Rapportage

Advisering toelaatbaarheid internetstemvoorziening waterschappen

Classificatie	**OPENBAAR**
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	12-08-2008
Versie	3.0
Business Unit	Forensics, Audits & Training
Auteurs	Bartek Gedrojc, Matthieu Hueck, Hans Hoogstraten, Mark Koek, Sjoerd Resink
Pagina's	75

OPENBAAR
Dit document is geclassificeerd als openbaar. Op het document zijn geen toegangsbeperkingen van toepassing.

Fox-IT BV

Olof Palmestraat 6
2616 LM Delft

Postbus 638
2600 AP Delft

Tel.: (015) 284 7999
Fax: (015) 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: 12-08-2008
Versie: 3.0
Status: Definitief

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
3.0	E-mail	W. Aarnink en L. Luijten, Ministerie van Verkeer en Waterstaat
3.0	E-mail	S. Bouwman, Waterschapshuis

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, Mark Koek, Sjoerd Resink,	Interne conceptversies
2.0	12-07-2008	Mark Koek	Eerste externe conceptversie
3.0	12-08-2008	Bartek Gedrojc, Mark Koek	Definitieve versie n.a.v. opmerkingen Ministerie en Waterschapshuis

Gerelateerde documenten

Versie	Datum	Omschrijving	Opmerkingen

Samenvatting

De Staatssecretaris van Verkeer en Waterstaat heeft in de Regeling waterschapsverkiezingen 2008 Fox-IT aangewezen als instelling om haar te adviseren over de beoordeling van de internetstemvoorziening die door de waterschappen is ontworpen voor de waterschapsverkiezingen van november 2008. De organisatie waarin de waterschappen samenwerken op ICT-gebied, het Waterschapshuis, heeft daartoe ingevolge artikel 5 van de Regeling 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 (juni 2008) moet worden vastgesteld dat dit kwaadwillenden diverse mogelijkheden biedt om de uitslag te beïnvloeden, het verkiezingsproces te saboteren en/of om op termijn 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 20 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 16 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.

In de Regeling waterschapsverkiezingen 2008 is Fox-IT aangewezen als instelling die de Staatsecretaris van Verkeer en Waterstaat adviseert 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 ten dele opgevolgd in RIES-2008. De sleutel *Kgenvoterkey* wordt nu door cryptografische hardware onvoorspelbaar gegenereerd. De stemsleutels *Kp* worden nog niet optimaal onvoorspelbaar gegenereerd, doordat ze allemaal afhangen van dezelfde sleutel *Kgenvoterkey* en doordat ze elk individueel afhangen van het Burgerservicenummer van de betreffende kiezer.

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 stempakket 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 RIES-2004 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.

Opmerking 2a

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

M – Kiezers worden goed voorgelicht over het vernietigen van de internetstemkaarten. 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 internetstemkaart
De verantwoordelijkheid van het vernietigen van de internetstemkaart ligt ook in RIES-2008 bij de kiezer. Met een internetstemkaart kan na de verkiezing met enig rekenwerk worden achterhaald op wie de kiezer heeft gestemd, mits de aanvaller weet van wie de internetstemkaart is (er staan geen identificerende gegevens op de kaart zelf, dus die zal de aanvaller moeten weten dan wel afleiden van andere papieren zoals de envelop).

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 zonder technische stemcode
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 zonder dat de kiezer zijn technische stemcode overlegt aan de "Umpire". Die moet de kiezer dan bewaard hebben, wat een risico oplevert voor het stemgeheim. Zie ook bevinding 5.4.

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 om 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 .

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 stempakketten 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 zonder dat de kiezers ook hun technische stemcodes overleggen? 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 anderen 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 als aanvulling op 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. Daarvoor is een geavanceerde inbraak nodig, of 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 Biinnenlandse 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 irrelevant maakt 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 in de documentatie niet aan of men instemt met deze bevinding en zo ja, op welke wijze hetzelfde probleem in de toekomst kan worden voorkomen. Daarbij moet worden aangetekend dat het Waterschapshuis zelf geen rol speelde in 2004, dat het ging om een test, en dat RIES sindsdien herhaaldelijk bij echte verkiezingen is gebruikt zonder dat vergelijkbare issues zijn geconstateerd.

