Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Beiträge der BFH zu vertrauenswürdigem E-Voting

Workshop „Vote électronique – Transparenz, Vertrauen, Akzeptanz“ in Bern

8. April 2016

Eric Dubuis

Präambel:

Verifizierbare E-Voting-Systeme fördern das Vertrauen in die Korrektheit der Stimm- bzw. Wahlresultate.

Inhalt

- UniVote
- Krypto-Bausteine
- Geplante Beiträge

UniVote

- Studentenratswahlen
  - Wahlen mit den Universitäten Bern, Zürich, Luzern, (Basel)
  - Wahlen mit der BFH
  - Abstimmungen: *Best Teacher Award*, Urabstimmung (Uni Basel)

- Seit 2013
  - Mehr als 8 Wahlen
  - Mehrere Abstimmungen
  - Grössen der Elektorate:
    Zürich: 26‘000; Bern: 13‘000; BFH: 6‘500; Luzern: 3‘000

- Basiert zu 100% auf dem Internet
- Registration der Wahlberechtigten geschieht via SWITCHaai
- Detaillierte Spezifikation des Wahlprotokolls

UniVote

Vertrauensbildende Elemente

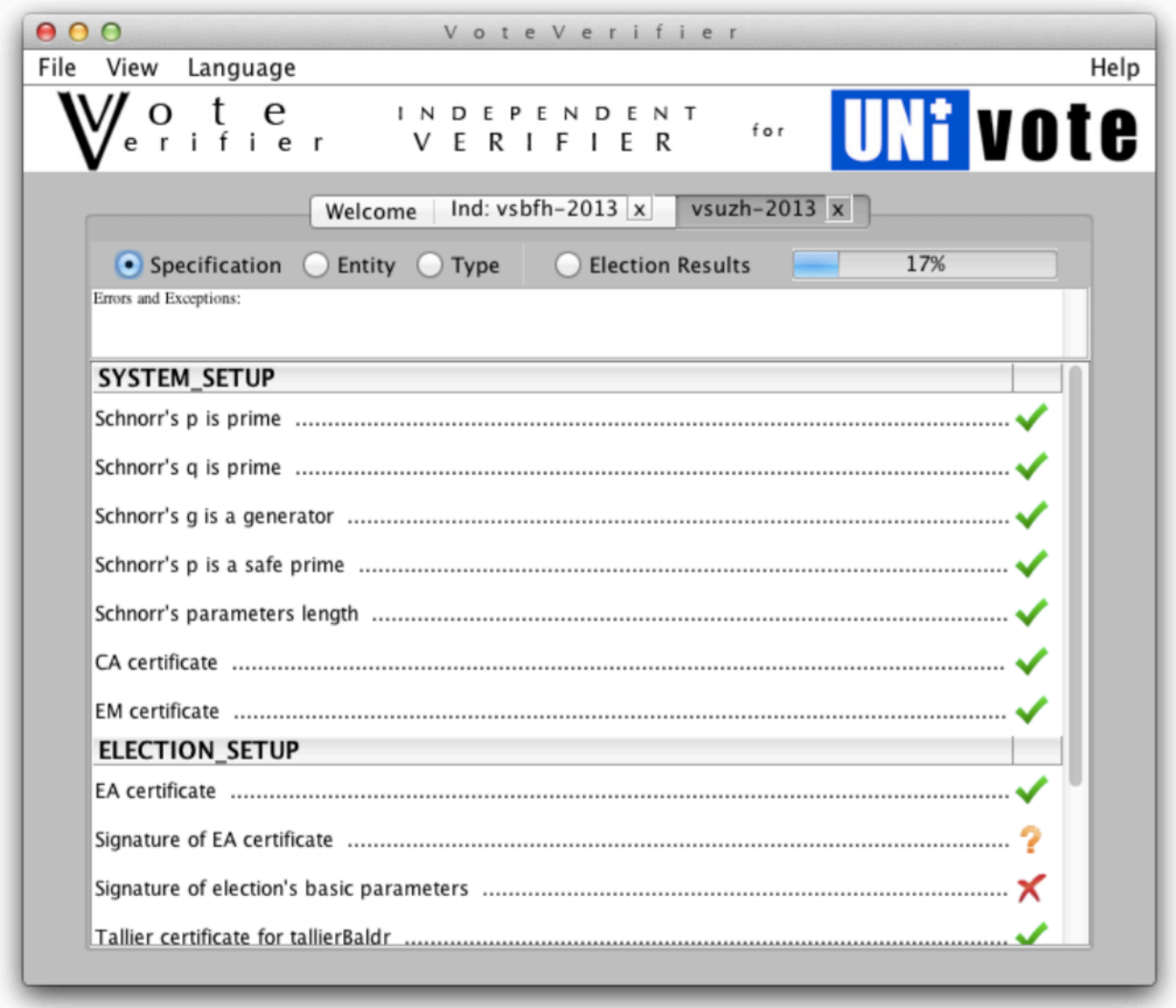
- Schlüsselpaar für die Stimmberechtigten
- Anonymisierter öffentlicher Schlüssel (*voting key*)
- Mischen der Stimmen (nötig wegen „*late registration*“)
- Trustees fürs Anonymisieren und Mischen
- Trustees fürs Entschlüsseln
- Öffentliches Anschlagbrett (*public bulletin board*)
- Verifikationsprogramm (Prototyp)

