HetWaterschapshuis

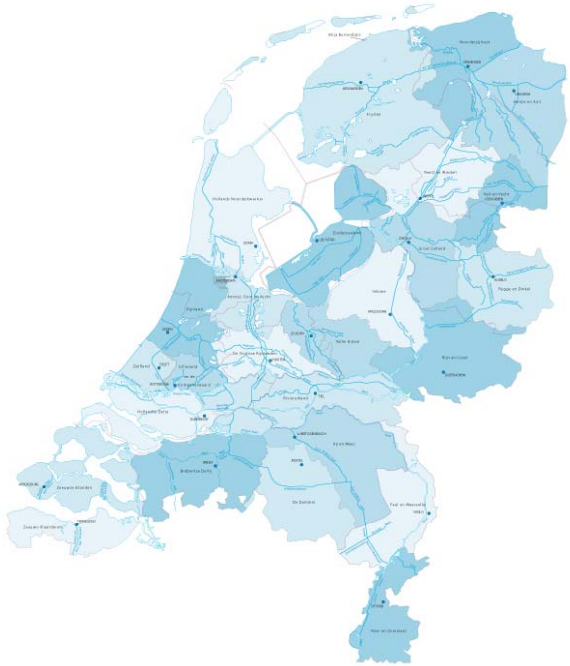
Elections through the Internet: can it be done in practice?

Piet Maclaine Pont / MullPon for
Het Waterschapshuis
pietpont@mullpon.com

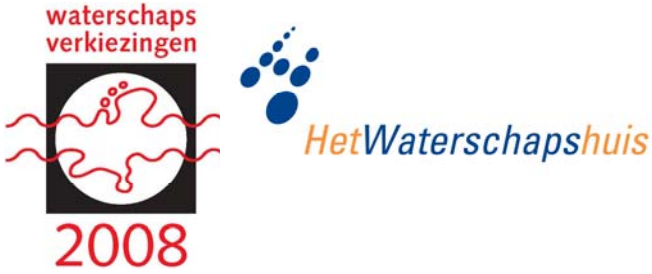
UOCAVA, DC - August 6-7, 2010

The Netherlands

- Kingdom, fully “controlled” by parliament
- Population: 16,605,164 (29 July 2010 12:04:10 GMT)
  (5.36 % of USA)
- Size: 41,528 km² (0.43 % of USA)



RIES?



- Why is RIES?
- And were did it come from?

It was a long walk...

HetWaterschapshuis

IBM (1968-1998)

- End-user --> consumer automation
  - Physical distribution
  - Supermarket scanning
- Pragmatic authentication
  - PC security
  - Smartcard development

Independent consultant (1999-current)

