Opzet van RIES nu en voor 2008

Piet Maclaine Pont / TTPI
voor Het Waterschapshuis

Utrecht, 15 mei 2007

Case Internetstemmen: RIES

RIES oorsprong: CHOOSE

1998: ISCIT (IBM Student Chipcard Innovation Team)

Mijn opdracht aan Herman Robers / TuD ICT:

"Ontwerp een Internet verkiezing systeem, gebaseerd op

- Algemene eisen
- Technische mogelijkheden bij kiezer
- Persoonlijke mogelijkheden van kiezer

gebaseerd op de situatie van nu."

CHOOSE eisen

- Algemene eisen
- Technische mogelijkheden bij kiezer
- Persoonlijke mogelijkheden van kiezer

→Hierover veel bekend bij en ontwikkeld door SURFnet

- SCK (Studenten Chip Kaart) 1993-2000
- Pragmatische authenticatie 1996-2003
  - Niegebach
  - Niegefoon
  - A-Select (nu onder meer: DigID)

Internetstemmen ...

... als er een balans is tussen

- Bruikbaarheid voor de kiezer thuis
- Controleerbaarheid en betrouwbaarheid
- Risico's van de thuis-PC op Internet
- Risico's bij andere toegepaste verkiezingstechnieken (zoals poststemmen)
- Alternatieven voor de kiezer om zijn Internetstem te vervangen
- Fouten in postbezorging stempakket en de herstelmogelijkheden daarvan

Basiseisen RIES

- RIES to be used on PC's without any changes
- RIES should be combined with the existing postal election system
- Replacement Election Packages
- RIES general requirements:
  - Only eligible persons can vote
  - No person can vote more than once
  - The vote is secret
  - Each (correctly cast) vote gets counted
  - The voters trust that their vote is counted

Specific requirements

- Authentication (only authorized voters can vote)
- Convenience (vote casting with minimal reqs on skills and equip)
- Secrecy (no one able to determine how individual votes)
- Uniqueness (no voter can cast more then one vote)
- Integrity (No modification of votes without detection)
- Accuracy (voting systems should record votes correctly)
- Reliability (Systems should work robustly, even in case of numerous failures)
- Verifiability (Verification of correct count in final tally)
- Audit ability (Reliable and demonstrably authentic election records)
- Non-coercibility (Voters should not be able to proof how they votes)
- Flexibility (Equipment should allow for a variety of ballot question formats)
- Certifiability (Systems should be tested against essential criteria)
- Transparency (Voters should be able to possess a general understanding of the whole system)
- Cost-effectiveness (Systems should be affordable and efficient)

CHOOSE en RIES op basis van DES Virtueel Stembiljet

CHOOSE en RIES op basis van DES Virtueel Stembiljet

- Ontwikkeld door P.G.Maclaine Pont/MullPon sinds 1998
  - Met IBM, SURFnet, TNO, Bell Identification, Alfa & Ariss, Rijnland, Magic Choice
  - NL octrooi 1023861
  - Internationale octrooien in aanvraag
  - 8 mensjaren ontwikkeling door uitvinder
  - 9 mensjaren ontwikkeling door partners
  - 35 "studenten" mensjaren ontwikkeling
- Toegepast in
  - 2000: als CHOOSE voor TUD
  - 2004: Rijnland en De Dommel
  - 2005: Rijnland
  - 2006: TK verkiezingen voor kiezers buiten NL

CHOOSE en RIES verschillen

- CHOOSE: smartcard per kiezer
  - Kp (Persoonlijke sleutel) in smartcard, echt geheim
  - Geen specifieke beperkingen aan lengte Kp of algoritme
  - Distributie Kp goed en eenvoudig uitvoerbaar
- RIES: alleen toetsenbord voor invoer Kp
  - Kp maximaal 8 bytes lang (16 tekens intoetsen)
  - Kp minimaal 8 bytes lang (sleutel uitputting)
  - Sleutel distributie via drukker/printer en post
  - Vervangende stempakketten noodzakelijk
  - Stemcontrole complexer (via Technische Stem)
  - Combinatie met Briefstemmen

RIES op basis van DES Virtueel Stembiljet

Algemene systematiek:

