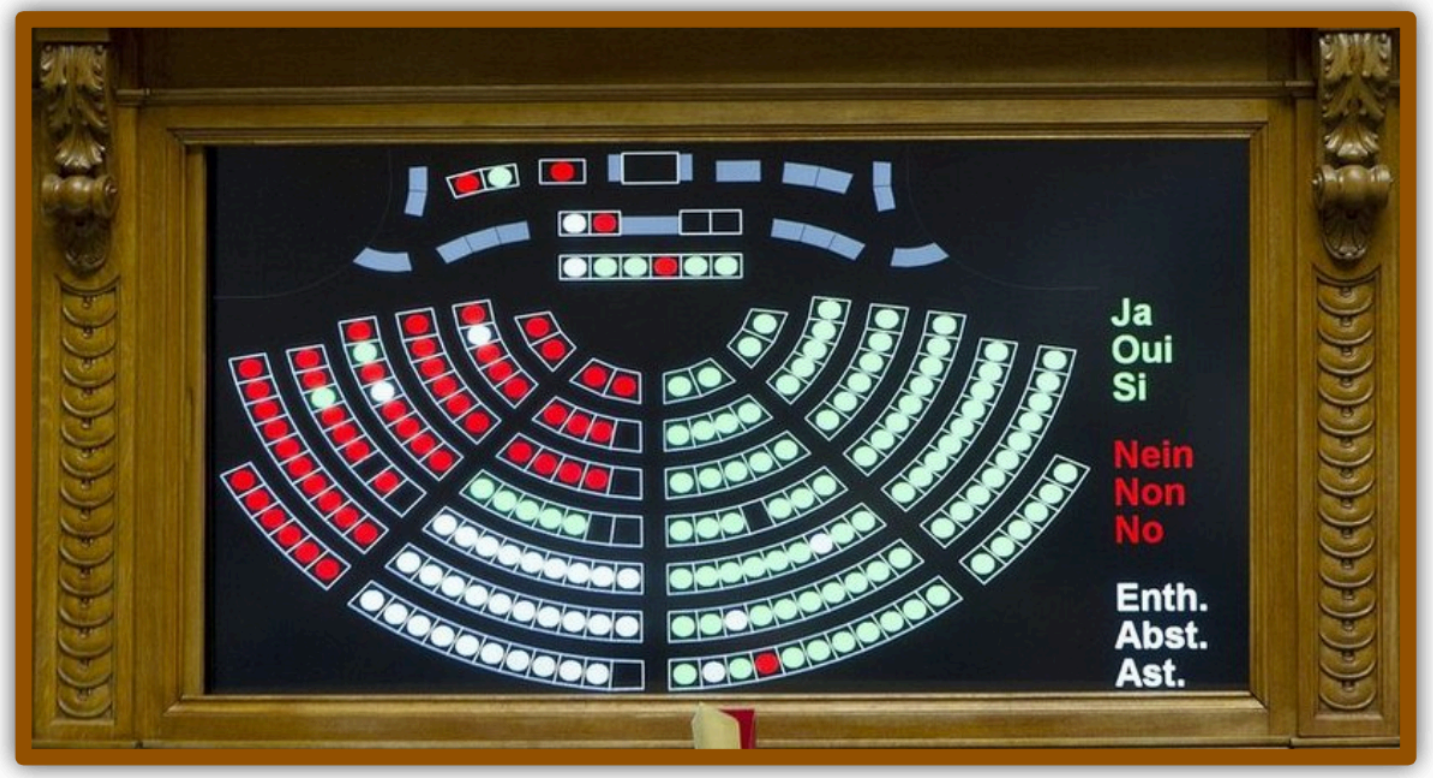
Sichere E-Voting-Systeme ➔ Vertrauen

Bildung von Vertrauen



Verifizierbarkeit

- ... kann man am besten so illustrieren



Verifizierbarkeit

- Verifizierbarkeit
  - individuelle
    Ist meine Stimme korrekt ins Ergebnis eingeflossen?
  - universelle
    Sind alle gültigen Stimmen korrekt gezählt worden?

Verifizierbarkeit – konkret angewendet

- Beispiel 1: Norwegisches System
  - Individueller Bestätigungscode
  - Schadprogramm (Hacker) kann dies nicht erraten
  - → individuelle Verifikation
- Beispiel 2: UniVote (BFH)
  - Wahldaten werden veröffentlicht
  - Öffentlichkeit kann das Wahlergebnis „nachzählen“
  - → individuelle und universelle Verifikation
- Obige Systeme sind aber nicht perfekt!

Anforderungen E-Voting

- Korrektheit des Resultats
  - Jede wahlberechtigte Person kann wählen
  - Niemand kann mehrfach wählen
  - Alle gültigen Stimmen werden gezählt
- Stimmgeheimnis und Anonymität
- Quittungsfrei
- Fairness
- Verfügbarkeit, Robustheit, Usability, Barriere frei, etc.

Lösungsansatz

Herausforderung

Entwicklung eines E-Voting-Systems mit teilweise widersprüchlichen Anforderungen:

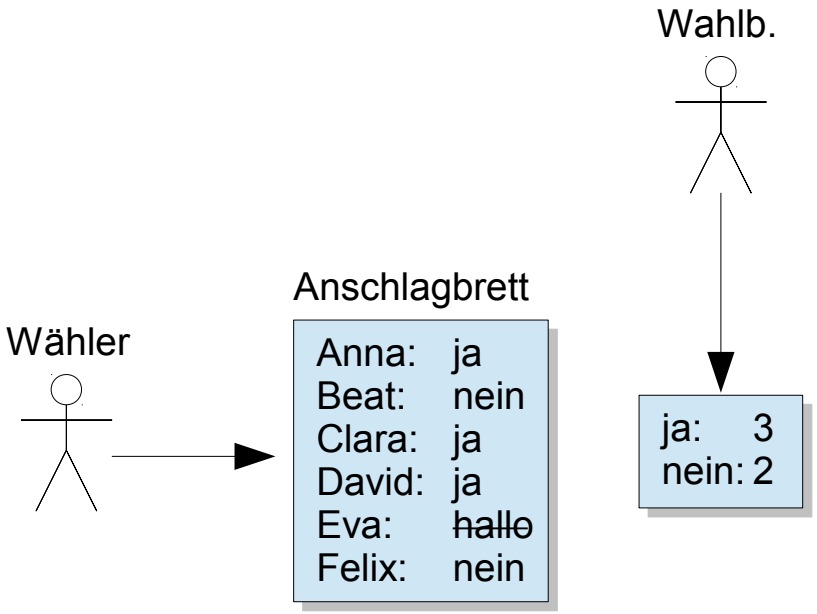
- Verifizierbarkeit ↔ Wahlgeheimnis
- Anonymität ↔ Wahlberechtigung

