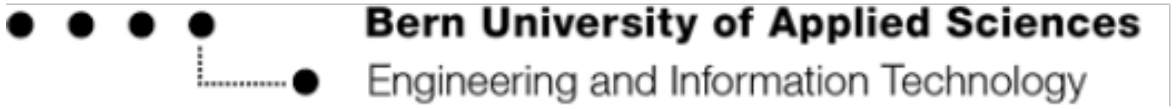


Transparency and Technical Measures to Establish Trust in Norwegian Internet Voting

Oliver Spycher and Melanie Volkamer

E-Voting Conference, 11-09-2011

Outline

- Background
- Measures for trust establishment
- Analysis of the Norwegian system
- Own contributions

Outline

- Background
- Measures for trust establishment
- Analysis of the Norwegian system
- Own contributions

Background

- Oliver Spycher
  - Researcher in electronic voting
  - PhD student at BFH and University of Fribourg
  - Member of the Swiss eVoting Competence Center
  - Part-project leader ″eVoting Security` Swiss Confed.
- Melanie Volkamer
  - PhD ″Evaluation of Electronic Voting` 2008
  - Senior researcher TU Darmstadt since 2008
  - Author of two Common Criteria PP for eVoting
  - OSCE mission to Estonia, 2007
  - Several presentations at CoE conferences

Background

- Paper: Measures to Establish Trust in Internet Voting
  - ICEGOV 2011
  - Norwegian, Estonian, Polyas and Helios System
- Paper: Transparency and Technical Measures to Establish Trust in Norwegian Internet Voting
  - VoteID 2011
  - Application to the Norwegian system in detail
- Mandate: k-resilience term for the Norwegian system

Outline

- Background
- Measures for trust establishment
- Analysis of the Norwegian system
- Own contributions

General Statement

Ensuring high security standards are a necessary condition for gaining trust (in electronic voting) that lasts and that is justified **but** high security standards are alone not sufficient for voters accepting a system and the result of the election.

- Define measures for trust establishement

Different Groups

- need to be convinced namely
  - Experts
  - Average voters

Experts

- Are independent / not part of the project team
- Understand security and cryptography
- Want to have access to detailed information to
  - Analyse security
  - Understand remaining risks
- Communicate with press

Average Voters

- Want to be included in discussions/decisions
- Want to understand the
  - Functionality of the system
  - Basic security features
  - Remaining risks
- Believe in independent experts
- Can be influenced by bad press
- Want to test the system
- Want to have a usable and accessible system
- Want to get support when necessary

Measures

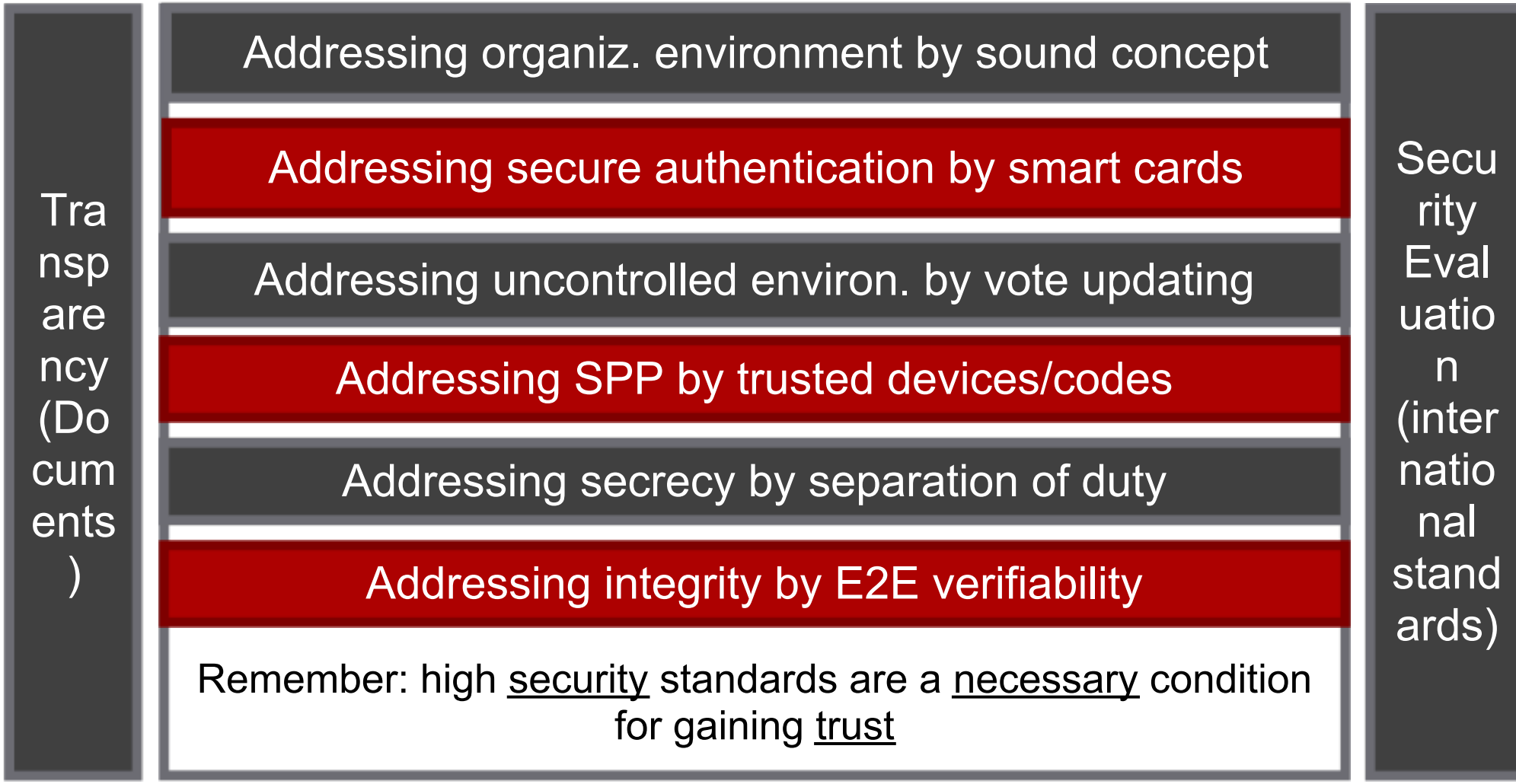
- Two types of measures
  - Security related ones

