# Reviews & Audits RIES 2008©

## *Samenvatting:*

Hoofdlijn: externe audits maken onderdeel uit van de ontwikkelcyclus van RIES door de jaren heen.

**2002 – 2004 (aanloop naar de waterschapsverkiezingen Rijnland en de Dommel):**
Eind 2002, in de aanloop van de waterschapsverkiezingen van 2004 heeft het Hoogheemraadschap van Rijnland een haalbaarheidsonderzoek omtrent stemmen via internet laten uitvoeren door TNO technische menskunde. Dit heeft geleidt tot de ontwikkeling van een prototype RIES (Rijnland Internet Election System) genaamd. In 2004 is het prototype op kritische aspecten onderzocht en beoordeeld door verschillende gerenommeerde expertise centra.

Begin 2004 heeft een team specialisten van Peter Landrock's Cryptomathic (in Aarhus, Denemarken) de cryptografische opzet beoordeeld en heeft TNO Human Factors uit Soesterberg de gebruikersvriendelijkheid van de implementatie tegen het licht gehouden, hebben de security experts van Madison Gurka uit Eindhoven de server- en netwerkopzet en beveiliging getoetst en voerde een team van Bart Jacobs (Katholieke Universiteit Nijmegen) externe penetratietests uit.

De feedback heeft geleidt tot verbeteringen in RIES waarna het systeem in oktober 2004 met succes is toegepast tijdens de waterschapsverkiezingen van Hoogheemraadschap van Rijnland en waterschap de Dommel.

**2005-2006 vervroegde toepassing voor KOA:**
In aanloop van de vervroegde tweede kamerverkiezingen van 2006, is RIES ingezet tijdens het experiment "Kiezen op Afstand" van het ministerie van binnenlandse zaken. De veranderende context maakte verdere ontwikkeling van RIES noodzakelijk. Door de scherper gestelde eisen, de naar voren geschoven verkiezingsdatum en de verder geëvolueerde stemdienst RIES was er een sterke noodzaak om het geheel van techniek, beheer en beveiliging maar ook processen en procedures kritisch tegen het licht te houden.

Onder de vlag van het projectteam *'Kiezen op Afstand'*, is de stemdienst (waar RIES een onderdeel van uitmaakte) uitvoering getest. In aanvulling op de reeds uitgevoerde onderzoeken naar RIES, is opdracht gegeven aan CIBIT om de broncode te beoordelen van de implementatie van RIES en heeft GOVCERT.NL een audit uitgevoerd op het beveiligingsniveau van de website waarmee een internetstem kon worden uitgebracht. Het systeem heeft de testen en onderzoeken met goedgevolg doorlopen, wat heeft geleidt tot succesvolle inzet van RIES tijdens de tweede kamerverkiezingen voor de Nederlandse kiezers in het buitenland.

**2006-2008 Landelijke Waterschapsverkiezingen 2008:**
Het najaar van 2008 staat in het teken van de eerste landelijke waterschapsverkiezingen. Bij het besluit hiertoe, door de waterschappen, is ook vastgelegd dat naast het vertrouwde stemmen per brief, iedere stemgerechtigde zijn stem via internet moet kunnen uitbrengen.

De waterschappen zullen bij de voorbereiding en uitoefening van deze nieuwe vorm van waterschapsverkiezingen intensief worden begeleid door de landelijke projectorganisatie. Het Rijnland Internet Election System, zal op de nieuwe context worden afgestemd onder de noemer RIES 2008. Het belang van her-evaluatie van eerdere uitgangspunten en onderzoeksdomeinen is onontbeerlijk. In 2008 worden relevante onderzoeken om rechtsgeldige verkiezingen te garanderen uitgevoerd. Verouderde onderzoeken zullen worden herhaald en voor niet eerder beoordeelde domeinen zullen nieuwe onderzoeken worden opgezet.

