Bern University
of Applied Sciences

Verifiable Student Board Elections with UniVote

Eric Dubuis & Rolf Haenni

July 15, 2013

Bern University
of Applied Sciences

UniVote: Project Overview

UniVote: Project Overview

- UniVote = Internet voting system for student board elections at Swiss universities
- 13 months development (February 2012 – February 2013)
- Previous elections
  - March 2013: University of Bern (11'000 students)
  - April 2013: Bern University of Applied Sciences (6'000 students)
  - May 2013: University of Zürich (26'000 students)
- Forthcoming elections
  - September 2013: University of Lucerne (3'000 students)
  - October 2013: University of Basel (13'000 students)
  - Next elections in 2015 (every 2nd year)
- Verification software available (independent student project)

Bern University
of Applied Sciences

UniVote: Demo

Bern University
of Applied Sciences

UniVote: System Properties

UniVote: System Properties

- PKI based on existing eID infrastructure
- Public bulletin board
  - All election data is published
  - No append-only or fault tolerance mechanisms yet
- Distribution of trust
  - Shared decryption key (3 decryptors, no threshold)
  - Two mix networks (each with 3 mixers, no proof yet)
- Extended voter privacy
  - Anonymity: mixing the public signature keys
  - Secrecy: mixing the votes
- Transparency (publication of source code and documentation)
- VoteVerifier: developed independently from specification

Bern University
of Applied Sciences

UniVote 2.0

UniVote 2.0

- UniVote 2.0 = Complete redesign of UniVote 1.0
  - Complete proof chain (incl. proof of correct mixing)
  - Independent append-only public bulletin board (UniBoard)
  - Improved underlying cryptographic library (UniCrypt)
  - Extended independent registration service (UniCert) for Google+, Facebook, Twitter, etc.
  - Full compatibility with specification
  - No red crosses in VoteVerifier
  - GUI support for multiple élection types
  - Improved documentation
- Scheduled for December 2014
- Open for collaborations