- DES virtueel stembiljet
- Persoonlijke geheime sleutel per kiezer
- Omgezet in 2x8 "34AN" code-tekens op Stemkaart (Stemcode)
- Stemcode uitsluitend bij kiezer
- Vooraf gepubliceerde controlebestanden
- "Stemprogramma" in browser via Javascript
- Persoonlijke sleutel in vercijferde OCR regel op Poststembiljet en Stembusbiljet
- Centrale combinatie alle stemmen
- Publicatie alle stemmen en aanpassingen controlebestanden

Hoofdelementen RIES

- Voorbereiding
  - Stemcode
  - Referentiebestand
- Stemperiode
  - Technische stem
  - Ontvangst-bevestiging
- Stemopname
  - Referentiewaarde
- Stemcontrole

Hoofdelementen RIES

2008

Voorbereiding:

- Alle kiezers bekend
- Alle lijsten & kandidaten bekend

→Cryptografische berekening:

- Stemcode
  - 16 tekens (8 bytes)
  - Uniek geheim kiezer, alleen bij hem
  - Tijdelijk bij productie en distributie stempakket
- Referentiebestand
  - Alle potentiële stemmen in beschermde vorm
  - Controle en uitslag berekening
  - Publiek

Hoofdelementen RIES

2008

Stemperiode:

- Kiezer gaat via PC naar verkiezing website
- Kiezer tikt Stemcode in op PC
- Stemcode verlaat nooit PC
- Anonieme controle op status kiezer door server
- Technische stem wordt in PC berekend uit kandidaat-nummer en Stemcode
- Technische stem wordt verstuurd naar server
- Kiezer ontvangt status, Technische stem en Ontvangst-bevestiging

Hoofdelementen RIES

2008

Stemopname:

- Omrekenen Poststemmen naar Technische stem
- Publiceer alle ontvangen Technische stemmen
- Omrekenen Technische stem naar Referentiewaarde
- Opzoeken Referentiewaarde in Referentiebestand
  - Geldige kiezer?
  - Meer geldige stemmen van deze kiezer?
  - Geldige kandidaat?
  - Pas tel-regels toe

→ Kan door iedereen worden uitgevoerd

Hoofdelementen RIES

2008

Stemcontrole:

- Door kiezer:
  - Komt zijn Technische stem voor in gepubliceerde Ontvangen Technische stemmen?
  - Leidt zijn Technische stem tot juiste kandidaat?

→Bij klachten:

Scheidsrechter valideert Ontvangst-bevestiging

Referentie bestand

2008

Referentie bestand doel

2008

- Publiek
- Bevat (hashes van) alle potentiële stemmen
- Mag na generatie niet gewijzigd, op statusbits na
- Wijzigingen statusbits alleen vanuit Helpdesk
- Helpdesk controleerbaar
- Bestand bepaalt per uitgebrachte stem
  - kandidaat waarvoor stem geldt
  - geldigheid

Referentie bestand struktuur

- In volgorde RnPID (Reference Pseudo Identity Voter n) (compleet: Kiezer, Vervangend of Test)
- Per RnPID
  - Iedere RnPotVote (Reference Potential Vote for Voter n: hash van iedere mogelijke Technische Stem) met Kandidaatnummer
  - Statusbits
    - Vervangend
    - Verstrekt
    - Vervallen

Verplichte publicaties

Referentiebestand

02010203.zip

Referentie bestand integriteitsbewaking

- Vooraf: publiek op internet, hash in krant
  - Omvat alle
    - Kiezers (aantal exact gelijk aan kiezers*kandidaten)
    - Vervangende stemcode referenties
    - Test referenties
  - Geen enkele wijziging toegestaan behalve statusbits
- Tijdens (en vooraf): Klachten van kiezers
  - Helpdesk verstrekkingen Vervangende pakketten
  - Proces Verbaal per transactie
  - Wijzigingen statusbits in Referentie bestand
- Na sluiting: publiek op internet, hash in krant
  - Uitsluitend statusbits Kiezers en Vervangende stemcodes mogen gemuteerd zijn

Na sluiting publiek

Op internet, met hash in krant:

- Ontvangen stemmen
- Alle verstrekte Ontvangstbewijzen (helft)
- Stand Statusbits Referentie bestand

