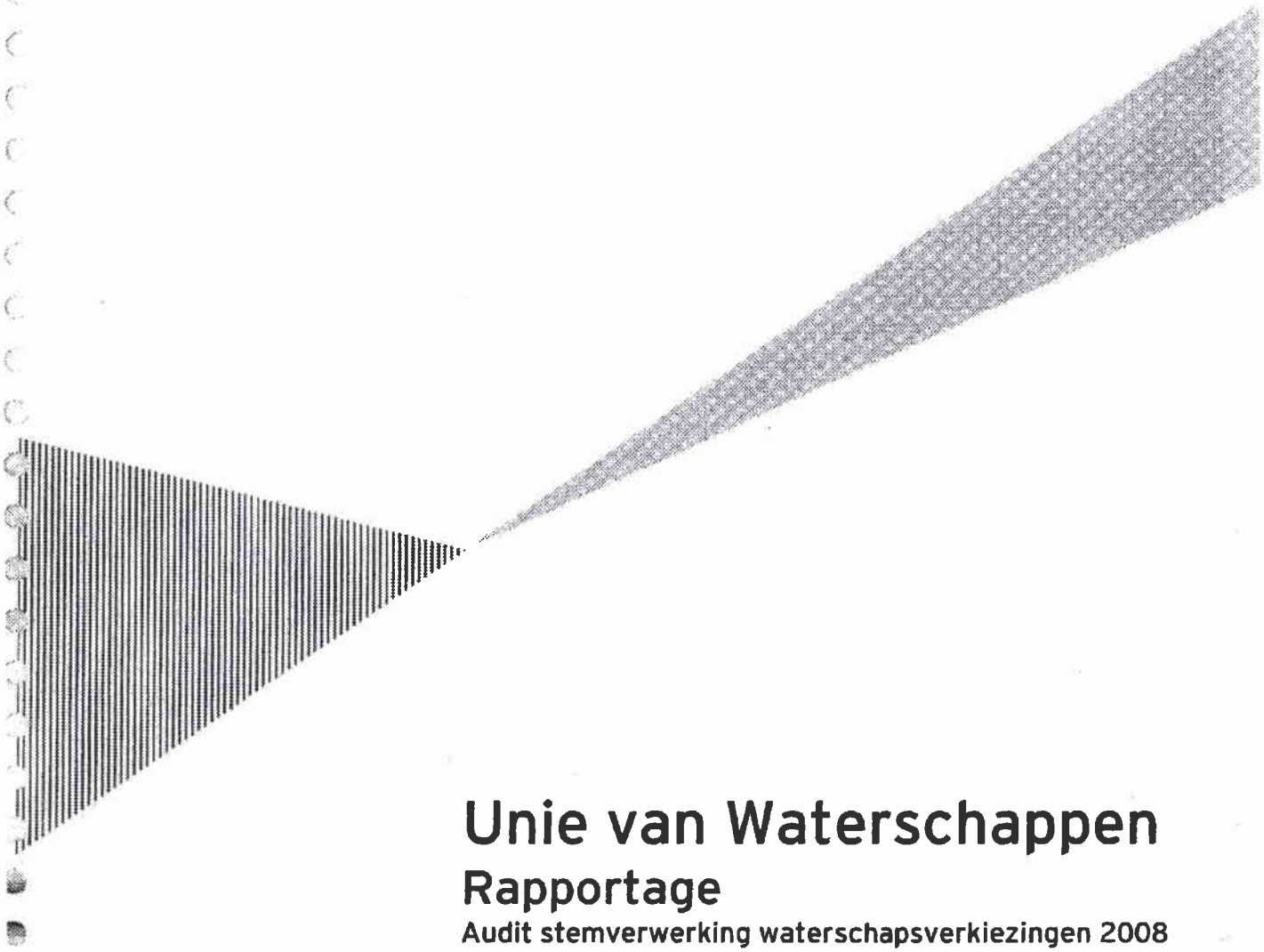
Bijlage 1



Unie van Waterschappen

Rapportage

Audit stemverwerking waterschapsverkiezingen 2008

ERNST & YOUNG

Quality In Everything We Do

ERNST & YOUNG

Inhoudsopgave

1	**Doelstelling en reikwijdte**	3
1.1	Doelstelling	3
1.2	Reikwijdte	3
2	**Aanpak**	3
3	**Beperking gebruik rapportage**	4
4	**Managementsamenvatting**	5
5	**Stemverwerkingsproces - opzet**	6
5.1	Briefstemmen	6
5.2	Technische werking	6
5.3	Helpdeskfunctie	8
6	**Uitgevoerde handelingen op 27 en 28 november 2008**	8
6.1	27 november	8
6.2	28 november	9
7	**Functioneren maatregelen waarborging stemgeheim**	9
7.1	Initialisatie RIPOCS	10
7.2	Aanmaken van printbestanden	10
7.3	Vernietigen printbestanden	10
7.4	Stemverwerking	10
8	**Risicoanalyse doorbreking stemgeheim**	10

Bijlagen

1	**Geraadpleegde documentatie**

Totaal aantal pagina's in dit rapport: 15

Ernst & Young Advisory
Eucldeslaan 1
3584 BL, UTRECHT
Postbus 3053
3502 GB, UTRECHT
Tel.: +31 (0)88 40 71 000
Fax: +31 (0)88 40 73 090
www.ey.nl

