E-Voting – Wie weit sind wir?

Prof. Dr. Eric Dubuis
Berner Fachhochschule

FAEL Novemberseminar
Zürich
5. November 2008

Inhalt

I. Einleitung, Historie

II. E-Voting-Protokolle

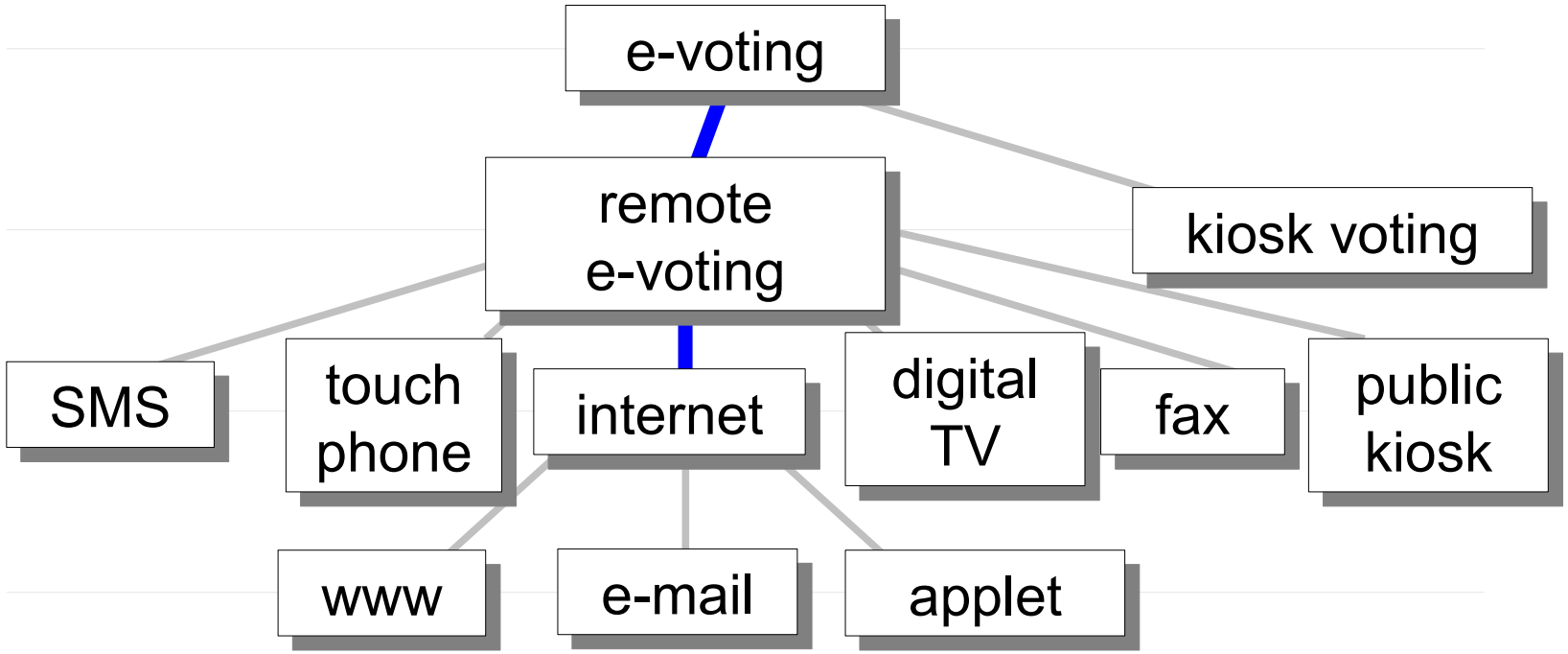
III. Secure Platform Problem

IV. Schluss

Einleitung

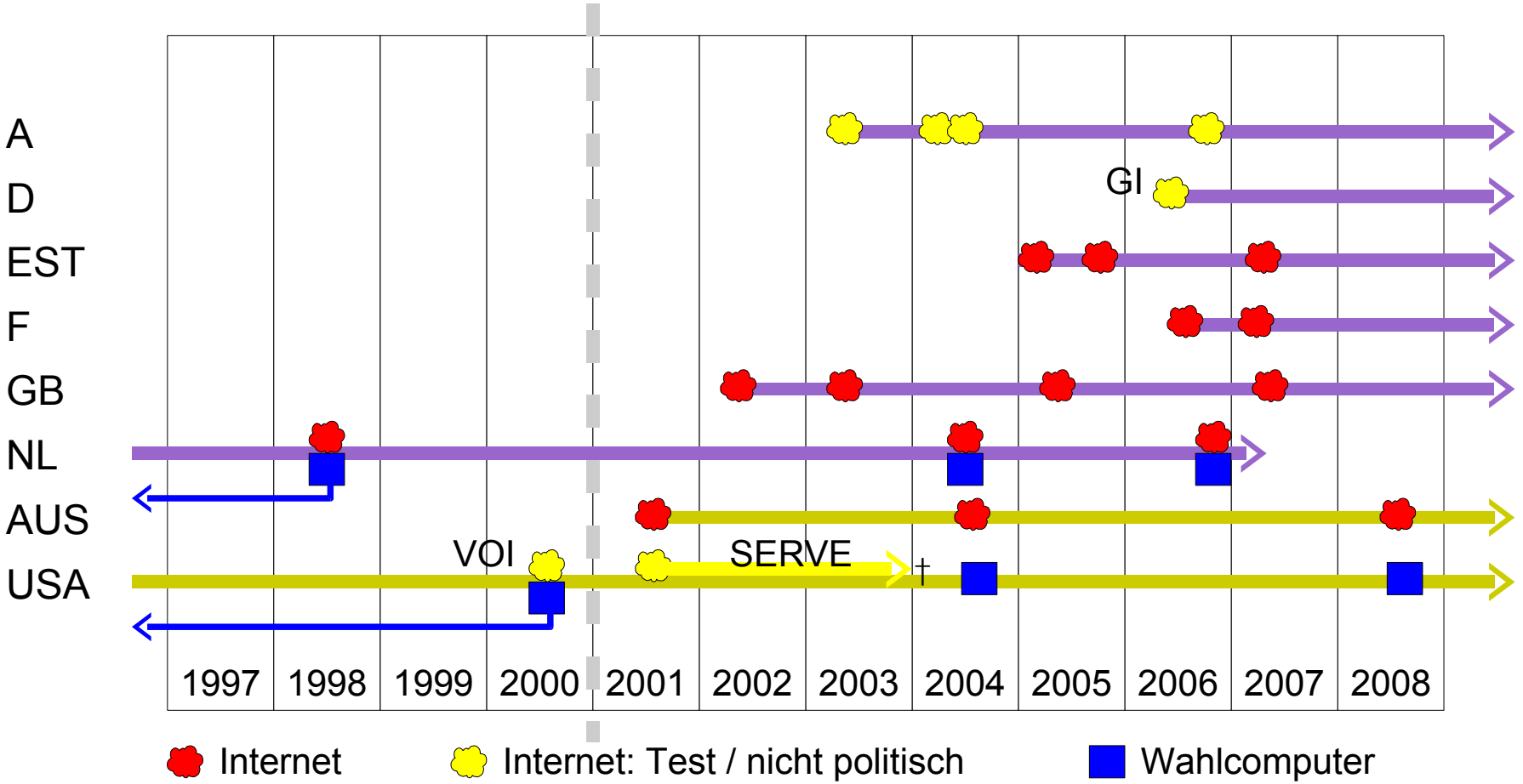