- Pragmatic authentication
- Internet election technology

My IBM years in photos

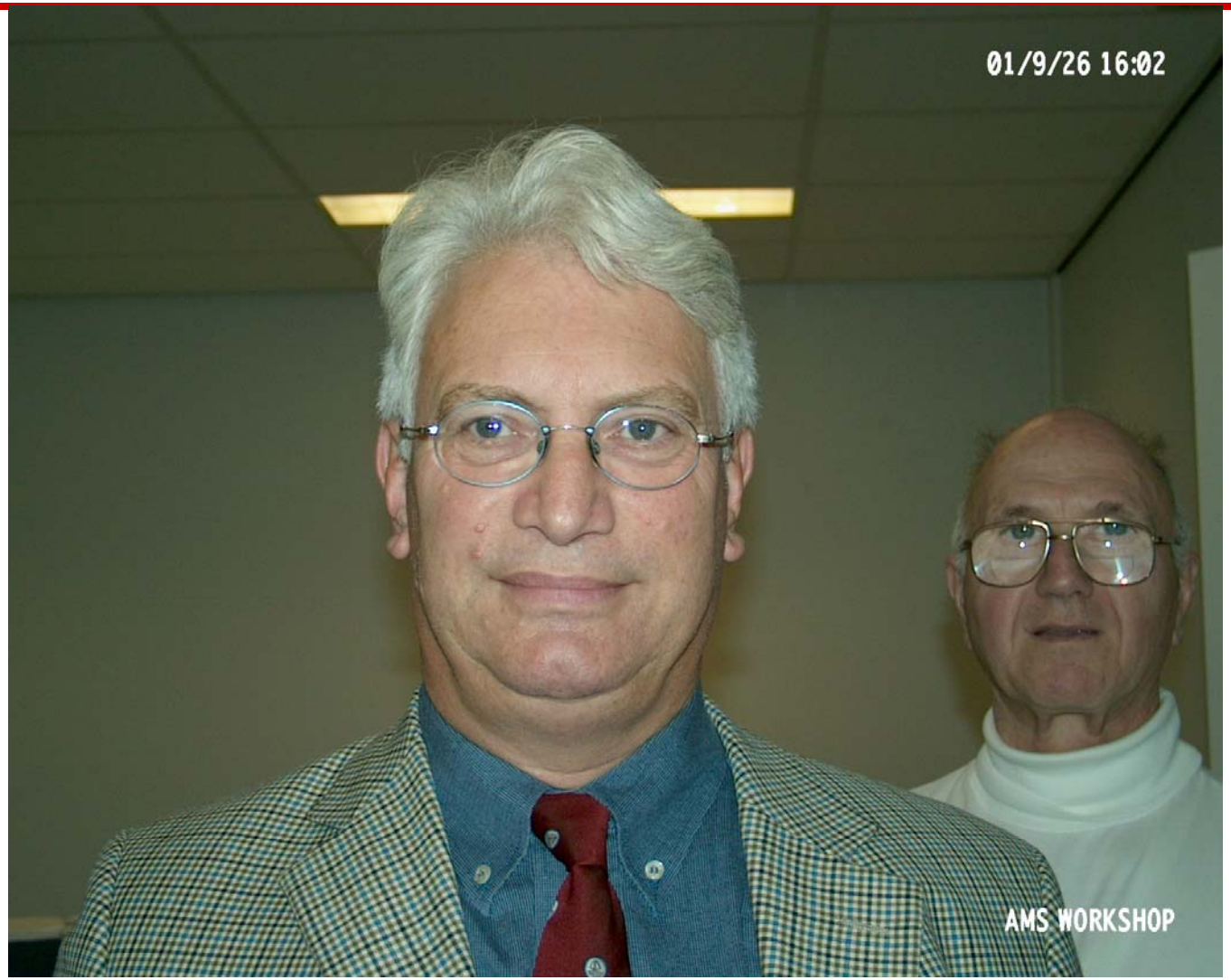
waterschaps verkiezingen 2008

HetWaterschapshuis

My IBM years in photos

waterschaps verkiezingen 2008

HetWaterschapshuis



My IBM years in photos

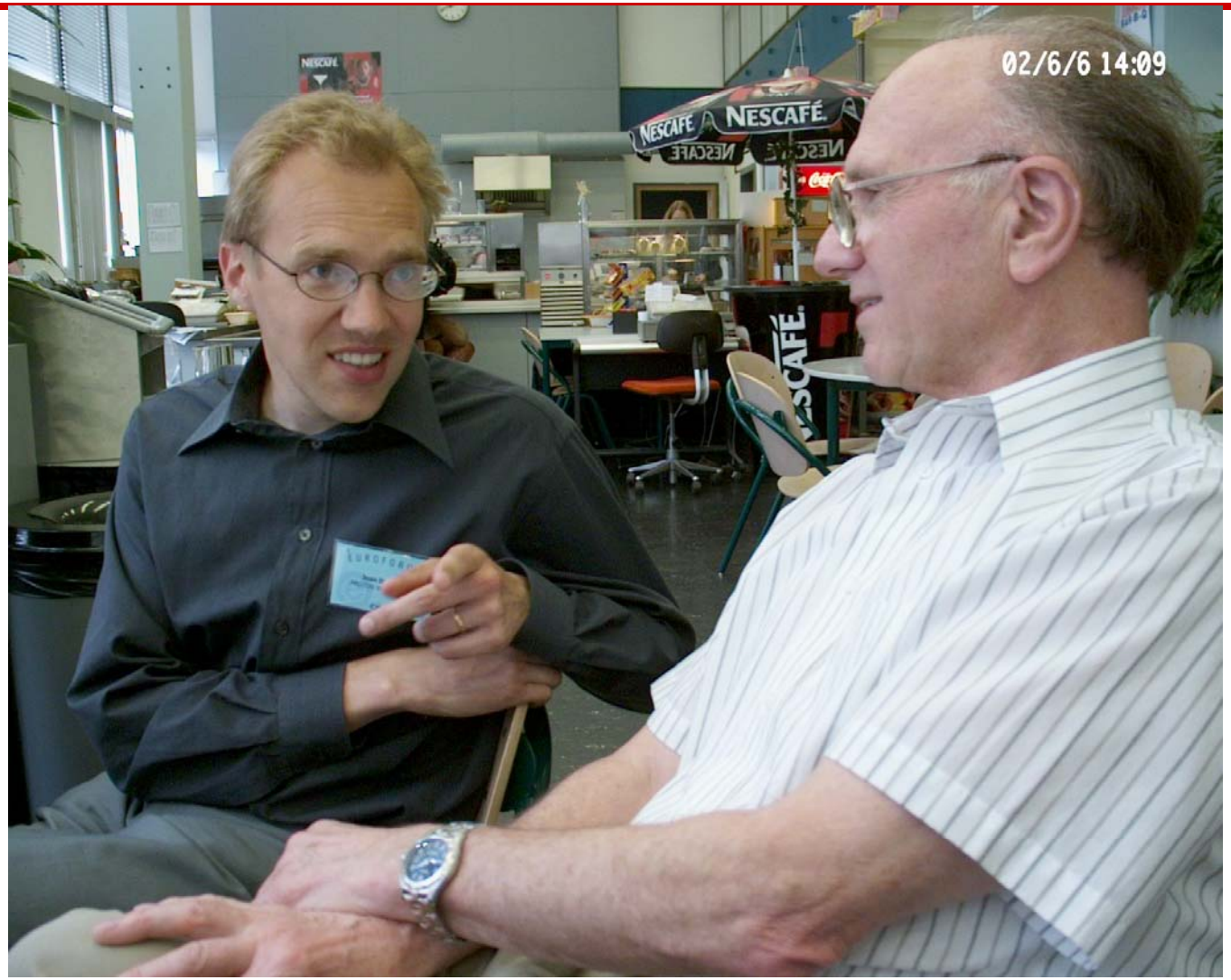
waterschaps verkiezingen 2008

HetWaterschapshuis

My IBM years in photos

waterschaps verkiezingen 2008