- Verwerkte Ontvangen stemmen
- Telling

Voorbeelden Verplichte publicaties

- publicatie initieel referentiebestand begin nov 2004.doc
- Doc1_webtxt.doc
- hashes_adv_nasluiting_20041119.doc

Notaris

- Escrow253 versie 2.doc

RIES op basis van DES Virtueel Stembiljet

- Toe te passen stemtechnieken

→ Met volledige controle door kiezer:
- Internet
- GSM telefoon

→ Met gedeeltelijke controle door kiezer:
- Post
- Stembus

→ Sterk beperkte controle door kiezer:
- Telefoon via toetsenbord

Specific requirements and RIES 1

Waterschaps 2008

- Authentication (only authorized voters can vote)
  - Voting card by mail to all voters
  - In case of complaint
    - Replacement Election Package
    - Original one invalidated
    - Validation Voting card possible through published Reference file
- Convenience (vote casting with minimal requirements on skills and equipment)
  - Voter can freely choose his voting method without any registration
  - RIES based on regular Internet facilities available to > 99% of voters with Internet
  - Voting instructions on voting card and self explanatory voting screens
  - Voter can interrupt his voting sequence at any time, continue from any location later
  - Voter can printout his Vote Receipt Conformation to proof casting of his vote
- Secrecy (no one able to determine how individual votes)
  - Unique and secret Voting Code per voter
  - Calculation of all sensitive data in closed environment without human access
  - Voting Card printing and distribution is sensitive; handled by specialized party
  - Each vote can only be generated by the voter himself; Validity can be determined by anyone without any link to the identity of the voter
  - Server process will not store any Internet Address information in relation to the vote; Voter is free to cast vote form any Internet address
- Uniqueness (no voter can cast more then one vote)
- Integrity (No modification of votes without detection)

Specific requirements and RIES 2

Waterschaps 2008

- Accuracy (voting systems should record votes correctly)
- Reliability (Systems should work robustly, even in case of numerous failures)
  - Individual vote calculated by script program in browser of voter, received from authenticated server through SSL
  - Multiple receipts of the same vote do not effect the final tally
  - Multiple receipts of different votes from the same voter will render all votes invalid
  - Use of postal mail and Internet both allowed for the same voter
  - SSL guarantees voter casting of his vote at the proper server
- Verifiability (Verification of correct count in final tally)
  - Reference file is published with guaranteed integrity
  - Size of Reference file and Voting Codes can be validated at any moment
  - Regular reports on received votes during vote casting guarantees completeness
  - All Received Votes are published with guaranteed integrity after closing of election
- Audit ability (Reliable and demonstrably authentic election records)
  - Precise reports on all steps
- Non-coercibility (Voters should not be able to proof how they votes)
  - Not required here; of theoretical value in case of (remote) postal elections systems

Specific requirements and RIES 3

Waterschaps 2008

- Flexibility (Equipment should allow for a variety of ballot question formats)
  - RIES supports several election system requirements (individual candidates; party election system; referendum)
- Certifiability (Systems should be tested against essential criteria)
  - Voter's PC environment is main problem here
  - JavaScript is open source and can be validated by anyone at election time
  - Server parts and functional implementations of RIES can be certified
  - Organizational parts should be judged as well (e.g. Helpdesk, separation of tasks between different parties)
- Transparency (Voters should be able to possess a general understanding of the whole system)
  - Any system with technical components is hard to understand for the general public
  - Open structure of RIES principles and implementation allows for inspection by any interested party
- Cost-effectiveness (Systems should be affordable and efficient)
  - RIES can be performed by virtually any Internet-browser type system at the client side and relatively simple server components

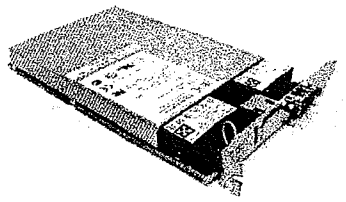
Verbeteringen RIES-2008

Waterschaps 2008

- Betere scheiding taken tussen partijen
- Struktuur Referentie bestanden
- Stembus implementatie
- Abel (*Abuse Elimination* niet gebruikte Stempakketten)
- Volledige server cryptografie in hardware
  - IBM 4764 Cryptographic Coprocessor
  - CCA (Common Cryptographic Architecture)
  - Device authentication
  - Internal key generation (Sleutels niet meer bij mensen bekend)
  - Toch backup
  - Extern controleerbaar / verifieerbaar
  - Hardware 'kraakvrij' (voldoet aan FIPS 140-2)
  - Stemcodes alleen onvercijferd bij (deel-) proces drukker/printer en kiezer