Unie van Waterschappen
T.a.v. de heer. E. Kraaij
Koningskade 40
2596 AA DEN HAAG

Utrecht, 19 januari 2010 jz/jb/60814319/sts10.692

Betreft: **Audit stemverwerking waterschapsverkiezingen 2008**

Geachte heer Kraaij,

Tijdens de waterschapsverkiezingen van 2008 zijn de computers die gebruikt worden voor het verwerken van de stemmen vastgelopen. Voor het verhelpen van dit incident is op 27 en 28 november 2008 de kluis waarin de RIPOCS servers stonden open geweest en is de RIPOCS applicatie op een server buiten de kluis geïnstalleerd ter verwerking van de vervangende stempakketten. De RIPOCS applicatie is onder andere verantwoordelijk voor het versleutelen van de stemgegevens. U heeft ons gevraagd een onderzoek uit te voeren naar de gang van zaken op 27 en 28 november 2008 met betrekking tot het stemgeheim.

Van 11 december 2009 tot 14 december 2009 hebben wij een screening uitgevoerd. Naar aanleiding van deze eerste screening hebben wij conform afspraak van maandag 14 december 2009 tot en met woensdag 13 januari 2010 een vervolgonderzoek uitgevoerd. In onderhavig rapport treft u onze bevindingen aan.

Dit rapport is op 1 januari 2010 in eerste concept en op 18 januari 2010 in tweede concept afgestemd met meest betrokkenen vanuit de Unie van Waterschappen en Het Waterschapshuis.

Vertrouwende erop u hiermee van dienst te zijn geweest, zijn wij uiteraard desgewenst graag bereid een nadere toelichting te geven.

Hoogachtend,
Ernst & Young Advisory

Drs. L.H.M. Verstegen RE
Senior Manager
IT Risk and Assurance

Ing. J.W.A.M. Otten RE
Partner
IT Risk and Assurance

Ernst & Young Advisory is een handelsnaam van Ernst & Young Accountants LLP. Dit is een limited liability partnership gevestigd in Engeland en Wales met registratienummer OC335594. In relatie tot Ernst & Young Advisory wordt de term partner gebruikt voor een (vertegenwoordiger van een) vennoot van Ernst & Young Accountants LLP. Ernst & Young Accountants LLP is statutair gevestigd te Lambeth Palace Road 1, London SE1 7EU, Verenigd Koninkrijk, heeft haar hoofdvestiging aan Boompjes 258, 3011 XZ Rotterdam, Nederland en is geregistreerd bij de Kamer van Koophandel Rotterdam onder nummer 24432944. Op onze werkzaamheden zijn algemene voorwaarden van toepassing, waarin een beperking van de aansprakelijkheid is opgenomen. Deze algemene voorwaarden zijn gedeponeerd bij de Kamer van Koophandel Rotterdam en zijn in te zien op www.ey.nl.

1 Doelstelling en reikwijdte

1.1 *Doelstelling*

In de wet- en regelgeving rondom de stemverwerking is opgenomen dat het geheime karakter van de stemming tijdens de verkiezingen voldoende gewaarborgd moet zijn. De doelstelling van ons onderzoek was vast te stellen of tijdens de stemverwerking van de waterschapsverkiezingen in 2008 als gevolg van de gang van zaken op 27 en 28 november 2008 het stemgeheim doorbroken heeft kunnen worden.

1.2 *Reikwijdte*

Wij hebben ons in het bijzonder gericht op de handelingen die zijn uitgevoerd op 27 en 28 november 2008. Wij merken op dat onze werkzaamheden niet zijn uitgevoerd overeenkomstig algemeen aanvaarde controle-, beoordelings- dan wel overige assurance-normen in Nederland, derhalve hebben wij geen assurance rapport opgesteld. Een algehele beoordeling van de gebruikte applicaties op juistheid en betrouwbaarheid maakte geen onderdeel uit van dit onderzoek. Het beoordelen van de betrouwbaarheid van de uitslag van de waterschapsverkiezingen in 2008 viel eveneens buiten de reikwijdte van dit onderzoek.

2 Aanpak

In het kader van onze werkzaamheden hebben wij de beschikbaar gestelde documentatie over de applicatie RIPOCS en de gang van zaken op 27 en 28 november 2008 beoordeeld. Wij verwijzen graag naar bijlage 1 voor een overzicht van de door ons geraadpleegde documentatie. Aanvullend daarop hebben wij gesproken met de volgende personen:

Naam	*Organisatie*	*Functie*
dhr. J. Gunter	Unie van Waterschappen	Projectleider waterschapsverkiezingen 2008
dhr. P.G. Maclaine Pont	MullPon	Via Het Waterschapshuis betrokken als Architect RIES
dhr. S. Bouwman	Het Waterschapshuis	Verantwoordelijk projectleider vanuit Het Waterschapshuis
dhr. M. Rijkschroeff	Hoogheemraadschap van Schieland en de Krimpenerwaard	Via Het Waterschapshuis betrokken als functioneel beheerder en projectleider RIES
dhr. J.L.M. van Bohemen	Collis	Op verzoek van Het Waterschapshuis aanwezig voor het schouwen van de initialisatie RIPOCS en bij het openen kluis op 27 en 28 november
dhr. H.J. van Dam	Collis	Accountmanager vanuit Collis voor Het Waterschapshuis

Op maandag 4 januari 2010 hebben wij op locatie bij Het Waterschapshuis gesproken met de heren Maclaine Pont, Bouwman en Rijkschroeff om meer inzicht te krijgen in de technische details van het stemverwerkingsproces en de gang van zaken rondom het openen van de kluis op 27 en 28 november 2008.

