Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Quelle: computerworld.ch

Aspekte der digitalen Identität am Beispiel eVoting

eGovernment Day Schaffhausen 2017

Prof. Dr. Eric Dubuis

Abteilung Informatik

Referent

- Prof. Dr. Eric Dubuis

Abteilungsleiter Informatik
Professor für Informatik

Leiter des Instituts RISIS an der BFH-TI
„Research Institute for Security in the Information Society“

Vorstellung E-Voting-Gruppe BFH

- Professoren: Dr. Kai Brünnler, Dr. Stephan Fischli, Dr. Rolf Haenni, Dr. Reto Koenig, Dr. Philipp Locher
- 2 Assistierende und wissenschaftliche Mitarbeitende
- Alumni: Dr. Oliver Spycher, Bundeskanzlei

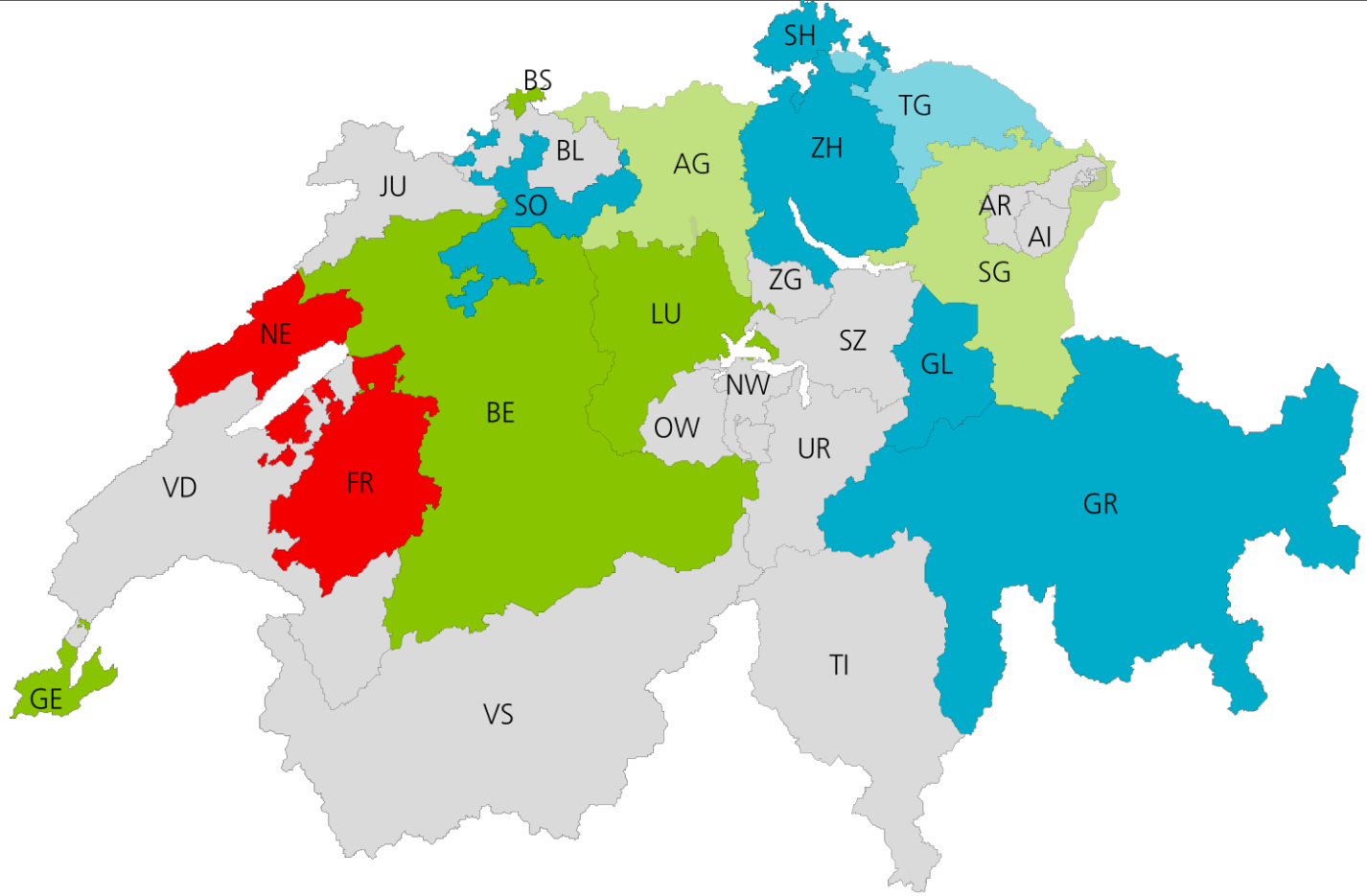
Bisherige Tätigkeiten im Bereich E-Voting