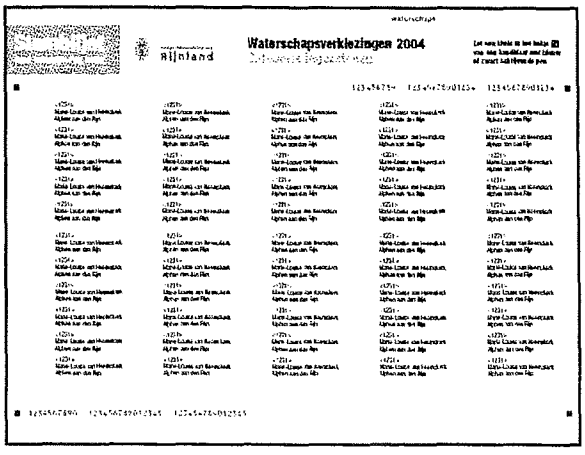
IBM 4764 Cryptographic Coprocessor

Waterschaps 2008

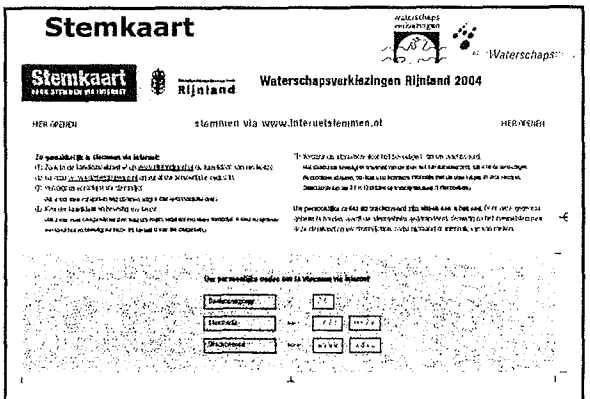


Verkiezingen via Internet

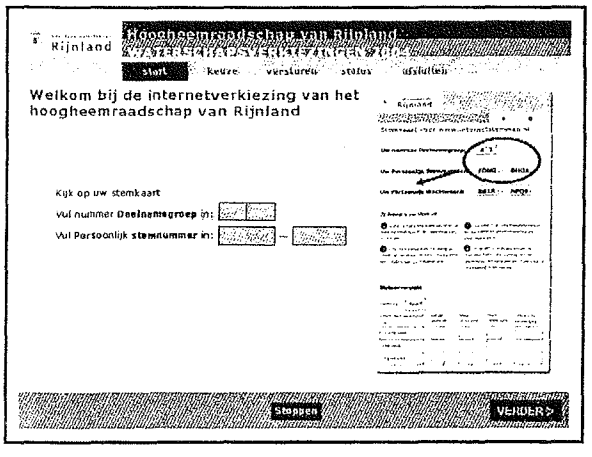
- Niet eenvoudig
- Wel goed uitvoerbaar
- Belangrijk beter controleerbaar dan postverkiezingen
- Belangrijk goedkoper dan postverkiezingen
- Goed te combineren met andere verkiezingstechnieken
- Goede oplossingen voor alle problemen