Kryptografische Zutaten

- Schlüssel und Zertifikate (PKI)
- Verteilte Schlüsselpaar-Erzeugung
- Digitale Signaturen (Schnorr)
- Blinde Signaturen
- Asymmetrische Verschlüsselung (El Gamal)
- Homomorphe Auszählung
- Mix-Netzwerke
- *Zero-Knowledge*-Beweise
- *Threshold*-Systeme

Idee des Anschlagbretts (1)

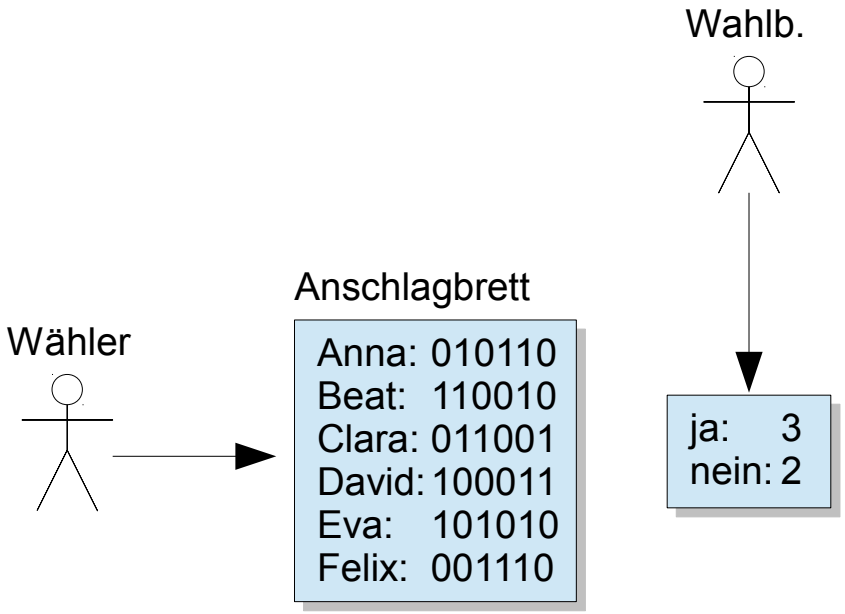
Wählende veröffentlichen ihre Stimmen



✓Ind. Verifizierbarkeit ✓Univ. Verifizierbarkeit
✗Wahlgeheimnis ✗Anonymität
✓Authentifizierung ✗Autorisierung
✓Integrität ✓Korrektheit
✗Gerechtigkeit ✗Quittungsfreiheit

Idee des Anschlagbretts (2)

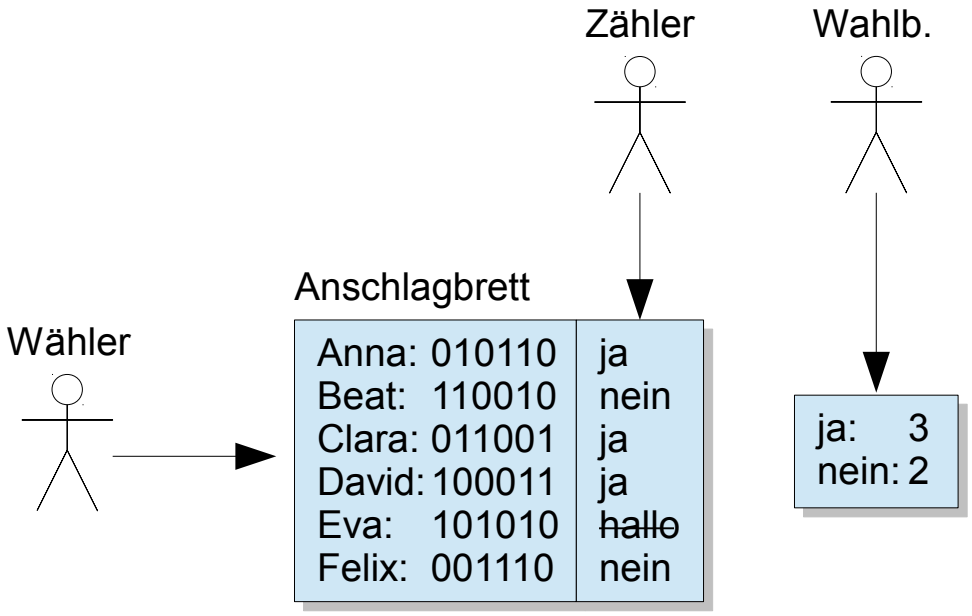
Wählende verschlüsseln ihre Stimmen



✓Ind. Verifizierbarkeit ✓Wahlgeheimnis ✓Authentifizierung ✓Integrität ✓Gerechtigkeit
✗Univ. Verifizierbarkeit ✗Anonymität ✗Autorisierung ✗Korrektheit ✗Quittungsfreiheit

Idee des Anschlagbretts (3)

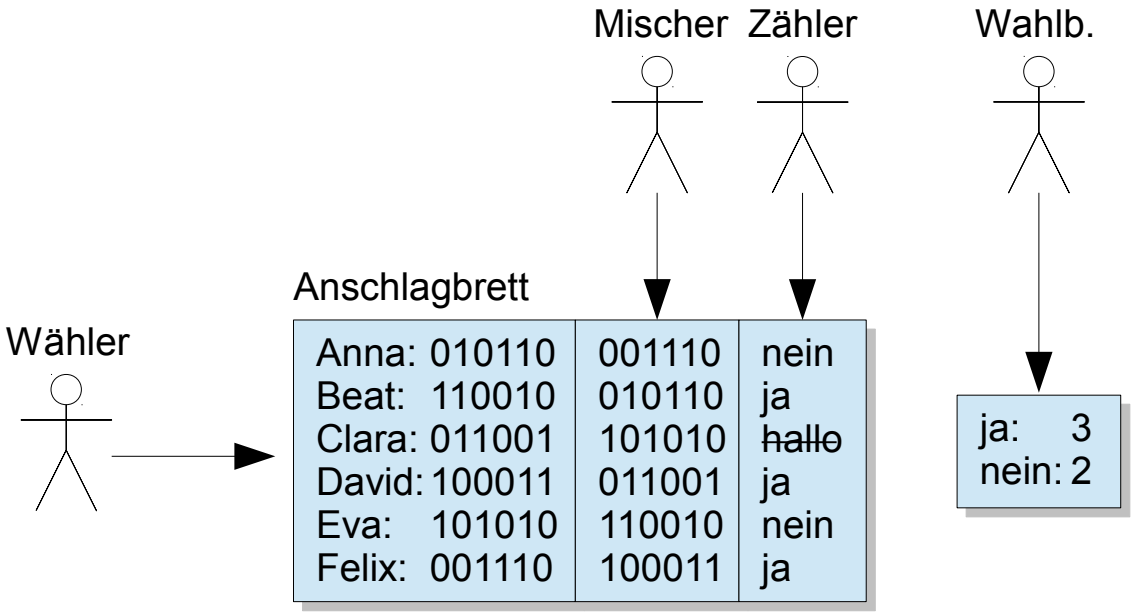
Zähler entschlüsselt Stimmen



✓Ind. Verifizierbarkeit ✓Univ. Verifizierbarkeit
✗Wahlgeheimnis ✗Anonymität
✓Authentifizierung ✗Autorisierung
✓Integrität ✓Korrektheit
✓Gerechtigkeit ✗Quittungsfreiheit