- Aktive Forschung seit 2008
- Zahlreiche Publikation
- UniVote für Studentenratswahlen
- Mitwirkung beim technischen Anhang der „Verordnung der BK über die elektronische Stimmabgabe“ (VEIeS, 15.1.2014)
- Spezifikation des Genfer Systems CHVote
- Mitwirkung im Bereich Verifikationssoftware für das Postsystem
- Realisierung eines weitern verifizierbaren E-Voting-System für Studentenratswahlen und Private

Agenda

- E-Voting-Situation in der Schweiz
- Verifizierbares E-Voting
- Digitale Identität bzw. Identifikator
- Vergleich und Fazit

E-Voting-Situation in der Schweiz



- System CHvote: entwickelt durch GE; angeschlossen sind BE, BS, LU; AG und SG planen, sich 2017 dem System anzuschliessen.
- Lösung der Post: FR, NE
- Laufendes Beschaffungsverfahren (ehemals Consortium Vote électronique)
- Consortium Vote électronique: Versuche mit der elektronischen Urne bis Ende 2015.
- 12 Kantone haben noch keine Versuche mit der elektronischen Stimmabgabe durchgeführt.

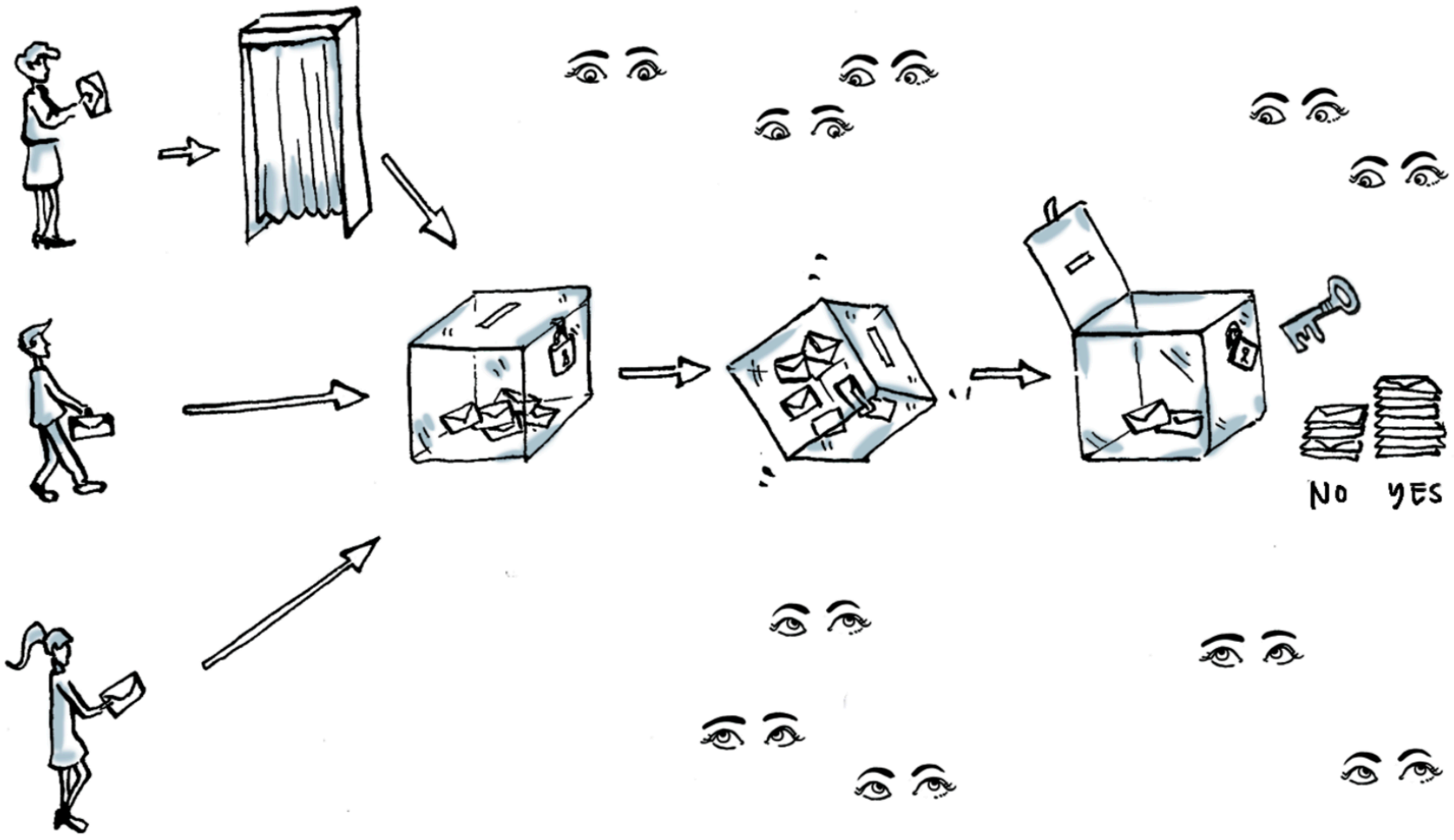
Quelle: Bundeskanzlei / Society Byte

Anforderungen an ein E-Voting-System

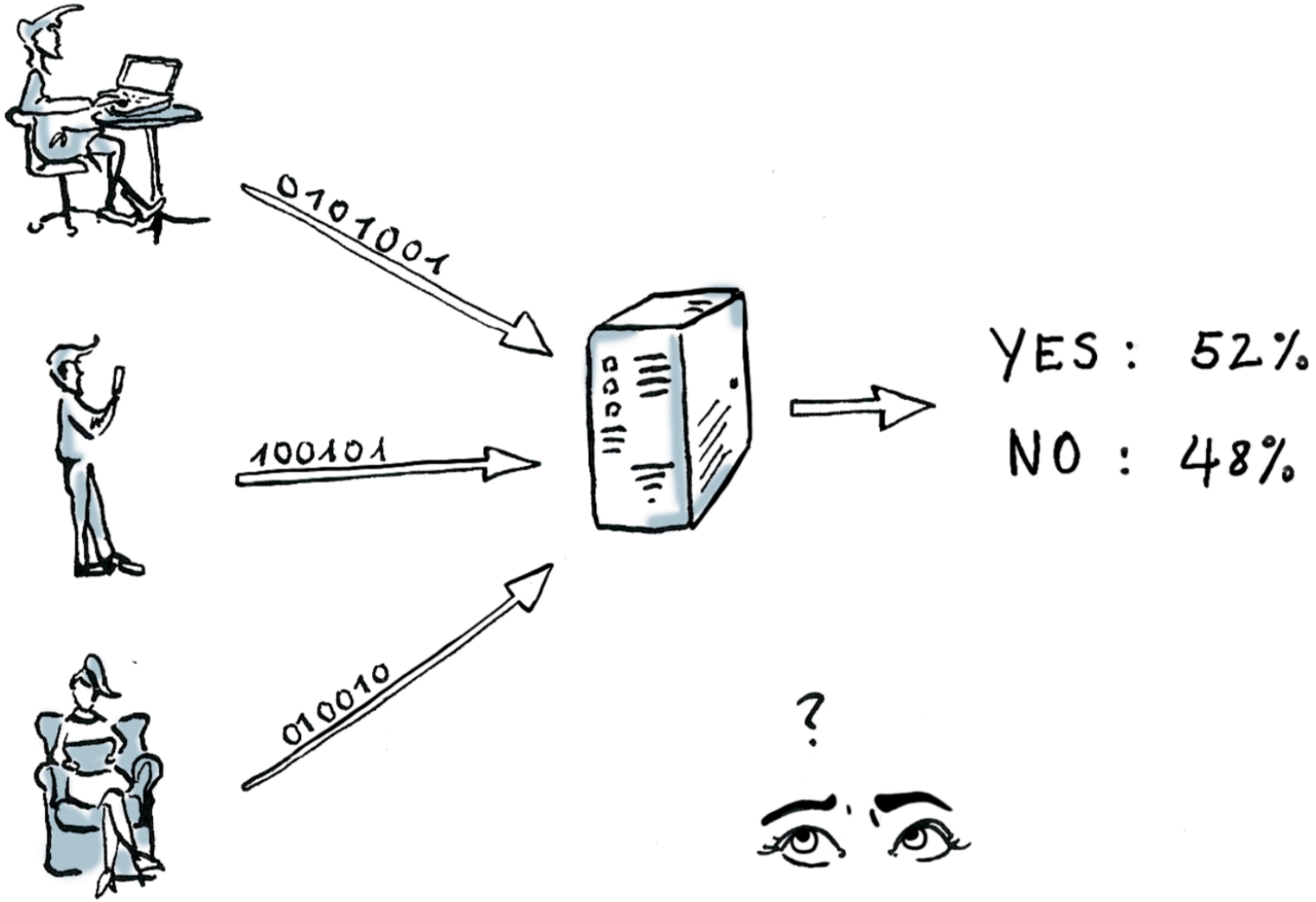
- Nur Stimmberechtigte, nur eine Stimme pro Stimmberechtigter
- Schutz der Privatsphäre: Wie ich abgestimmt habe, ist geheim
- Ich kann nicht beweisen, wie ich abgestimmt habe
- Verifizierbarkeit:
  - Wurde meine Stimme gezählt?
  - Wurde richtig gezählt?