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 beheerschermen (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 vanuit het algemene uitgangspunt dat meer gebruikte encryptiemethoden aan meer onderzoek zijn onderworpen. Wel moet worden opgemerkt dat MDC al sinds de jaren ’80 door IBM wordt gebruikt in haar cryptografische producten en dat er ondanks die lange tijd geen problemen met het algortime bekend zijn.

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). In reactie op dit rapport vatte het Waterschapshuis de impact van deze kwetsbaarheden te lichtvaardig op door te stellen dat actie op dit punt beperkt kon blijven tot het kiezen van een korte domeinnaam en kiezers erop te wijzen dat deze direct moet worden ingevoerd.

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 ten behoeve van SURFnet 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 (28). Dit is met name belangrijk voor mensen met een visuele handicap.

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.

Dat betekent dat door de manier waarop de eisen zijn geformuleerd de stemsite formeel niet aan deze eisen kan voldoen.

Het Waterschapshuis gaat in haar reactie (20) niet uitgebreid in op deze analyse, maar beperkt zich tot de mededeling dat niet alle bevindingen in 2008 zullen zijn opgelost.

In nadere gesprekken heeft het Waterschapshuis aangegeven dat er wel degelijk uitgebreid aandacht is besteed aan de toegankelijkheid van de stemsite voor visueel gehandicapten.

Bevinding 2.12. Stemsite werkt niet goed in sommige browsers

De conclusie van de regressietest (36) 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 haar reactie (20) aan hier geen prioriteit aan te geven voor 2008. Gebruikers hebben met het gratis beschikbare Mozilla Firefox een alternatief.

In nadere gesprekken heeft het Waterschapshuis aangegeven deze zaken wel voor november 2008 te zullen oplossen.

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. De regelgeving rondom de waterschapsverkiezingen staat meerdere kanalen toe, dus formeel kan RIES-2008 aan deze aanbevelingen niet voldoen. Dubbeltellingen worden voorkomen, dus dit betreft vooral een formaliteit.

Wel is het theoretisch mogelijk dat een stem na te zijn uitgebracht ongeldig wordt gemaakt, ofwel doordat de kiezer nogmaals stemt per post, ofwel als door een technische storing de databases op de 3 locaties waar zich servers van de stemdienst bevinden niet of niet tijdig synchroniseren; in dat geval zijn kiezers in staat om nogmaals per internet te stemmen. Als de tweede stem op een andere kandidaat wordt uitgebracht worden beide stemmen ongeldig.

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 gedocumenteerd

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.

Het Waterschapshuis heeft aangegeven dat een proefstemsite wel is voorzien voorafgaand aan de verkiezingen, waarmee wel aan aanbeveling 22 zou worden voldaan.

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 identificatiemethode bij gelijke naam en gelijk adres niet gedocumenteerd

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.

De waterschappen hebben aangegeven dat hiertoe wel degelijk een mechanisme is ontwikkeld met een unieke identificerende code. Deze methode is niet onderzocht maar aannemelijk is dat in de praktijk wel zal worden voldaan aan de aanbeveling van de Raad van Europa.

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 op, 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 geven.

Ten overvloede merken wij op dat, hoewel de navolgende bevindingen in de tegenwoordige tijd zijn gesteld, het onderzoek van Fox-IT plaatsvond in juni 2008. Zie ook paragraaf 1.4.