Idee des Anschlagbretts (4)

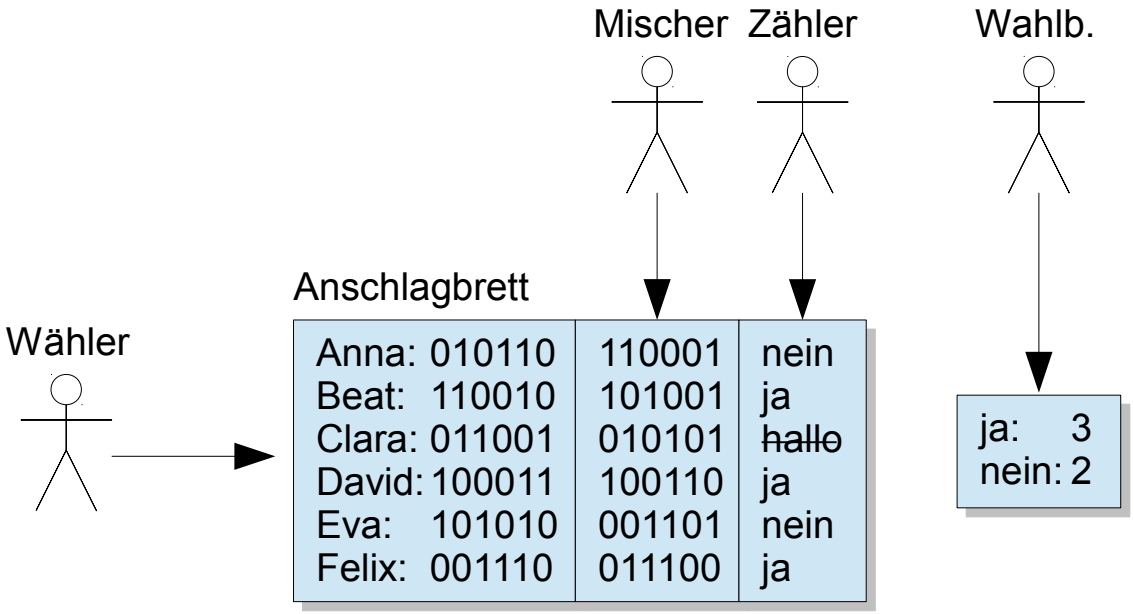
Verschlüsselte Stimmen werden gemischt



✓Ind. Verifizierbarkeit ✓Univ. Verifizierbarkeit
✗Wahlgeheimnis ✗Anonymität
✓Authentifizierung ✗Autorisierung
✓Integrität ✓Korrektheit
✓Gerechtigkeit ✗Quittungsfreiheit

Idee des Anschlagbretts (5)

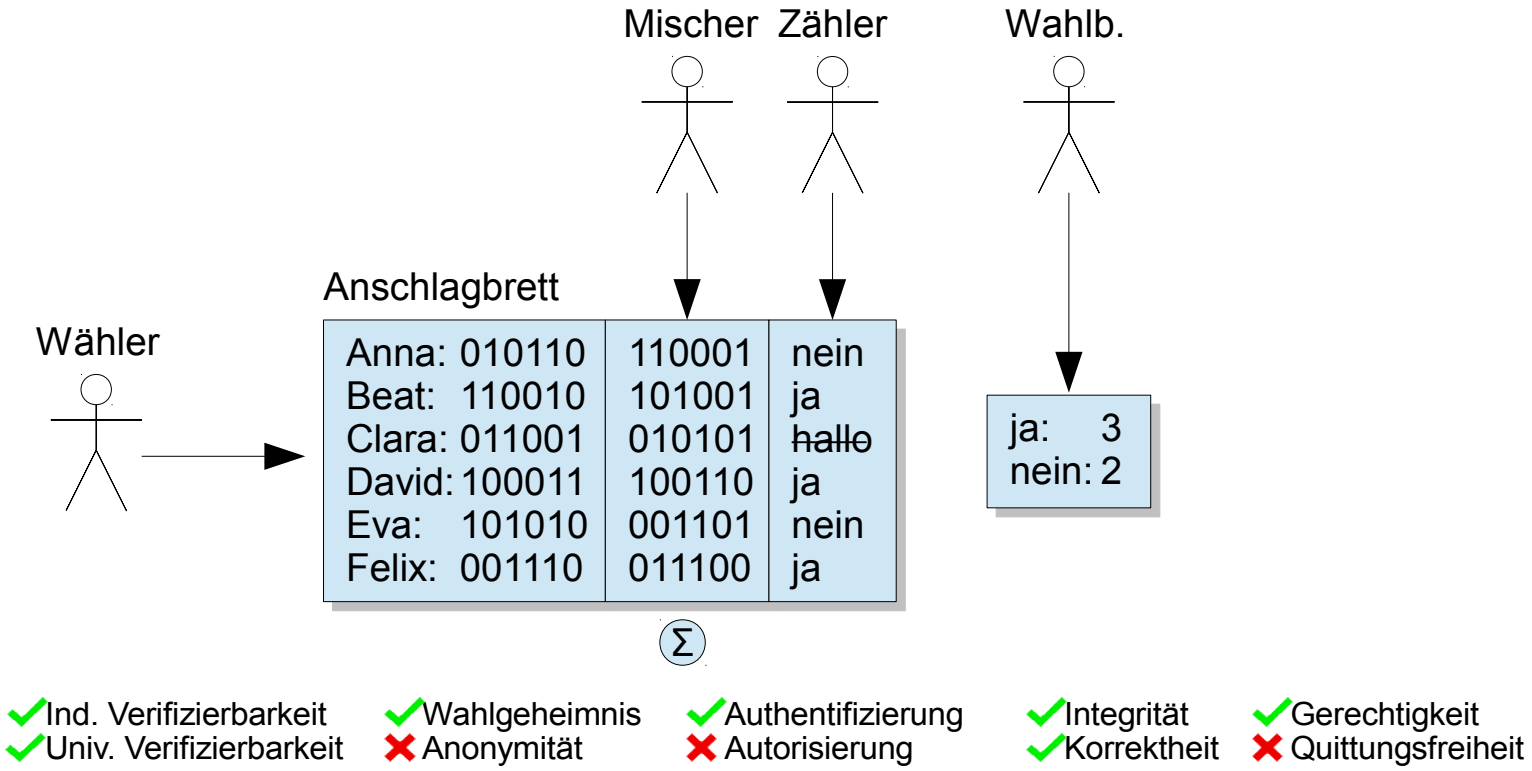
Verschlüsselte Stimmen werden kryptografisch gemischt