Klassifizierung E-Voting-Systeme

Klassifizierung nach EU-Empfehlung Rec(2004)11

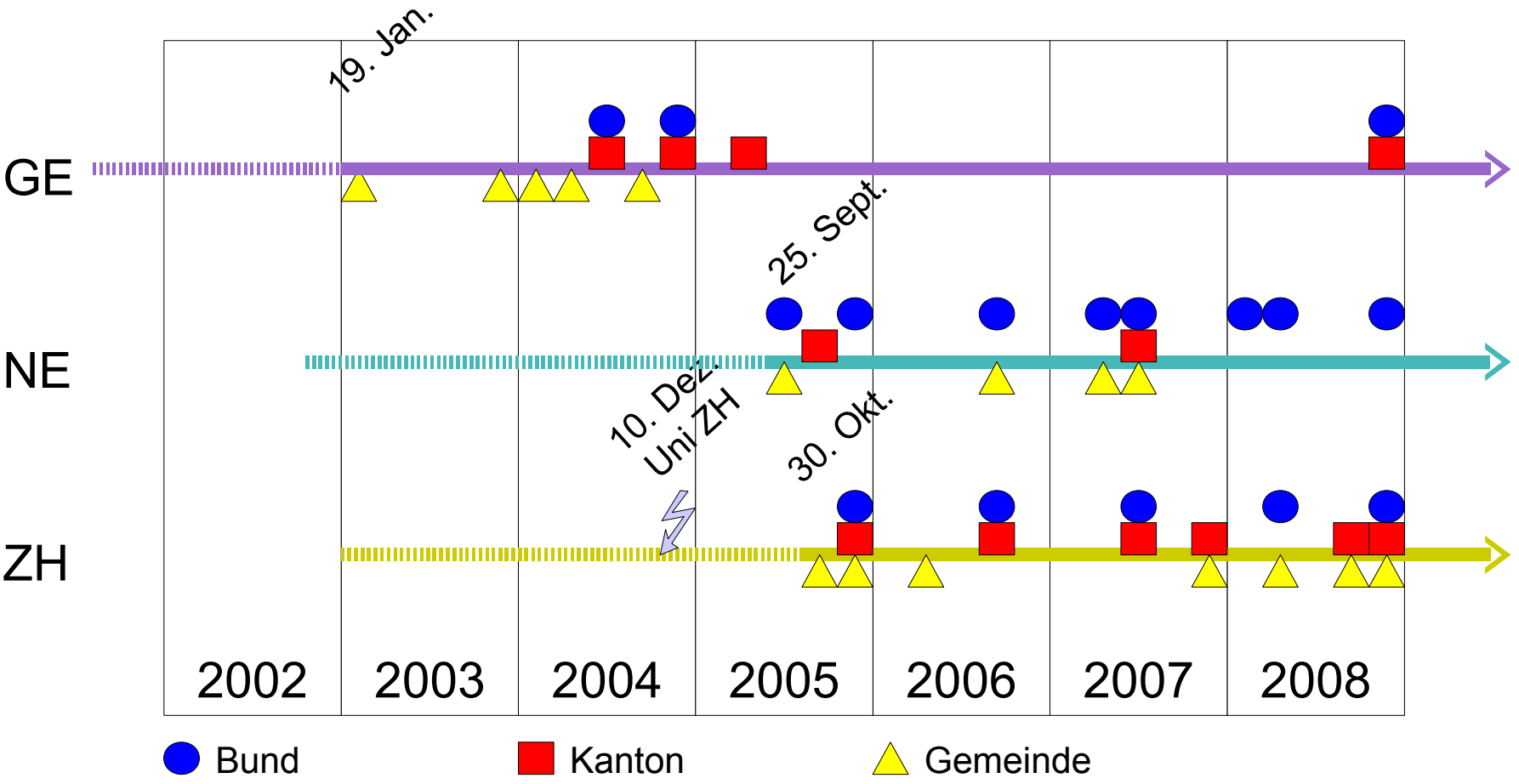


(Politische) Abstimmungen und Wahlen Ausland

(Auszug)



Politische Abstimmungen und Wahlen CH

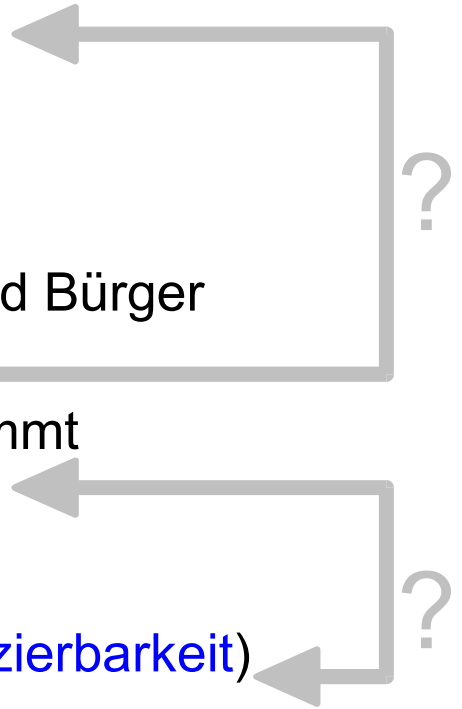


Sicherheit: Was ist anders als bei E-Commerce?