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/pla
in;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=aWdub3Jlc3RhdHVzP
WZhbHNlJnJlc3BpZD1mY2QxNDRmNTUwNDFhZTU3N2RmYmI1YThkNTI2MTc1YyY%3D&text_group=S
electeer+de+lijst+van+uw+voorkeur+of+selecteer+%27blanco+stem%27%3Cbr%3E+en+kl
ik+op+%27Verder%27.%3Cbr%3E+&text_candidate=Maak+uw+keuze+en+klik+op+%27Verder
%27.&text_group_infomsg=Er+zijn+nog+meer+lijsten%2C%3Cbr%2F%3E+klik+op+de+scro
llbar+--%3E&text_candidate_infomsg=Er+zijn+nog+meer+kandidaten%2C%3Cbr%2F%3E+k
lik+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+natuurlijk%3A800100010303%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
|700a76ba928c6036-d7f181f9ccc44df1|%68%74%74%70%3a%2f%2f%77%77%77%2e%66%6f%78%
2d%69%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
|700a76ba928c6036-d7f181f9ccc44df1|6D72CFFA
```

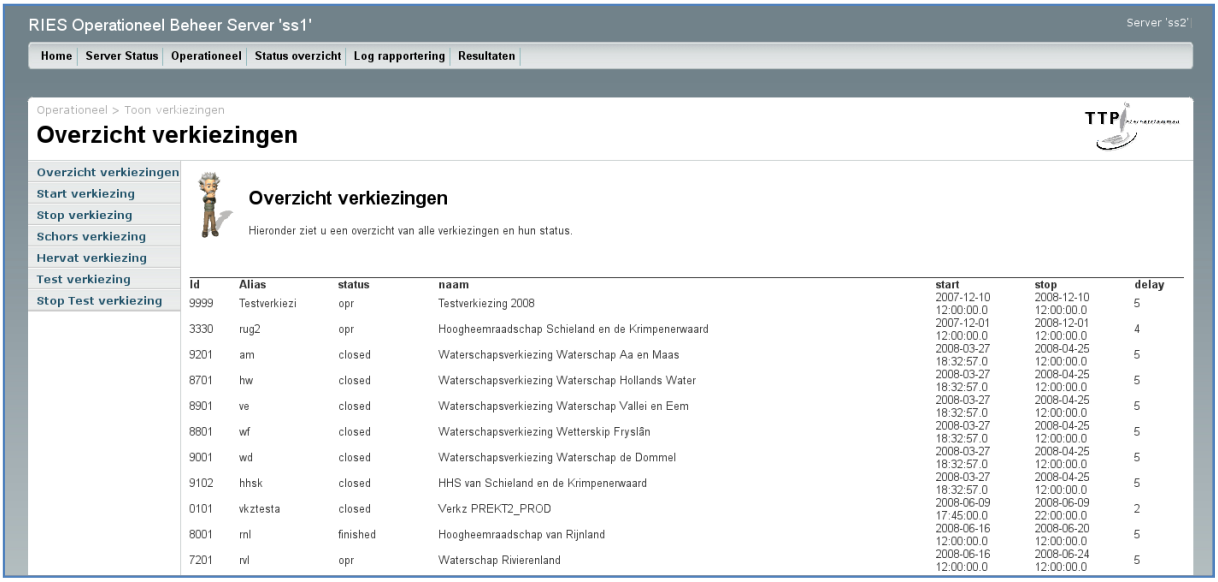
Een ander scenario is dat de kiezer heeft gestemd op de PC van iemand anders, op het werk, bij vrienden of familie, of in een internetcafé. Een volgende gebruiker zou uit de browsergeschiedenis (als deze niet gewist wordt) de gebruikte technische stemcodes kunnen achterhalen.

Bevinding 4.7. Beheerschermen zichtbaar via het internet

Er kunnen beheerschermen 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.

Deze schermen stellen 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 beheerschermen kwetsbaar zijn voor XSS:

```
https://stem.surfnet.nl/server/%5C../admin/server?req=results&subreq=store&pag
eid=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 stemserver te versterken.

De volgende URL veroorzaakt een loop van HTTP-aanvragen naar de 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. Beheerschermen geven informatie vrij

De aangetroffen beheerschermen geven 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&pag
eid=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 aangetroffen beheerschermen zijn 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 schermen kwetsbaar zijn voor SQL injection:

De databasegebruiker is `ries`:

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

Een tabel met de naam `status`:

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

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

Het is mogelijk dat de leverancier van de software de oude versie wel heeft bijgewerkt om bestand te zijn tegen de bekende kwetsbaarheden in deze versie. Er is niet gepoogd om de kwetsbaarheden daadwerkelijk te misbruiken.

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. Veiligheidsniveaus van symmetrische algoritmen ECRYPT 2007

Veilig-heids-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):

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

$$RnC1_n = MDC[DESmac_{Kp_n}(f(C1, ElID, AbelPI_n))] \quad \text{kandidaat 1} \quad [4]$$

$$RnC2_n = MDC[DESmac_{Kp_n}(f(C2, ElID, AbelPI_n))] \quad \text{kandidaat 2}$$

$$\vdots \qquad \vdots$$

$$RnCm_n = MDC[DESmac_{Kp_n}(f(Cm, ElID, AbelPI_n))] \quad \text{kandidaat } m$$

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

$$RnC1_{n+1} = MDC[DESmac_{Kp_{n+1}}(f(C1, ElID, AbelPI_{n+1}))] \quad \text{kandidaat 1}$$

$$RnC2_{n+1} = MDC[DESmac_{Kp_{n+1}}(f(C2, ElID, AbelPI_{n+1}))] \quad \text{kandidaat 2}$$

$$\vdots \qquad \vdots$$

$$RnCm_{n+1} = MDC[DESmac_{Kp_{n+1}}(f(Cm, ElID, AbelPI_{n+1}))] \quad \text{kandidaat } m$$

