13. DFN-CERT Workshop
Sicherheit in vernetzten Systemen

Internetwahlsysteme in der Praxis

Jörg Helbach

Warum elektronisch wählen?

- Steigerung der Wahlbeteiligung
- Kostensenkung
- schnelleres Wahlergebnis
- Anspruch der Mitglieder an die 'Fach'gesellschaft GI

Wahlgrundsätze

- Allgemein
- Unmittelbar
- Gleich
- Frei
- Geheim

WWW.GI-EV.DE

Dimensionen elektronischer Wahlen

- Recht
- Politik
- Gesellschaft
- Technik

Klassifizierung

Ein Wahlsystem heißt **elektronisches Wahlsystem**, wenn es durch elektronische Hilfsmittel unterstützt wird.

Klassifizierung (2)

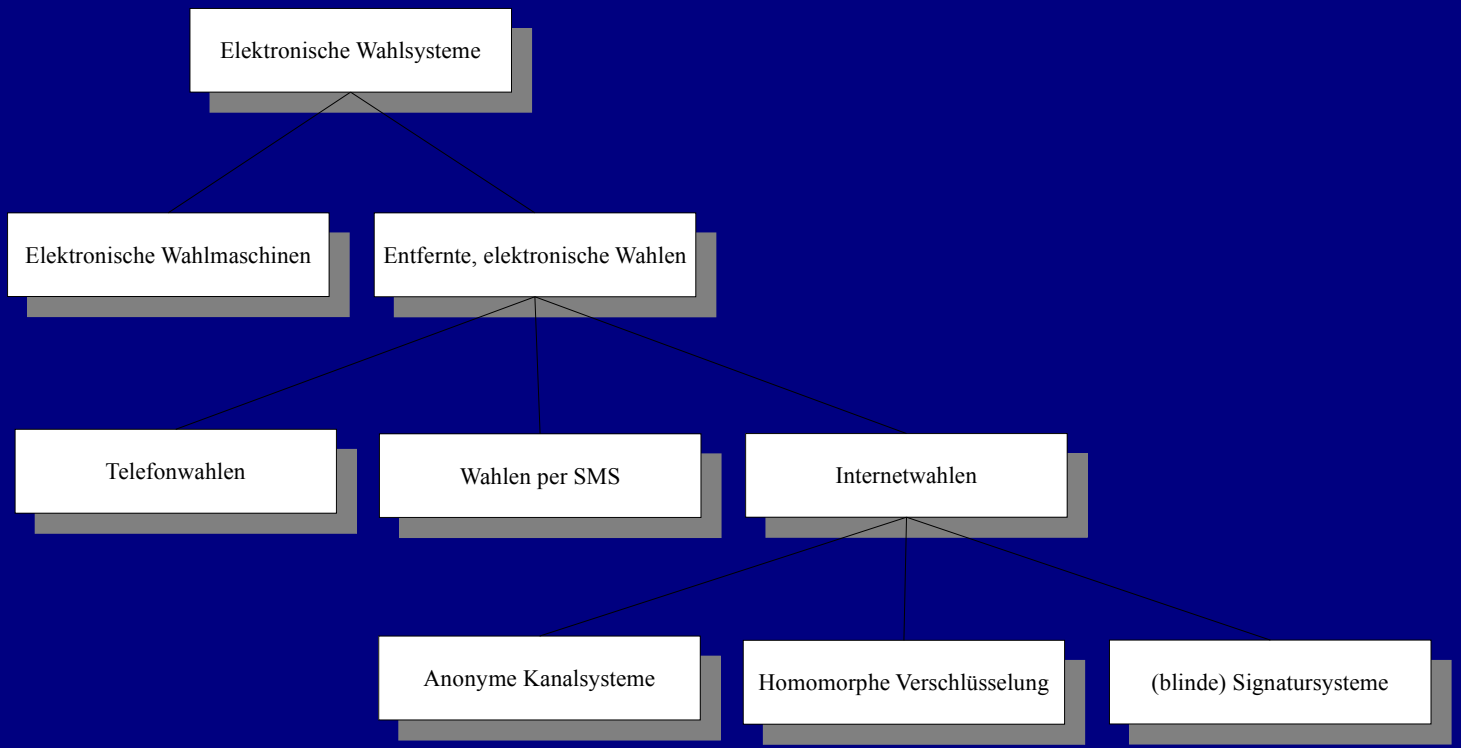
- Wahlmaschinen
- Entfernte Wahlen
  - Telefon
  - SMS
  - Internetwahlen