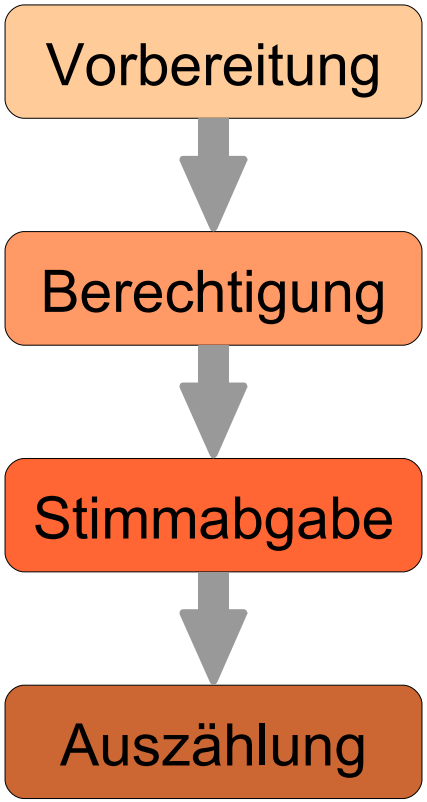
- Es ist unmöglich, einen Störfall wieder gutzumachen
- Unterschiedliche, zum Teil konkurrierende Sicherheitsanforderungen
- Erfolgreicher Angriff → **Man weiss es nicht!**
  (E-Banking: Erkennbar am Kontoauszug)

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
  - wurde meine Stimme gezählt? (individuelle Verifizierbarkeit)
  - wurde richtig gezählt? (universelle Verifizierbarkeit)



Abstimmungsprozess (vereinfacht)



- Stimmregister
- Identitäten (ID, PIN, ...)

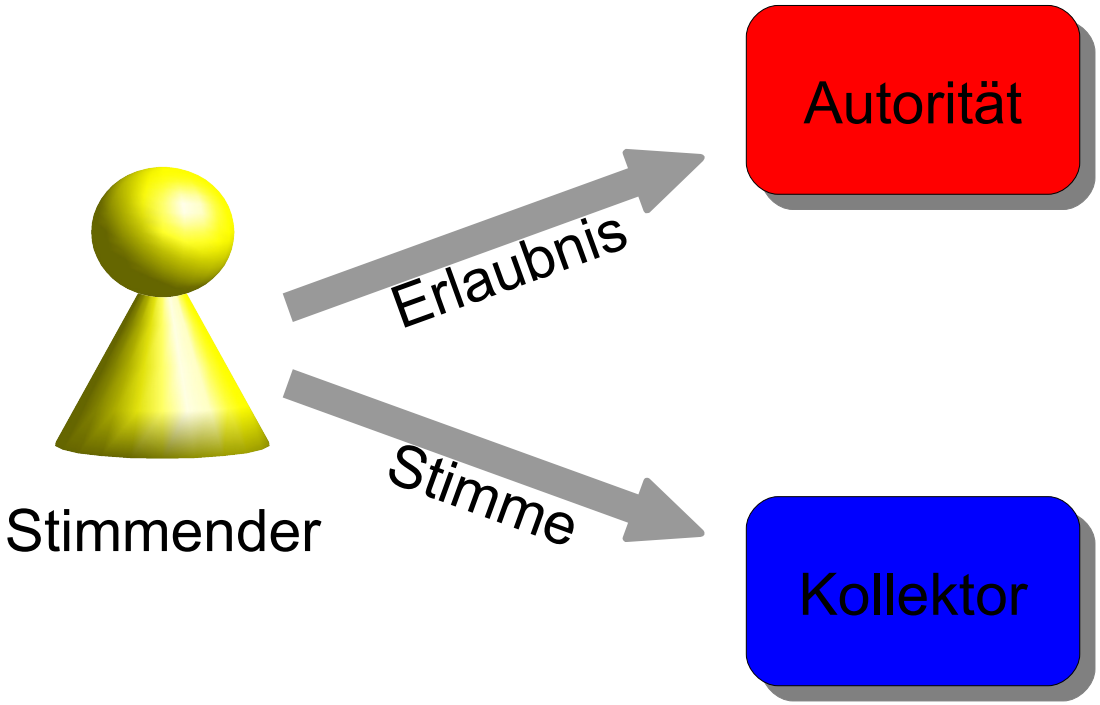
- Autorisation
- nur 1 Stimme

- sichere Stimmabgabe
- Stimmen geheim bis zur Auszählung

- zuverlässiges Resultat
- Vertrauen

E-Voting-Protokolle

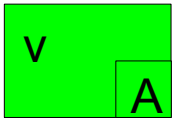
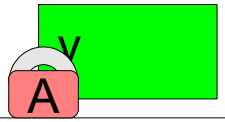
E-Voting-Protokolle: Entitäten

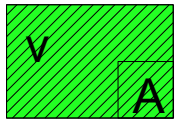
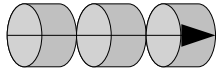
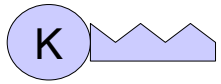


Meistens: **2** Entitäten

manchmal 1, manchmal 3 oder mehr

Piktogramme für Stimmende und kryptographische Primitiven

Identität des Stimmenden	
Stimme v	
Durch A signierte Stimme v	
v verschlüsselt, A hat den Schlüssel zum Entschlüsseln	

Stimme v, blind signiert von A	
Sicherer Kanal	
Anonymer Kanal	
Schlüssel zum Entschlüsseln	

