E-Voting und E-Banking – der Unterschied

Prof. Dr. Eric Dubuis
Berner Fachhochschule
Technik und Informatik
Research Institute for Security in the Information Society
E-Voting Group

Basel Landschaft, Motion Mohn

(Eingabe: 28.1.2010, überwiesen: 28.1.2011)

- […] für Auslandschweizerinnen und -schweizer von grossem Nutzen ist.

- E-Voting darf das **Stimm- und Wahlgeheimnis in keinem Fall gefährden**, das **Ergebnis darf nicht verfälscht** werden können […].

- Die **Pilotprojekte** in den Kantonen Genf, Neuenburg und Zürich haben gezeigt, dass E-Voting nicht nur machbar, sondern **auch sicher** ist. So stellen die **Sicherheitsrisiken heute keine unüberwindbaren Schranken** mehr dar.

Situation in den Niederlanden

- bis 2008: Wahlcomputer in den Wahllokalen

- Der niederländische Ministerrat hat beschlossen, Wahlen in dem Land künftig **nur mit Papier und Bleistift** abhalten zu lassen, solange es keine geeignete Alternative gebe. [...].
  (Heise online 19.05.2008)

Situation in Deutschland

Entscheid Bundesverfassungsgericht:

- [...]. Die **Wähler** hätten **nicht die abgegebenen Stimmen und die Auszählung kontrollieren können**, argumentieren die Richter. […]
  (Heise online, 03.03.2009)

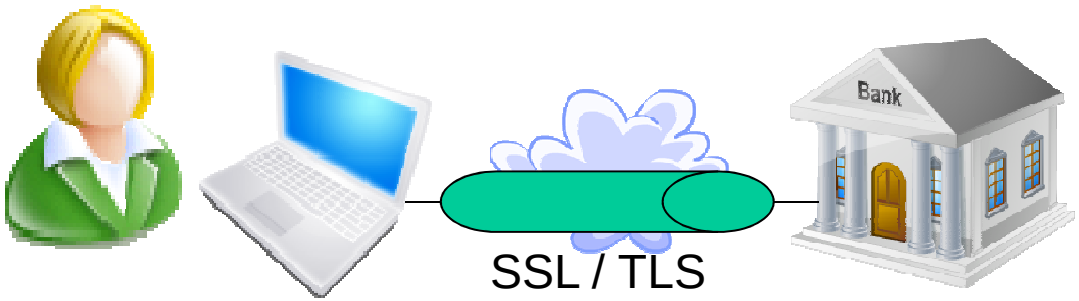
- Argument : „Beim Einsatz elektronischer Wahlgeräte müssen die wesentlichen Schritte der Wahlhandlung und der Ergebnisermittlung vom Bürger zuverlässig und ohne besondere Sachkenntnis überprüft werden können.[…]“
  (Bundesverfassungsgericht, Urteil vom 03.03.2009)

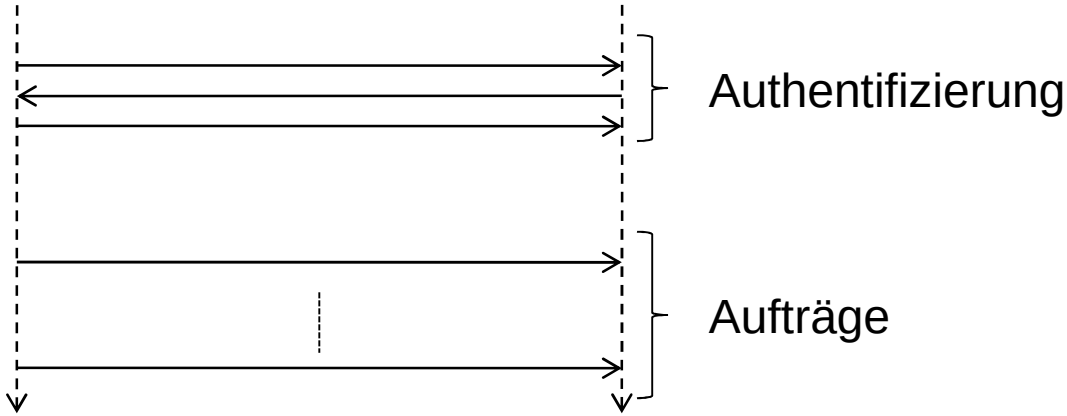
Inhalt

E-Banking – vereinfacht

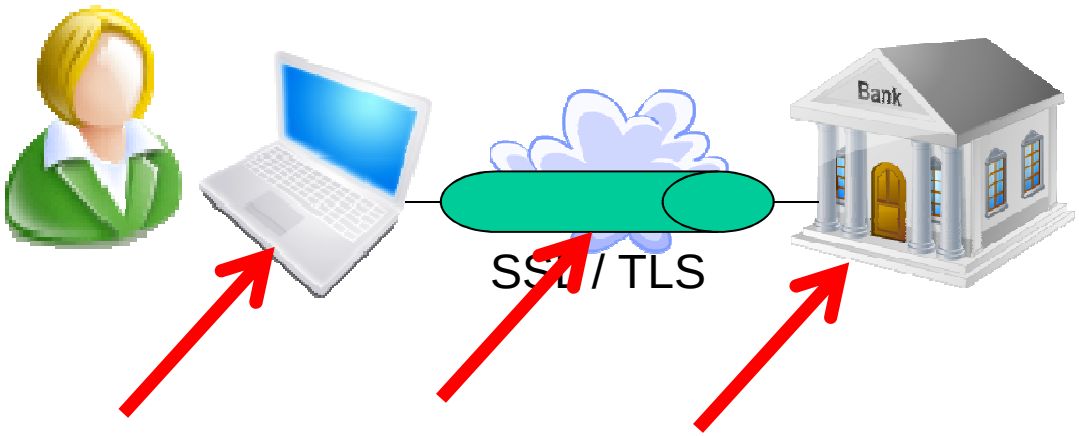
- Vertrag
- Bank kennt Kunde
- Dienste:
  - Bargeldbezug (Bancomat)
  - E-Banking (Internet)