In 2008 zal de EIPSI van de TU Eindhoven een analyse maken van de algehele veiligheid van RIES 2008. Daarnaast zal de RIES 2008 implementatie na oplevering wederom aan een broncode beoordeling onderhevig worden gesteld door een onafhankelijk gerenommeerde expertise centrum.

## 2002 – 2004 (Ries - Rijnland)

| **Organisatie** | **TNO Technische Menskunde, Soesterberg** |
|---|---|
| Titel | **ELS: Beveiligings- en gebruikersaspecten van elektronisch stemmen voor het Hoogheemraadschap van Rijnland** |
| Datum | 19 dec 2002 |
| Auteur ('s) | |
| Bestandsnaam | http://www.rijnlandkiest.nl/contents/pages/00000109/rapporttno.pdf |
| Onderzoeksvraag | Door TNO uitgevoerd haalbaarheidsonderzoek naar het gebruik van stemmen per telefoon en stemmen per PC (via internet) bij de waterschapsverkiezingen van 2004 van het Hoogheemraadschap van Rijnland. Onderzoek is gericht op twee aspecten, namelijk de techniek (kan een betrouwbaar kiessysteem worden aangeboden) en de houding van de burger (gebruiksvriendelijkheid en gebruikersacceptatie van een dergelijk systeem). |

| **Organisatie** | **Cryptomathic, Aarhus, Denmark** |
|---|---|
| Titel | **Review of RIES**<br>( The Cryptographic Design and comments) |
| Datum | 21 januari 2004 |
| Auteur('s) / Betrokkenen | |
| Bestandsnaam | Review of RIES_cryptomathic_comments_20040126.doc<br>http://www.surfnet.nl/bijeenkomsten/ries/salomonson.ppt |
| Onderzoeksvraag | Review of Ries is een security review van het 'Rijnland Internet Election System' |

| **Organisatie** | **TNO Technische Menskunde, Soesterberg** |
|---|---|
| Titel | **Human factor aspects of the voter screens ,**<br>referentie: Memo TNO-TM 2004-M006 |
| Datum | 27 januari 2004 |
| Auteur ('s) | - |
| Bestandsnaam | M006 Resultaten Quickscan Myra van Esch.pdf |
| Onderzoeksvraag | Het Hoogheemraadschap van Rijnland heeft een prototype ontwikkeld van een systeem dat het mogelijk maakt elektronisch een stem uit te brengen voor de waterschapsverkiezingen. TNO Technische Menskunde is gevraagd om in dit stadium van de ontwikkeling, voor de daadwerkelijke implementatie, eventuele knelpunten m.b.t. de gebruiksvriendelijkheid op te sporen. Een onderdeel van deze quickscan is vast stellen op hoofdlijnen of het systeem voldoet aan de richtlijnen die zijn opgesteld voor 'Universal Accessibility' (o.a. in het kader van het 'drempels weg'-initiatief). Naar aanleiding van de vastgestelde knelpunten in het systeem zal in overleg met Rijnland bepaald worden voor welke knelpunten oplossingen zullen worden uitgewerkt. |

| **Organisatie** | **Netpanel,** in opdracht van **Burger@Overheid, ICTU Den Haag** |
|---|---|
| Titel | **E-stemmen: Laat jij je digitale stem gelden ?**<br>Evaluatie-onderzoek van het online stemmen |
| Datum | Juli 2004 |
| Auteur ('s) | - |
| Bestandsnaam | http://burger.overheid.nl/files/def_rapport_stemmen.pdf |
| Onderzoeksvraag | Voor deze meting onder het Publiekspanel geldt de volgende onderzoeksvraag:<br>'Hoe worden door burgers de procedures bij het online stemmen en bij de stemcontrole ervaren? ' |