E-Voting-Protokolle: *Basis-Bausteine*

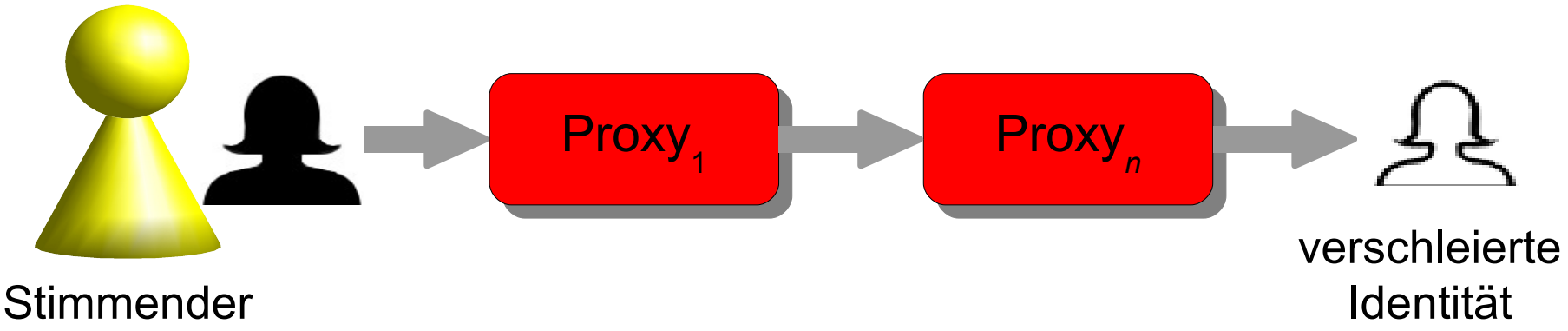
- symmetrische Verschlüsselung: $c = E(m, k)$
- symmetrische Entschlüsselung: $m = D(c, k)$
- kryptografische Prüfsumme: $h(m)$
- öffentlicher Schlüssel: Xe
- privater Schlüssel: Xd
- asymmetrische Verschlüsselung: $c = E(m,Xe)$
- asymmetrische Entschlüsselung: $m = D(c,Xd)$
- signierte Meldung: $s = S(m,Xd)$
- Validierung der signierten Meldung: $V(s,Xe) \in \{richtig, falsch\}$

E-Voting-Protokolle: *Blinde Signatur*

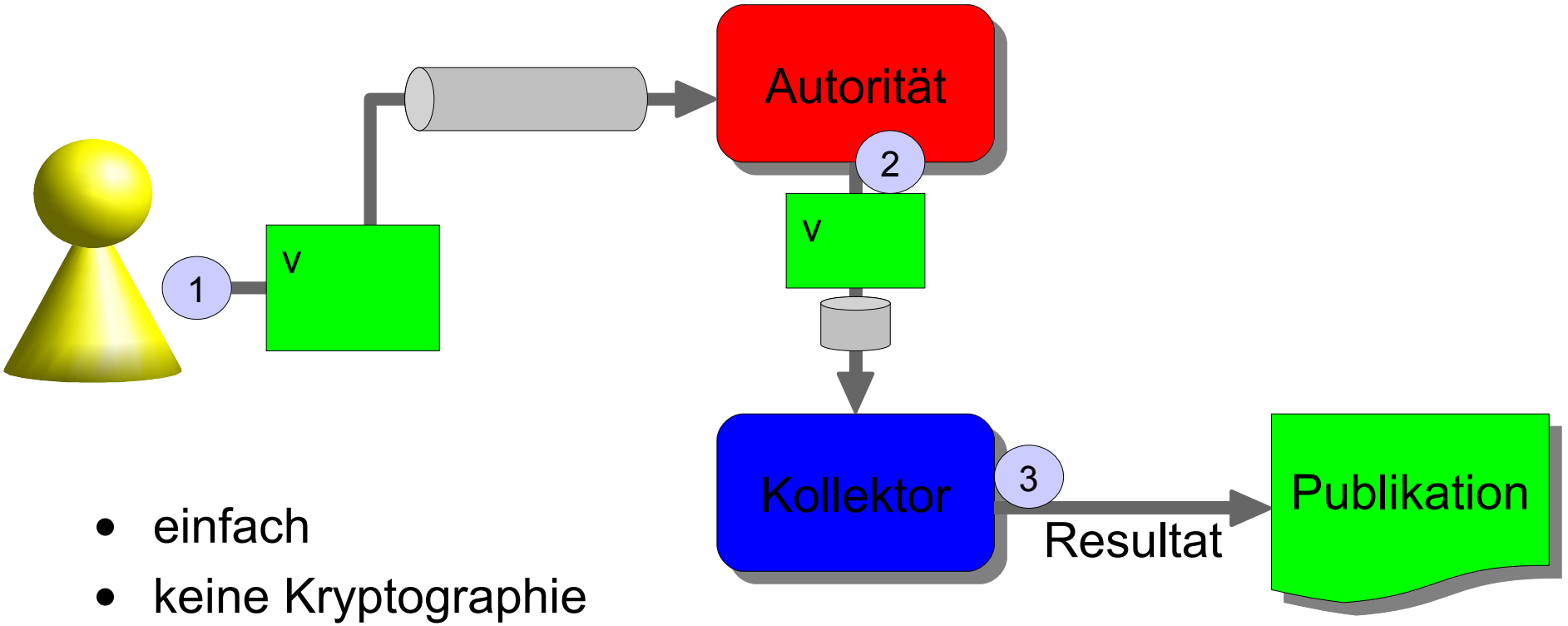
- Idee:
  Eine Meldung *m* wird von Person *X* signiert, ohne dass *P* den Inhalt von *m* kennt.
- Chaum (1983)
- Zufallszahl: *r* (relative Primzahl zu *N*)
- Blindisierungsfaktor: r^{Xe}
- Blindisierte Meldung: $m \times r^{Xe}$
- Blinde Signatur von *m*: $s' = S(m \times r^{Xe}, Xd)$
- Signatur von *m*: $s = s' \times r^{-1} = S(m, Xd)$

E-Voting-Protokolle: *Anonyme Kanäle*

- Idee:
  Versand einer Meldung *m* über einen Kanal so, dass der Ursprung von *m* unbekannt ist
  - Mix-Net (Chaum, 1981)
  - DC-Net (Chaum, 1988)
  - Onion routing (Goldschlag, Reed, Syverson, 1999)