HetWaterschapshuis



My IBM years in photos

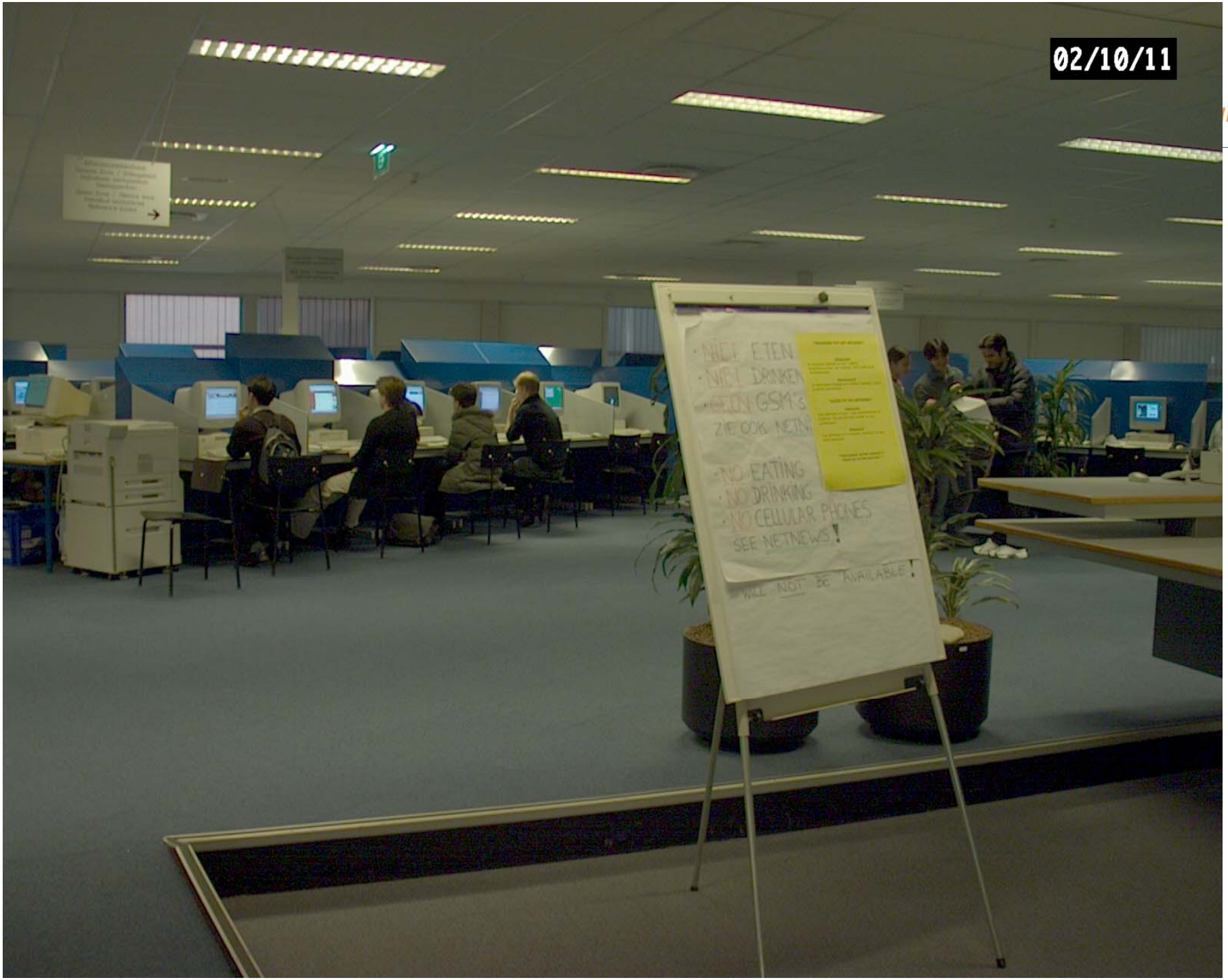
My independent years

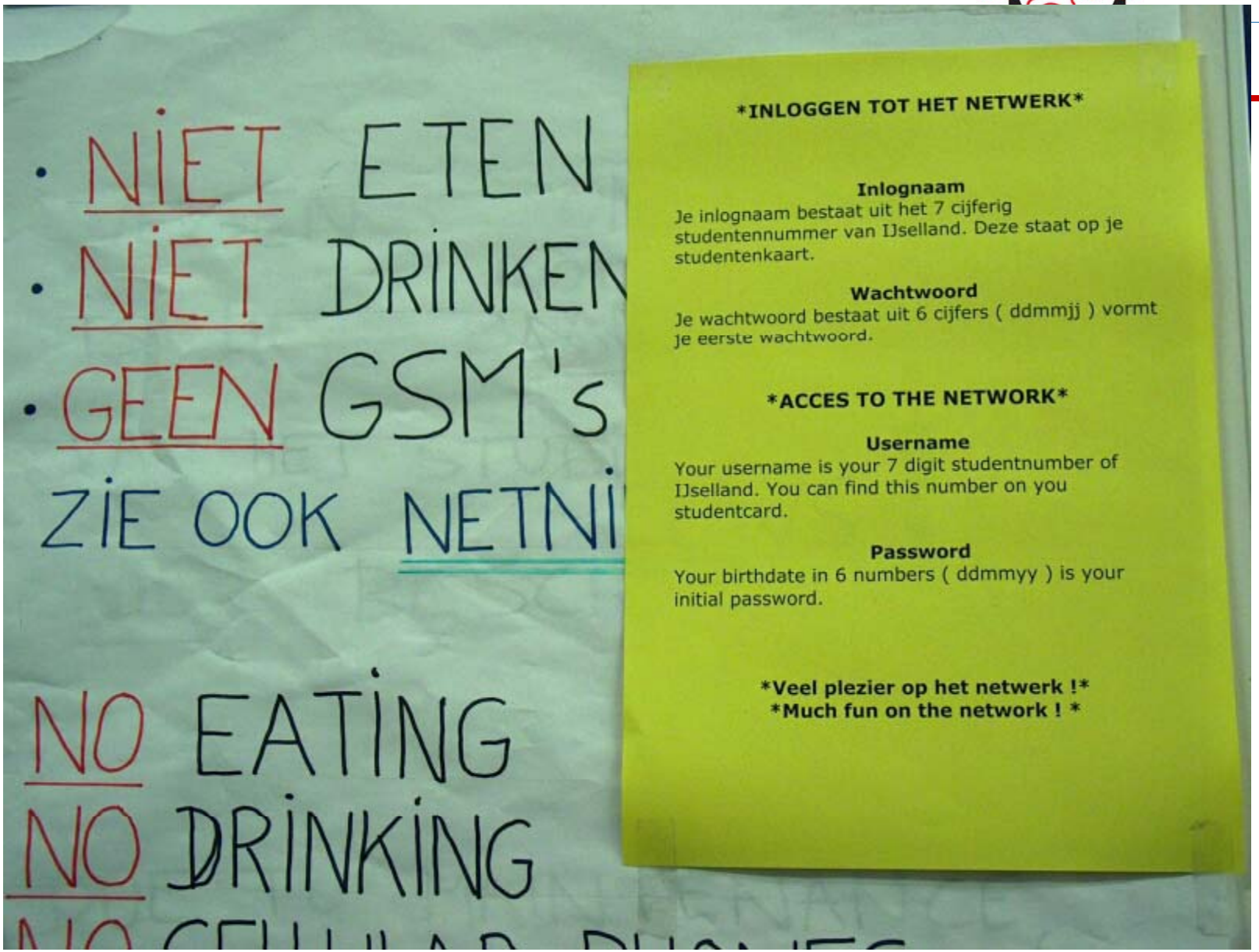
waterschaps verkiezingen 2008

HetWaterschapshuis

Pragmatic Authentication

Focus on higher education in Holland


02/10/11
NIET ETEN
NIET DRINKEN
GEEN GSM'S
ZIJE OOK NETNEWS
NO EATING
NO DRINKING
NO CELLULAR PHONES
SEE NETNEWS!
WILL NOT BE AVAILABLE!