Verifizierbares E-Voting

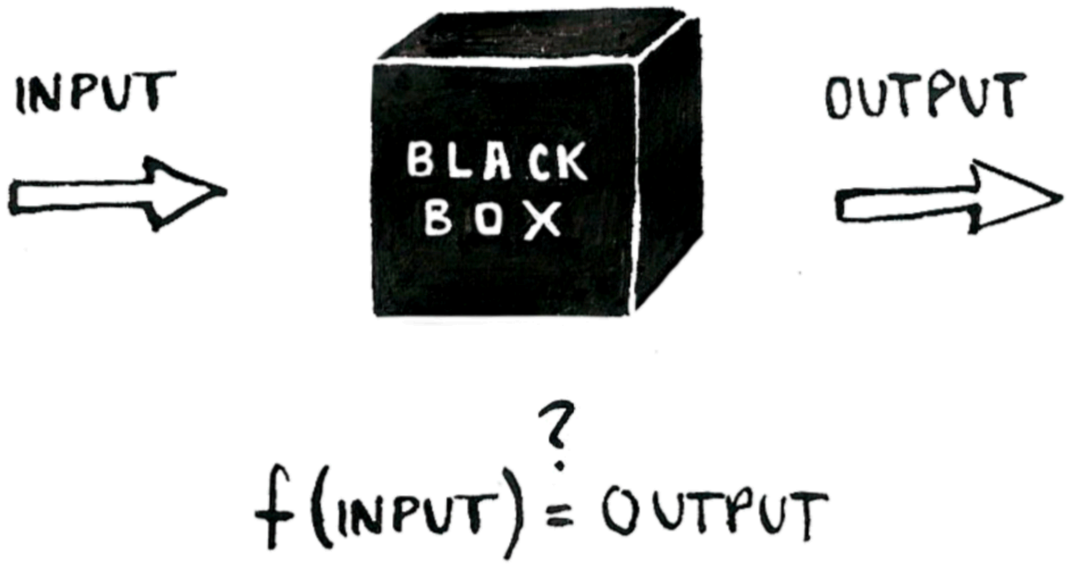
Traditionelles Abstimmen



Mittels E-Voting?