… 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
$VnPID = MDC[DESmac_{Kp_1}(f(ElID))]$	$VnCx = MDC[DESmac_{Kp_1}(f(C2, ElID, AbelPI_1))]$
$VnPID = MDC[DESmac_{Kp_2}(f(ElID))]$	$VnCx = MDC[DESmac_{Kp_2}(f(C8, ElID, AbelPI_2))]$
⋮	⋮
$VnPID = MDC[DESmac_{Kp_x}(f(ElID))]$	$VnCx = MDC[DESmac_{Kp_x}(f(C7, ElID, AbelPI_n))]$

[6]

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 26 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 26 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:

$$p = \frac{1\,\text{miljoen}}{7{,}205 \cdot 10^{16}} \approx \frac{2^{20}}{2^{56}} = 2^{-36} \approx 0{,}000000000014\,55$$

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:

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

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?

We hebben enige tests uitgevoerd om vast te stellen hoe snel een gewone thuis-PC stemcodes zou kunnen berekenen (zie Appendix C). Op basis van deze tests is het een redelijke aanname dat een gangbare thuis-PC 1 miljoen *RnPID*-waarden per seconde kan berekenen.

Hierdoor kunnen we het volgende berekenen:

$$\frac{\text{Te proberen waarden van RnPID}}{\text{Berekenbare waarden per seconde}}=\frac{2^{36}}{1.000.000}=\frac{68.719.476.736}{1.000.000}=68{,}719\,\text{sec}\approx 19\,\text{uur}$$

In minder dan een etmaal zijn wij in staat om 2^{36} RnPID-waarden te berekenen met de daarbij horende stemsleutel. 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 in het stempakket vermeld 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:

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

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

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:

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

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 onder 26 waterschappen of dat er één grote verkiezing is in heel Nederland 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 uit te breiden door meerdere computers tegelijkertijd in te zetten, bijvoorbeeld door het gebruik van een botnet of door een oproep te doen via een populaire weblog. Als oplossingsrichting heeft het Waterschapshuis voorgesteld om het referentiebestand niet voorafgaand aan de verkiezingen te publiceren. Dat is een belangrijke wijziging van het systeem die in strijd is met de huidige regelgeving, maar die het niettemin waard is om nader te onderzoeken.

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. "Umpire"-functie kan niet alle disputen oplossen; krijgt inzicht in de uitgebrachte stem
De Umpire-functie is niet in staat alle disputen op te lossen (zie ook EiPSI (10), p. 47). Het nut van de kwitantie *VotRecConCnt* is beperkt. Een kiezer kan niet valideren of de waarde die hij heeft ontvangen na het stemmen correct is. Ook kan een kiezer een valse waarde presenteren en beweren dat de stemserver deze heeft verzonden. Daarnaast kan een kiezer beweren dat hij eigenlijk op een andere kandidaat heeft gestemd, oftewel dat het systeem dit foutief heeft opgeslagen (een correcte kwitantie voor een andere stem). De Umpire kan anomalieën vaststellen, maar het is niet helder dat hij ze allemaal kan oplossen. Ook kan de Umpire niet veel met de kwitantie op zichzelf. Bij een dispuut moet de kiezer zijn technische stemcode hebben opgeslagen, iets dat in het algemeen niet aan te raden is omdat zijn stem eruit zou kunnen worden afgeleid. De kwitantie bewijst eigenlijk alleen dat de kiezer de technische stemcode niet heeft vervalst, maar ook echt zo heeft uitgebracht.

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 in de stembescheiden. 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 stembescheiden 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 stempakket in handen komt van een aanvaller hij niet in staat moet zijn een geldige stem uit te brengen.

Als een aanvaller een stempakket steelt of bemachtigt van een geldige kiezer is hij in staat om via de gepubliceerde informatie de AbelPI te achterhalen die hoort bij het stempakket. 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
⋮	⋮
$RnCm_n = MDC[DESmac_{Kp_n}(f(Cm, ElID, AbelPI_n))]$	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. Tevens moet worden opgemerkt dat de AbelPI als beveiligingsmaatregel bij het poststemmen van zeer beperkte waarde is als ook internetstemmen wordt toegepast, aangezien met behulp van de stemsite kan worden gevonden wat de AbelPI moet zijn op het poststembiljet.