Op dinsdag 5 januari 2010 hebben wij kort telefonisch overleg gehad met de heer Gunter over de procedurele gang van zaken in het stemverwerkingsproces. Naar aanleiding van dit gesprek hebben wij op donderdag 7 januari 2010 op locatie bij de Unie van Waterschappen negen vernietigingsrapporten van PricewaterhouseCoopers ingezien.

Op donderdag 7 januari 2010 hebben wij eveneens een gesprek gehad met de heer Van Bohemen en de heer Van Dam op locatie bij Collis teneinde meer inzicht te krijgen in de rol van Collis en een review uit te voeren op eventueel beschikbare evidence. Naast het rapport van Collis 'Audit RIPOCS' [3] bleek bij Collis geen verdere verslaglegging voorhanden te zijn.

3 Beperking gebruik rapportage

Deze rapportage is alleen bestemd voor de Unie van Waterschappen en deze rapportage of onderdelen of samenvattingen daarvan mogen niet mondeling of schriftelijk aan derden beschikbaar worden gesteld zonder onze voorafgaande schriftelijke toestemming. Voorzover het de Unie van Waterschappen is toegestaan rapporten aan derden beschikbaar te stellen, zal het rapport origineel, volledig en ongewijzigd beschikbaar worden gesteld. Indien u dit product van onze werkzaamheden aan derden ter beschikking stelt, dient u hen erop te wijzen dat zij daar zonder onze uitdrukkelijke voorafgaande schriftelijke toestemming geen rechten aan kunnen ontlenen. Het verstrekken van deze toestemming kan omgeven zijn met nadere voorwaarden.

De Unie van Waterschappen mag onder de bovenstaande voorwaarden het rapport verstrekken aan de staatssecretaris van Verkeer en Waterstaat. Het Waterschapshuis, de Waterschappen en de vaste tweede kamer commissie voor Verkeer en Waterstaat. Gezien het aantal personen en instanties dat een kopie van het rapport ontvangt willen we hier nogmaals de vetrouwelijkheid van dit rapport benadrukken. Deze personen mogen dus niet zonder uitdrukkelijke schriftelijke voorafgaande toestemming het rapport verstrekken aan derden. Eventueel kan de Unie van Waterschappen overwegen te werken met genummerde exemplaren of andere maatregelen hiertoe treffen.

Bij de uitvoering van onze opdracht hebben wij gebruik gemaakt van informatie die is verstrekt door medewerkers van de Unie van Waterschappen en door betrokkenen onder verantwoordelijkheid van Het Waterschapshuis (zie hoofdstuk 2). Wij zijn afhankelijk van deze personen ten aanzien van de juistheid en volledigheid van de verstrekte informatie. Wij kunnen geen verantwoordelijkheid aanvaarden voor wijzigingen in de door ons gehanteerde feiten en omstandigheden na de datum waarop wij de desbetreffende werkzaamheden hebben afgerond.

4 Managementsamenvatting

De werkwijze van RIPOCS en de handelingen op 27 en 28 november 2008 zijn aan ons mondeling toegelicht door de betrokken personen vanuit de Unie van Waterschappen en Het Waterschapshuis. De toelichting wordt slechts gedeeltelijk ondersteund door documentatie, mede doordat, conform de geldende wet- en regelgeving, de gebruikte servers, stemmen en een gedeelte van de documentatie is vernietigd, drie maanden nadat over de toelating van de benoemden onherroepelijk is beslist. .

Op basis van de ons meegedeelde informatie omtrent de afhandeling van de incidenten op 27 en 28 november 2008 en gezien de wijze waarop het stemverwerkingsproces is ingericht zijn wij van mening, dat het risico beperkt is dat het stemgeheim is doorbroken op 27 en 28 november 2008. Voor het doorbreken van het stemgeheim op 27 en 28 november 2008 waren namelijk combinaties van gegevens en personen noodzakelijk. Zoals hierboven vermeld is niet alle documentatie en bewijslast meer aanwezig, aangezien deze conform de geldende wet- en regelgeving deels is vernietigd, en derhalve kan niet worden vastgesteld dat deze theoretische combinaties zich niet hebben voorgedaan. Het is derhalve op dit moment niet meer mogelijk om vast te stellen dat het stemgeheim niet doorbroken is geweest.

Naar aanleiding van de gebeurtenissen rondom de waterschapsverkiezingen in 2008 adviseren wij in de calamiteitenplannen voor de waterschapsverkiezingen niet alleen rekening te houden met de calamiteit zelf, maar ook met de vraag hoe achteraf vastgesteld kan worden dat juist gehandeld is. Wij geven in overweging een onafhankelijke toezichthouder zowel tijdens de calamiteit als achteraf vast te laten stellen dat de verkiezingen juist en vertrouwelijk zijn verlopen. Dit kan bijvoorbeeld worden gerealiseerd door direct na de verkiezingen een audit uit te laten voeren en gedurende de calamiteiten een audit met onderliggend dossier uit te voeren.