✓Ind. Verifizierbarkeit ✗Univ. Verifizierbarkeit
✓Wahlgeheimnis ✗Anonymität
✓Authentifizierung ✗Autorisierung
✓Integrität ✗Korrektheit
✓Gerechtigkeit ✗Quittungsfreiheit

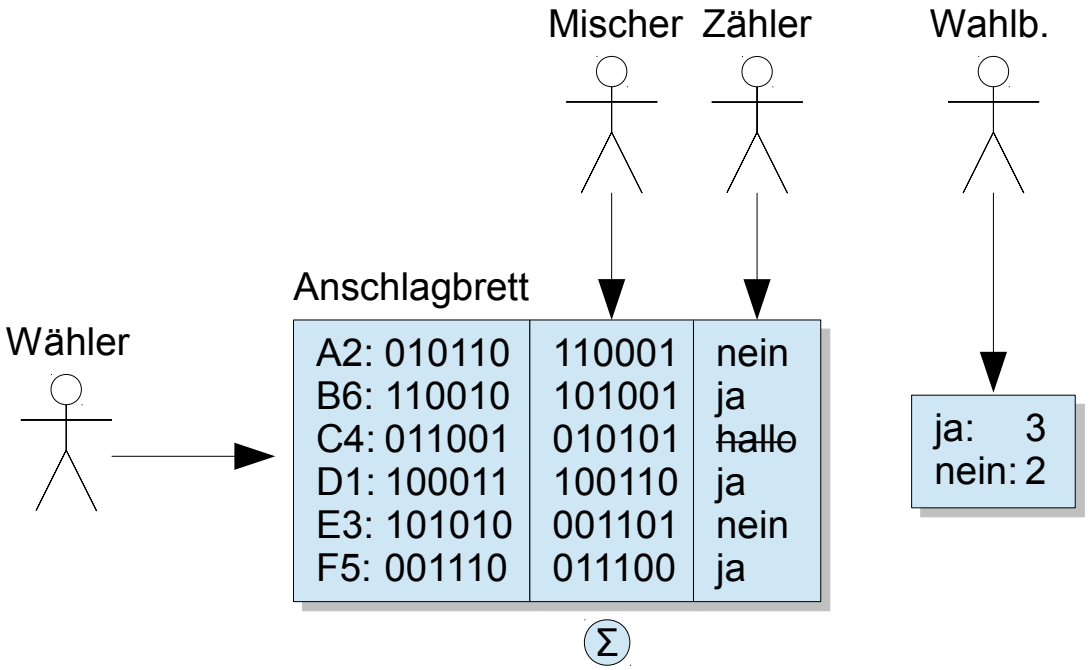
Idee des Anschlagbretts (6)

Mischer beweist die Korrektheit des Mischens



Idee des Anschlagbretts (7)

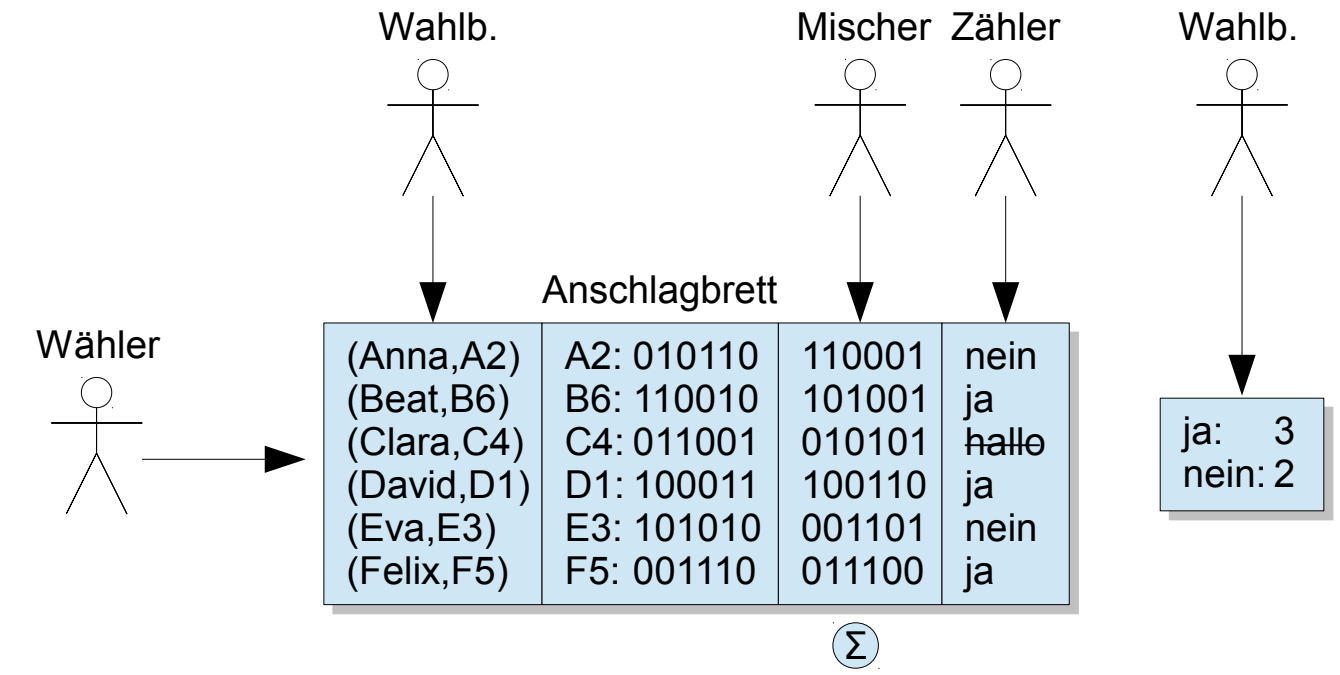
Wählende Stimmen mit einem Pseudonym ab



✓Ind. Verifizierbarkeit ✓Univ. Verifizierbarkeit ✓Wahlgeheimnis ✓Anonymität ✗Authentifizierung ✗Autorisierung ✓Integrität ✓Korrektheit ✓Gerechtigkeit ✗Quittungsfreiheit