E-Banking – Ablauf

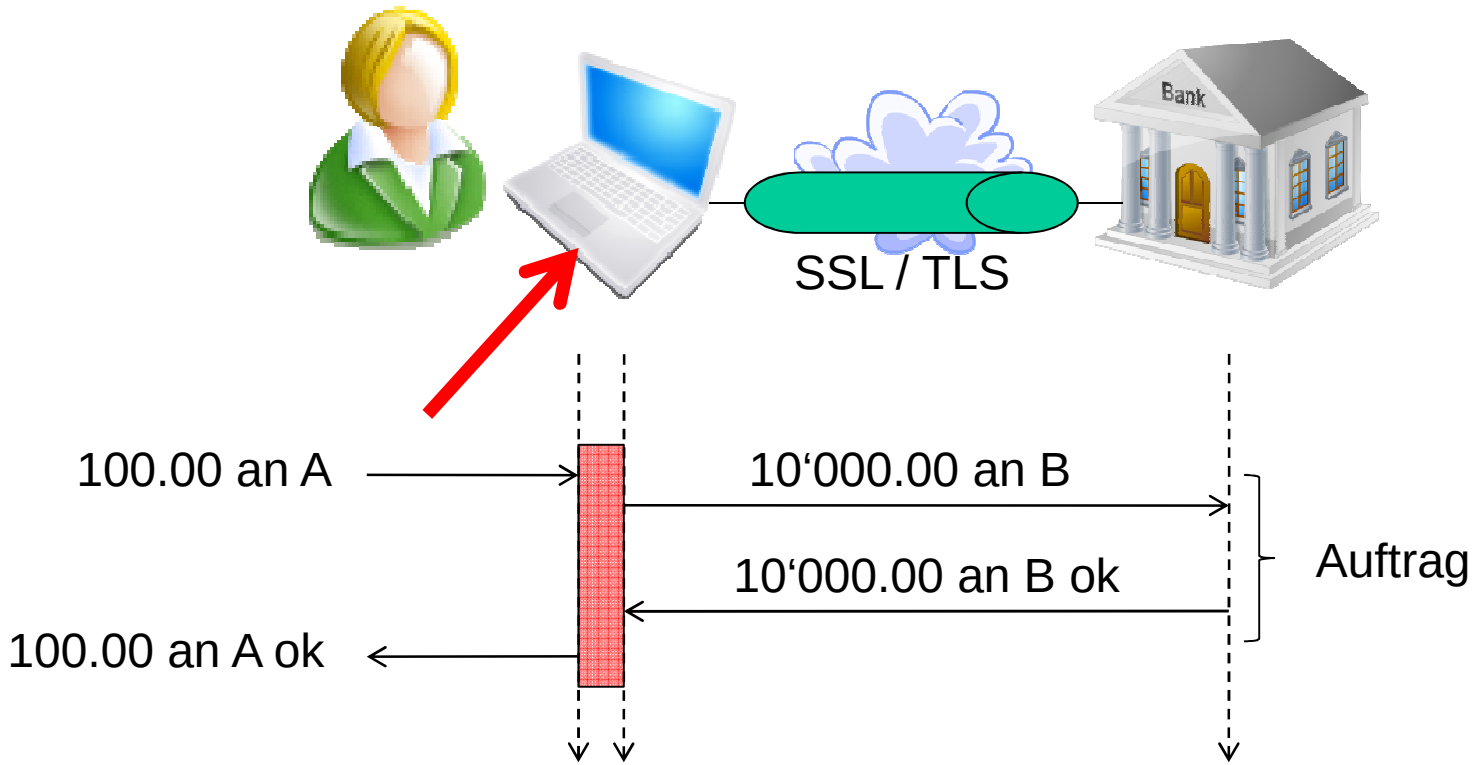




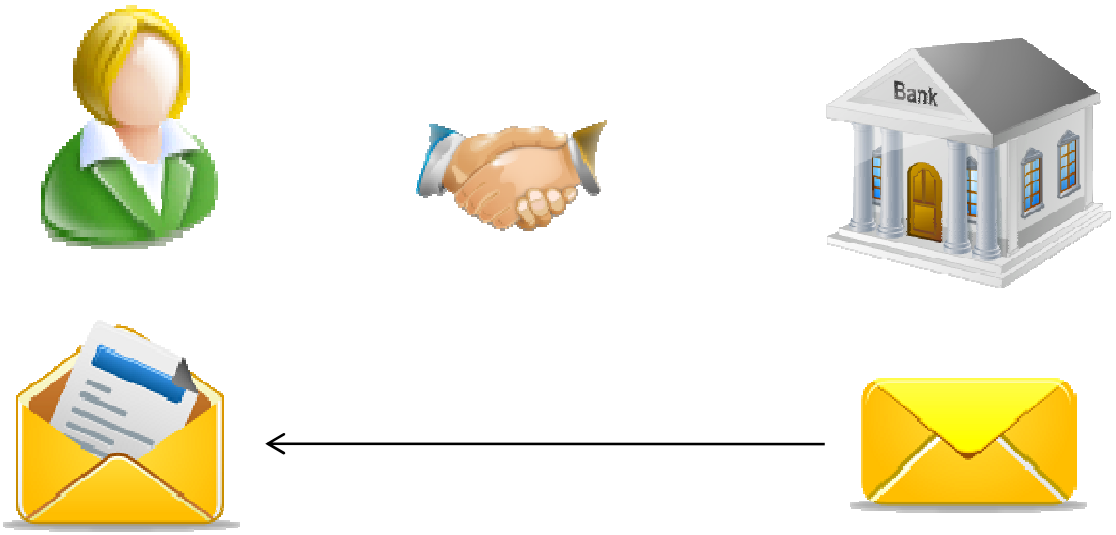
E-Banking – Angriffspunkte



E-Banking – Malware



E-Banking – Auszug



E-Banking – Fazit

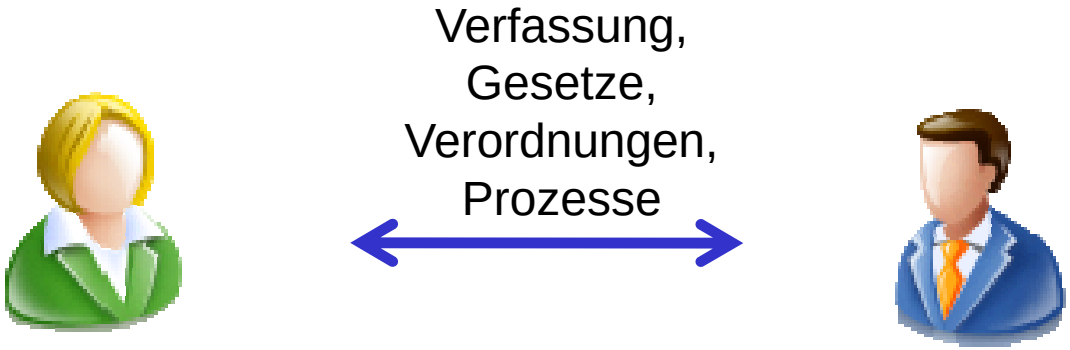