Klassifizierung (3)

Internetwahlsysteme

- Anonyme Kanalsysteme
- Homomorphe Verschlüsselung
- (blinde) Signatursysteme

Klassifizierung (4)



Grundlegende Herausforderungen

- Authentifizierung vs. Anonymität
- Weitergabe von Authentifizierungsdaten
- Manipulation der Voten

WWW.GI-EV.DE

Anforderungen der GI

- Anforderungen an den Hersteller
  - Ausreichende Systembeschreibung
  - Source-Code-Analyse Dritter
  - Idealfall: Open-Source

Anforderungen der GI (2)

- Anforderungen an die Wahlserver
  - Administration nur im Vier-Augen-Prinzip
  - Protokollierung

Anforderungen der GI (3)

- Anforderungen an die Wahlsoftware
  - GI-Satzung
  - Einfache Bedienung

Getroffene Maßnahmen

- Experten-Gremium (Hochschulen, PTB)
- Anforderungskatalog für internetbasierte Vereinswahlen
- Quellcode-Review
- Leitfaden um Mindestmaß an Sicherheit zu erreichen

Das Wahlsystem POLYAS

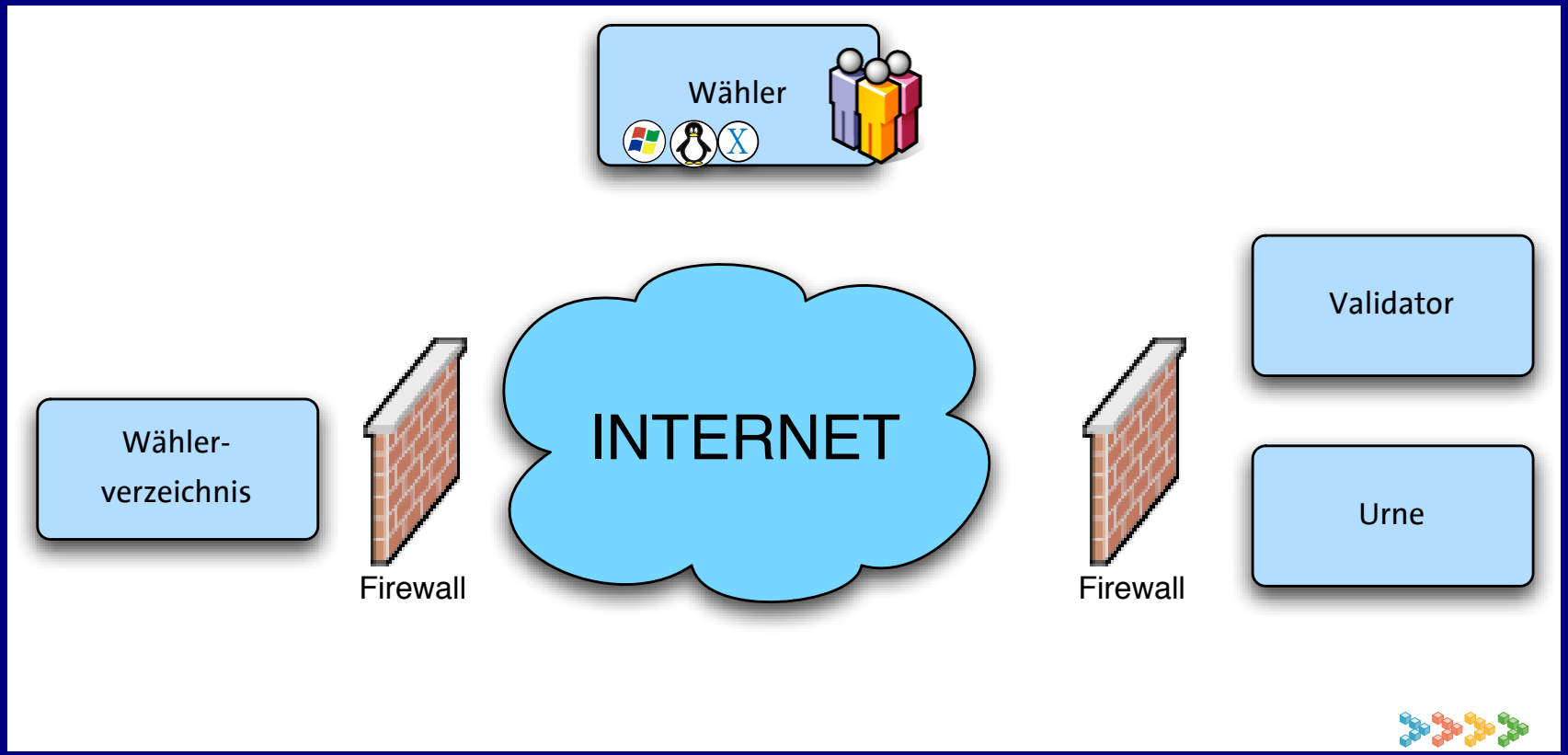
- klassisches Signatursystem
- benannt nach George Pòlya (1887-1985)
- Seit 1996 im Einsatz
- ca. 310.000 abgegebene Stimmen[1]
- Pin/Wahl-PIN bzw. SmartCard