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?*

Conclusies betreffen de internetstemvoorziening zoals in juni 2008 in ontwikkeling. Zie ook paragraaf 1.4.

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 5 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 aanvullend te zijn bij poststemmingen, niet om een fysieke stembusgang te vervangen.

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.

- **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 volledigheidshalve naar bevindingen 2.11 en 2.12, die echter geen significante moeilijkheden in de praktijk betekenen.

6.3 Overzicht van opmerkingen en verbeterpunten

In onderstaande tabel worden de bevindingen van Fox-IT samengevat. Bevindingen kunnen leiden tot acceptatie van de constatering, of kunnen aanleiding geven tot aanpassingen.

Nr.	Pag.	Bevinding
2.1	9	Gedateerde methoden voor versleutelen van gevoelige informatie
2.2	11	Machtspositie Waterschappen en SURFnet
2.3	12	Tijd-/datuminformatie mag niet worden opgeslagen
2.4	13	Stem kan achterhaald worden met internetstemkaart
2.5	13	Stemkwitantie is niet falsificeerbaar zonder technische stemcode
2.6	15	*Insiders* kunnen stemmen vervangen
2.7	16	Stemserver in 2004 niet adequaat afgesloten, bevinding niet opgevolgd
2.8	16	Technische beveilingstest serverconfiguratie niet uitgevoerd
2.9	17	Risico van relatieve onbekendheid MDC-2
2.10	18	Geen calamiteitenplan
2.11	19	Stemsite voldoet niet aan toegankelijkheidseisen overheidswebsites
2.12	19	Stemsite werkt niet goed in sommige browsers
3.1	20	Toegankelijkheid en bedieningsgemak
3.2	20	Kiezer kan stem later ongeldig maken
3.3	20	Versleutelde stemmen worden opgeslagen
3.4	20	Foutmelding meldt niet dat ook blanco kan worden gestemd
3.5	20	Anonimiteit niet onbeperkt gewaarborgd
3.6	21	Uitproberen stemsysteem niet gedocumenteerd
3.7	21	Kwitantie en stembevestiging in strijd met aanbevelingen Raad van Europa
3.8	21	Eenduidige identificatiemethode bij gelijke naam en gelijk adres niet gedocumenteerd
3.9	21	Sporen van stem worden niet uitgewist
3.10	21	Integriteit van logsysteem niet gewaarborgd
4.1	22	Stembureau kan afgebroken stemmen inzien
4.2	23	Versienummer systeemsoftware leesbaar
4.3	23	Verouderde versie van systeemsoftware met bekende beveiligingsfouten
4.4	23	Servermappen zijn in te zien
4.5	24	Kwitantie is manipuleerbaar
4.6	24	Technische stemcodes in browsergeschiedenis
4.7	24	Beheerschermen zichtbaar via het internet
4.8	25	Beheerschermen kwetsbaar voor Cross-Site Scripting (XSS)
4.9	25	Mogelijkheid om *Denial-of-Service*-aanval te versterken
4.10	26	Beheerschermen geven informatie vrij
4.11	26	Beheerschermen kwetsbaar voor databasemanipulatie door middel van *SQL Injection*

4.12	27	Verouderde versie van database met bekende beveiligingsproblemen
4.13	27	Ondersteuning voor onveilige versleuteling als kiezer erom vraagt
5.1	32	Stemgeheim beperkt houdbaar
5.2	36	Geldige stemcodes genereerbaar tijdens stemperiode
5.3	37	Referentiebestand niet gesorteerd
5.4	37	"Umpire"-functie kan niet alle disputen oplossen; krijgt inzicht in de uitgebrachte stem
5.5	37	Drukker beschikt over geheime sleutels
5.6	37	Logging-dilemma: veiligheid versus stemgeheim
5.7	37	Onduidelijkheid documentatie
5.8	37	Digitale handtekening met publieke sleutel
5.9	38	Toevoeging geboortejaar (*AbelPI*) heeft geen functie

6.4 Slotwoord

Fox-IT hoopt met dit rapport een goed overzicht te hebben geboden van de in juni 2008 nog bestaande issues in de internetstemvoorziening, en een goede basis te leveren voor voortgaande verbetering van wat in opzet een elegant systeem voor internetstemmen is.

