Bern University
of Applied Sciences

Verifizierbare Internet-Wahlen an Schweizer Hochschulen mit UniVote

Rolf Haenni & Eric Dubuis

INFORMATIK 2013, Koblenz, 17. September 2013

Table of Contents

Bern University
of Applied Sciences

Project Overview

Project Overview

- UniVote = Verifiable Internet voting system for student board elections at Swiss universities

  https://www.univote.ch

- 13 months development (February 2012 – February 2013)
  - 1 main developer and server administrator (50% assistant)
  - 1 PhD student (25% developer for UniVote)
  - 4 professors (protocols, specification, system design, ...)
- Source code and documentation publicly available:

  https://www.univote.ch/documentation

- Verification software available (independent student project)

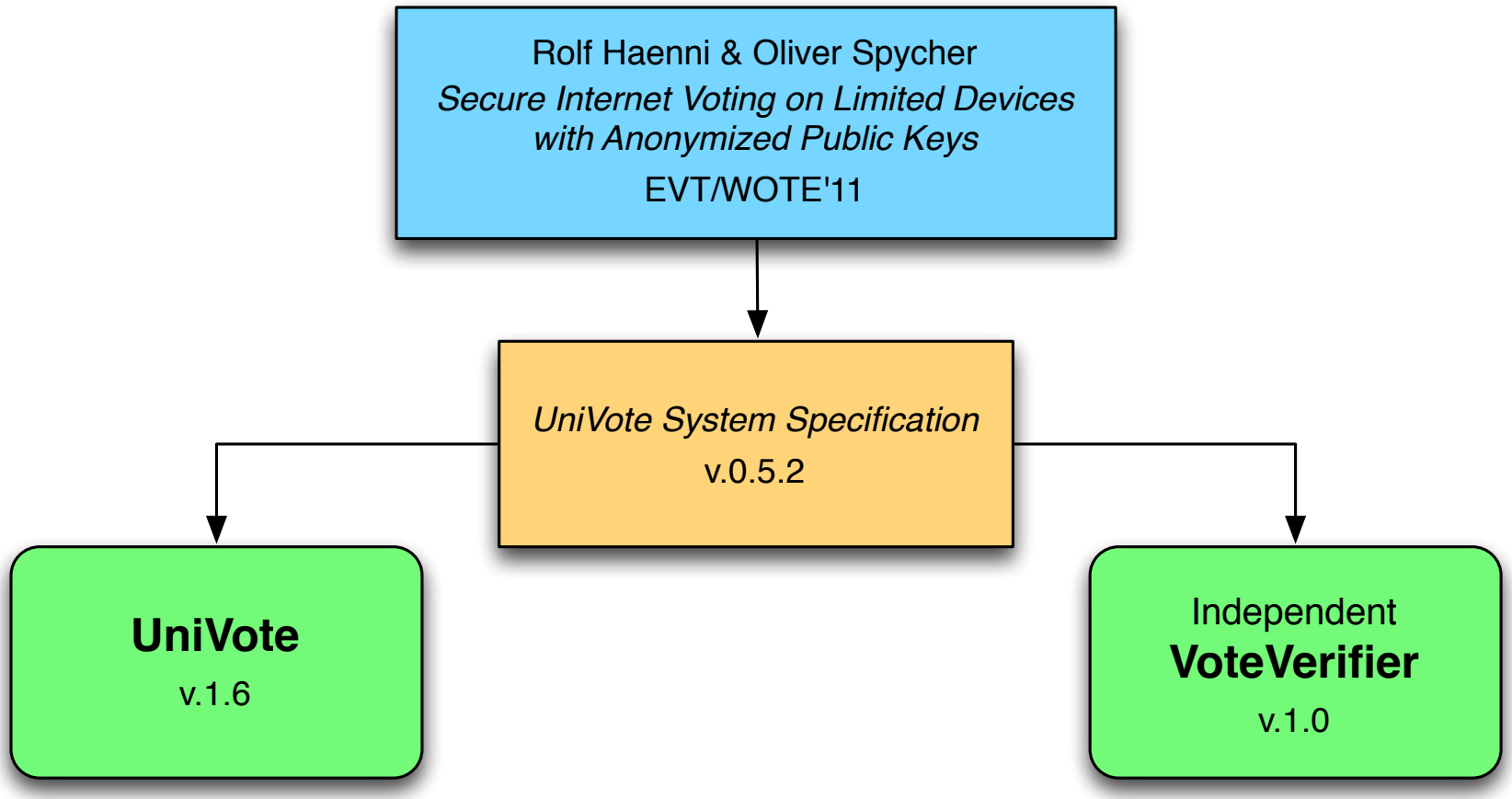
Previous and Future Elections

- Previous elections
  - March 2013: University of Bern (11'000 students)
  - April 2013: Bern University of Appl. Sciences (6'000 students)
  - May 2013: University of Zürich (26'000 students)
- Forthcoming elections
  - September 2013: University of Lucerne (3'000 students)
  - October 2013: Best Teacher Award, University of Lucerne
  - November 2013: University of Basel (13'000 students)
- Forthcoming elections
  - Student initiatives at the University of Zürich
  - Next elections in 2015 (every 2nd year)