- Die Kundin ***merkt*** am Ende der Abrechnungsperiode, dass etwas nicht stimmt.

… und wie ist es beim E-Voting?

Inhalt

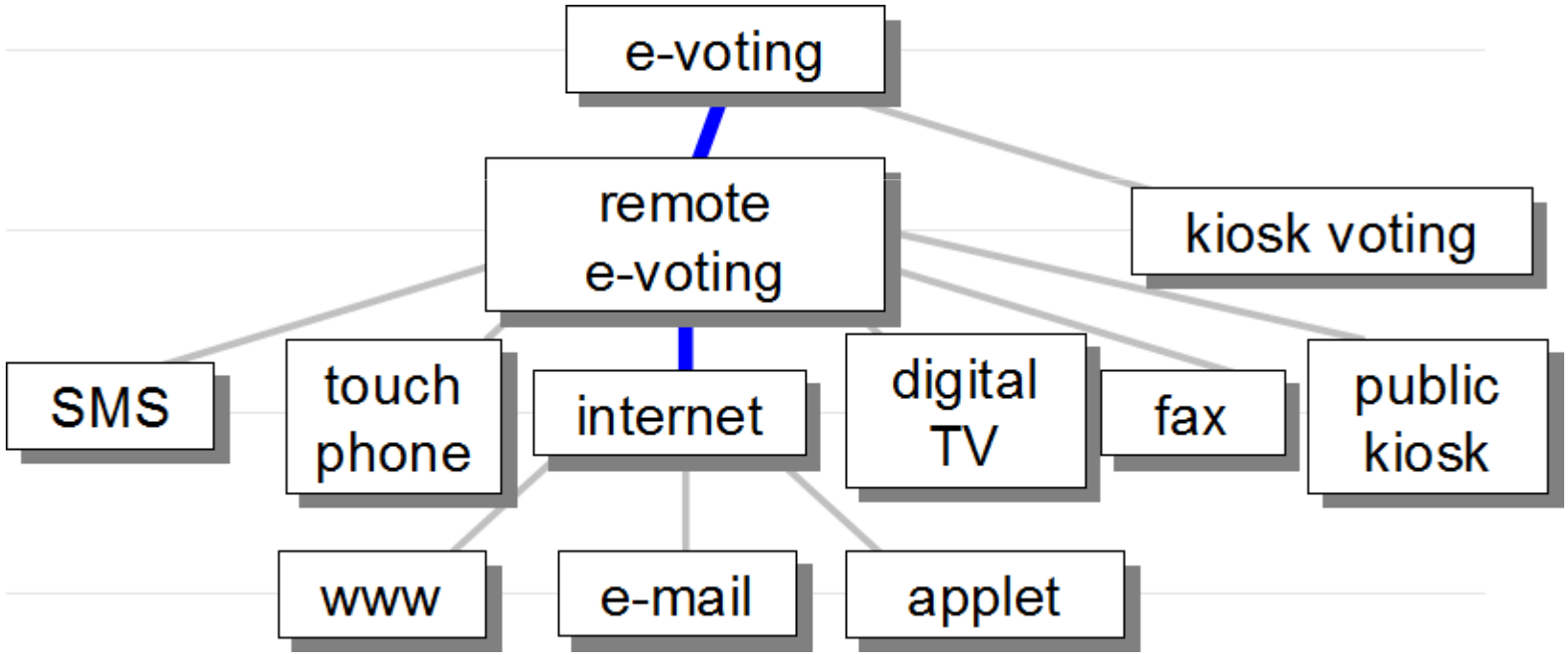
1. E-Banking
2. **„Back-Box“-E-Voting-Systeme**
3. Verifizierbare E-Voting-Systeme
4. Selectio Helvetica als Beispiel
5. Fazit