• NIET ETEN
• NIET DRINKEN
• GEEN GSM's
ZIE OOK NETNI
NO EATING
NO DRINKING
INLOGGEN TOT HET NETWERK
Inlognaam
Je inlognaam bestaat uit het 7 cijferig studentennummer van IJselland. Deze staat op je studentenkaart.
Wachtwoord
Je wachtwoord bestaat uit 6 cijfers (ddmmjj) vormt je eerste wachtwoord.
ACCES TO THE NETWORK
Username
Your username is your 7 digit studentnumber of IJselland. You can find this number on you studentcard.
Password
Your birthdate in 6 numbers (ddmmyy) is your initial password.
Veel plezier op het netwerk !
*Much fun on the network ! *

waterschaps verkiezingen 2008

HetWaterschapshuis

SURFSPOT.NL

waterschaps verkiezingen

Het Waterschapshuis

Niegefoon and Niegebach both chipcard based

waterschaps verkiezingen

HetWaterschapshuis

1998 - 2003:
Internet elections

waterschaps verkiezingen 2008

HetWaterschapshuis

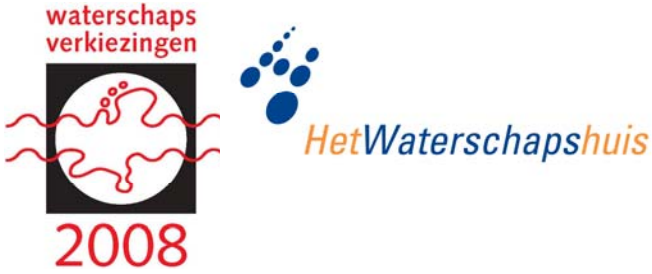
Photo's ISCIT wISCIT

Photo's ISCIT wISCIT

waterschaps verkiezingen 2008

HetWaterschapshuis

The Netherlands



- Kingdom, fully controlled by parliament
- Population: 16,605,164 (29 July 2010 12:04:10 GMT)
- Size: 41,528 km² (0.43 % of USA)
- Government levels
  - Centrally located in The Hague
  - State level (12 states: “provincies”)
  - City level (430 municipalities)
  - District Water Boards (26, regionally located)

NL Elections ...

...from a government point of view:

- Formally key topic
- No systems approach
- Major flows in today's system
  (Major elements not transparent)

NL Elections …

HetWaterschapshuis

No systems approach

- Just very general isolated issues
  - Vote secrecy
  - Reliability
  - Tally and recount
  - Independent recount
  - Safe for internal and external intrusion
- Incident driven
- Exclusively driven by government lawyers
  - Why change?
- Major legal discrepancies
  - Ruling on vote distributions over parliament seats
  - Council of Europe (CoE) ruling on electronic elections

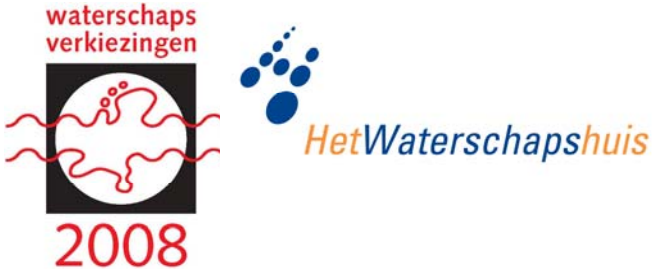
NL Elections …

Major flows in today's system

Major elements not transparent:

- Management of List of eligible voters
- Voting by proxy
- Results consolidation
  - Within each municipality (430, each with 10 to 500 Polling Committee's)
  - Of all 430 municipalities

Experiments require special legislation



Main aspects:

- To avoid detailed classical legislative requirements
- To allow for Competitive Dialogue instead of regular Tender
    - Development requires close cooperation of
        - Government
        - Knowledge sources
        - Market parties
- Has to follow Council of Europe ruling/advice
- Restricted time period

→ Lead time: many years

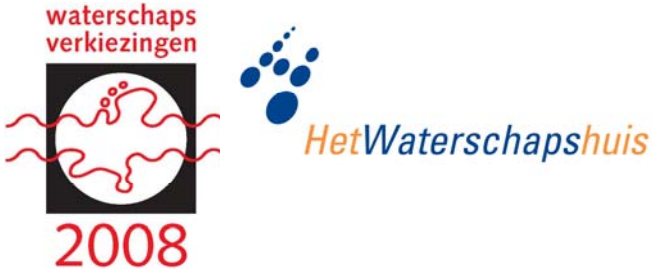
Development started with Water Boards

HetWaterschapshuis

Main aspects:

- Postal elections for all eligible voters
- No voter registration
- Not under Home Office jurisdiction
- Arm length distance from Electoral Council

Main differences NL vs. USA



- Voter registration
  - NL: none (except expats)
  - USA: always --> more possibilities
- Government ruling
  - NL: centralized
  - USA: by local electoral administration
- Electoral Council
  - NL: centralized (although just legal supervision)
  - USA: ?