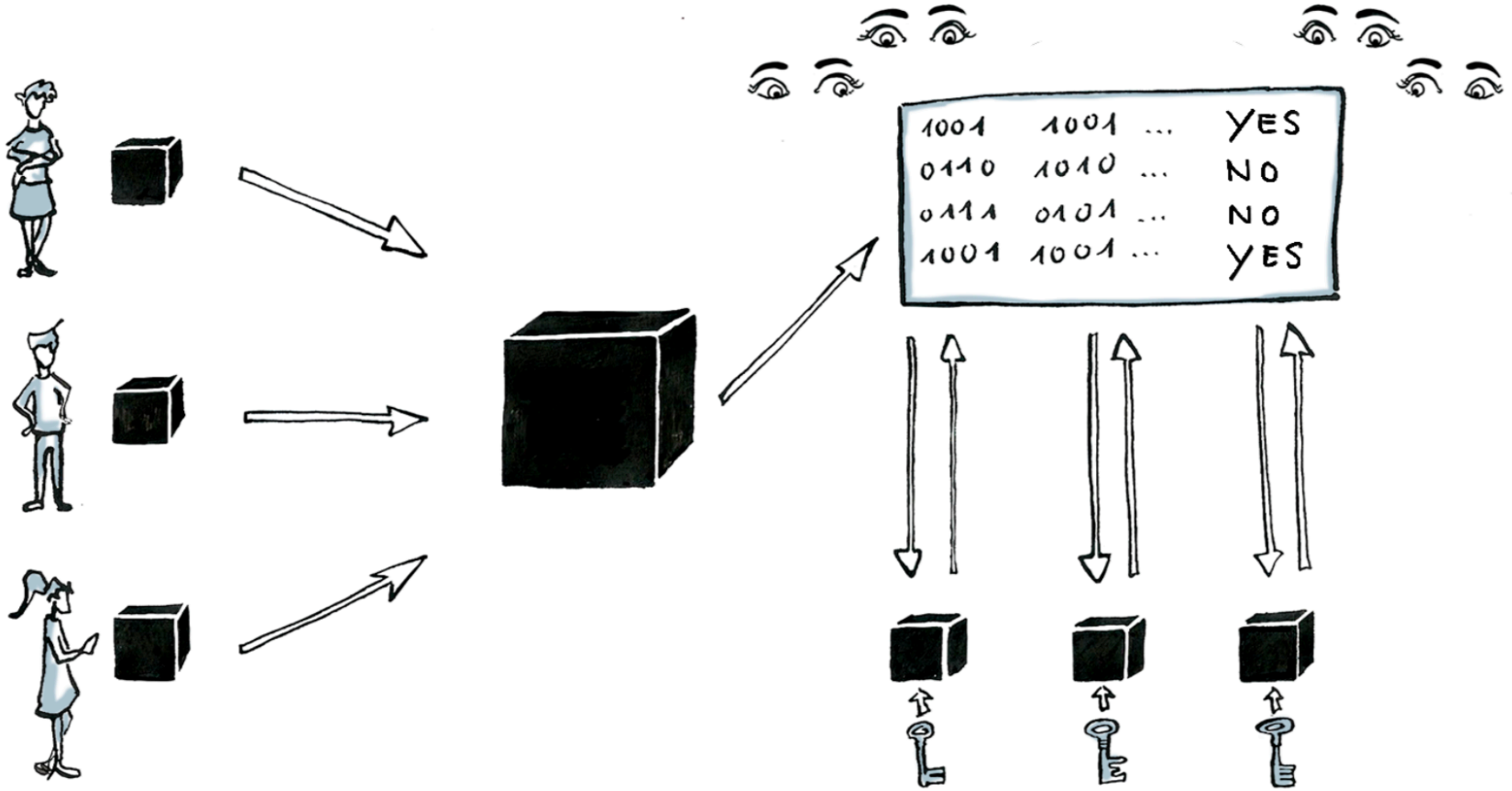


Es wäre eigentlich einfach...