E-Voting – Bürger ↔ Verwaltung



E-Voting – Klassifizierung nach

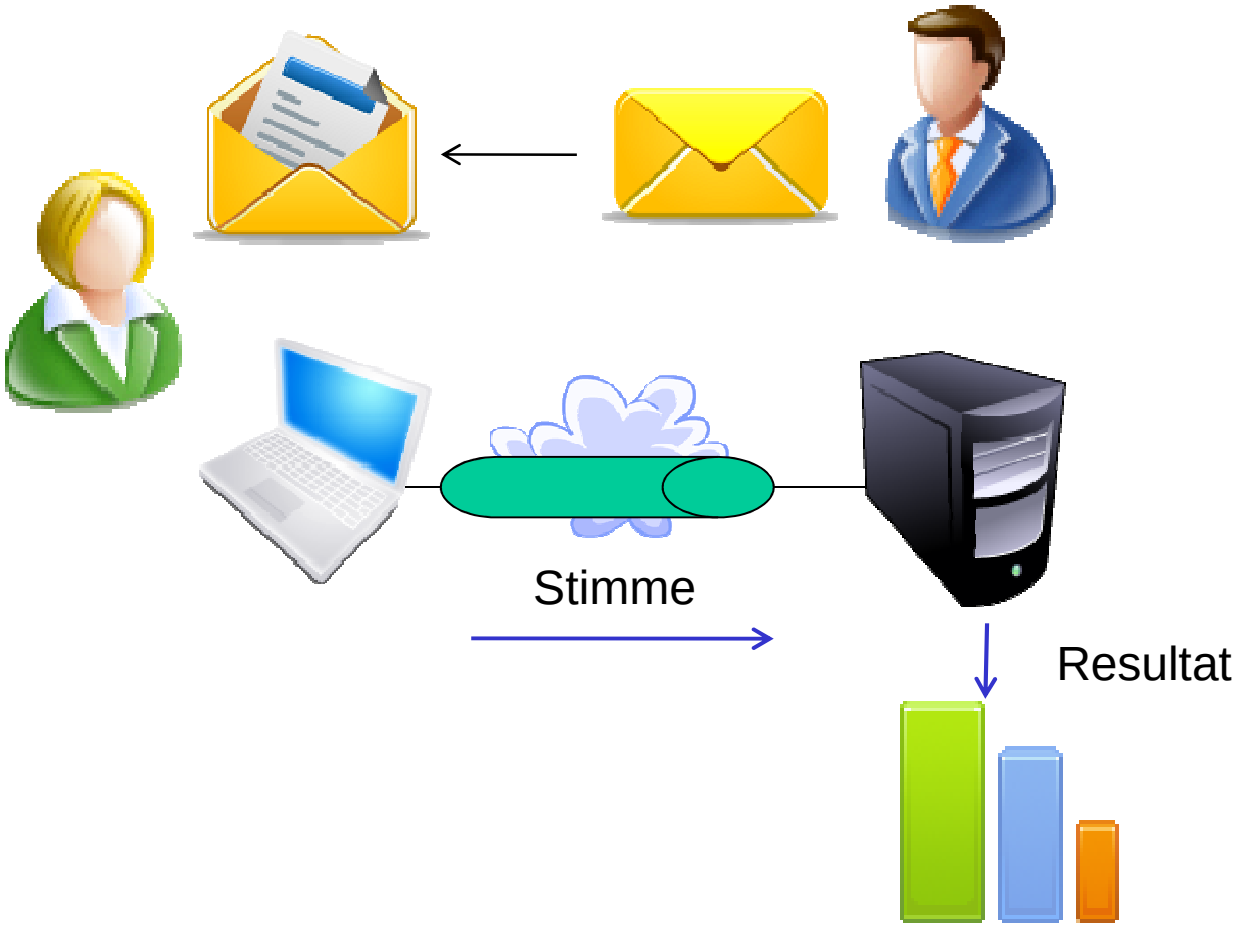
EU-Empfehlung Rec (2004)11



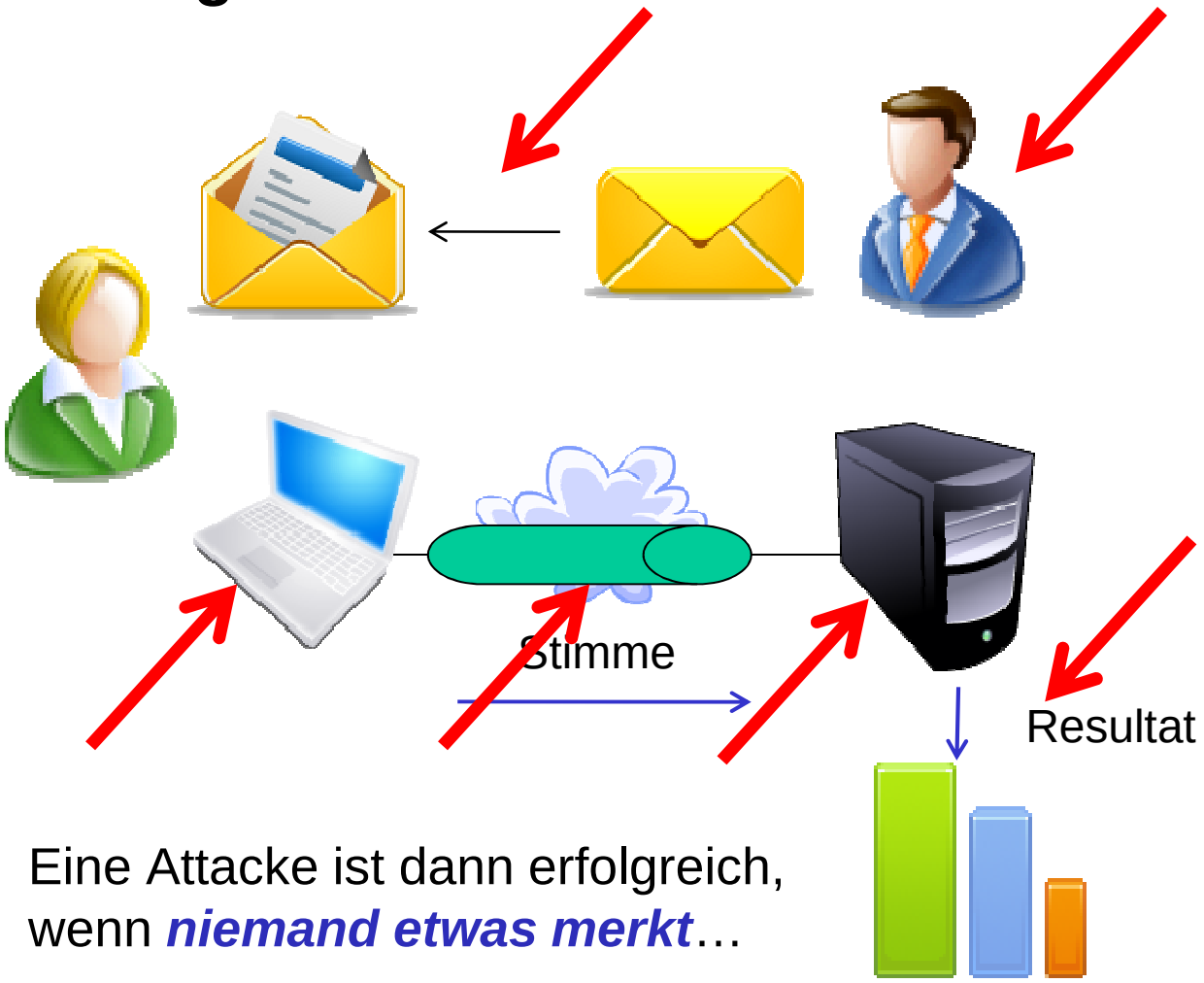
E-Voting – Anforderungen

- „Demokratie“
  - nur Bürger mit Stimmrecht (Berechtigung)
  - nur 1 Stimme pro Bürger (1 Stimme)
- Schutz der Privatsphäre
  - keine Beziehung herstellbar zwischen Stimme und Bürger (Anonymität)
  - Abstimmender kann nicht beweisen, wie abgestimmt (keine Quittung)
- Verifizierbarkeit (Stimmende, Beobachter)
  - wurde meine Stimme gezählt? (individuelle Verifizierbarkeit)
  - wurde richtig gezählt? (universelle Verifizierbarkeit)
  - wurden keine unberechtigten Stimmen gezählt?

E-Voting – vereinfacht



E-Voting – vereinfacht



- 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?