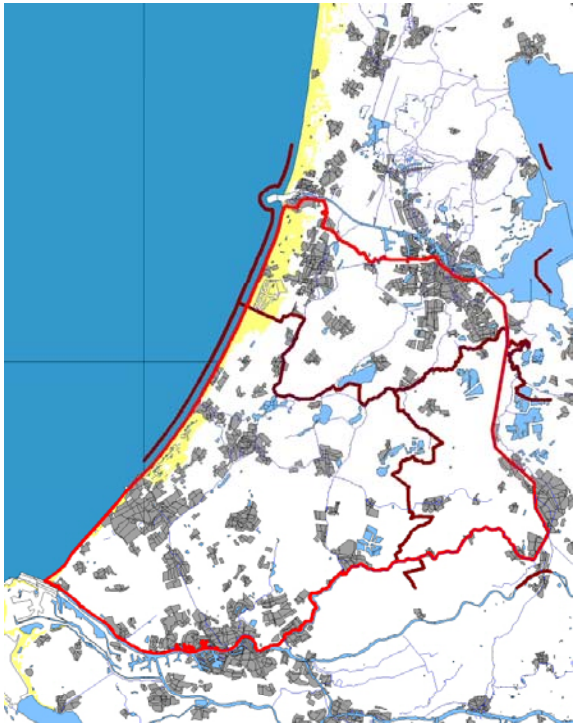
26 Water Boards in The Netherlands

waterschaps verkiezingen 2008

HetWaterschapshuis

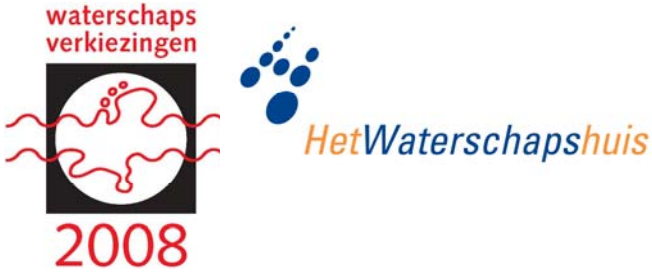
Rijnland District Water Control Board

Rijn Delta



Rijnland: 1100 km^2;
1.3 million people

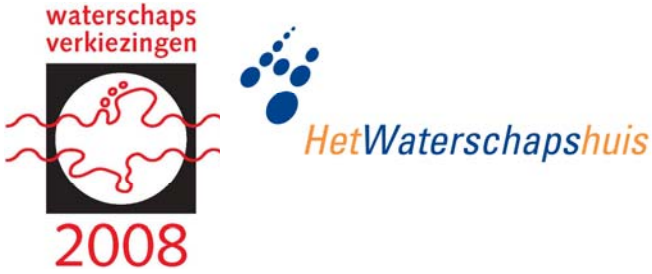
Water board election 2004 with RIES



- 35% voters used it (72,235)
- 86 % positive user feedback and zero negative
- Flawless in processing
- Full validation by independent parties

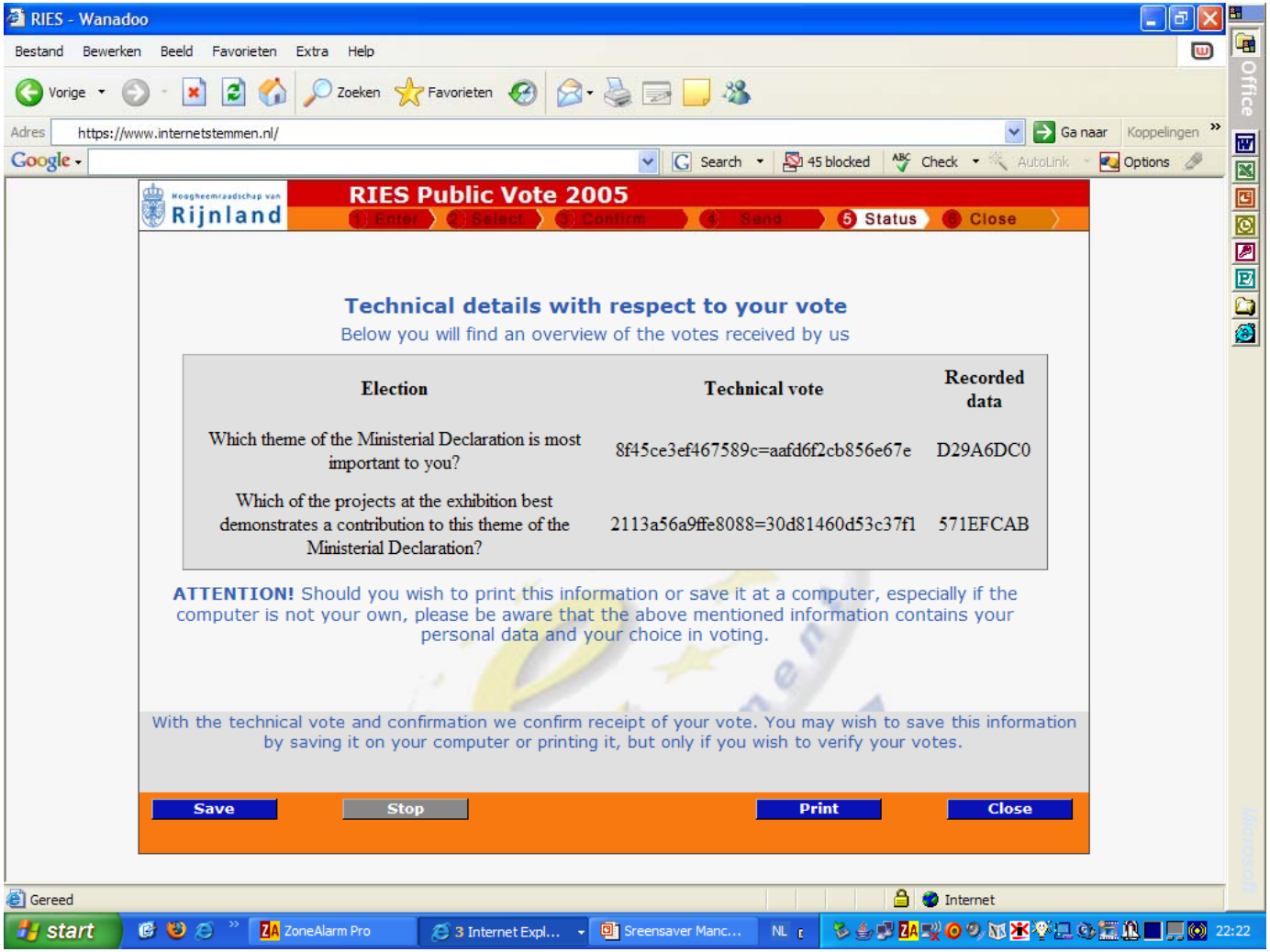
- **What is RIES and how did we get there?**