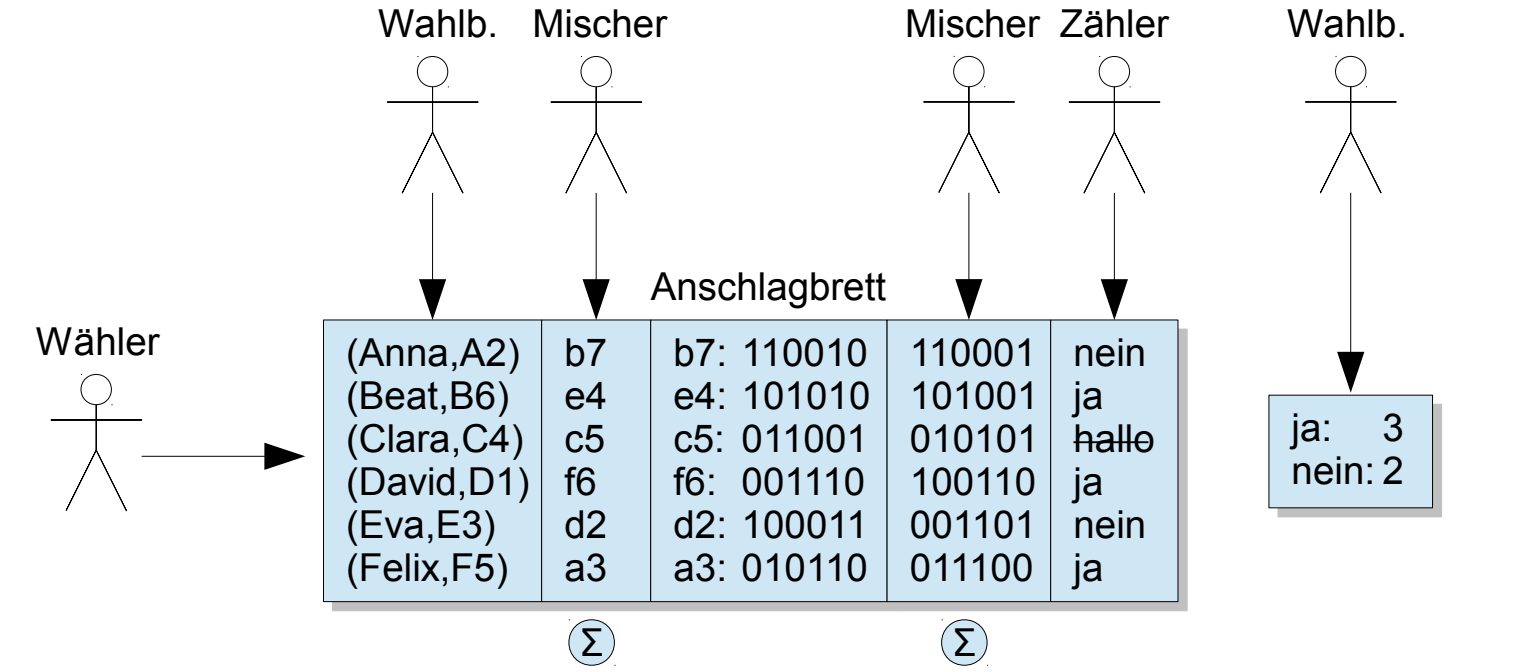
Idee des Anschlagbretts (8)

Pseudonyme werden von der Wahlbehörde zertifiziert



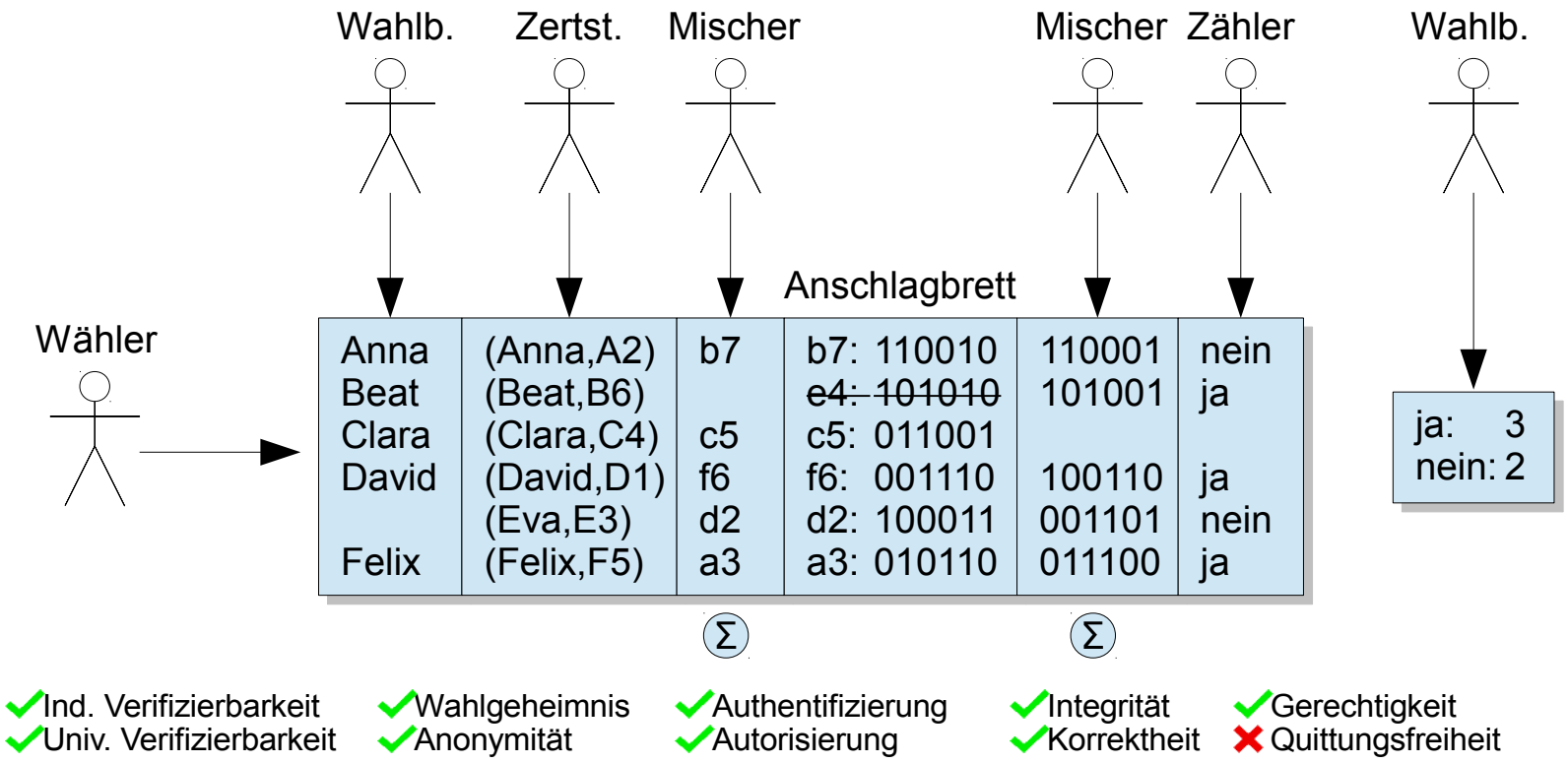
Idee des Anschlagbretts (9)