[1] Stand: Dezember 2005

Das Wahlsystem POLYAS (2)

- javabasierte Webanwendung (Tomcat)
- Linux, Trusted Solaris
- relationale, transaktionssichere DB (PostgreSQL)
- Module für: Wahlvorbereitung, -durchführung und -auszählung

Beteiligte Systeme



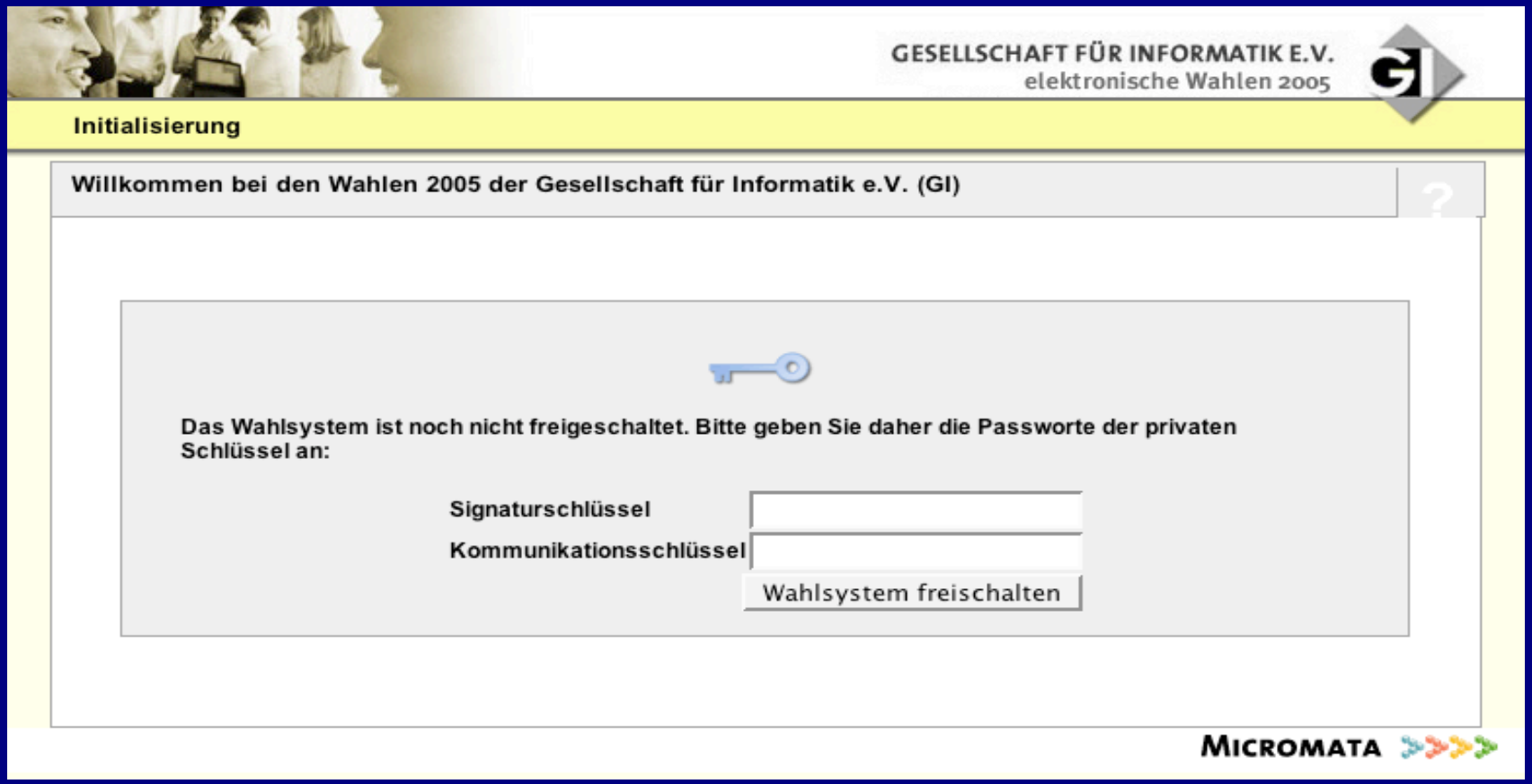
Wahlvorbereitung

- Export der Wählerdaten in eine Textdatei
- POLYAS-Modul
  - SQL-Datei für Wählerverzeichnis
  - SQL-Datei für Validator
  - Daten für Wahlversand (mit PGP verschlüsselt)