Inhalt

Verifizierbare E-Voting-Systeme (I)

Ein paar Prinzipien:

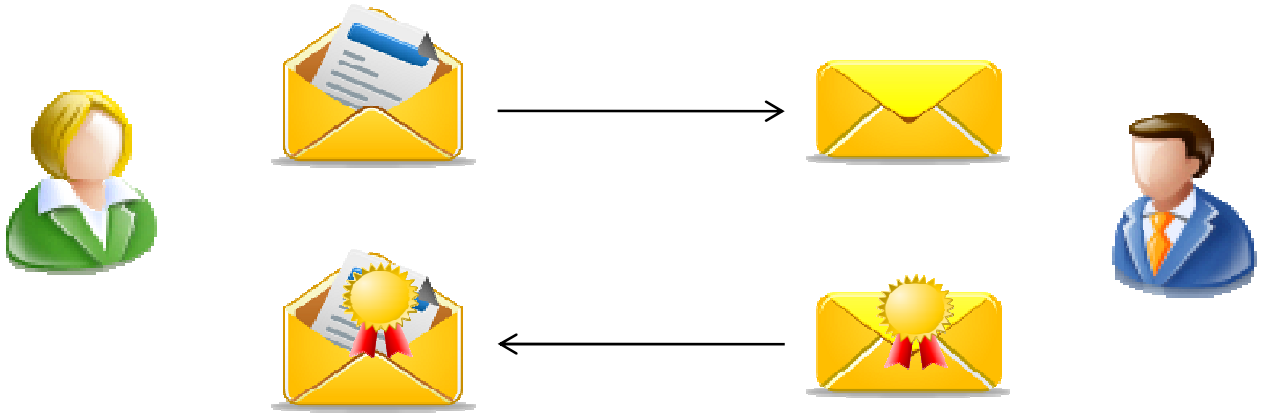
- Möglichst alle Informationen sind ***öffentlich*** (Ausnahme: private Schlüssel)
- Abgegebene Stimmen sind ***verschlüsselt***, ***öffentlich***
  - sie werden erst beim Zählen entschlüsselt
  - oder: sie werden gar nie entschlüsselt
    ➔ homomorphe Kryptographie
- Private Schlüssel werden auf *N* vertrauenswürdige Personen ***aufgeteilt***
  - Erst wenn *K* Personen, z.B. ½ *N* < *K* < *N,* kooperieren, können diese den privaten Schlüssel anwenden

Verifizierbare E-Voting-Systeme (II)

Ein paar Prinzipien (Fortsetzung):

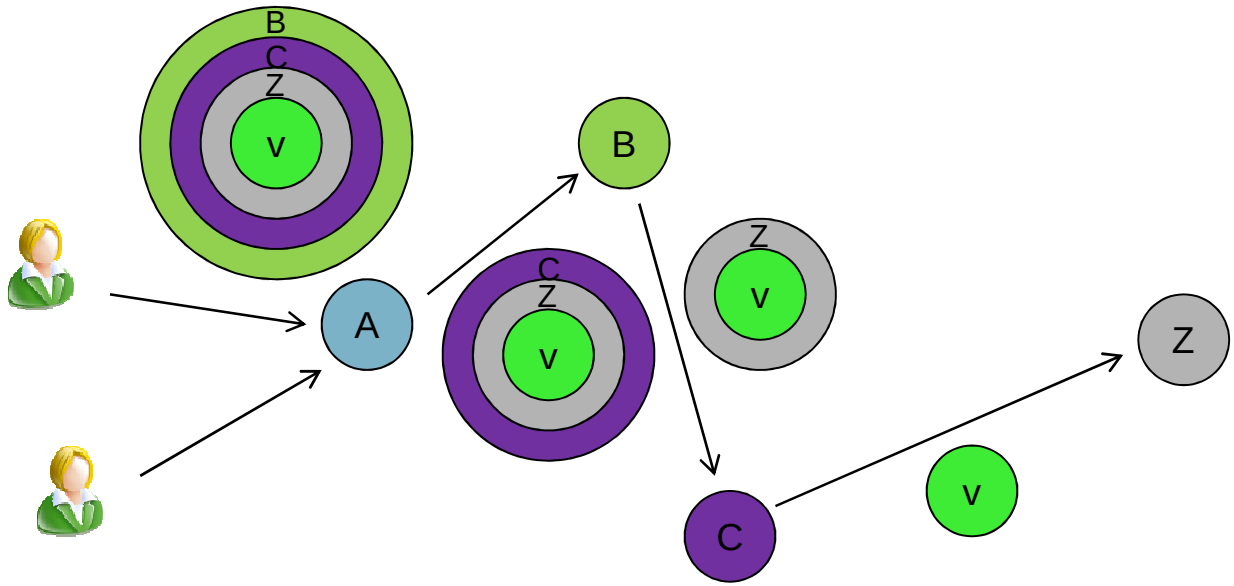
- Die ***Nicht-Verknüpfbarkeit*** von Stimmen mit Stimmenden wird mittels ***kryptographischer Mittel*** gewährt (und nicht prozeduralen)
- weitere…

Bausteine: Blinde Signaturen



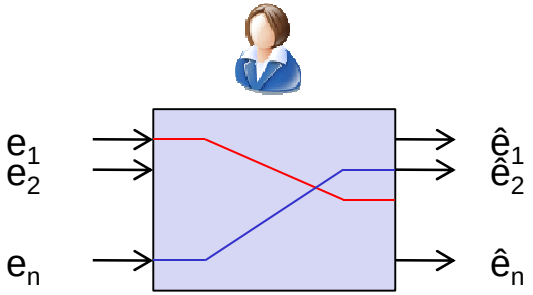
- Öffentlicher Schlüssel e, privater Schlüssel d, Zufallszahl r
- Blendungsfaktor: r^e
- Verblendete Meldung: $m \times r^e$
- Blinde Signatur: $s' = S(m \times r^e, d)$
- Signatur: $s = s' \times r^{-1} = S(m, d)$