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, op dit moment 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/augustus 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.
65. **The OpenSSL Project.** www.OpenSSL.org. [Online]

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 waterschapsverkie-zingen 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 aanbevelin-gen 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		
Uitgangspunten (Principes)		
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.

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.	Voldoet niet 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.	Voldoet niet 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, ongeachte 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.
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.	Voldoet niet 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.	Voldoet Conceptueel Voldoet niet Afhankelijk van implementatie	Wanneer 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 bevinding 3.4.
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.

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.	Voldoet niet 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.

Procedurele voorzorgsmaatregelen		
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.

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.
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		
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.
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.

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.
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.	Voldoet niet 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.	Voldoet niet Conceptueel Voldoet niet 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.	Voldoet niet Conceptueel Voldoet niet Afhankelijk van implementatie Best effort	Zie opmerking bij aanbeveling 51.
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 demogelijkheid 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.
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		
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.
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.
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.
Beveiliging		
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.	Voldoet niet 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.	Voldoet niet 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 of geboortedatum. Bij stempakketten 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. Noot: de waterschappen hebben aangegeven dat hier een ongedocumenteerde procedure voor bestaat, zie ook bevinding 3.8.
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.
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.
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.	Voldoet niet 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.
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.
Controleerbaarheid (Audit)		
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.
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.
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.
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.
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	

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.

Appendix C Snelheidsmeting genereren stemcodes

EiPSI vermeldt in (10) de aanname dat een courante PC (een Pentium 4 met een kloksnelheid van 3 GHz) 2 miljoen DES-encrypties per seconde zou kunnen uitvoeren (pagina 44, voetnoot 7). Op basis van die aanname zou een dergelijke PC in 29 uur een geldige stemcode kunnen genereren.

Om deze bewering te verifiëren heeft Fox-IT programmacode geschreven waarmee kan worden getest of dergelijke snelheden inderdaad haalbaar zijn. Daarbij is gebruik gemaakt van de *open source* cryptografische programmabibliotheek "OpenSSL" (65).

We gebruiken de OpenSSL-functies `MDC2` en `DES_cbc_cksum` (die gelijk is aan een DESmac). De *message* die we gebruiken is `80011201` en de initialisatievector blijft 0. We berekenen dus: *MDC2*(*DESmac_Kp*(80011201)) 1 miljoen keer waarbij we *Kp* telkens met 1 ophogen. *Kp* is in deze context de gezochte enkelvoudige DES-sleutel.

Getest is met de volgende programmacode:

```
#include <stdio.h>
#include <string.h>
#include <stdlib.h>
#include <unistd.h>
#include <openssl/des.h>
#include <openssl/mdc2.h>

int main()
{
        int i = 0;
        int j = 0;
        DES_cblock key = { 0, 0, 0, 0, 0, 0, 0, 0 } ;
        const_DES_cblock static_iv = { 0, 0, 0, 0, 0, 0, 0, 0 } ;
        DES_cblock mac;
        DES_key_schedule schedule;
        MDC2_CTX mdc2_context;
        unsigned char hash[MDC2_DIGEST_LENGTH];
        char *message = "80011201";
        const size_t message_len = strlen(message);

        while (j < 1000000) {
                DES_set_key_unchecked(&key, &schedule);

                DES_cbc_cksum((unsigned char *) message, &mac, message_len,
                                        &schedule, &static_iv);

                MDC2_Init(&mdc2_context);
                MDC2_Update(&mdc2_context, mac, sizeof(mac));
                MDC2_Final(hash, &mdc2_context);

                /* Increase the DES key, but skip the LSB from each byte */
                for (i = 0; i < 8; ++i) {
                        key[i] += 2;
                        if (key[i] != 0) break;
                        if (i == 7) exit(0);
                }
                ++j;
        }

        return 0;
}
```