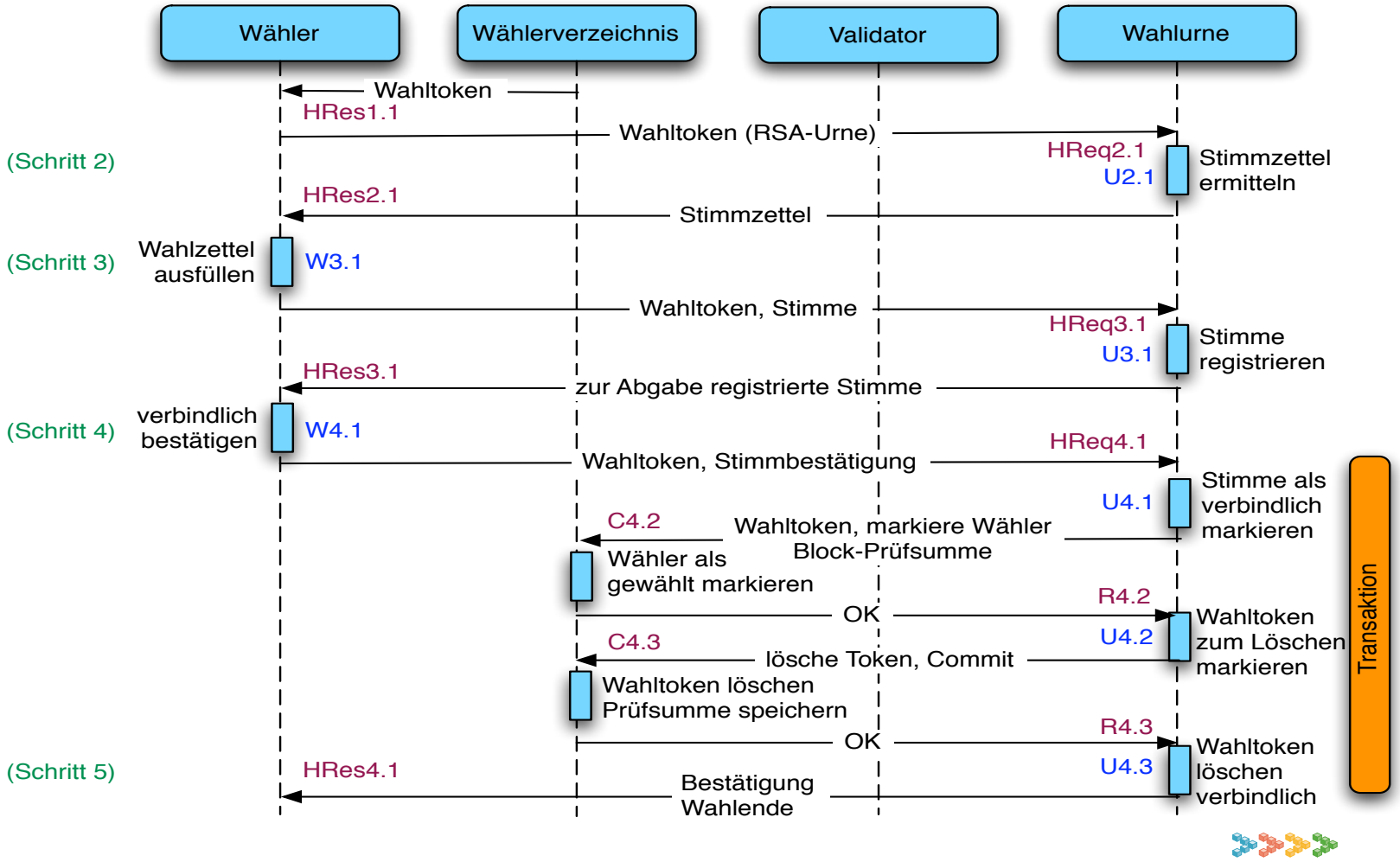
Wahlvorbereitung (2)

- Druck der Anschreiben auf Endlosrolle
- Personalisierung der Anschreiben (Adresse, Wahl-PIN, Data Matrix Code)
- Haftetikett (Rubbelfeld), Falzen, Kuvertieren
- Kamera-Erfassung des DMC

Start des Wahlsystems



Der Wahlvorgang



Wahlauszählung

- Auswertung des Wählerverzeichnisses
  - Export in XML-Datei
  - Hat Wähler an elektronischer Wahl teilgenommen?
  - Signatur unverändert?
  - Prüfsummen

Wahlauszählung (2)

- Auswertung der Urne
  - Export in XML-Datei
  - Auflistung aller Stimmen in 30er Blöcken
  - Prüfsummen
  - Zusammenfassung des Wahlergebnisses

Fazit

Ziele erreicht?

- Steigerung der Wahlbeteiligung
-
-

Fazit

Ziele erreicht?

- Steigerung der Wahlbeteiligung ✓
- Kostenreduktion
-

Fazit

Ziele erreicht?

- Steigerung der Wahlbeteiligung ✓
- Kostenreduktion ✓
- schnelleres Ergebnis

Fazit

Ziele erreicht?

- Steigerung der Wahlbeteiligung ✓
- Kostenreduktion ✓
- schnelleres Ergebnis ✓

Fazit (2)

Restrisiken

- PIN/WahI-PIN
- DOS/dDOS
- Malware auf Wahlclients

Fazit (3)

Ausblick

- (Weitere) Penetration Tests
- CC-Profil für vereinsbasierte, elektronische Wahlen
- Modul für Gliederungen der GI
- Elektronische Präsidiumswahl 2006

WWW.GI-EV.DE

Vielen Dank für Ihre Aufmerksamkeit.
Haben Sie Fragen?