Anonymous Proof-of-Presence Groups for Messaging and Voting

PoP Team

Students: Céline Camacho, Gabriel Fleischer, Sébastien Fulpius, Raoul Gerber, Jean-Baptiste Michel, Romain Pugin, Nicolas Raulin, Ouriel Sebbagh, Alexis Tabin, Maxime Würsch

Pr. Bryan Ford, Advisor
Pierluca Borsò, Advisor Louis-Henri Merino, Supervisor Haoqian Zhang, Supervisor
Outline

1. Problem
2. Concept
3. Communication
4. Application
5. Demo
6. Conclusion
How to guarantee online accountability while preserving anonymity?
Proof of Personhood

Problem

Concept

Communication

Application

Demo

Conclusion

- Bind physical to virtual identities
- Verify rather than identify
- One person one vote
- Pseudonym parties
Proof of Personhood

- Bind physical and virtual identities
- Verify rather than identify
- One person one vote
- Pseudonym parties
The Concept

- Applied Proof of Personhood
The Application

- Web and Android front-end, Go and Scala back-end
- QR Code
  - Organizer
  - Identity
- Local Autonomous Organization (LAO) creation and modification
- Schedule events (meetings, roll-call, poll, vote)
Communication

Publish Subscribe pattern
- Channels, Publishers and Subscribers
- Easily scalable

Web Sockets
- Persistent, full duplex, connections
- Easy to use
Communication

Messages are signed with an Elliptic Curve Digital Signing Algorithm (EdDSA)
The witness ecosystem:

- Make the system easier to trust
- Human validation on important data and events
- Compensate for an organizer failure or for a dishonest organizer
Core features

- Create and update LAO
- Create and close events
- Join a LAO
- Witness signing
- QR code generation & scanning

Extensions

- Vote event
- Witness routing messages
- Multi-organizer LAO
Demo

To launch a new organization please enter a name for the organization (you can change it later)

Organization name

LAUNCH

CANCEL
Conclusion

- Core functionalities implemented
  - User Interfaces for front-end
  - Organizer back-end
- Base for future work
  - Interaction with back-end
  - Witness back-end server
Q & A

Problem
Concept
Communication
Application
Demo

Conclusion