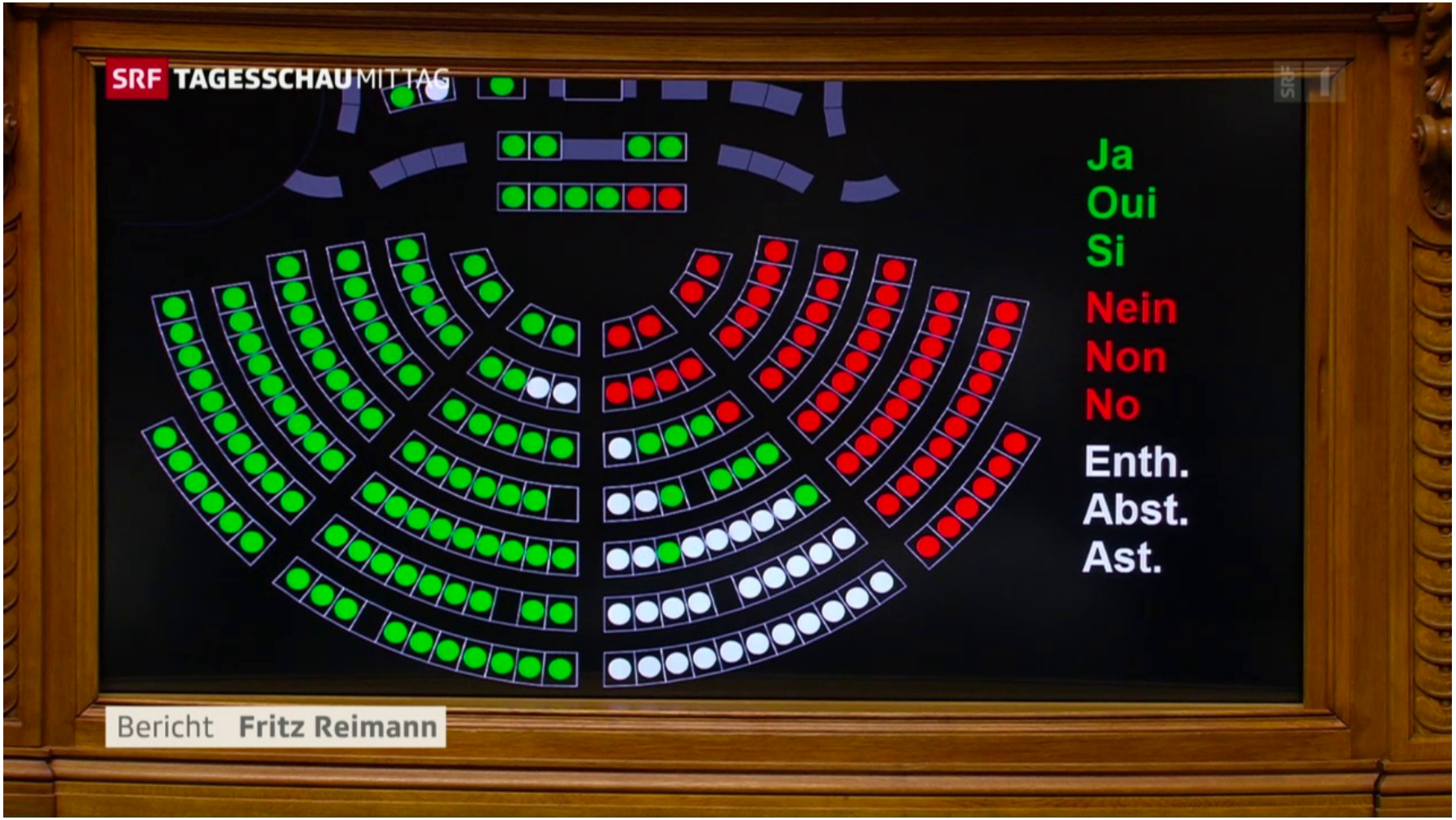


... wenn nicht Beobachtbarkeit und (z.B.) Stimmgeheimnis in Widerspruch stünden

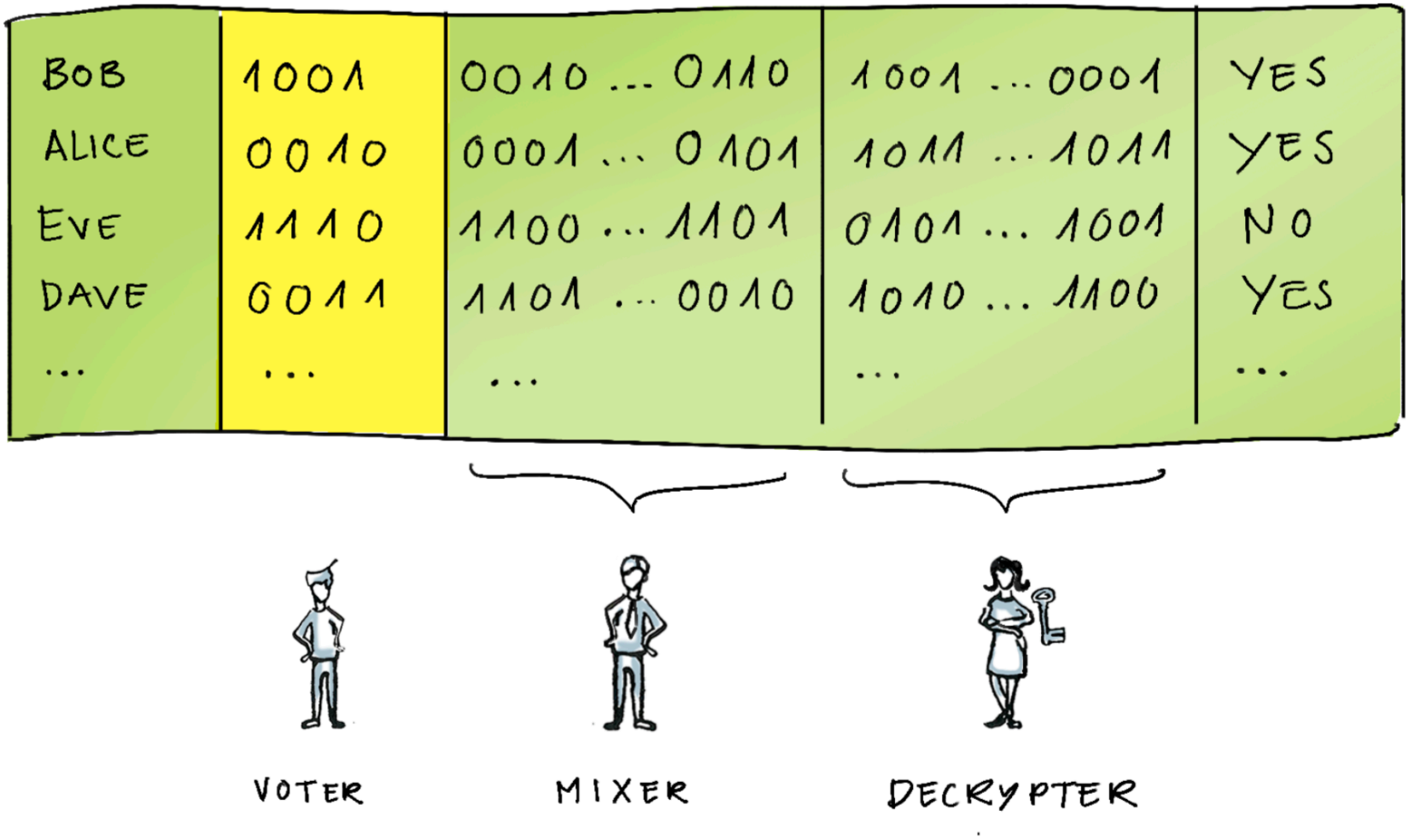
Die Beobachtbarkeit muss her



Öffentliches Anschlagbrett



Wo spielt die Identität eine Rolle?



Digitale Identität bzw. Identifikator

Definition „Digitale Identität“

„Jede mögliche Form von technisch abgebildeten Daten, die zu einer Person gehören“

- Daten zur eindeutigen Authentifizierung, z.B. Adresse, Name, biometrische Daten
- Daten zur pseudonymen Identifizierung, z.B. Login, Passwörter, Foren-Namen