 To convince experts and average voters

- Non or only indirectly security related ones

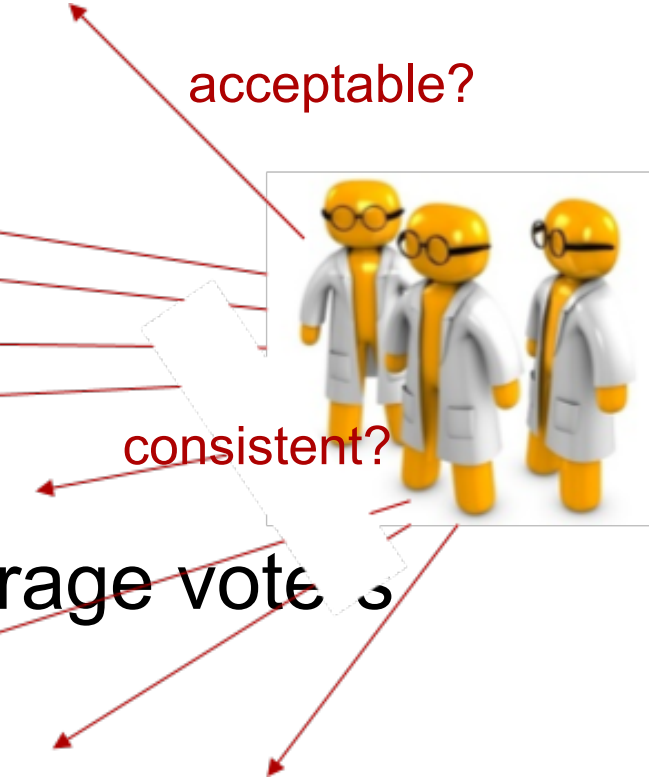
 Mainly for average voters

Security Related Ones



Transparency

- Requirements document
- Voting protocol
- Technical documentation
- Source code
- Description of key management
- Evaluation documents and reports
- Abstract system description for average vote



Non-Security Ones

- Open dicussion
- Transparency
  - Tender, project plan, budget
  - Involved parties and their roles/duties
  - Platform to raise questions
  - ¯ .
- Usability / accesibility
- Test election