| **Organisatie** | **Security of Systems - Faculteit der Natuurwetenschappen, Wiskunde en Informatica, Radboud universiteit Nijmegen** |
|---|---|
| Titel | Server audit van RIES<br>'externe penetratietests onder leiding van Bart Jacobs' |
| Datum | 23 juli 2004 |
| Auteur ('s) | - |
| Bestandsnaam | report KUN.pdf<br>http://www.surfnet.nl/bijeenkomsten/ries/hubbers.pdf |
| Onderzoeksvraag | Als Security of Systems groep hebben wij de opdracht gekregen om van buitenaf te proberen de stemserver aan te vallen tijdens de Burger @ Overheid test, lopende van woensdag 30 juni, 09.00 uur tot donderdag 8 juli, 12.00 uur, gevolgd door een tweede periode lopende van vrijdag 9 juli, 09.00 uur tot maandag 12 juli, 18.00 uur.<br><br>Hierbij was het de bedoeling dat wij zoveel mogelijk zonder informatie te krijgen over het systeem vanuit het projectteam, de server zouden onderwerpen aan een test. En dus alleen gebruik mochten maken van de informatie publiekelijk is gemaakt. |

| **Organisatie** | **Faculteit der Natuurwetenschappen, Wiskunde en Informatica, Radboud universiteit Nijmegen** |
|---|---|
| Titel | **Stemmen via internet geen probleem**<br>Automatisering Gids #42 |
| Datum | 15 okt. 2004 |
| Auteur ('s) | - |
| Bestandsnaam | http://www.cs.ru.nl/B.Jacobs/PAPERS/ries_populair.pdf |
| Onderzoeksvraag | Internetstemmen kan op een veilige manier gebeuren. Eind september, begin oktober is ervaring opgedaan met het `Rijnland Internet Election System' bij de waterschapsverkiezingen voor het Hoogheemraadschap Rijnland. Bart Jacobs en Engelbert Hubbers analyseren wat er precies gebeurt als er via internet wordt gestemd, hoe veilig het is en waar de zwakke plekken zitten. |

| | |
|---|---|
| **Organisatie** | **Faculteit der Natuurwetenschappen, Wiskunde en Informatica, Radboud universiteit Nijmegen** |
| Titel | **RIES – Internet Voting in Action** |
| Datum | December 2004 |
| Auteur ('s) | - |
| Bestandsnaam | http://unpan1.un.org/intradoc/groups/public/documents/Other/UNPAN024871.pdf |
| Onderzoeksvraag | RIES stands for Rijnland Internet Election System. It is an online voting system that has been used twice in the fall of 2004 for in total over two million potential voters. In this paper we describe how this system works. Furthermore we describe how the system allowed us to independently verify the outcome of the elections—a key feature of RIES. To conclude the paper we evaluate possible threats to this system and describe some possible points for improvement. |

| | |
|---|---|
| **Organisatie** | **Madison Gurka, Eindhoven** |
| Titel | **Crystal-box security evaluation,**<br><Alleen gedrukte variant beschikbaar HWH><br>**<status: vertrouwelijk>** |
| Datum | 2004 |
| Auteur ('s) | - |
| Bestandsnaam | - |
| Onderzoeksvraag | Beoordeling van de RIES server- en netwerkopzet bij SURFnet op het gebied van beveiliging. |

## 2006 – 2007 (Kiezen op Afstand)

| **Organisatie** | **GOVCERT, Den Haag** |
|---|---|
| Titel | **Webapplicatie-scan Kiezen op Afstand**<br>Status: Vertrouwelijk.<br>Referentie: DW/ET/AH/6105 |
| Datum | 01 september 2006<br><vetrouwelijk> |
| Auteur ('s) | - |
| Bestandsnaam | Technische scan KOA-1.0.pdf |
| Onderzoeksvraag | In opdracht van het ICTU-programma 'Kiezen op Afstand' heeft GOVCERT.NL een scan uitgevoerd op de website www.internetstembureau.nl. Het doel van de scan is het verkrijgen van inzicht in het huidige ICT-beveiligingsniveau van de applicatie. Door middel van een technische scan is de functionele werking van de applicatie in de productieomgeving getest op bekende kwetsbaarheden. Alleen de technische werking van de applicatie is onderzocht, de architectuur van de achterliggende systemen is niet beoordeeld. Dit rapport beschrijft beknopt de resultaten van de uitgevoerde scan. |