Comfort and Transparency: user's perspective

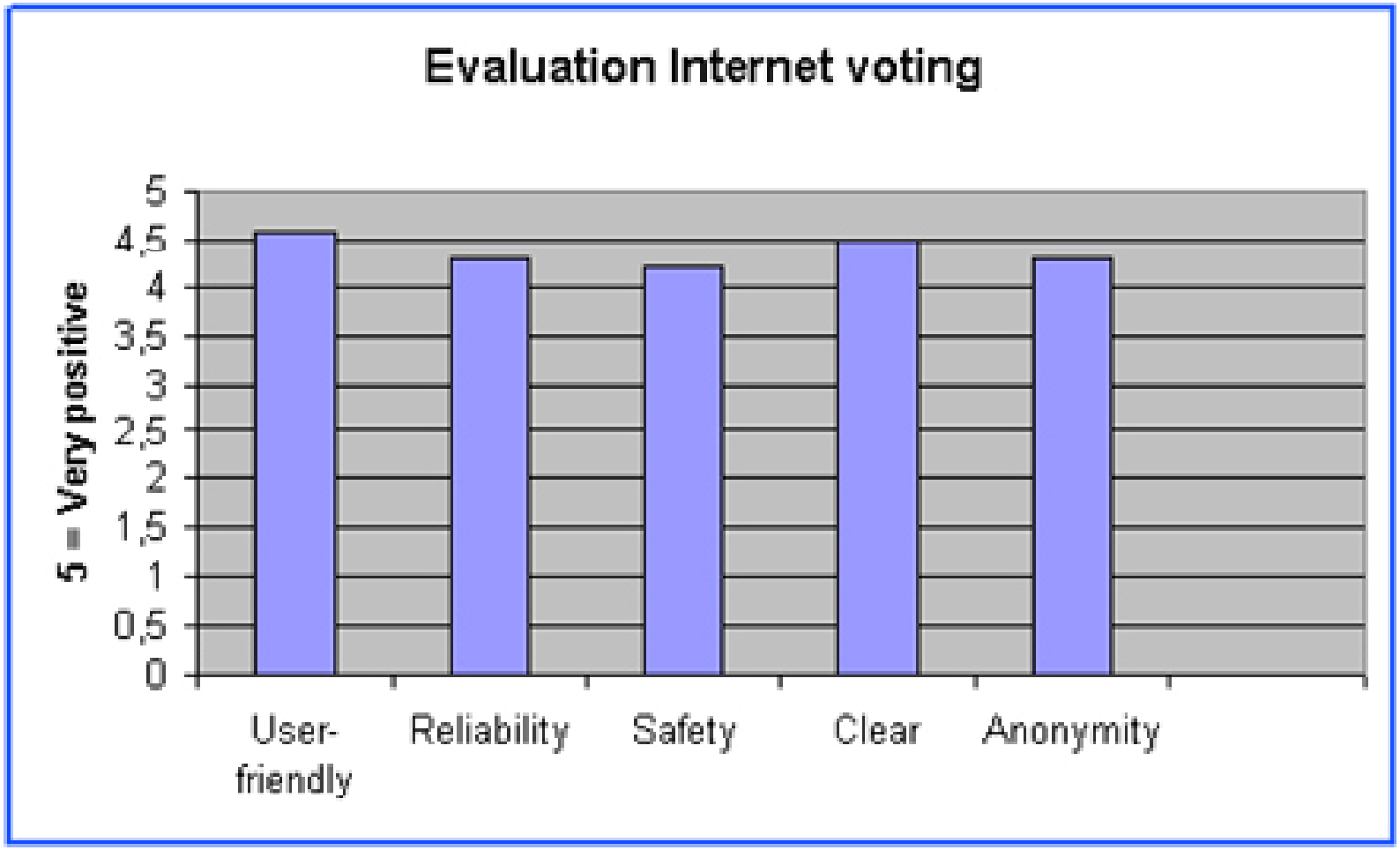


- Ability to cast vote in different ways and several times
- Ability to check if their vote was actuall y cast and counted in the tally; 70% of the voters stressed this as important
- 99% should be able to use the system on their regular Internet attached PC
- Meets the formal government criteria for elections (transparency, etc etc)

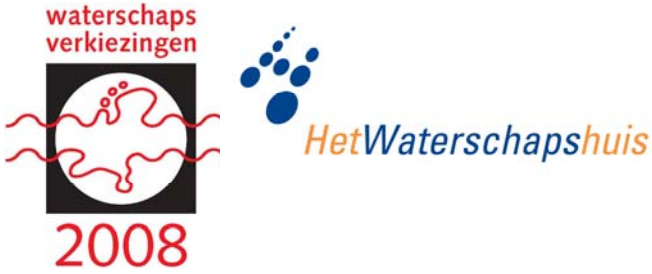
Validation of votes: thrustworthy election



Transparency and accountability ´appreciated´



RIES Internet elections



RIES_participaing_voters_Inet.doc

→ Over 140,000 Internet voters used RIES in 4 formal elections (2004-2006)

→ N.B. In 2008 RIES was deployed for the postal elections for all Water Boards for 13,500,000 eligible voters

RIES based on DES Virtual Ballot System

- Developed by Pieter G. Maclaine Pont/MullPon since 1998
  - With IBM, SURFnet, TNO, Bell Identification, Alfa & Ariss, Rijnland, Magic Choice
  - NL patent 1023861 (extended “Robers” protocol)
  - International patents in process
  - 8 man-year development by inventor
  - 9 man-year development by partners
  - 35 “student” man-year development

- Internet elections applied at
  - 2000: CHOOSE for Polytechnic University Delft
  - 2004: Water boards Rijnland and De Dommel
  - 2005: Rijnland re-election, SURFnet work council
  - 2006: Parliament elections for non-resident Dutch voters

RIES based on DES Virtual Ballot System

Some main facts:

- 2005 EU eGovernment Good Practice Label
- 2006 UN Public Service Award

- Country-wide water board elections in 2008

→ All with intensive cooperation of SURFnet

RIES based on DES Virtual Ballot System

General characteristics:

- DES virtual ballot (extended “Robers” protocol)
- Personal secret cryptographic voter key
- Translated in 2x8 “34AN” characters on Votingcard (Voting code)
- Voting code exclusively with voter
- Public validation files published before election start
- “Casting application” in browser via Javascript
- Personal voter key in encrypted OCR line on Postal ballot (and regular ballot where applicable)
- Central combination of all casted votes (TTPI)
- Publication of all casted votes and adjustments to validation files