Bausteine: Anonyme Kanäle



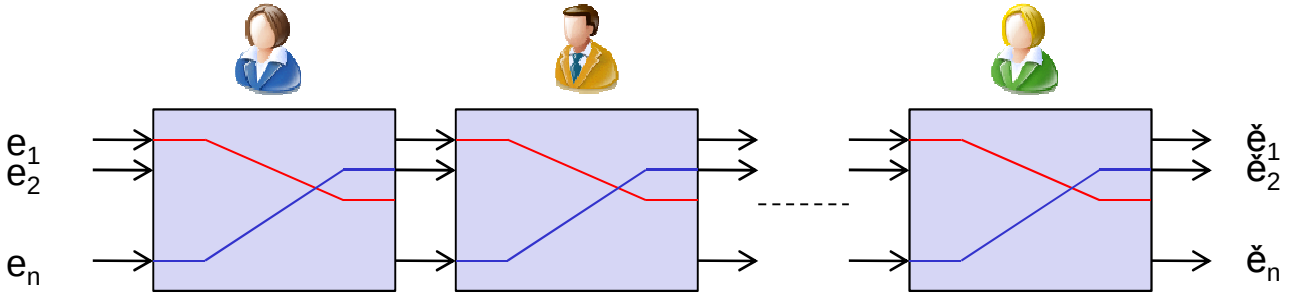
- „*Chaum mix*“ (Chaum, 1981) als Basis, „*onion routing*“ (Reed et al., 1998)
- Meldung *v* erreicht *Z*, ohne dass *Z* weiss, von wem sie stammt