| **Organisatie** | **CIBIT, Bilthoven** |
|---|---|
| Titel | Beoordeling KOA, Een beoordeling van de integriteit van "Kiezen op Afstand"<br>**Broncode review "Kiezen op Afstand"** |
| Datum | 11 september 2006 |
| Auteur ('s) | - |
| Bestandsnaam | http://www.minbzk.nl/aspx/download.aspx?file=/contents/pages/83575/eindrapportcibit.pdf |
| Onderzoeksvraag | In het kader van "Kiezen op Afstand" heeft CIBIT een broncodebeoordeling uitgevoerd naar de implementatie van de waarborgen van de stemdienst. Dit is gebeurd op basis van onderzoek naar de constructie en implementatie van de applicatie. De waarborgen van het stemgeheim, uniciteit, kiesgerechtigheid, integriteit, controleerbaarheid, hertelling zijn allemaal ingevuld door de stemdienst. Ook zijn er afhankelijkheden van de operationele inrichting en beveiliging in kaart gebracht die noodzakelijk zijn om aan de waarborgen te voldoen. |

| **Organisatie** | **Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Den Haag** |
|---|---|
| Titel | **Risicoanalyse Kiezen op Afstand**<br>Stemmen via internet voor kiezers in het buitenland<br>status Definitief, versie 1.1 |
| Datum | 03 april 2007 |
| Auteur ('s) | |
| Bestandsnaam | risicoanalyse.pdf |
| Onderzoeksvraag | Dit document inventariseert de mogelijke risico's die zich kunnen voordoen bij een experiment waarbij de kiezers in het buitenland (ook) kunnen stemmen per internet.<br>Voor het inventariseren en rangschikken van de risico's is gebruik gemaakt van meerdere invalshoeken. De gehanteerde invalshoeken zijn:<br>- Risico's per stap in het stemproces.<br>- Politiek-bestuurlijke risico's.<br>- Organisatorische risico's.<br>- Juridische risico's.<br>- Technische / Operationele risico's. |

| **Organisatie** | **Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Den Haag** |
|---|---|
| Titel | **Evaluatie van het experiment Internetstemmen**<br>Tweede Kamer verkiezingen 2006, Project Kiezen op Afstand |
| Datum | 26 april 2007 |
| Auteur ('s) | |
| Bestandsnaam | http://www.minbzk.nl/aspx/download.aspx?file=/contents/pages/84854/iievaluatierapportkoainternetstemmen.pdf |
| Onderzoeksvraag | De evaluatie van het experiment met internetstemmen bij de Europese Parlementsverkiezingen 2004 bevatte zeven aanbevelingen. Hieronder wordt beschreven in welke mate deze zijn opgenomen in het experiment 2006.<br><br>1. Bied de kiezers in het buitenland opnieuw de mogelijkheid om per internet of telefoon te stemmen bij de eerstvolgende verkiezingen.<br>2. Onderzoek de mogelijkheden om de structurele en incidentele kosten van het stemmen per internet- en telefoon tot het minimum terug te brengen.<br>3. Wijs een instantie aan om een onafhankelijk oordeel te geven over de betrouwbaarheid van de technische voorzieningen.<br>4. Ga na onder welke voorwaarden de registratie per internet zou kunnen plaatsvinden.<br>5. Onderzoek de mogelijkheden om de authenticatieprocedure dusdanig aan te passen dat het verlies van de toegangscode geen fataal gevolg heeft.<br>6. Bij een vervolgexperiment kan de ondersteuning verminderd worden.<br>7. Onderzoek de mogelijkheid voor een kortere stemperiode. |

