RIES

Rijnland Internet Election System

Zürich, 12. Mai 2005

Jan Meijer
Rijnland Internet Election System

- Built for Rijnland, a Dutch water management body, elected board
- Oldest democratically elected body in .nl
- 1.2 million voters
- Used postal elections so far
- Experimented with using phone in elections
- Turned to Internet voting
  - decrease cost
  - increase voter turn-up
Rijnland Internet Election System

- Built on work done over 10 years by (w)ISCIT
- Enables combining postal and Internet votes
- Uses the 'Robers' voting protocol
- Protocol used in student representation elections of the Technical University of Delft in 1999 using DES smartcards
- \textit{RIES} uses \textit{DES}, \textit{pseudoIDs}, \textit{javascript}
- Close to no demands on end user equipment (equal to Internetbanking requirements)
Rijnland Internet Election System

- Rijnland organises elections
- TTPI (Piet MaclainePont (MullPon) and Arnout Hannink (MagicChoice) run the technical side of the election
- SURFnet makes sure the systems are up and (properly) running
RIES features

• Simple
  – 99.9% of voters were able to vote

• Ballot secrecy assured
  – sensitive operations done at client side
  – no voter secrets leave the client
  – no voter secrets shared with election authorities
  – Vulnerable only at the initial stage (where voter secrets are linked to individual voters): proper organisation solves this (TTP)

• Verifiable
  – voters can verify their vote has been counted in the election outcome without disclosing their 'proof of vote'
RIES voting protocol (simplified)
RIES network and server design

Required:
- Performance (23 new SSL connects/sec)
- Cheap
- Simple
- Robust
- Secure
Considering:
Leads to:

- 2 physically separated independently operating locations
- Load balancing using DNS Round Robin
- Using standard (open source) components
- Using existing infrastructure where possible
- Security: no 'add-on' but integral part of the design
RIES setup
SURFnet Hoogwaardig internet voor hoger onderwijs en onderzoek
System management

• Only three ways 'in'
  – physical
  – through the voting service (publicly accessible)
  – through the management plane
• System management access completely separated from 'normal' Internet usage
• System management traffic completely separated from voting traffic
• Measuring = knowing
• Monitoring = controlled derailment
Security measures

- By design
- Common sense
- Layering and compartimentalizing
- Software with a good track-record
- Simplicity (no abuse of what is not there...)
- Eyes & ear
- SURFnet-CERT and an Incident Response Policy
- Be prepared to have it fail
Experiences

• Rijnland, Sep 2004:
  - eligible voters: 1,363,787
  - number of seats: 36
  - postal votes: 160,647
  - Internet votes: 72,235

• Dommel, Nov 2004:
  - eligible voters: 878,118
  - number of seats: 35
  - postal votes: 120,201
  - Internet votes: 50,196

• Rijnland partial re-election, April 2005:
  - eligible voters: 127,778
  - number of seats: 1
  - postal votes: 13,390
  - Internet votes: 6,490
Experiences

Opkomst cumulatief (%)
Experiences

Opkomst per uur

- Rijnland
- Dommel
Experiences

- it worked and performed as desired and designed
- Money was not key
- small team, highly motivated, much knowledge, much improvisation
- .

Future

- RIES-public
- 1 election for all waterboards in 2008
- Adapt system for use for
  - smaller elections (university councils etc.)
  - government use
  - association board elections
  - voting during meetings (political parties, associations etc.)
  - popularity votes
More information

- http://www.surfnet.nl/info/bijeenkomsten/archief/bijeenkomst_content.jsp?objectnumber=18002
- jan.meijer@surfnet.nl