- Persönliche Merkmale, z.B. Vorlieben, Hobbies, Religion, Lebensumfeld
- nicht unbedingt von jedem einer Person zuordenbar, z.B. IP-Adresse ist Teil der digitalen Identität, aber nur vom Internet-Provider zuordenbar

Quelle: Landeszentrum für Datenschutz Schleswig Holstein, 2007, http://bit.ly/2npBgpS (2.12.2017)

Identifikator

„Ein Identifikator (auch Kennzeichen) ist ein mit einer bestimmten Identität verknüpftes Merkmal zur eindeutigen Identifizierung des tragenden Objekts.“

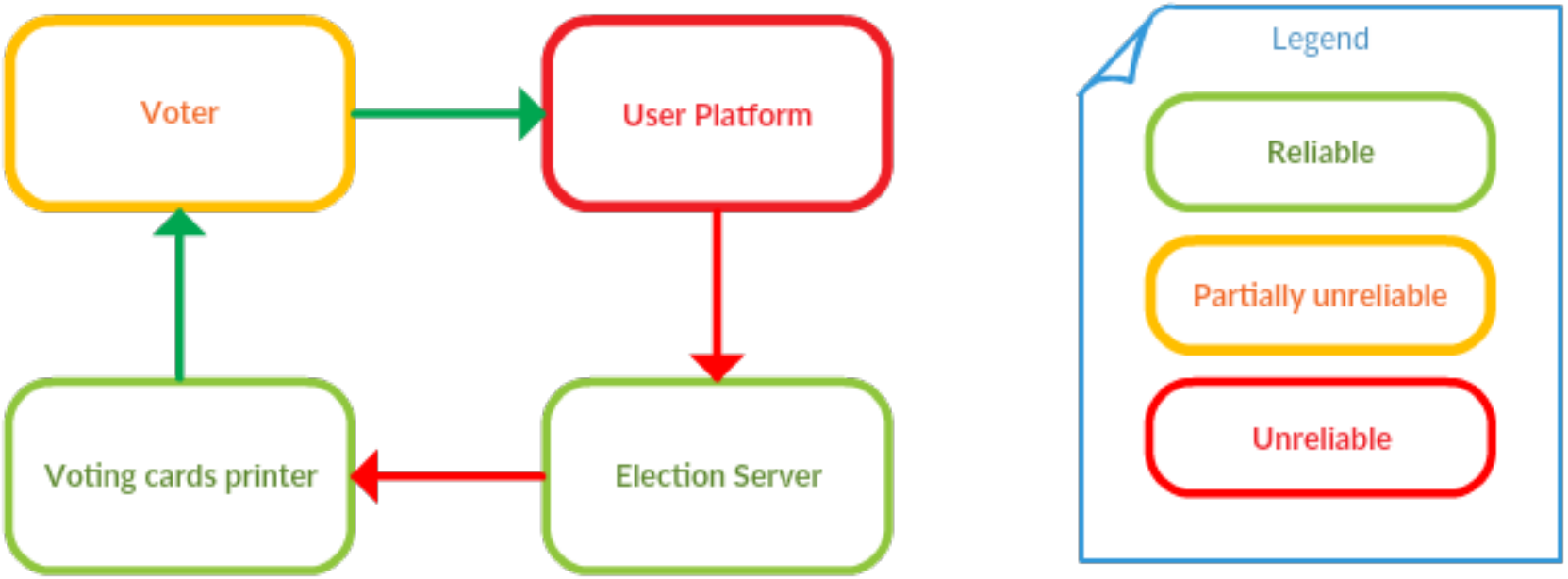
Wikipedia (2.12.2017)