Bern University
of Applied Sciences

System Overview

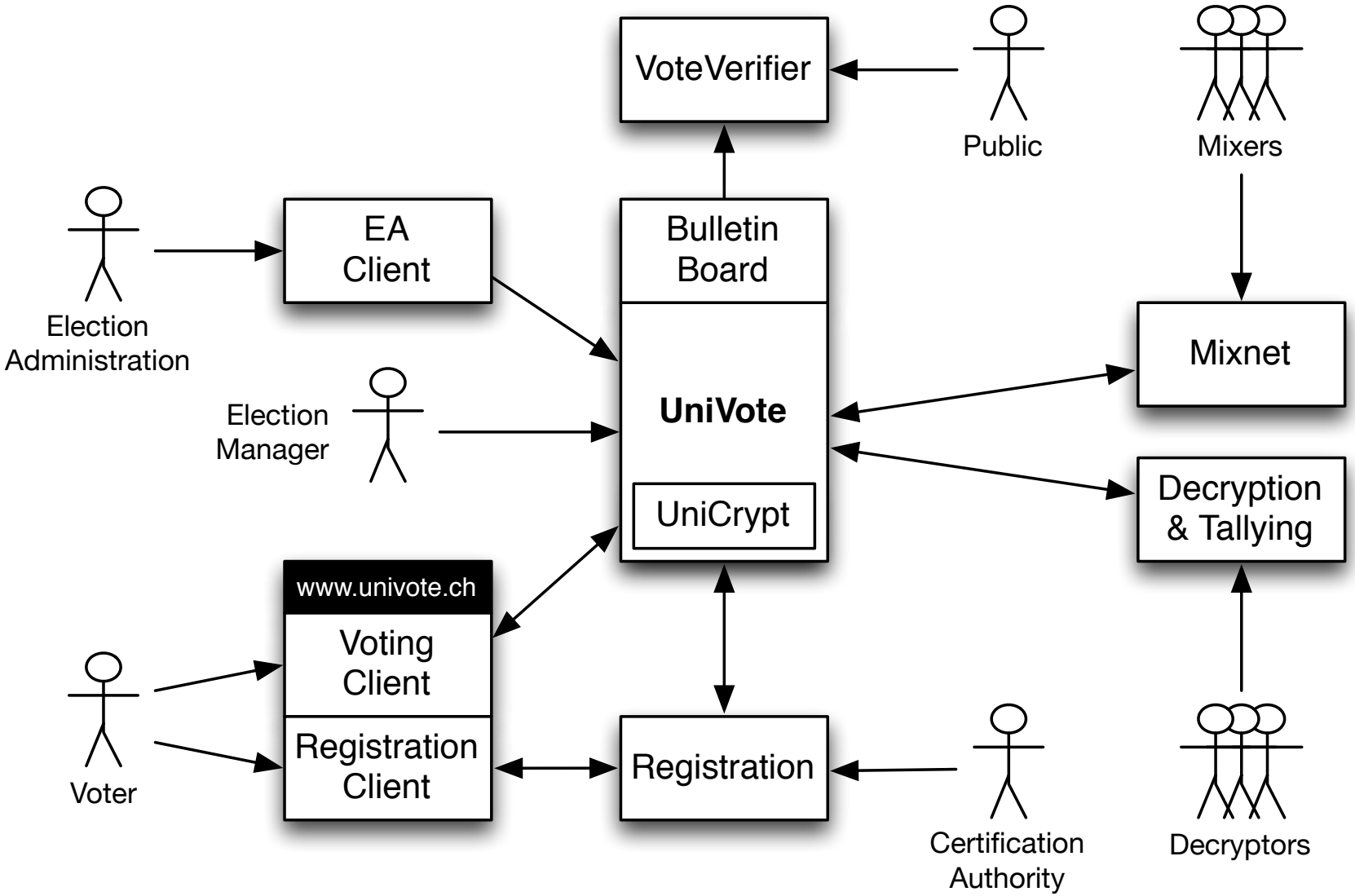
System Specification



System Properties

- PKI based on existing eID infrastructure (SWITCHaai)
- 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)

System Components



Technologies

- Web Client
  - Javascript
  - AJAX
  - jQuery
  - Leemon
  - SWITCHaai
- Server
  - Java EE (EJB, JPA, JCA)
  - Web Services (SOAP)
  - GlassFish 3.x Application Server
- Development
  - NetBeans
  - Maven
  - Jenkins Build Server

Demo

Conclusion and Outlook

Problems

- Time management: up to 3 months behind schedule
- Insufficient tests: bugs “discovered” by voters
- Voter roll inconsistencies: non-unique identifiers, . . .
- Network breakdown during election period (11 hours)
- Browser support: IE6, IE7, . . .
- Deviations from specification (discovered by VoteVerifier)

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 election types
  - Improved documentation
- Scheduled for December 2015
- Open for collaborations