Bausteine: Re-Encryption Mix-Nets



$\hat{e}_i = R(e_{\pi(i)}, r_i)$: re-encryption

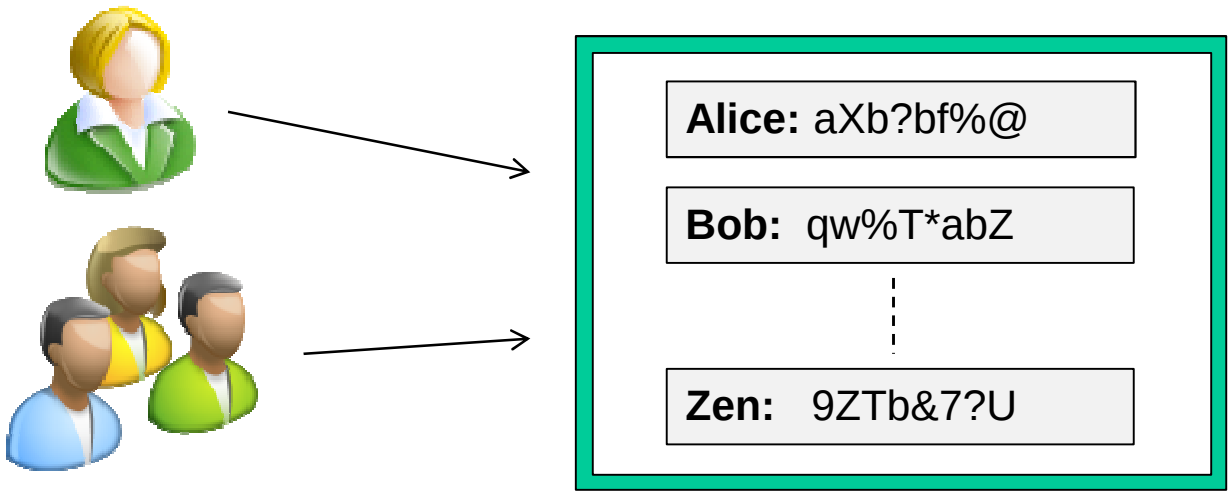
plus Beweis



Legende

e_i, $\hat{e}_i$, $\check{e}_i$: verschlüsselte Stimmen

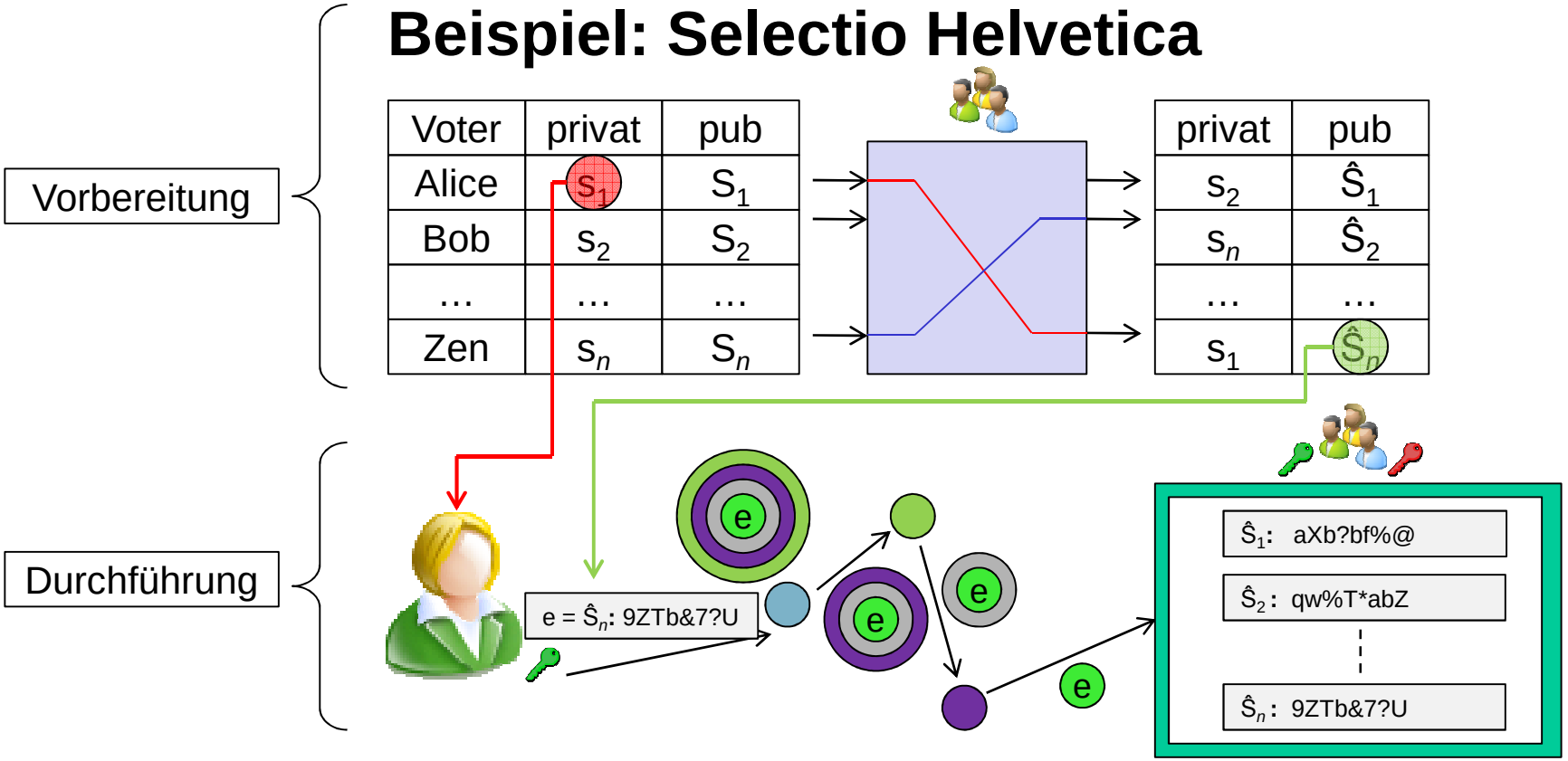
Bausteine: Öffentliches Bulletin Board



- Stimmen und Beweise werden am Anschlagbrett veröffentlicht
- Reale Identitäten (wie obiges Beispiel) oder Pseudonyme erscheinen neben den Stimmen
- Alice verifiziert ihre Stimme
- Alle verifizieren das Gesamtresultat

Inhalt

Beispiel: Selectio Helvetica



- Grundlage für baloti.ch
- erlaubt Stimm-Revokation (z.B. bei Stimmzwang)

Selectio Helvetica – Zusammenfassung

Voraussetzung:

- sichere Plattform bei den Stimmenden (Privatsphäre!)

Eigenschaften:

- individuelle Verifizierbarkeit
  Stimmende können ihre Stimmen verifizieren
- universelle Verifizierbarkeit

Aber:

- Alice kann Dritten beweisen, wie sie gestimmt hat
- Somit kann sie genötigt werden, auf bestimmte Art zu stimmen ➔ Ausweg: Stimme revozieren

Inhalt

Vergleich E-Voting mit E-Banking

Aspekt	E-Voting	E-Banking
Gegenstand	Volkswille	Geld