Identifikator für den Einmalgebrauch

- Systeme der Post und Genf
- Heisst auch „Initialisierungscode“ (www.evoting.ch)
- Identifikation
  - Post: Initialisierungscode + Geburtsjahr
  - Genf: Voter ID + PIN + Geburtsdatum
- Nur einmal zu verwenden

- Via vertrauenswürdigem Postkanal zugesandt
- … zusammen mit weiteren Informationen
  - **Prüfcodes**
  - Bestätigungscode
  - Finalisierungscode

Vertrauensmodell



Quelle: https://www.ge.ch/document/evoting-chvote/telecharger

E-ID bzw. öffentlicher Schlüssel als Identifikator

- Im Kontext von E-Voting:
  - *öffentlicher* Schlüssel
  - assoziiert mit (natürlicher) Person
  - *privater* Schlüssel auf physikalischem Träger
- Wiederholt verwendbar (falls nicht kompromittiert)
- Zustellung von Prüfcodes: macht keinen Sinn
  - digital: da Plattform mitlernt
  - auf Papier: da Postkanal eliminiert werden soll

Vergleich und Fazit

Die beiden Identitäten im Vergleich (I)

	ID für Einmalgebrauch	E-ID
Preisgabe der ID / Abtretung Stimmrecht	möglich	**sehr unwahrscheinlich**
Stimmenverkauf	möglich	ev. einfacher (Quittung)
Nötigung	möglich	ev. einfacher (Quittung)
„family voting“	möglich	möglich
Individuelle Verifikation / (un-) sichere Plattform	**„cast-as-intended“** „recorded-as-cast“ „counted-as-recorded“	- „recorded-as-cast“ „counted-as-recorded“
Benutzerfreundlichkeit	gering	**ev. besser / kein Postkanal**

Die beiden Identitäten im Vergleich (II)

	ID für Einmalgebrauch	E-ID
Autonomität / Selbstbestimmtheit	kein Unterschied	
Stimmgeheimnis (Privatheit)	kein Unterschied / Stimmgeheimnis ist gewahrt (Annahme: Sichere Benutzerplattform)	
Anonymität (Privatheit)	nicht möglich	**u.U. möglich**
Verantwortung Schutz der ID	geringer	hoch
Profiling	geringer	eher möglich (falls keine Anonymität)
Überwachung	kein Unterschied	

Fazit

- Die E-ID vereinfacht viele Prozesse zwischen Bürger und Staat
- Es macht Sinn, die selbe E-ID auch für Prozesse zwischen Bürger und Wirtschaft einzusetzen
- Beim Einsatz der E-ID beim E-Voting fällt der Postweg weg (grosser Vorteil für die Auslandschweizerinnen und -schweizer)

- Aber: Die E-ID löst nicht *a priori* das Problem der unsicheren Benutzerplattform → zusätzliche Massnahmen sind notwendig

Vielen Dank

Prof. Dr. Eric Dubuis
Berner Fachhochschule
RISIS
2501 Biel
Switzerland