Stemkaart

waterschaps verkiezingen

HetWaterschapshuis

Stemkaart
VOOR STEMMEN VIA INTERNET

Hoogheemraadschap van Rijnland

Waterschapsverkiezingen Rijnland 2004

HIER OPENEN

stemmen via www.internetstemmen.nl

HIER OPENEN

Zo gemakkelijk is stemmen via internet:

① Zoek in de kandidatenkrant of op www.rijnlandkiest.nl de kandidaat van uw keuze.
② Ga naar www.internetstemmen.nl en vul al uw persoonlijke codes in.
③ Vervolgens verschijnt uw stembiljet.
(Als u voor meer categorieën mag stemmen, krijgt u daar eerst informatie over.)
④ Kies uw kandidaat en bevestig uw keuze.
(Als u voor meer categorieën uw stem mag uitbrengen, verschijnt een nieuw stembiljet. U kiest nu opnieuw een kandidaat en bevestigt uw keuze. Dit herhaalt u voor alle categorieën.)
⑤ Verstuur uw stem(men) door het bevestigen van uw wachtwoord.
(Het stembureau bevestigt de ontvangst van uw stem met een statusoverzicht. Wilt u na de verkiezingen stemcontroles uitvoeren, dan kunt u nu technische informatie over uw stem krijgen en deze bewaren. Stemcontrole kan van 9 t/m 12 oktober op www.rijnlandkiest.nl/stemcontrole.)

Uw persoonlijke codes en wachtwoord zijn alleen aan u bekend. Door deze gegevens geheim te houden, wordt uw stemgeheim gegarandeerd. Vernietig na het internetstemmen deze stemkaart en uw stembiljetten, zodat niemand er misbruik van kan maken.

Uw persoonlijke codes om te stemmen via internet

Deelnamegroep	>	26	
Stemcode	>>	162f	ms2e
Wachtwoord	>>>	WWWW	xdx2

waterschaps

Stembiljet

VOOR STEMMEN PER BRIEF

Hoogheemraadschap van **Rijnland**

Waterschapsverkiezingen 2004
Categorie Ingezetenen

Zet een kruis in het hokje ☒ van één kandidaat met blauw of zwart schrijvende pen

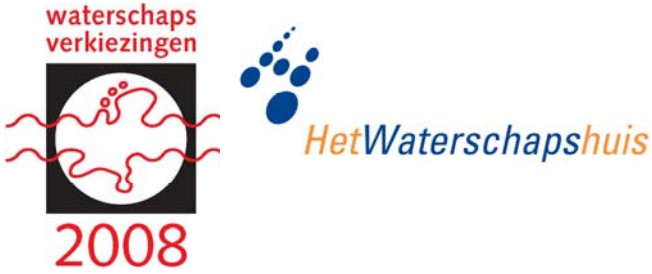
123456789 12345678901234 12345678901234

☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn
☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn
☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn
☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn
☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn
☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn
☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn
☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn
☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn
☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn	☐ <1231> Marie-Louise van Heemskerk Alphen aan den Rijn

1234567890 123456789012345 123456789012345


waterschaps verkiezingen
2008
Waterschapsverkiezingen 2008
Poststembiljet
voor stemmen per post
Waterschap Rivierenland
<Naam Kiesdistrict>
950112011 0000000009753085 2089361494981754
Stap 1:
Kies een lijst. Kruis het hokje voor de lijst van uw keuze aan met een blauw of zwart schrijvende pen.
1 Europese Kleurenpartij (EKP)
2 Planten voor het Volk (P.v.h.V)
3 EUROPESE WEERMANNEN
4 Algemene Materialen Partij (AMP)
5 Europese Dieralliantie (EDA)
6 VKP
7 Lijst Vrede Zij Met U!
8 Lijst Smaak
9 Partij van de Sport (PVDS)
10 t Partijtje
11 Alliantie Vernieuwing en Democratie
12 Alliantie Vernieuwing geplakt
13
14 Dè dläcriétën pärtij ë
15
16 C.U.V.V.D.P.V.D.A.C.D.A.D66
17 12345678901234567890123456789012345
18 abcdefghijklmnopqrstuvwxyz123456789
19 ABCDEFGHIJKLMNOPQRSTUVWXYZ123456789
20 9
21
Stap 2:
Kies nu de kandidaat waarop u wilt stemmen. Kruis het hokje voor de naam aan met een blauw of zwart schrijvende pen.
1 Nummer 1
2 Nummer 2
3 Nummer 3
4 Nummer 4
5 Nummer 5
6 Nummer 6
7 Nummer 7
8 Nummer 8
9 Nummer 9
10 Nummer 10
11 Nummer 11
12 Nummer 12
13 Nummer 13
14 Nummer 14
15 Nummer 15
Stap 3:
Vul uw geboortejaar in.
Om misbruik van uw stembiljet te voorkomen, verzoeken we u vriendelijk om de laatste twee cijfers van uw geboortejaar in te vullen.
Mijn geboortejaar:
1 9
Neem de laatste 2 cijfers van het geboortejaar over in bovenstaande vakjes
28-11-1974
Nadat u Stap 1 t/m 3 heeft ingevuld kunt u uw ingevulde stembiljet in de bijgevoegde antwoordenvelop verzenden.
Stuur uw stembiljet op voor 26 november 2008.

Main elements RIES



- Pre-preparation
  - Set formal responsibilities
  - List of eligible voters
  - List of candidates
  - Publication set-up
- Preparation
  - Voting code
  - Validation file (“Referentiebestand”)
  - Publications
- Voting period
  - Technical vote
  - Receipt-confirmation
- Tally
  - Reference value
  - Publications
- Vote count validation

RIES

Minimal exchange of data over Internet:

- Simple ballotbox server
- Internet PC as independent as possible
  - START:
    - Server: SSL
    - PC: receives server script with list of candidates
    - local input (by voter)
    - Server: reads status, verfies earlier casts from this voter
  - Vote cast: local (by voter)
  - Sending in the vote:
    - local input (by voter)