Kunde	Bürger/Bürgerin	Bankkunde
Identifikation	• nur zur Legitimation • Stimme nicht verknüpfbar	permanent
Privatsphäre	universeller Schutz	Schutz nur gegenüber Dritten
Individuelle „Richtigkeit“	schwierig, da Quittung unerwünscht	monatlicher Auszug
Universelle „Richtigkeit“	schwierig	-
Verteilung des Risikos	alle sind betroffen	einzelner Kunde

Fazit – Geschlossene Wahlsysteme

- Geschlossene Wahlsysteme („*black box*“-Systeme) bedingen ***prozedurale Sicherheit***
- Es ist kaum möglich, diese zu beobachten (OECD-Forderung)
- Ist die prozedurale Sicherheit nicht gewährt, so können der Schutz der Privatsphäre und die Korrektheit des Ergebnisses nicht garantiert werden

Fazit – Verifizierbare Wahlsysteme

- Offene, verifizierbare Wahlsysteme basieren auf mehreren Krypto-Bausteinen.
- Sie ermöglichen die ***individuelle*** und ***universelle*** Verifizierbarkeit
- Sie sind komplizierter als geschlossene Wahlsysteme, dafür können Zertifizierungsprozeduren vereinfacht werden

- Offene Probleme
  - sichere Plattform
  - Langzeitarchivierung von Cipher-Texten
  - Quittungsfreiheit

Vielen Dank