Pseudonyme werden kryptografisch gemischt

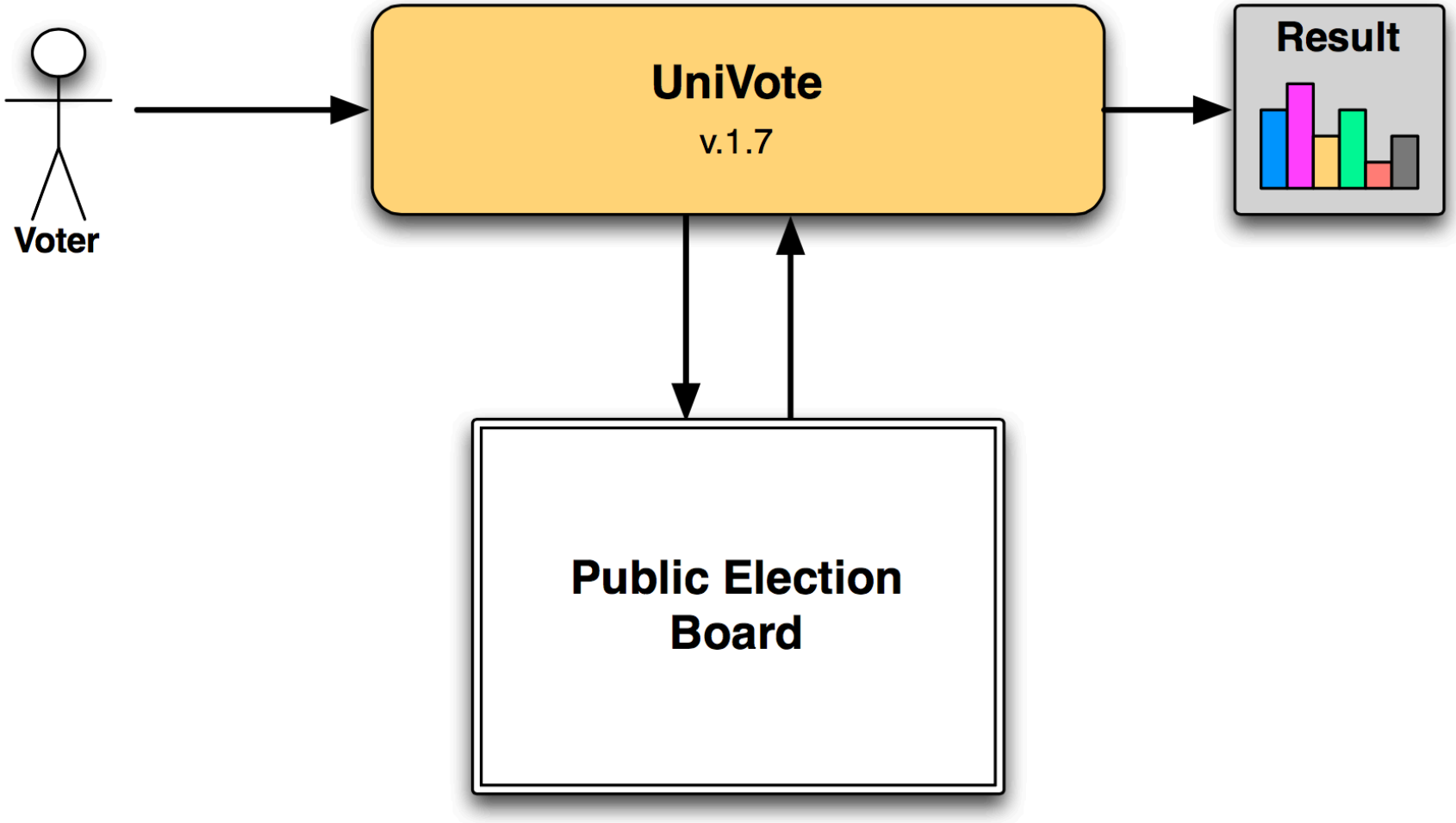


Idee des Anschlagbretts (10)

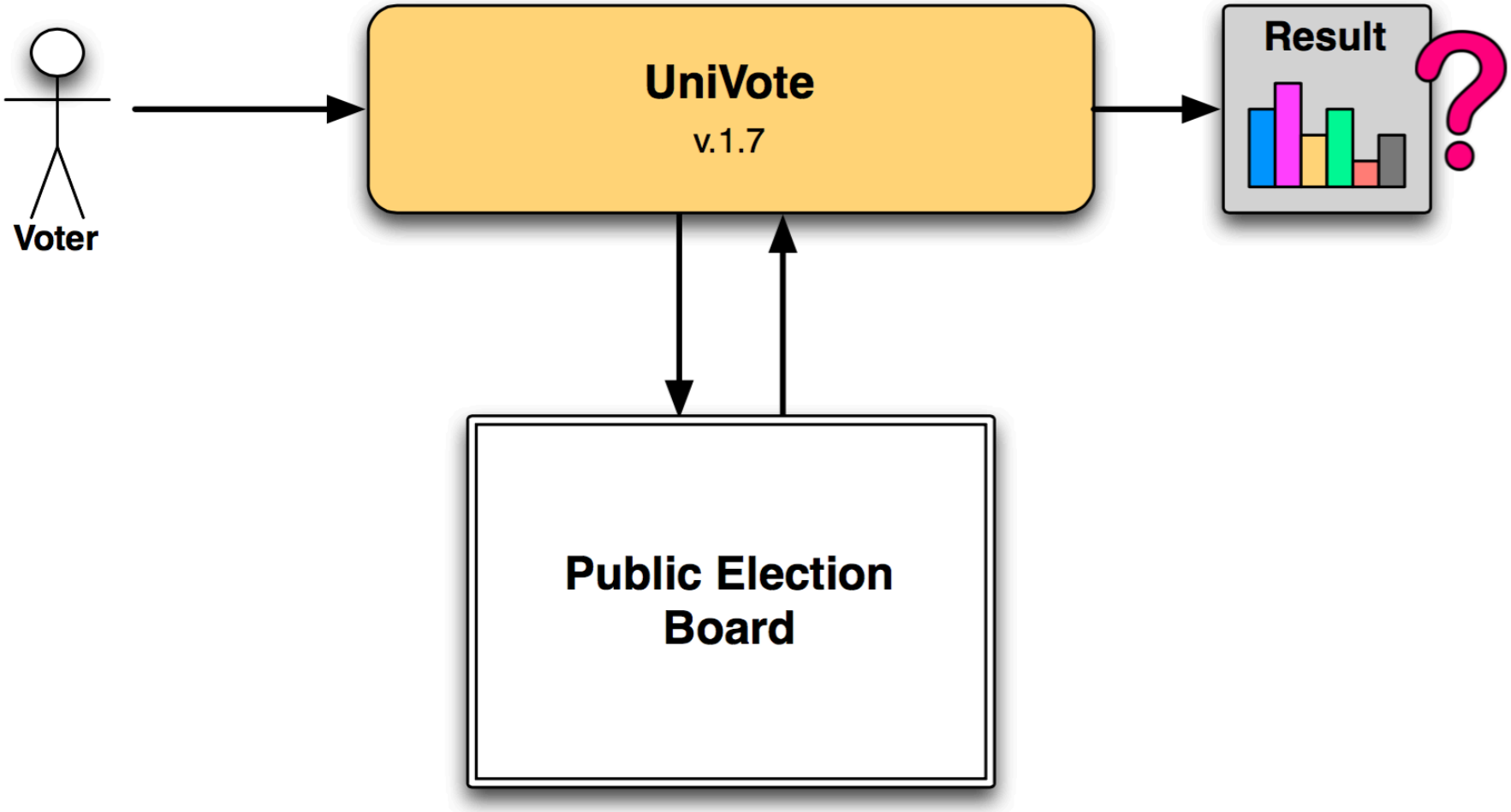
Walbehörde veröffentlicht Wählerverzeichnis