Op dit moment is op Europees en Nederlands niveau geen toetsingskader beschikbaar rondom de waarborging van het stemgeheim tijdens verkiezingen. Daarom is ervoor gekozen diverse partijen onderzoek te laten doen naar de gebruikte software, technische en procedurele maatregelen. Zo is de tijdens de verkiezingen gebruikte software is door Collis onderworpen aan een code-review met betrekking tot security. Om in de toekomst meer zekerheid te verkrijgen over de geïmplementeerde set van maatregelenraden wij aan de voor de verkiezingen de daadwerkelijk geïmplementeerde software te laten certificeren.

In hierna volgende hoofdstukken is in meer detail uitgeschreven wat de opzet van het stemproces is (5), welke handelingen hebben plaatsgevonden op 27 en 28 november 2008 (6), hoe de maatregelen rondom het waarborgen van het stemgeheim gefunctioneerd hebben en de analyse van de risico's rondom het doorbreken van het stemgeheim (8).

5 Stemverwerkingsproces - opzet

In dit hoofdstuk geven wij informatie over de inrichting van het stemverwerkingsproces tijdens de waterschapsverkiezingen in 2008. Wij betrachten hierbij geen volledigheid, maar hebben dit hoofdstuk opgenomen ter onderbouwing van onze risico inschatting in de management samenvatting. Onderstaande beschrijving is gebaseerd op de ontvangen documentatie en informatie uit interviews.

5.1 *Briefstemmen*

Van 13 tot 25 november 2008 kozen de ingezetenen van de waterschappen in Nederland de leden van de categorie ingezetenen van het algemeen bestuur van deze waterschappen. Deze verkiezingen hebben plaatsgevonden door middel van de voorziening 'briefstemmen'. Hiertoe zijn stempakketten samengesteld die, op basis van gegevens uit de gemeentelijke basisadministratie, naar kiesgerechtigden zijn verzonden. Het stempakket bevatte een stembiljet waarmee de kiezer een stem kon uitbrengen. Om te voorkomen dat een kiezer twee keer kon stemmen, was elk stembiljet voorzien van een unieke code die was gekoppeld aan het geboortejaar van de betreffende kiezer. Op basis van deze code en het door de kiezer op het biljet in te vullen geboortejaar kon de geldigheid van het stembiljet worden vastgesteld.

Uitgebrachte stemmen zijn door het bedrijf 'Service Point' te Alphen aan den Rijn ingescand en omgezet naar 'technische stemmen' die vervolgens door Het Waterschapshuis konden worden gevalideerd en geteld waarna de uitslagen konden worden meegedeeld aan de waterschappen.

Tijdens de waterschapsverkiezingen in 2008 had elk van de 26 waterschappen een helpdesk ingericht. Deze helpdesks konden vervangende stempakketten uitreiken en activeren en daarnaast stembiljetten als 'te blokkeren' aanmerken (bijvoorbeeld omdat een vervangend stempakket werd verzonden). Het Waterschapshuis heeft voorafgaand aan de telling de te activeren stembiljetten geactiveerd en de te blokkeren stembiljetten geblokkeerd.

Teneinde het stemgeheim te waarborgen, is het van het grootste belang dat na het uitbrengen van de stem de unieke code op het stembiljet niet gekoppeld kon worden aan de NAW-gegevens van de betreffende kiezer.

5.2 *Technische werking*

RIES (*Rijnland Internet Election System*) is een reeks systemen voor elektronische verkiezingen via het internet. RIES is gebruikt voor het verwerken van de 'briefstemmen' in de waterschapsverkiezingen van 2008. Drie RIES-onderdelen zijn van belang bij de stemverwerking: RIPOCS (zie paragraaf 5.2.1), Portal (zie paragraaf 5.2.2) en de helpdeskfunctie (zie paragraaf 5.3).

5.2.1 RIPOCS

RIPOCS (*RIES Isolated Portal Crypto System*) is verantwoordelijk voor de cryptografische berekeningen, waaronder:

- het genereren van de unieke stemcodes zoals deze op de stembiljetten zijn gedrukt;
- het aanmaken van een versleuteld bestand (C10) voor de drukker waarin de unieke codes gekoppeld zijn aan kiezersgegevens (zoals naam, adres, woonplaats);
- het 'deblokkeren' van uitgereikte 'vervangende stempakketen' en het blokkeren van verstuurde stempakketten waarvoor vervangende stempakketten is uitgereikt of die om andere reden in de helpdesk applicatie als 'te blokkeren 'zijn aangemerkt.

Met betrekking tot RIPOCS is in dit onderzoek het volgende van belang:

- de RIPOCS-systemen zijn opgeborgen in een verzegelde kluis, waarmee de servers fysiek beveiligd zijn voor toegang door onbevoegden;
- RIPOCS communiceert uitsluitend met Portal: Portal kan bestanden klaarzetten in een input directory, RIPOCS haalt deze bestanden batchgewijs op, voert bewerkingen uit en plaats resultaten in een output directory die alleen door Portal kan worden benaderd;
- RIPOCS genereert in de PREPARE-fase een referentiebestand waarin een 'hash' is opgenomen van de pseudo-identiteit van de kiezer (gebaseerd op ondermeer de 'verkiezings-id' (uniek per verklezing) en het kiezersnummer) en een 'hash' van iedere potentiële stem per kiezer (onder andere gebaseerd op het geboortejaar van de kiezer);
- RIPOCS berekent in de 'PREPARE-fase' voor elke kiezer de code voor de stemkaart die samen met de NAW gegevens in bestand (C10) wordt vastgelegd;
- dit C10 bestand wordt direct tijdens het genereren binnen RIPOCS versleuteld met de public key van de drukker (RSA, sleutellengte 2048 bits, gecertificeerd door DigiNotar) en wordt na compleet te zijn door RIPOCS in de output directory weggeschreven (dus in vercijferde vorm);
- genereren van het C10 bestand voor een verkiezing is alleen mogelijk tijdens PREPARE-fase voor die verkiezing. Deze beperking is zo geprogrammeerd in RIPOCS. Terugkeren naar eerdere status is in RIPOCS niet mogelijk. Daarnaast zijn de voor deze berekening op RIPOCS benodigde kiezersgegevens (K10 bestanden) direct na de Prepare berekening van RIPOCS gewist. Op RIPOCS blijven per verkiezing alleen een aantal algemene parameters en de Referentiebestanden aanwezig.

5.2.2 Portal

Portal is een netwerkapplicatie die communicatie met RIPOCS mogelijk maakt door bestanden weg te schrijven in een 'input-directory' (waaruit RIPOCS deze batchgewijs ophaalt) en door bestanden in te lezen uit de 'output-directory' (waarin RIPOCS bestanden wegschrijft). Portal is ondermeer door stembureaus via een beveiligde VPN verbinding over internet te benaderen. In Portal is de volgende informatie beschikbaar, welke relevant is voor dit onderzoek:

- versleutelde printbestanden (C10) voor de drukker (zie 7.2);
- kiezerslijsten (K10): dit betreft de lijsten waarop het kiezersnummer staat in combinatie met de NAW gegevens. Deze lijsten zijn gebruikt voor het blokkeren van de uitgereikte stempakketten;
- lijst met vervangende stempakketten (K11): Een overzicht van de mogelijk uit te reiken vervangende stempakketten per Waterschap.

5.3 *Helpdeskfunctie*

Indien een kiezer een vervangend stempakket aanvraagt, wordt op basis van een controle op de NAW gegevens in de helpdeskfile het originele stempakket gemarkeerd als 'blocked' en het toegestuurde vervangende stempakket gemarkeerd als 'active'. Het zoeken naar de NAW gegevens in de helpdeskfile verliep gedurende de verkiezingen in eerste instantie extreem traag. Wij merken op dat naar aanleiding hiervan is de zoekfunctionaliteit van de helpdesk aangepast. Deze wijziging heeft geen invloed op de maatregelen rondom het waarborgen van het stemgeheim gehad.

Elke helpdesk levert na de verkiezingen twee files aan de RIPOCS applicatie: 'blocked.txt' en 'activate.txt' (de zogenaamde helpdesk mutaties). Deze files bevatten respectievelijk de kiezersnummers van de kiezers waarvoor het stembiljet moet worden geblokkeerd en de 'pseudo-kiezersnummers' van de vervangende pakketten die moeten worden geactiveerd. Dit 'activeren' en 'deactiveren' vindt plaats op RIPOCS door middel van het wijzigen van 'statusbit' in het referentiebestand.

Bij het tellen van de stemmen worden vervolgens alleen de geactiveerde stemmen meegenomen.

6 Uitgevoerde handelingen op 27 en 28 november 2008

In dit hoofdstuk geven wij informatie over uitgevoerde handelingen op 27 en 28 november 2008 in relatie tot het stemgeheim. Wij betrachten hierbij geen volledigheid, maar hebben dit hoofdstuk opgenomen ter onderbouwing van onze risico inschatting in de management samenvatting. Onderstaande beschrijving is gebaseerd op de ontvangen documentatie en informatie uit interviews.

Voor de volledigheid merken wij op dat het van Collis ontvangen rapport 'Audit RIPOCS' [3] daar helaas ook geen uitkomst voor biedt. Dit rapport is een verslag van de activiteiten van Collis op 27 en 28 november 2008, zonder onderliggend dossier.

6.1 *27 november*

Op 27 november liep de verwerking van de vervangende stempakketten vast. Het bleek hierbij te gaan om een storing in de RIPOCS machines. Ten behoeve van werkzaamheden diende de RIPOCS kluis open gemaakt te worden. Op dat moment is de kluis geopend onder toezicht van Securitas en Collis. Securitas heeft vastgesteld dat de verzegeling van de kluis in tact was op het moment van openen van de kluis. Onder toezicht van Collis zijn vervolgens de volgende acties uitgevoerd op de RIPOCS machines:

- analyse uptime en geheugen gebruik RIPOCS server;
- herstart van de RIPOCS servers na het herconfigureren van het geheugen van de servers;
- analyse logfiles.

De herstart van de RIPOCS servers was niet succesvol. De verwerking van de helpdesk mutaties was nog steeds niet mogelijk. Vervolgens is onder toezicht van Securitas en Collis de kluis gesloten en opnieuw verzegeld.