UniVote

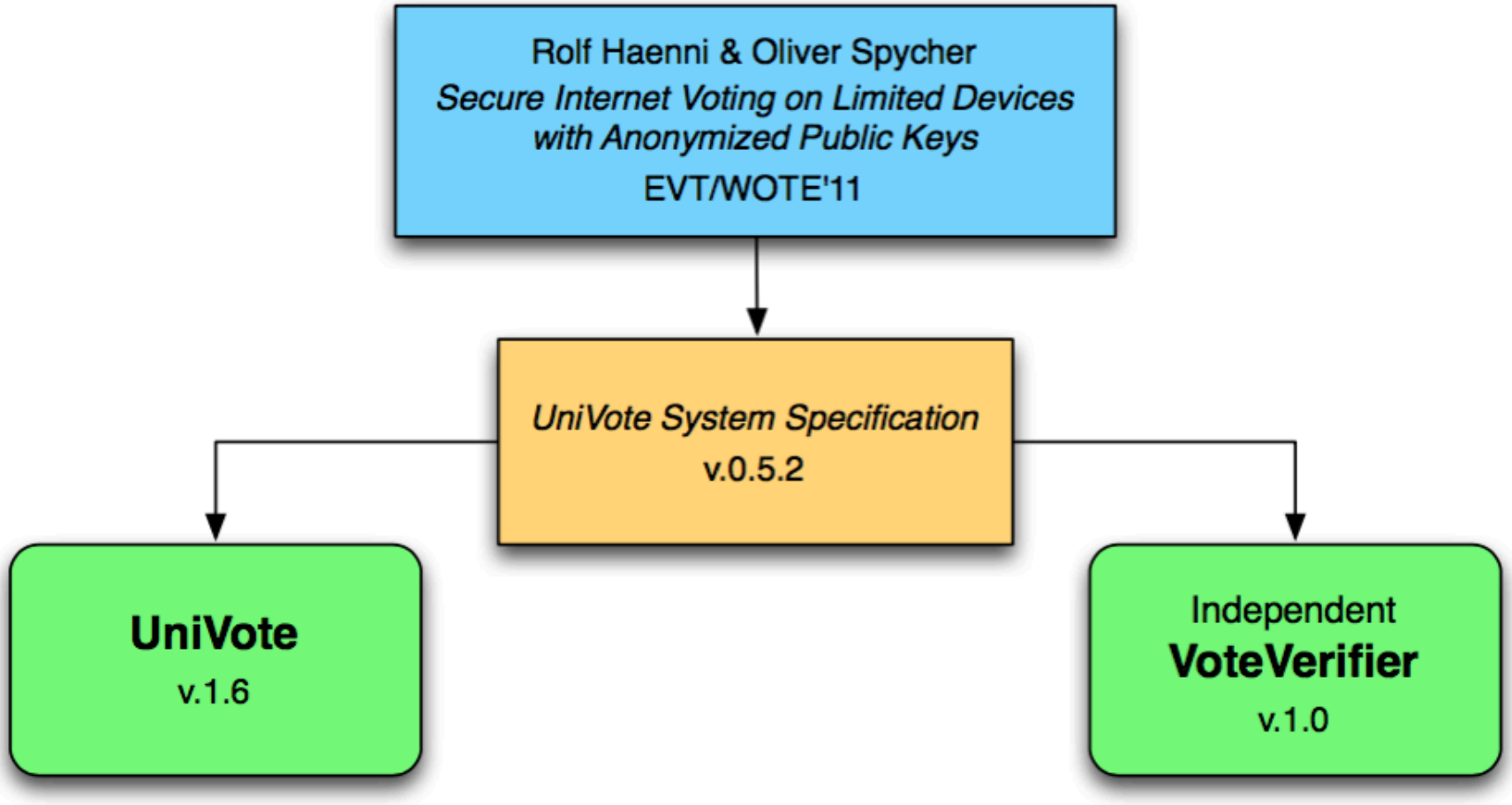
Trust Assumptions

- Plattform des Stimmberechtigten arbeite korrekt
- Die „*ever-lasting privacy*“ sei kein Problem

UniVote


VoteVerifier
File View Language Help
Vote Verifier
INDEPENDENT VERIFIER for UNIvote
Welcome
Ind: vsbfh-2013 x
vsuzh-2013 x
Specification
Entity
Type
Election Results
17%
Errors and Exceptions:
SYSTEM_SETUP
Schnorr's p is prime
Schnorr's q is prime
Schnorr's g is a generator
Schnorr's p is a safe prime
Schnorr's parameters length
CA certificate
EM certificate
ELECTION_SETUP
EA certificate
Signature of EA certificate
Signature of election's basic parameters
Tallier certificate for tallierBaldr

UniVote


Rolf Haenni & Oliver Spycher
Secure Internet Voting on Limited Devices with Anonymized Public Keys
EVT/WOTE'11
UniVote System Specification
v.0.5.2
UniVote
v.1.6
Independent
VoteVerifier
v.1.0

Kryptographische Elemente

- DL (*discrete logarithm*) basierte Signaturverfahren fürs Signieren der Wahlzettel
  - → Erlaubt die anonyme Abgabe einer Stimme
- Homomorphe Verschlüsselung der Wahlzettel
  - → Erlaubt das Mixen der Stimmen
- *Non-interactive Zero Knowledge Proofs*
  - → Beweist, dass Stimme von Stimmenden ist
  - → Beweist die Korrektheit der Wiederverschlüsselungen der Mischer
  - → Beweist die Korrektheit der Permutationen der Mischer