## 2008 (Landelijke Waterschapsverkiezingen)

| | |
|---|---|
| **Organisatie** | Uitvoering: **EIPSI,** Technische Universiteit Eindhoven (TU/e)<br>Opdrachtnemer: **LaQuSo,** TU/e ,Radboud Universiteit Nijmegen |
| Titel | **Werktitel: "Beschrijving en analyse van de veiligheid van RIES"** |
| Datum | Juni 2008 |
| Auteur ('s) | |
| Bestandsnaam | 07 10 18 Waterschapshuis offerte RIES_retour aangepast.doc |
| Onderzoeksvraag | De scope van het onderzoek betreft de technische, organisatorische en procedurele aspecten van de veiligheid van het RIES-systeem in zijn algemeenheid, met aparte aandacht voor:<br>- RIES-KOA zoals gebruikt bij de Tweede Kamerverkiezingen in november 2006;<br>- RIES-2008 zoals nu in ontwikkeling voor de waterschapsverkiezingen van 2008.<br><br>Het begrip veiligheid moet hier begrepen worden als het voldoen aan algemeen aanvaarde criteria die voor verkiezingssystemen in zijn algemeenheid en internet-verkiezingssystemen in het bijzonder gelden, gericht op het aanvaardbaar houden van de risico's van verkiezingsfraude. Bij de analyse komt een breed spectrum aan eigenschappen en perspectieven aan bod, waaronder bruikbaarheid. |

| | |
|---|---|
| **Organisatie** | < een onafhankelijke audit-organisatie met bewezen ervaring op dit vlak, details nog niet bekend> |
| Titel | **Broncode review** |
| Datum | Medio 2008 |
| Auteur ('s) | - |
| Bestandsnaam | - |
| Onderzoeksvraag | broncode review van RIES 2008, qua opzet vergelijkbaar met de broncode review KOA uitgevoerd door CIBIT in 2006. |

| | |
|---|---|
| **Organisatie** | - |
| Titel | **Extern Review op eerder uitgevoerde onderzoeken** |
| Datum | Medio 2008 |
| Auteur ('s) | - |
| Bestandsnaam | - |
| Onderzoeksvraag | <een onafhankelijke organisatie gaat in 2008 reeds uitgevoerde onderzoeken beoordelen, details nog niet bekend> |

| | |
|---|---|
| **Organisatie** | **Alfa-informatica, Rijksuniversiteit Groningen** |
| Titel | **Onderzoek naar usability aspecten van het poststembiljet en de webinterface** |
| Datum | 2008 |
| Auteur ('s) | - |
| Bestandsnaam | - |
| Onderzoeksvraag | Probleemstelling: Beoordeling van de opzet van het poststembiljet (Waterschapsverkiezingen 2008) waarbij de kiezer wordt verzocht zijn geboortejaar in te vullen. Geen of foutieve opgave van geboortejaar maakt het stembiljet ongeldig. |

## Prijzen: United Nations Public Service Award 2006:

- Region: Europe and North-America:
- Winnaar in categorie 1:*"Improving transparency, accountability and responsiveness in the public service"*
- http://unpan1.un.org/intradoc/groups/public/documents/un/unpan022965.pdf

## Testen Mastertestplan Projectgroep KOA 2006

Het ICTU programma "Kiezen op Afstand" maakte in 2006 gebruik van de RIES stemdienst (Rijnland Internet Election System). De stemdienst is hiervoor aangepast aan de specifieke (wettelijke) vereisten voor Tweede Kamer verkiezingen. Onder het begrip "stemdienst" wordt het geheel van techniek, beheer, beveiliging, processen en procedures verstaan. De stemdienst is derhalve meer dan alleen een webserver

In opdracht van de ICTU programmamanager "Kiezen op Afstand" 2006 is een mastertestplan opgesteld, waarin de het gehele testtraject rondom KOA 2006 is uitgewerkt.