6.2 *28 november*

Op vrijdagochtend 28 november is besloten om onder toezicht van Securitas de verwerking van de helpdesk mutaties te laten plaatsvinden op een server buiten de kluis. Deze zogenaamde 'externe ontwikkelmachine' was een niet-ingerichte machine die speciaal voor het geval van calamiteiten voorafgaand aan de verkiezingen apart gezet is. Het betreft een server die door SURFnet op 28 november 2008 is voorzien van de basisinrichting gelijk aan de servers die reeds eerder ingericht waren en in de kluis stonden.

Vervolgens is de RIPOCS applicatie geïnstalleerd op deze server en heeft Collis vastgesteld dat het hierbij om identieke software ging, dus de software op de extra machine was gelijk aan de software op de machines in de kluis.

Teneinde deze server te kunnen gebruiken, is een aparte kluis (in een over-kluis) geopend waarin een vervangende geïnitialiseerde IBM 4764 PCI-X cryptocard gereed lag. Een bijhorende USB-stick met vercijferde crypto sleutels was opgeslagen in een andere kluis (in de over-kluis), ook deze kluis is geopend. Met behulp van de geïnitialiseerde IBM 4764 PCI-X cryptocard en de bijbehorende USB-stick en het bijbehorende wachtwoord van Het Waterschapshuis is vervolgens de RIPOCS applicatie opnieuw gestart.

De nieuw ingerichte RIPOCS machine is vervolgens door de systeembeheerder van SURFnet via een parameter in het status.xml bestand per verkiezing in de fase 'Tally'gebracht, zodat het mogelijk werd helpdeskmutaties te verwerken. Omdat het systeem geen koppeling had met Portal werden het voor iedere verkiezing benodigde referentiebestand en de benodigde helpdesk mutatie bestanden per USB-harddisk overgebracht naar het nieuw in gebruik genomen systeem. De resultaten zijn ook op deze wijze weer overgebracht naar Portal.

Vervolgens is de kluis onder toezicht van Collis en Securitas geopend om de 3 RIPOCS servers in de kluis in een status te brengen zodat de verwerking verder kon gaan met de offline verwerkte helpdeksmutaties.

Vervolgens konden de K30 bestanden via de Portal verwerkt worden en startte Het Waterschapshuis de tellingen van de stembussen per waterschap.

7 Functioneren maatregelen waarborging stemgeheim

In dit hoofdstuk geven wij informatie over de wijze waarop de maatregelen die betrekking hebben op het stemgeheim tijdens de waterschapsverkiezingen in 2008 hebben gefunctioneerd. Wij betrachten hierbij geen volledigheid, maar hebben dit hoofdstuk opgenomen ter onderbouwing van onze risico inschatting in de management samenvatting. Navolgende beschrijving is gebaseerd op de ontvangen documentatie en informatie uit interviews.

7.1 *Initialisatie RIPOCS*

Op verzoek van Het Waterschapshuis heeft Collis voorafgaand aan de verkiezingen twee code-reviews op RIPOCS uitgevoerd (zie [6] en [7]). Tevens heeft Collis tijdens de initialisatie van de drie RIPOCS systemen erop toegezien dat de geïnstalleerde versie in productie gelijk is aan de versie die aan Collis is overhandigd voor een code review (zie [5] en [8]).

Een notaris heeft toezicht gehouden op het initialiseren van de IBM 4764 PCI-X cryptocard en het verzegelen van de kluis waarin RIPOCS is opgeborgen. Hiervan is door de notaris proces-verbaal opgemaakt (zie [5]).

7.2 *Aanmaken van printbestanden*

Zowel de sleutel waarmee de unieke stemcode werd gegenereerd als de publieke sleutel van de drukker die gebruikt werd voor het versleutelen van het C10 bestand beide werden opgeslagen in de IBM 4764 PCI-X cryptocard. Deze kaart is zo ontworpen dat uitsluitend tijdens de initialisatiefase sleutels kunnen worden ingeladen en kopieën van de kaart kunnen worden gemaakt. De kopieën van de kaart werden in een aparte kluis opgeslagen. Tijdens de initialisatiefase van de IBM 4764 PCI-X cryptocard zijn drie kopieën gemaakt van de kaart. Verder is de IBM 4764 PCI-X cryptocard (die beschikt over een nauwkeurige interne klok) zo was ingesteld dat slechts in een beperkt tijdsvenster van de kaart gebruik gemaakt kon worden.

7.3 *Vernietigen printbestanden*

PricewaterhouseCoopers heeft negen rapporten uitgebracht die een feitenrelaas bevatten van de verwijdering van de printbestanden, backups, de 'private key' van de drukker en enkele 'restfiles'. In één van deze rapporten staat ondermeer beschreven hoe de printbestanden (en 'restfiles') op 11 november zijn verwijderd van twee Portal systemen; één in Utrecht (ries-utr-portal-1) en één in Nijmegen (ries-nij-portal-1).

7.4 *Stemverwerking*

De stemmen zijn volgens protocol verwerkt tot het moment dat een incident optrad op de RIPOCS machines. Dit incident en de wijze waarop hier is gereageerd is beschreven in hoofdstuk 6. Vervolgens is de verdere verwerking van de stemmen uitgevoerd conform het protocol.