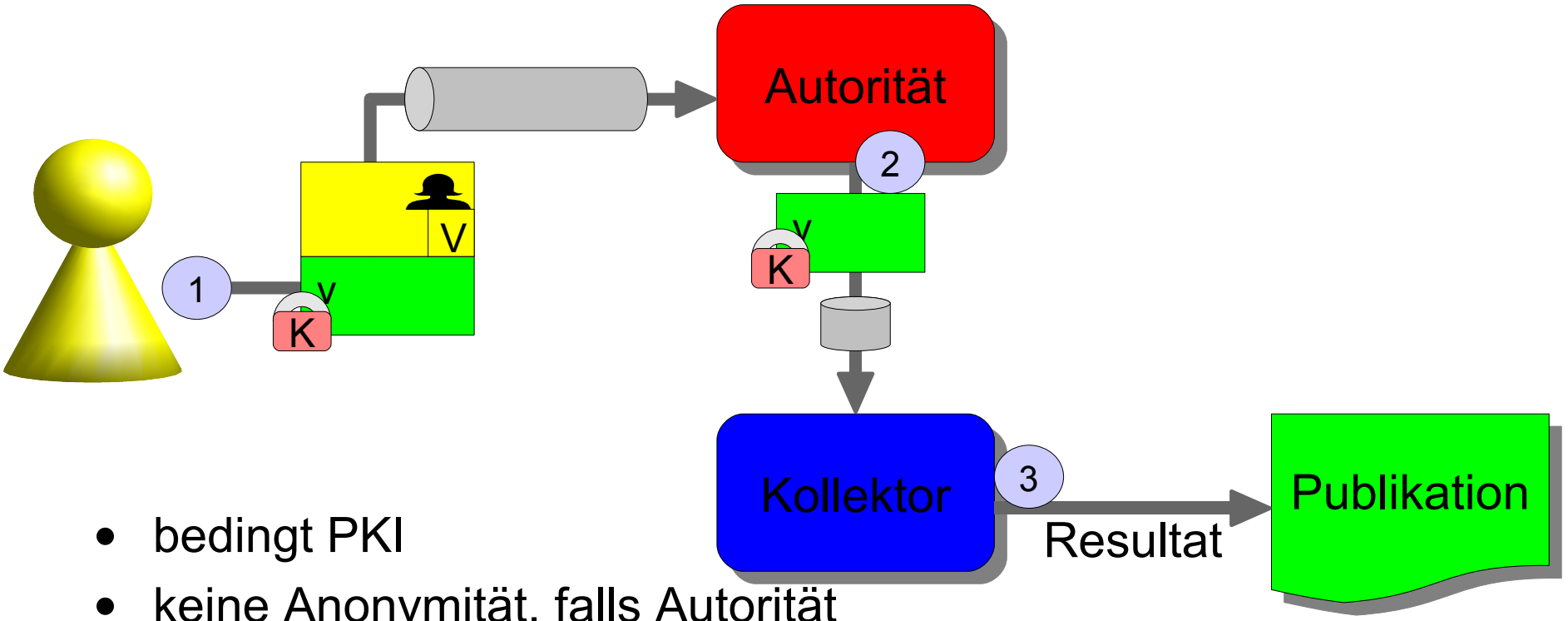


Ein zu simples E-Voting-System



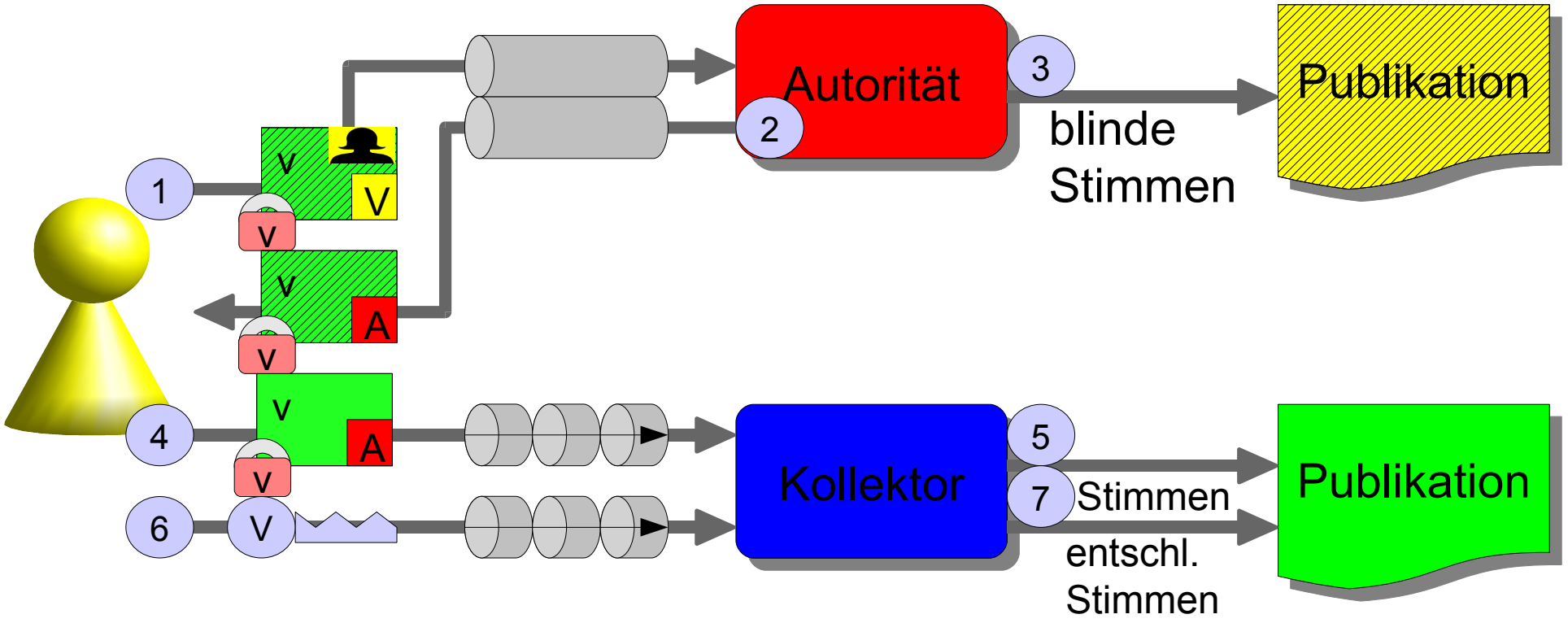
- einfach
- keine Kryptographie
- verletzt viele Anforderungen