| | |
|---|---|
| 1) **Bouw / programma / unittest** | De bouw / programma / unittest is een door de ontwikkelaar in het laboratorium uitgevoerde test, die moet aantonen dat een programma of programmadeel aan de in de technisch specificaties gestelde eisen voldoet. De meest elementaire onderdelen van het systeem worden getest. |
| 2) **FAT (Functionele Acceptatie Test)**: | Het doel van de FAT is aantonen dat de tijdens het increment ontwikkelde objecten/systeemdelen voldoen aan de daarvoor opgestelde functionaliteit. |
| 3) **Performance test** | De performancetests dient zich te richten op de verwerkingscapaciteit van de stemdienst en niet op de functionaliteit. In een gecontroleerde omgeving wordt belasting gegenereerd voor het testobject en wordt de performance van het testobject gemeten. |
| 4) **Beveiligingstests** | |
| - Penetratietest (Govcert) | De penetratietest heeft tot doel te testen hoe moeilijk het is om een computernetwerk binnen te dringen. |
| - DDOS (Denial of Service) | De belastbaarheid van het testobject wordt onderzocht door het systeem zó te belasten dat het systeem overbelast raakt. |
| - Source Code review | Een review van de source code door een specialistische onafhankelijke partij zorgt ervoor dat met redelijke mate van zekerheid kan worden vastgesteld dat de software geen verborgen of foutieve elementen bevat. |
| - Social Engineering | De zwakste schakel bij het beveiligen van een systeem of netwerk is de mens. Social engineering is een techniek waarbij een kwaadwillende een aanval op een computersysteem tracht te ondernemen door bij de gebruikers en/of beheerders van het systeem vertrouwelijke of geheime informatie los te krijgen. |
| - Encryptie / hash test | In de stemdienst worden meerdere encryptiemethodes gebruikt. Een (literatuur) onderzoek om te bestuderen of de gebruikte methodes voldoende beveiliging biedt geeft een goed beeld van de mogelijkheid tot het kraken van de data |

| | |
|---|---|
| **5) Usability test** | Het usability onderzoek is een gebruikersonderzoek waarmee de usability (gebruiksvriendelijkheid) van de stemdienst onderzocht wordt. Omdat ontwerpers als expert-gebruikers van het systeem worden beschouwd vanwege hun ervaring met het systeem die zij tijdens de ontwikkeling hebben opgedaan, worden voor het onderzoek toekomstige eindgebruikers uitgenodigd om het systeem te testen. Met een eenvoudige test kan met behulp van een kleine groep gebruikers relatief snel tot 80% van de grootste knelpunten opgespoord worden. |
| **6)**<br>- **Accessibility test**<br>- **Browser compatibility test** | - De accessibility test richt zich op de toegankelijkheid van het systeem.<br>- De browser compatibility test heeft als doel om de compatibiliteit van de gerealiseerde applicatie onder verschillende, meest gebruikte browsers en platformen te testen. |
| 7) **Beheersmatige tests** | |
| - Disaster recovery test | In het geval van een ernstige calamiteit met betrekking tot de beschikbaarheid van de systemen is het van belang dat er een plan aanwezig is hoe er omgegaan dient te worden met de situatie |
| - Failover test | Het doel van een Fail over test is na te gaan of de genomen herstelmaatregelen in de productie omgeving adequaat werken |
| **8) Keten (integratie) test** | Het doel van de ketentest is vaststellen dat de hoofdprocessen door de onderliggende systemen correct ondersteund worden. |
| **9) Schouwplan** | Doel van het schouwplan is om aan te geven in welke mate de stemdienst (organisatie en techniek) gereed is voor de aanvang van de stemming. |

## Testen project Waterschapsverkiezingen 2008, Het waterschapshuis.

Voor de Waterschapsverkiezingen in 2008 waarbij gebruik wordt gemaakt van RIES 2008. Het gaat om een verder ontwikkelde versie van de indertijd gebruikte versie van RIES 2007 voor KOA.

Audits en Reviews die in het verleden zijn uitgevoerd op de voorloper van RIES 2008 zullen grotendeels overnieuw worden uitgevoerd.