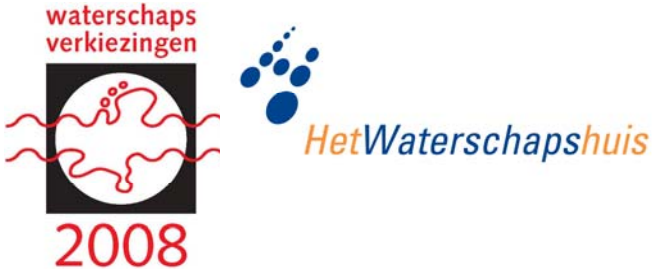
    →Server: calculates receipt-confirmation

    →Server: update status
  - STATUS: local (by voter)

Validating the Electronic Tally

- By voter himself: Based on all published election data
- By independent experts or involved parties
    - Candidates
    - Radboud University
    - By anyone with the desire to do so
- No specific “validation of sold vote” problem

Tally validation



- New
- Needed
  - How can the voter effectively file complaints with traditional elections?
- Validation procedure
  - By voter himself
  - Independent expert verifies voter complaint
  - Arbiter determines if complaint is right
  - Impact on election results?
- Accuracy in all procedures should be much higher compared to conventional elections

Multi disciplinary approach needed

HetWaterschapshuis

- Dimitris A. Gritzali: “Principles and requirements for a secure e-voting system ”
- Edited by Dimitris A. Gritzali” Secure Electronic Voting”
- Laurence Monnoyer-Smith: “e-democracy”
- Christopher G. Reddick (University of Texas at San Antonio, USA): “Handbook of Research on Strategies for Local E-Government Adoption and Implementation: Comparative Studies” Pages: 231-249: Janita Stuart (Stuart Controls Ltd, New Zealand); Val Hooper (Victoria University of Wellington, New Zealand)

STS-approach essential for these kind of processes!

Major flaws (RIES-2008)

HetWaterschapshuis

(Just postal voting with RIES for 13,500,000 voters)

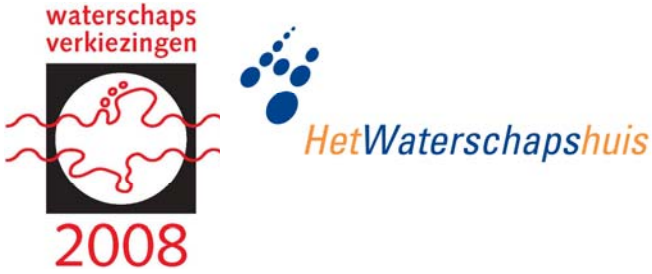
- Ruling for pre-elective publication of Reference file
  - Approx.300,000,000 clear/cipher text combinations
  - Underestimate of today's PC DES processing capabilities

  → Instead of rule change: Internet voting forbidden
- Inadequate testing Response processor data
  - High accuracy requirements underestimated by vendor (no escape: frozen dates couldn't be shifted)
  - Operated isolated from Architecture team

  → RIPOCS reset during production (fault to be opened)
- Politics & publicity
  - Active opponent group

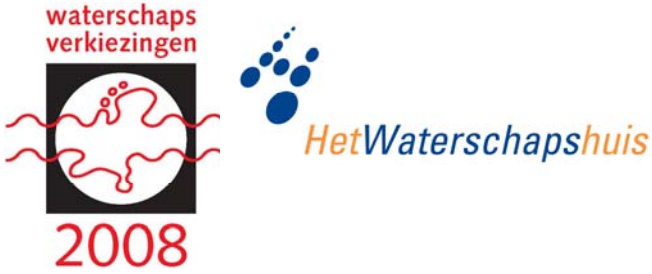
  → stream of negative publication

Risk assessment



- No formal process
- Instead scaling-up through rough steps with increasing risks
  - 1998-1999 wISCIT:
    - test elections
    - Risk research of specific elements
  - 2000 wISCIT:
    - CHOOSE (Student Board Polytechnic University of Delft)
  - 2003 TNO:
    - Feasibility study
  - 2004-2005 Rijnland: Water Board elections at
    - Rijnland
    - De Dommel
  - 2006 Home Office & Rijnland:
    - Expat voting Dutch parliament
  - 2008 Het Waterschapshuis
    - Countrywide Water Boards elections

Risk assessment



Independent reviews

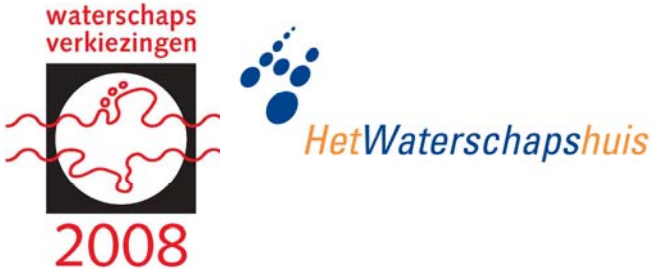
- TNO, Delft (initial feasibility)
- Cryptomathic, AarHus (DK) (crypto design)
- TNO Human Factors, Soesterberg (voter screens)
- Madison Gurka, Eindhoven (crystal box security evaluation of server and network design)
- Radbout University (Bart Jacobs team) (external network & server penetration tests)
- Burger&overheid, ICTU, Den Haag (large scale end-user evaluation)
- Extensive specialist auditing for Dutch Home Office (2006 parliament elections)
- EIPSI, TuE, Eindhoven (Description and Analysis of the RIES Internet Voting System, on request by Het Waterschapshuis (HWH))
- Collis, Leiden (Review integrity RIPOCS source code, on request by HWH)
- Fox-IT, Den Haag (overall technical evaluation for Ministry of Transport & Communications)

Tradeoffs

- RIES costs
  - Design, implementation, testing & operation (small complete team: SURFnet, TTPI, HWH)
    → relatively low
- Audit & external consultancy: expensive part (out of line)

- Example: 2006 KOA project
  - Total budget > EUR 2,500 K
  - RIES costs EUR 500 K

What Else?



- RIES & Patent open source
  - Website www.openries.nl
    - Partly in Dutch
    - Full English translation < EU 25K

- Unconventional investigation of total project aspects (Science Technology & Society)
  - See other high-tech project failures
    - Bruno Latour: “Aramis”
    - Polly Maclaine Pont: “Dutch Student Chipcard”
    - Laurence Monnoyer Smith: “e democracy”
  - Local talent: Polly Maclaine Pont (pmaclaine@gmail.com)