- *Commitments*
  - → Zwingt die Trustees mit den „richtigen“ Werten (Schlüssel, ...) zu operieren

→ Java Krypto-Bibliothek *UniCrypt*

Herausforderungen

- *Secure Platform Problem*
  - Es braucht „*trust anchor*“ bei den Stimmberechtigten
  - Heute: Papier (mit „*return codes*“)
  - Morgen?
- *Everlasting Privacy / Perfect Privacy*
  - Stimmberechtigter hat Schlüsselpaar, öffentlicher Schlüssel wird publiziert
  - *Commitment* und NIZKP fürs Publizieren der Stimme
  - Braucht **anonymer** Kanal
- Robustes, vertrauenswürdiges Anschlagbrett
  - Dedizierte Lösung (Doktorarbeit)
  - Verlinkung mit Blockchain-Technologie wird geprüft

Geplante Kooperationen

- Genf
  - Mitwirkung beim Erstellen / Spezifizieren des Protokolls
  - Mitwirkung beim *Proof-of-Concept*
- Post/Neuchâtel
  - Analyse des Protokolls
  - Verifikations-Software

Zusammenfassung

Die E-Voting-Gruppe der BFH hat...

- Erfahrung mit dem Bau eines E-Voting-Systems
- Erfahrung mit der Realisierung einer Verifikations-Software
- Erfahrung mit der Erstellung von detaillierten Spezifikationen
- Erfahrung mit der Erstellung von Krypto-Bausteinen

Anstehende Herausforderungen aus Sicht BFH sind...

- Das *Secure Platform Problem*
- Das öffentliche Anschlagbrett
- *Die ever-lasting / perfect privacy*