Eine Verbesserung: Kryptographie alleine genügt nicht



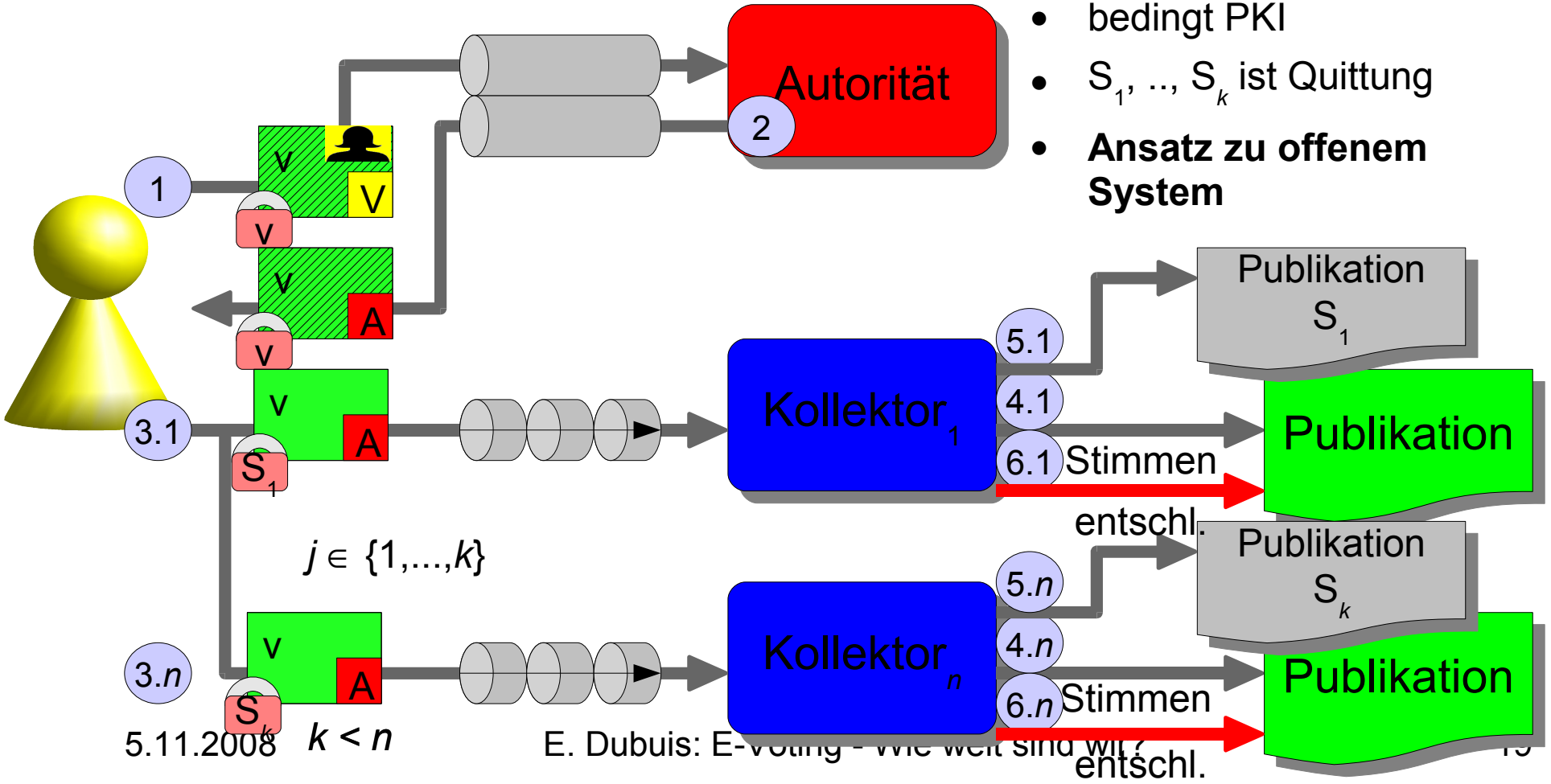
- bedingt PKI
- keine Anonymität, falls Autorität und Kollektor kooperieren

Weitere Verbesserung (Fujioka et al. 1992)



- bedingt PKI
- Stimmender 2 Mal engagiert
- Quittung

Weitere Verbesserung dank Schwellwertverschlüsselung (partieller Ansatz)