8 Risicoanalyse doorbreking stemgeheim

Naar aanleiding van de aan ons mondeling verstrekte informatie over de stemverwerkingsprocessen, de werking van de software en de gebeurtenissen op 27 en 28 november 2008 hebben wij een risicoanalyse uitgevoerd op de mogelijkheden ter doorbreking van het stemgeheim op 27 en 28 november 2008. Voor het doorbreken van het stemgeheim op 27 en 28 november 2008 zijn combinaties van gegevens en personen noodzakelijk. Hierna beschrijven wij enkele van die theoretische combinaties en lichten wij toe waarom wij het risico daartoe beperkt inschatten. De mondelinge toelichtingen en de verstrekte verslagen worden slechts gedeeltelijk ondersteund door documentatie, mede omdat conform de geldende wet- en regelgeving een deel van de documentatie is vernietigd. Hierdoor is het niet mogelijk om onderstaande onomstotelijk vast te stellen.

Combinatie 1

- Onversleuteld C10 bestand (bestand voor drukker, bevat unieke code en NAW-gegevens van kiezers).
- Ontvangen stemmen bestand (door RIPOCS tot "algemeen RIES formaat" ontcijferde informatie voor iedere verkiezing op basis van de bestanden met uitgebrachte stemmen, aangemaakt door responsverwerker).
- Het (gepubliceerde) Referentiebestand voor de betreffende verkiezing.

Samenvatting
Het C10 bestand kan alleen ontsleuteld worden door de 'private key' van de drukker. De voor de verkiezing gegenereerde bestanden bij de drukker zijn vernietigd zoals beschreven in de rapporten van PricewaterhouseCoopers. Samenspanning met de drukker is noodzakelijk om een onversleuteld C10 bestand te verkrijgen. Ons onderzoek was hierop niet gericht.

Combinatie 2a

- Ontvangen stemmen bestand (door RIPOCS tot "algemeen RIES formaat" ontcijferde informatie voor iedere verkiezing op basis van de bestanden met uitgebrachte stemmen, aangemaakt door responsverwerker).
- K10 bestand waarin zowel het kiezersnummer als de NAW-gegevens van kiezers zijn vermeld (beschikbaar voor de 26 helpdesks van de stembureaus ten behoeve van het verstrekken van vervangende stembiljetten).
- Geïnitialiseerde IBM 4764 PCI-X cryptocard en bijhorende USB-stick met sleutelbestand en bijhorend wachtwoord (in bezit bij een medewerker van Het Waterschapshuis).
- Het (gepubliceerde) referentiebestand voor de betreffende verkiezing.
- Bij uitvoering op één van de RIPOCS machines in de kluis: samenwerking met de drukker om toegang tot het in RIPOCS opnieuw gegenereerde C10 bestand te krijgen.
- Dit alles binnen de door de IBM 4764 PCI-X cryptocard toegestane tijdsvenster.

Samenvatting
De sleutel die wordt gebruikt voor het genereren van het C10 bestand is door DigiNotar gecertificeerd en tijdens de initialisatiefase op de IBM 4764 PCI-X cryptocard geladen. Na de initialisatiefase kan de eenmaal ingeladen sleutel niet worden aangepast.Ter ontsleuteling van het printbestand is dus ook samenspanning met de drukker noodzakelijk. Ons onderzoek was hierop niet gericht.

Combinatie 2b

- Ontvangen stemmen bestand (door RIPOCS tot "algemeen RIES formaat" ontcijferde informatie voor iedere verkiezing op basis van de bestanden met uitgebrachte stemmen, aangemaakt door responsverwerker).
- K10 bestand waarin zowel het kiezersnummer als de NAW-gegevens van kiezers zijn vermeld (beschikbaar voor de 26 helpdesks van de stembureaus ten behoeve van het verstrekken van vervangende stembiljetten).
- Geïnitialiseerde IBM 4764 PCI-X cryptocard en bijhorende USB-stick met sleutelbestand en bijhorend wachtwoord (in bezit bij een medewerker van Het Waterschapshuis).
- Het (gepubliceerde) Referentiebestand voor de betreffende verkiezing.
- Uitvoering op de RIPOCS server waar de programmatuur is aangepast.
- Dit alles binnen de door de IBM 4764 PCI-X cryptocard toegestane tijdsvenster.

Samenvatting
Voor toegang tot de cryptokaart was een samenwerking tussen Securitas en Het Waterschapshuis nodig. Collis verklaard vastgesteld te hebben dat de op de externe server geïnstalleerde applicatie identiek is aan de applicatie die op de oorspronkelijke servers is geïnstalleerd. Op basis van de beschikbare documentatie hebben wij dit niet kunnen vaststellen. Bovenstaande combinatie kan zich alleen voordoen bij een samenspanning tussen Het Waterschapshuis (voor toegang tot de cryptokaart en de USB-stick), Securitas (voor toegang tot de kluis) en een persoon met kennis van RIPOCS.

Combinatie 2c

- Ontvangen stemmen bestand (door RIPOCS tot "algemeen RIES formaat" ontcijferde informatie voor iedere verkiezing op basis van de bestanden met uitgebrachte stemmen, aangemaakt door responsverwerker).
- K10 bestand waarin zowel het kiezersnummer als de NAW-gegevens van kiezers zijn vermeld (beschikbaar voor de 26 helpdesks van de stembureaus ten behoeve van het verstrekken van vervangende stembiljetten).
- Geïnitialiseerde IBM 4764 PCI-X cryptocard en bijhorende USB-stick met sleutelbestand en bijhorend wachtwoord (in bezit bij een medewerker van Het Waterschapshuis).
- Het (gepubliceerde) Referentiebestand voor de betreffende verkiezing.
- Bij uitvoering op een andere 'aanvals' server: eigen programmatuur om de nodige berekeningen en bewerkingen uit te voeren.
- Dit alles binnen de door de IBM 4764 PCI-X cryptocard toegestane tijdsvenster.