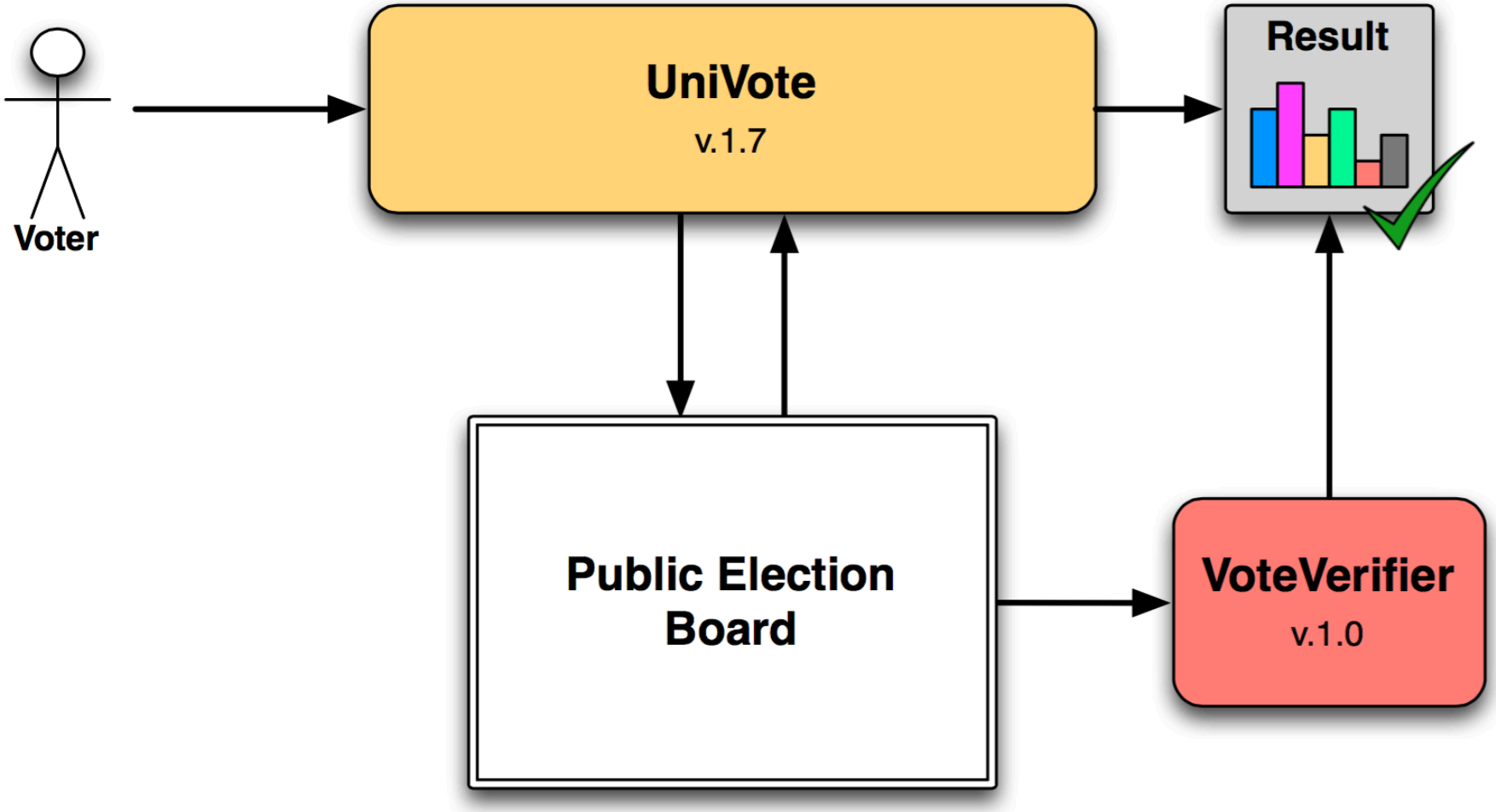
Realisierung (1)