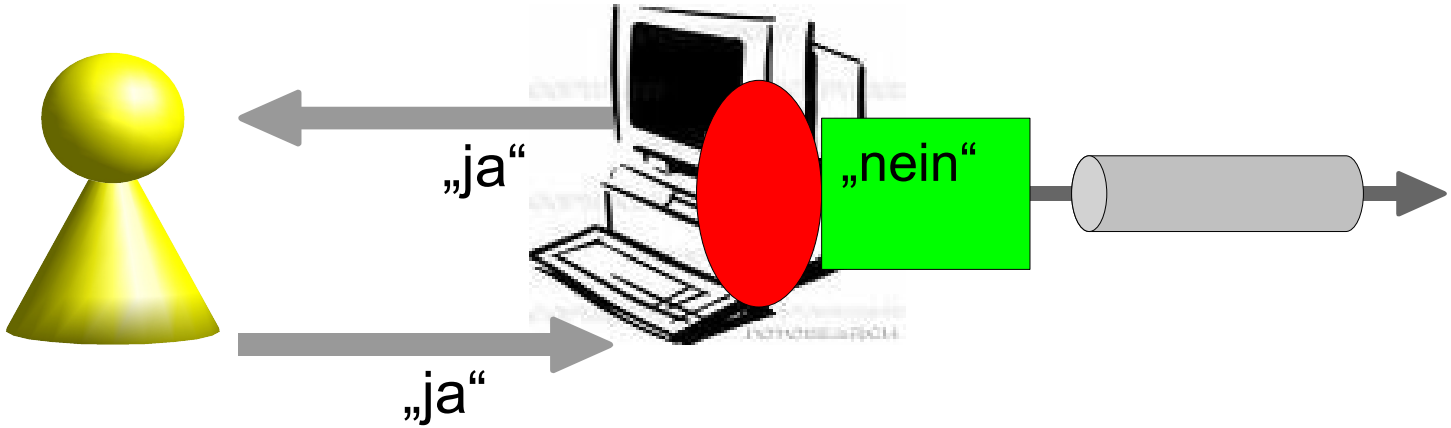


- bedingt PKI
- S_1, .., S_k ist Quittung
- **Ansatz zu offenem System**

Secure Platform Problem

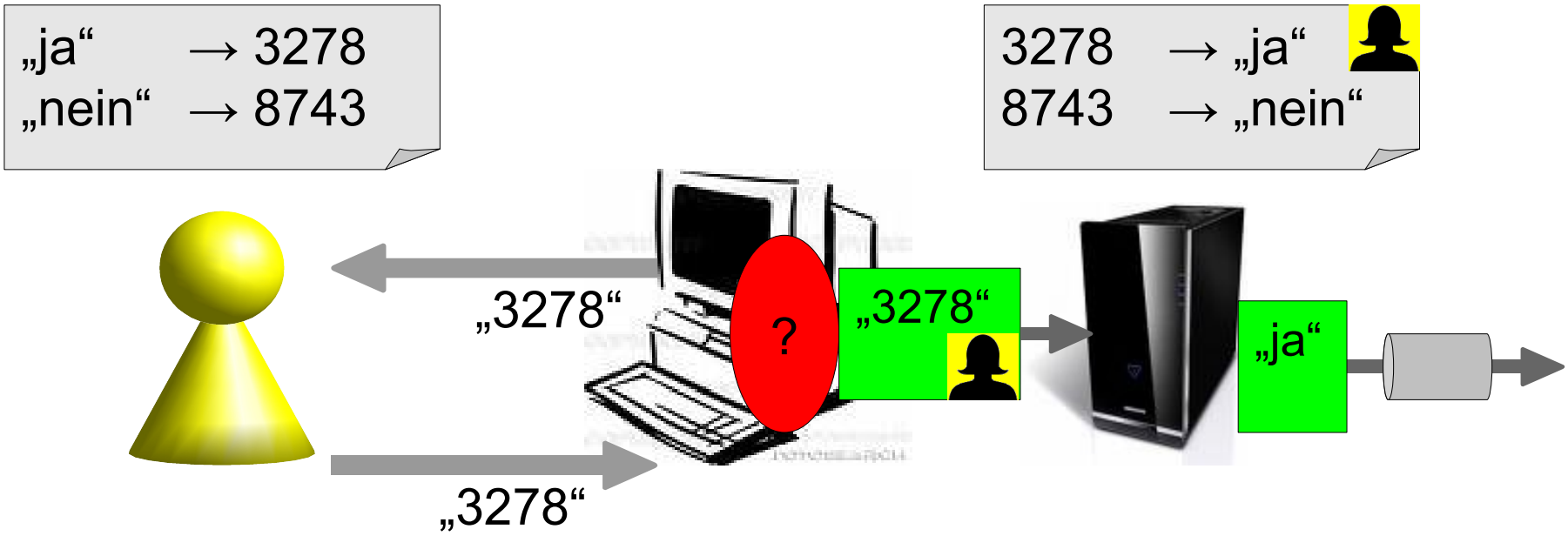
Secure Platform Problem

- Die Plattform des Stimmbürgers ist gefährdet!
- Gefahren sind:
  - Computer-Viren
  - Trojaner



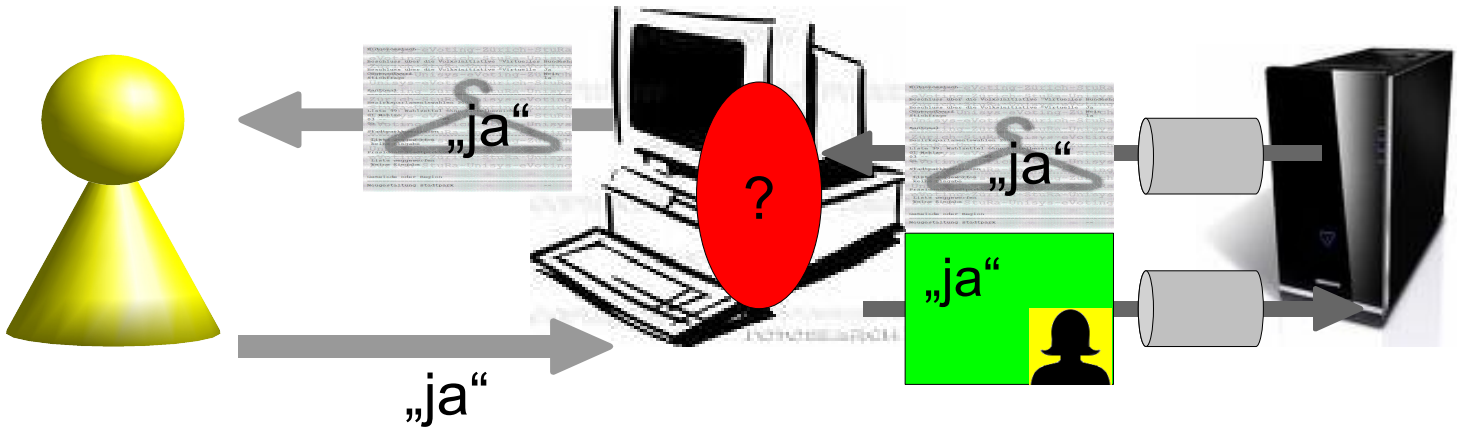
Secure Platform Problem: Abhilfe durch Codes

