

E-Collecting Hackathon Team 9

Christian Killer, Alessandro de Carli, Lukas Schönbächler,
Andreas Gassmann, Michelle Fund, William Dan, Hao Wang

Prosignum

Phasenübersicht

- **Phase 1:** Pragmatischer Datenschutz ← **Fokus heute**
- **Phase 2:** Erweiterte Sicherheit
- **Phase 3:** Vollständige Privacy-Implementierung

Kernprinzipien für Phase 1

- Integration mit bestehender E-ID-Infrastruktur
- Parallelbetrieb mit Papierkanal
- Föderale Anschlussfähigkeit (Gemeinden, Kantone)
- Einfache Verifizierung durch Stimmregister

Phase 1: Pragmatismus & Integration

Technischer Ansatz

- E-ID-Authentifizierung (Swiyu)
- Digitale Signierung
- Verschlüsselte Speicherung / Confidential Compute*

Herausforderungen

- Föderale Heterogenität der Stimmregister
- Deduplizierung zwischen digital und Papier
- Datenschutz vs. Verifizierbarkeit

DEMO

Vorteile

Vorteile

- **Simple und pragmatisch:** keine komplexe Kryptographie
- **Schnell umsetzbar:** nutzt bestehende E-ID
- **Vertraute Infrastruktur:** Stimmregister bereits etabliert
- **Niedrige Einstiegshürden** für Gemeinden

Vertrauensannahmen & Nachteile

Vertrauensannahmen

- Vertrauen in Gemeinden/Stimmregister
- Vertrauen in E-ID-Provider
- Vertrauen in Bundeskanzlei
- Vertrauen in das Endgerät der Stimmberechtigten (z. B. Apple, Google etc.)

!! Fehlende Resilienz, Privatsphäre und Verifizierbarkeit

- Keine kryptografische Verifizierung
- Keine Auditierbarkeit für Stimmberechtigte
 - in Phase 2/3 adressieren (ZKP, Homomorphe Verschlüsselung)