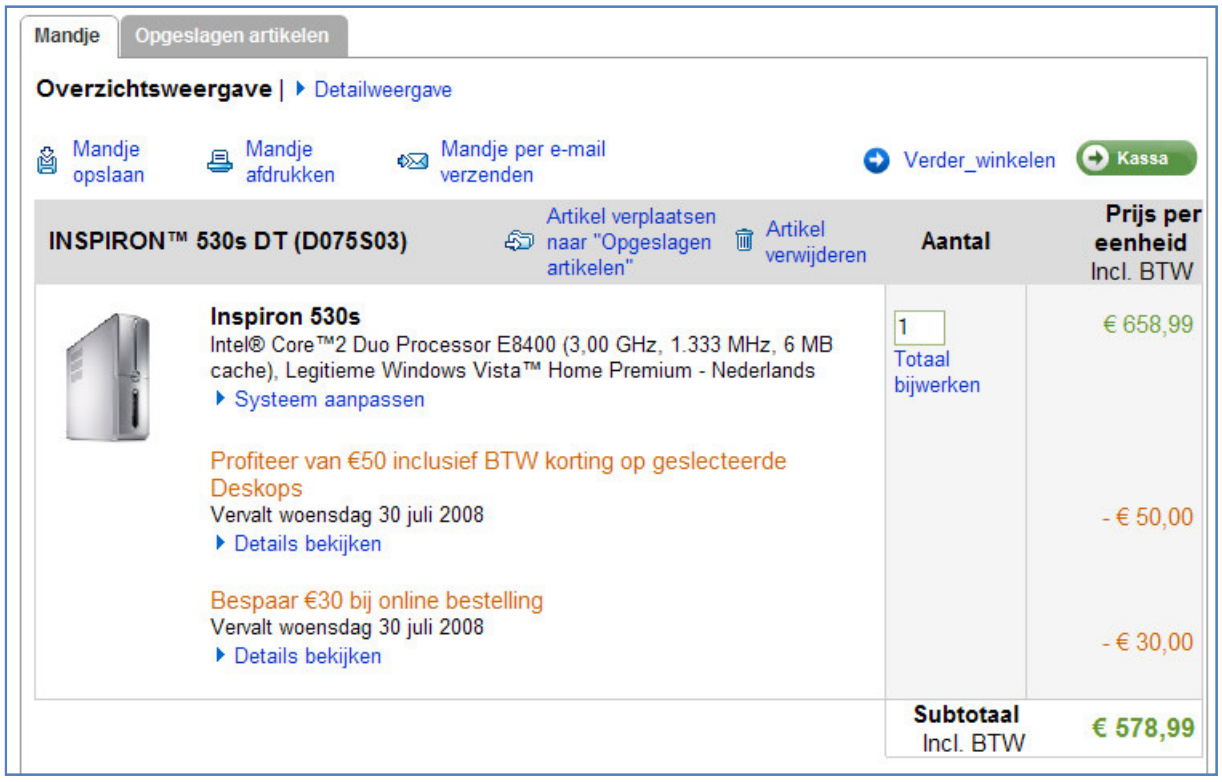
Ook is getest, door het programma in twee gelijktijdig uitvoerbare delen te splitsen, of dit proces op systemen met meerdere cores per CPU inderdaad sneller verliep. Dit bleek het geval, het aflopen van de zoekruimte is op te splitsen in meerdere onafhankelijke stukken waardoor een *dual core* precies dubbel zo snel kan zoeken en een *quad core* precies vier maal zo snel als een PC met enkelvoudige processor.

Bovenstaande code is getest op een aantal computersystemen, met de volgende resultaten:

Soort systeem	Processor	Clock speed	Bus speed	L2 Cache	Aantal cores	Programma klaar in	Geldige code binnen
Laptop	Intel T2500	2 GHz	667 MHz	2 MB	2	1,068 sec	21 uur
Laptop	Intel T7300	2 GHz	800 MHz	4 MB	2	0,941 sec	18 uur
Desktop PC	Intel E8400	3 GHz	1333 MHz	6 MB	2	0,644 sec	13 uur

Het gaat hier nadrukkelijk niet om bijzondere apparatuur. Het snelste systeem uit de tests van Fox-IT is op dit moment verkrijgbaar als kant-en-klare thuis-PC van (bijvoorbeeld) Dell voor een bedrag van € 579,- (zie afbeelding).

Op basis van deze metingen concludeert Fox-IT dat de aanname zoals vermeld door EiPSI zelfs nog aan de voorzichtige kant is. Om berekeningen te vereenvoudigen gaat dit rapport daarom uit van een gemiddelde zoektijd van 1 seconde voor 1 miljoen sleutels op een gemiddelde, gangbare thuis-PC.



Afbeelding van de website van een PC-leverancier genomen in juli 2008, een courante thuis-PC met de rekencapaciteit om binnen 13 uur geldige stemcodes te berekenen