- Geheime Codes pro Stimmbürger



Secure Platform Problem: Abhilfe durch Bild

- Stimmzettel als Bild



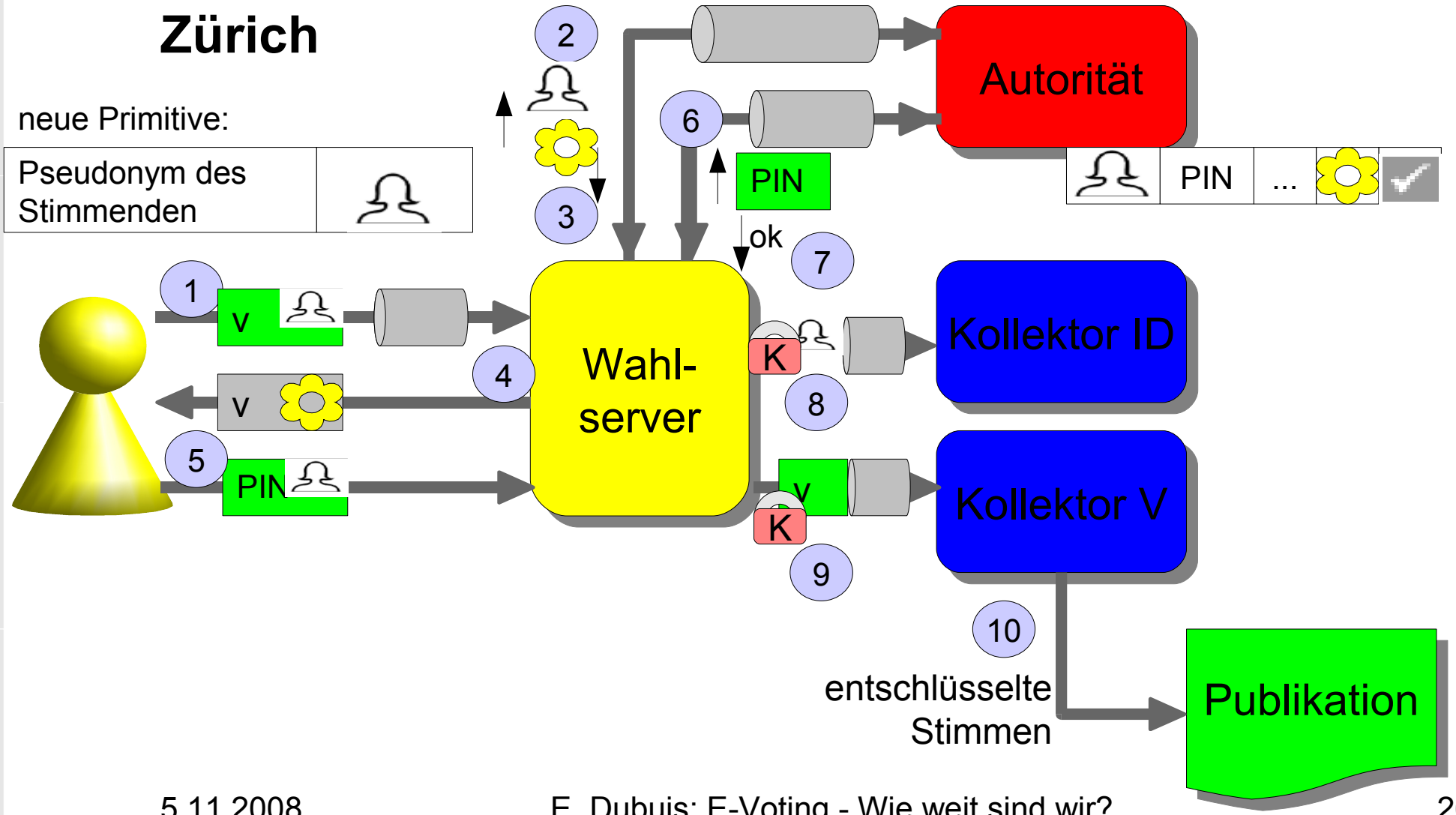
Schluss

CH-Systeme im Überblick

	Identifkator	Protokoll			Quittung
GE	Einmal-ID	unbekannt			keine
NE	permanente ID				verschlüsselte Quittung
ZH	Einmal-ID				keine

Angaben ohne Gewähr, nicht wertend

Zürich


neue Primitive:
Pseudonym des Stimmenden
2
3
6
Autorität
PIN
PIN
...
ok
7
1
v
4
Wahl-server
K
Kollektor ID
8
v
5
PIN
v
K
Kollektor V
9
10
entschlüsselte Stimmen
Publikation

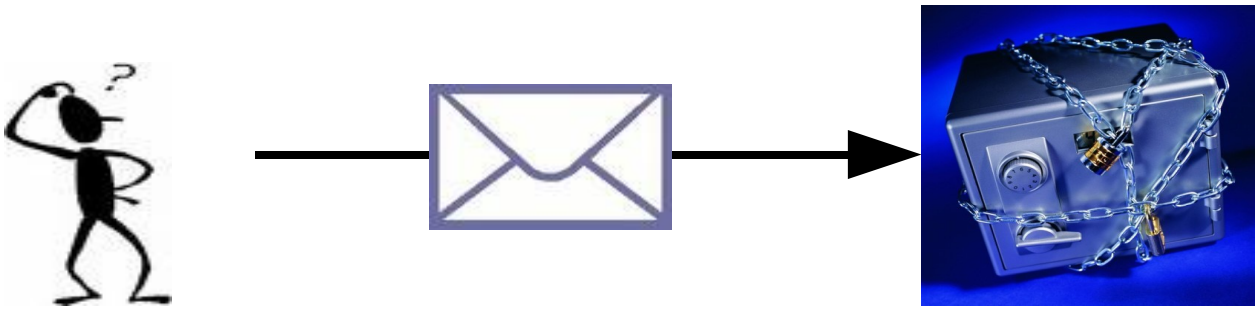
Fazit

- Mit Papier und Urnen durchgeführte Abstimmungen oder Wahlen sind einfach und überschaubar
- Andererseits: E-Voting-Systeme, speziell solche via Internet, sind äusserts schwierig
- Dazu braucht es ein Arsenal an kryptographischen Primitiven (blinde Signaturen, anonyme Kanäle und mehr)
- Weitere, offene Frage (nebst dem SPP-Problem):

Frage der Transparenz

- *„Die Auszählung der Stimmen in einem Wahllokal ist für jeden nachvollziehbar, die Speicherung der Stimme in einem Zentralcomputer nicht.“*

Johann Hahlen, Bundeswahlleiter, 18.09.2001



Vielen Dank!