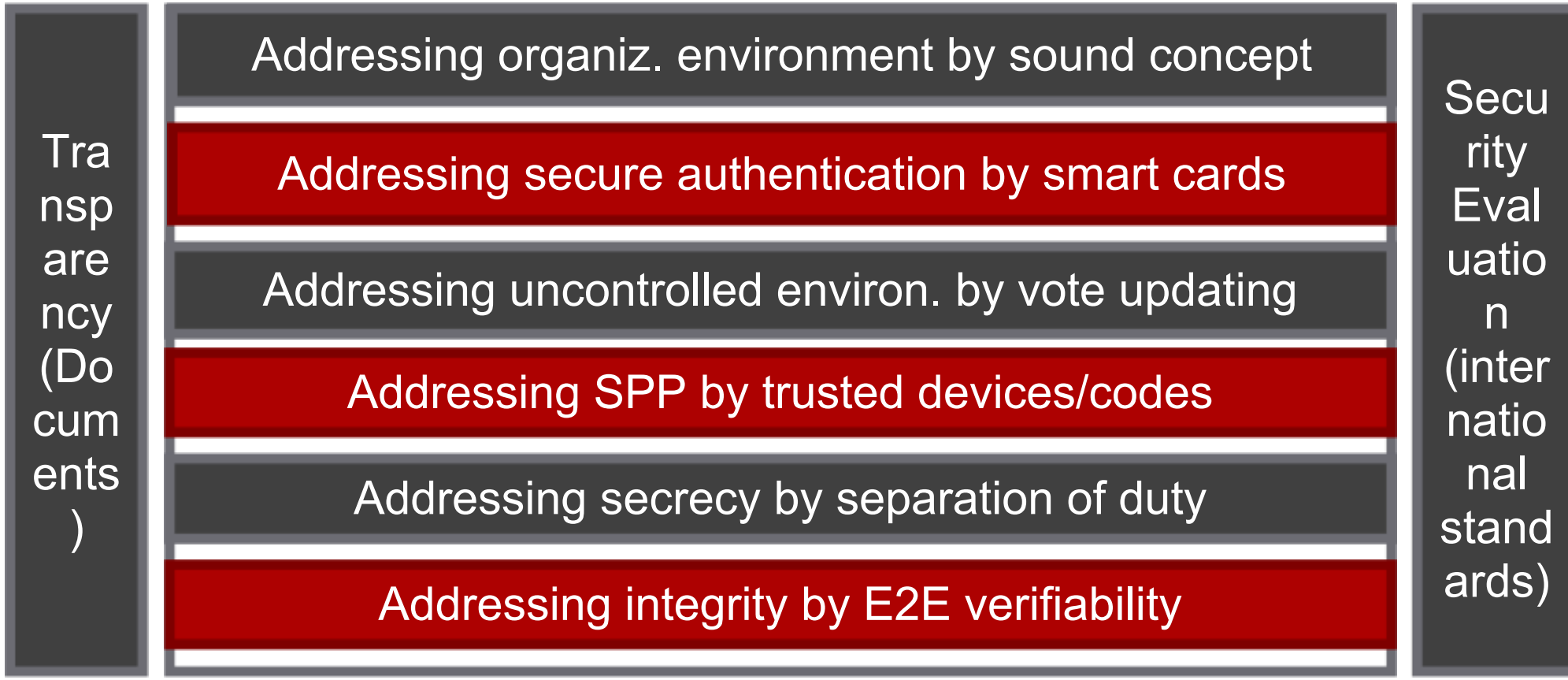
Pitfalls

- Some measures come along with pitfalls
  - In general budget and time
  - Verifiabiliy complexity / usability
  -
  - Decision for or against implementing the measures depends on society, law, type of election

Outline

- Background
- Measures for trust establishment
- Analysis of the Norwegian system
- Own contributions

Security Related Ones



Security Related Ones (1)

- Transparency
  - Many documents online
  - First-hand info from E-valg and manufacturer
- Integrity/E2E verifiability
  - [cast as intended] Malicious software on the voter's PC cannot manipulate if mobile phone works correctly
  - [recorded as cast] Need to trust at least 1 of 2
  - [tallied as recorded] Need to trust at least 1 of x
  - [only eligible voters] Need to trust 1 of 4 + x (BUT!)

Security Related Ones (2)

- Secrecy / Separation of Duty
  - 1 could violate (AuthS)
  - 2 (VCS and RCG)
  - Election board cannot
  - 6 or 1 (6 * EB / DCS) with 1 (RCG / VCS / CS / AS)
- Secure Platform Problem
  - Malicious PC could still violate secrecy
- Uncontrolled environment
  - Vote-updating is implemented

Security Related Ones (3)

- Secure authentication
  - Only MinID available
- Organizational environment
  - Data Centers have ISMSs based on 27001
- Security evaluation
  - Planned if decided to apply internet voting more broadly
  - Common Criteria Security Targets available

Non-Security Ones

- Open dicussion
  - Forum
  - With time
- Usability / accessibility
  - During election
- Test election
  - With pre-system (without SMS)

Outline

- Background
- Measures for trust establishment
- Analysis of the Norwegian system
- Own contributions

Own Contribution (1)

Problem: Voter receives SMS and success message on PC but vote is not counted if VCS deletes it

Solution:

- RCG stores in addition encrypted votes signed by voters
- CS takes votes into account which are either stored by RCG or VCS

 If voter receives SMS and success message on PC then his vote will be counted if at least 1 of 2 is trusted

Own Contribution (2)

For each voter VCS holds a secret value to pre-compute the SMS return codes. (v^s)

Problem: If RCG had known just 1 such value, it could have broken the secrecy of all voters. ($s=K^{ID}$)

Solution:

- If RCG knows just 1 such value, it can only break the secrecy of that particular voter. (s = AES_K(ID))

Own Contribution (3)

The system incorporates a well-established open-source library for cryptographic operations.

Problem: This library contained a bug. (ElGamal generators selected as non-quadradic residuals of Zp*)

Solution:

- We made Bouncy Castle aware and they fixed it in time.

Summary

- Probably most transparent electronic voting project
- One of the few systems addressing verifiability
- Probably the only one in use that addresses the secure platform problem
- One of the few projects that aims for a Common Criteria certificate (EAL4+)

- Some proposals for further improvements

Thank you for your attention!

Questions?