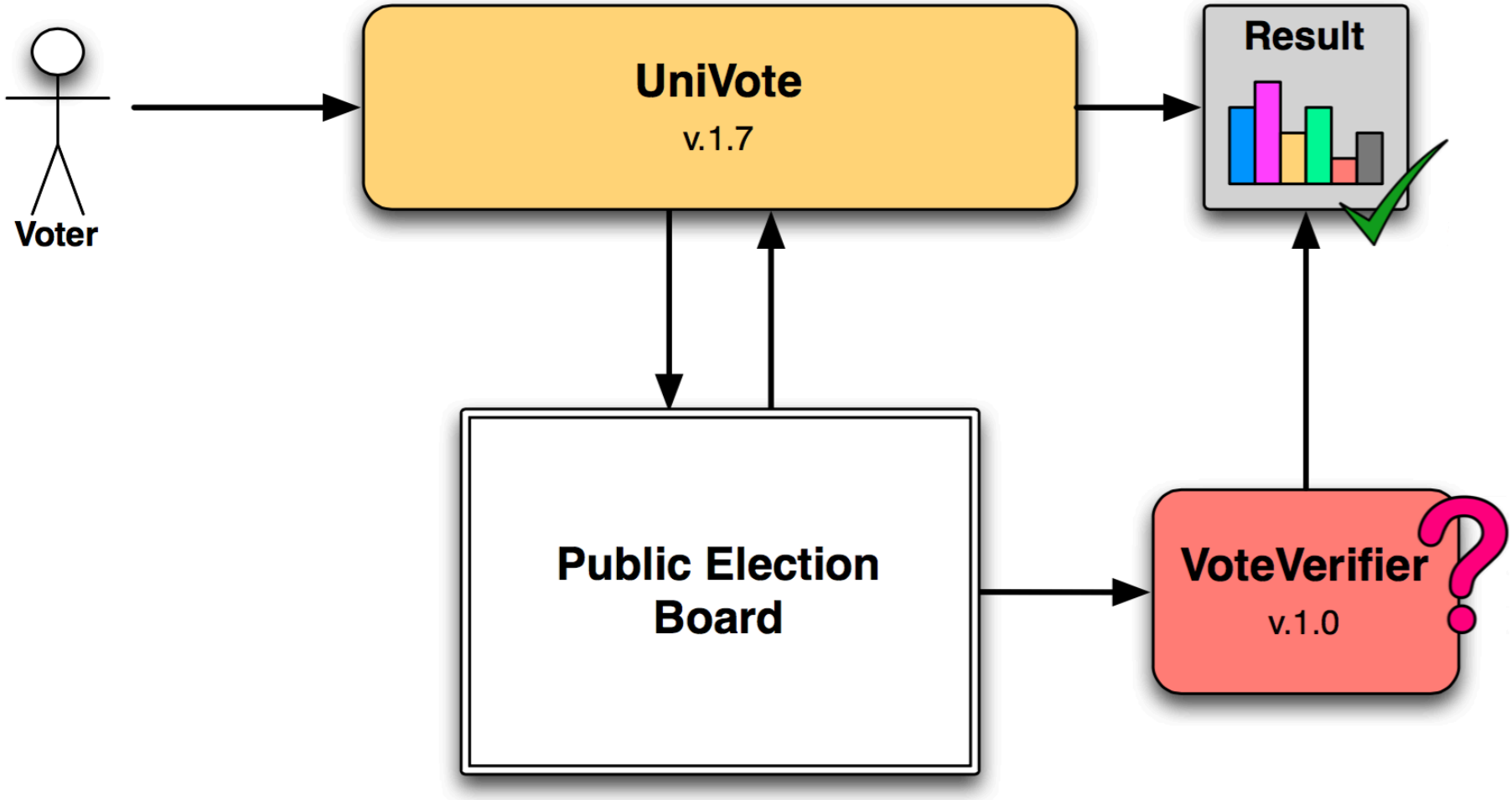
Realisierung (2)



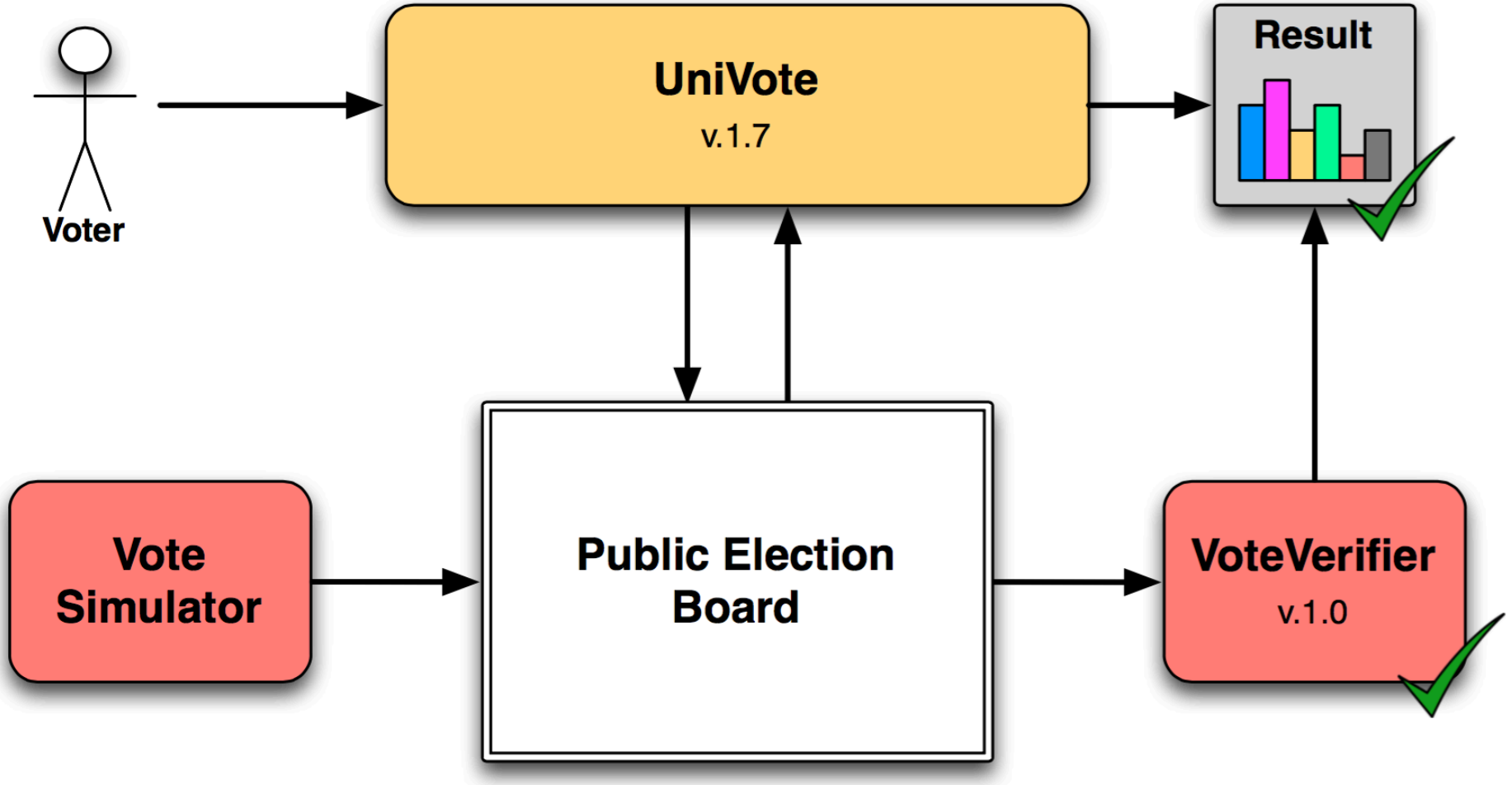
Realisierung (3)



Realisierung (5)



Realisierung (6)



Offene Probleme

Kann ich meinem Computer trauen?

- Neue Wege gefragt – Zusammenarbeit Wirtschaft / Behörden?

Weitere offene Probleme

- Anschlagbrett versus Langzeitsicherheit
- Anschlagbrett versus Nötigung

  „*Italian attack*“

Fragen / Diskussion

Vielen Dank – Fragen / Diskussion

Prof. Dr. Eric Dubuis
Berner Fachhochschule – RISIS
eric.dubuis@bfh.ch