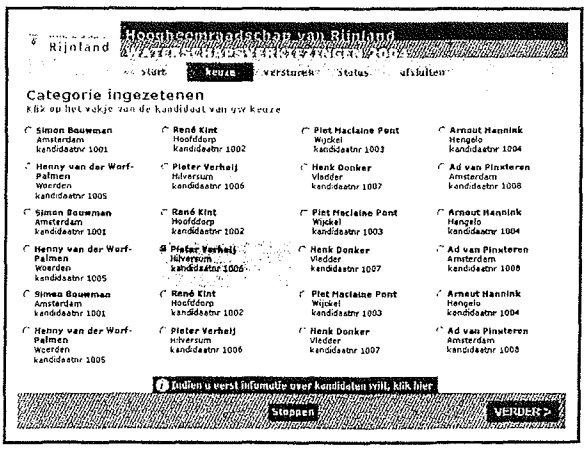


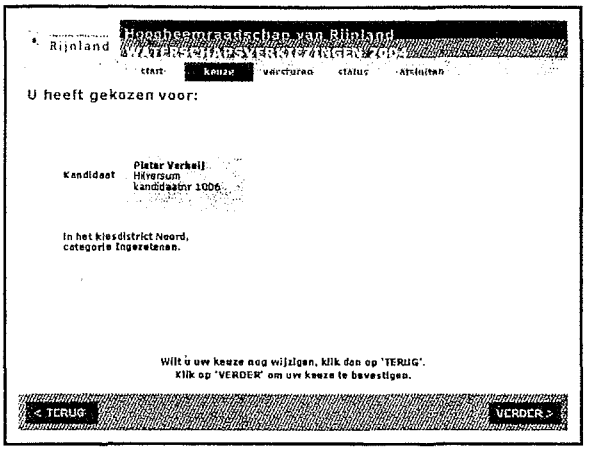
Stemkaart

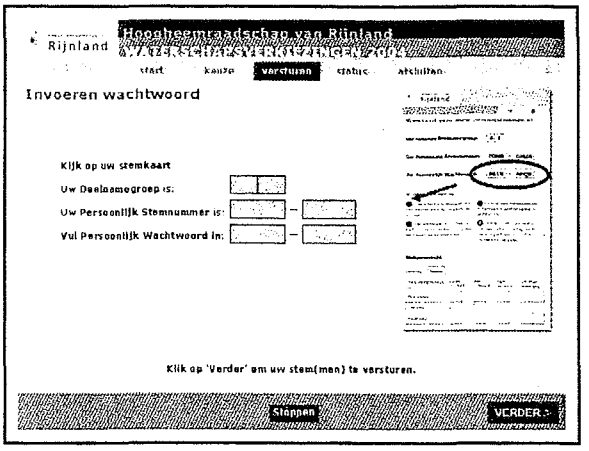


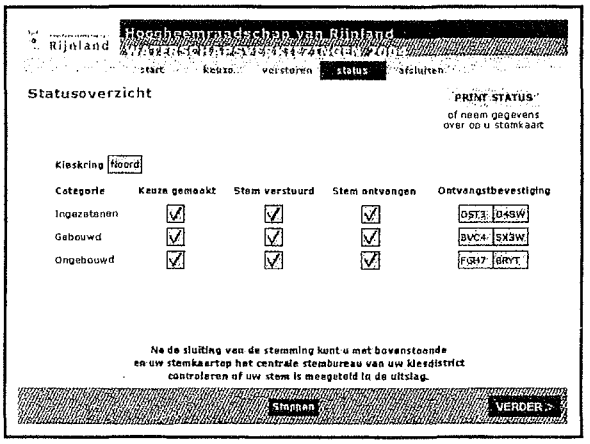
Demonstratie RIES











RIES

Minimale data-uitwisseling over Internet:

- Eenvoudige stembus server
- Internet PC zo zelfstandig mogelijk
  - START:
    - Server: SSL
    - Server: ontvangst script van server met kandidatenlijst
    - lokaal input (bij kiezer)
    - server: leest status, controleert op eerder stemmen
  - KEUZE: lokaal (bij kiezer)
  - VERSTUREN:
    - lokaal input (bij kiezer)
    - →server: berekent ontvangst bevestiging
    - →Server: update status
  - STATUS: lokaal (bij kiezer)

Controle Elektronische Uitslag

- Door kiezer zelf: Op basis van gepubliceerde brondata
- Door onafhankelijke groep namens kiezers
  - Kandidaten
  - Radboud Universiteit
  - Door iedereen die dat wil
- Geen specifiek "controleerbare verkoop stem" probleem

Verkiezingen via Internet

- Niet eenvoudig
- Wel goed uitvoerbaar
- Belangrijk beter controleerbaar dan postverkiezingen
- Belangrijk goedkoper dan postverkiezingen

Verkiezingen via Internet

- Niet eenvoudig
- Wel goed uitvoerbaar
- Belangrijk beter controleerbaar dan postverkiezingen
- Belangrijk goedkoper dan postverkiezingen
- Goed te combineren met andere verkiezingstechnieken
- Goede oplossingen voor alle problemen

Einde