Samenvatting
Voor toegang tot de cryptokaart was een samenwerking tussen Securitas en Het Waterschapshuis nodig. Bij deze mogelijkheid moet op een aparte server met aangepaste RIPOCS programmatuur gewerkt worden. Hiervoor is samenspanning noodzakelijk met SURFnet voor de infrastructuur en met Het Waterschapshuis, voor toegang tot de cryptokaart en de USB-stick.

Bijlage 1 Geraadpleegde documentatie

Ref.	Titel	Auteur(s)	Versie	Datum
1	Functioneel ontwerp RIES-2008	Piet Maclaine Pont, Arnout Hannink, Jacques Hoeijenbos, Marco Rijkschroeff, Jacques Schuurman	0.9	23 juni 2008
2	Verslag van werkzaamheden	Simon Bouwman	definitief	29 november 2008
3	Audit RIPOCS	Hans van Bohemen	1.0	1 december 2008
4	Bijzonderhedenrapportages	R. Oosterwijk, F. Paardenkooper, E. Colle	-	27 en 28 november 2008
5	Afschriften proces-verbaal initialisatie RIPOCS	Harriet van Zenderen (Notaris)	-	10 oktober 2008
6	Review integriteit RIPOCS broncode	Collis	-	30 juni 2008
7	Tweede review integriteit RIPOCS broncode (v1.1)	Collis	1.0	22 augustus 2008
8	Status en initialisatie RIPOCS release 1.3	Hans van Bohemen, Klaas Mateboer	1.2	25 september 2008
9	Description and Analysis of the RIES Internet Voting System	Engelbert Hubbers, Bart Jacobs, Berry Schoenmakers, Henk van Tilborg, Benne de Weger	1.0	24 juni 2008
10	HW-CRYPTO, Cryptographic architecture for RIES-2008 and IBM 4764 PCI-X cryptocard	Piet Maclaine Pont	1.0	22 augustus 2008
11	Samen naar Beter, evaluatie landelijke waterschapsverkiezingen 20098	BMC onderzoek	-	april 2009
12	Protocol waterschapsverkiezingen 2008 (art. 2.45, vierde lid Waterschapsbesluit)	Zulayka Belliot (Collis), Simon Bouwman (Het Waterschapshuis), Marianne van der Veen (Het Waterschapshuis), Jord Schreurs (Het Waterschapshuis)	-	7 oktober 2008
13	Beknopte beschrijving voorziening briefstemmen waterschapsverkiezingen 2008	Unie van Waterschappen, Het Waterschapshuis	1	9 oktober 2008
14	Brief 08.1348/TdB/BW/NK	Drs. A de Bos RE RA (Managing Director DigiNotar)	-	29 oktober 2008

Ref.	Titel	Auteur(s)	Versie	Datum
15	Analyse uitslag berekening van de Portal	Hans van Bohemen (Collis)	1.0	9 oktober 2008
16	Advisering toelaatbaarheid internetstemvoorziening waterschappen	Bartek Gedrojc, Matthieu Hueck, Hans Hoogstraten, Mark Koek, Sjoerd Resink (allen Fox-IT)	3.0	12 augustus 2008
17	RIES 2008: WV-STUF, Standaard Uitwisseling Formaat	Piet Maclaine Pont (MullPon vof), Suze Maclaine Pont (MS Insulinde), Arnout Hannink (Magic Choice b.v.)	0.98	-
18	Sourcecode RIPOCS	Magic Choice b.v.	1.0	24 juni 2008
19	Evaluatie voorziening internetstemmen RIES Aanbevelingen van de Raad van Europa	-	-	6 juni 2008
20	Feitenrelaas van clearing van versleutelde C10 bestanden Bezoek op 11 november 2008 bij SURFnet, Utrecht	PricewaterhouseCoopers	-	6 januari 2010
21	Visit RRD Moore, Cosne-sur-Loire Dealing with confidential files	PricewaterhouseCoopers	-	30 oktober 2008
22	Visit RRD Moore, Cosne-sur-Loire Destroying confidential files 16 oktober 2008	PricewaterhouseCoopers	-	30 oktober 2008
23	Visit RRD Moore, Cosne-sur-Loire Destroying confidential files 22 oktober 2008	PricewaterhouseCoopers	-	4 november 2008
24	Visit RRD Moore, Cosne-sur-Loire Destroying confidential files 30 oktober 2008	PricewaterhouseCoopers	-	4 november 2008
25	Visit RRD Moore, Cosne-sur-Loire Destroying confidential files 7 november 2008	PricewaterhouseCoopers	-	29 december 2008
26	Visit RRD Moore, Cosne-sur-Loire Destroying back-up tape 30 oktober 2008	PricewaterhouseCoopers	-	13 november 2008

Ref.	Titel	Auteur(s)	Versie	Datum
27	Visit RRD Moore, Cosne-sur-Loire Destroying back-up tape 7 november 2008	PricewaterhouseCoopers	-	29 december 2008
28	Visit RRD Moore, Cosne-sur-Loire Destroying CD private key 6 september 2008	PricewaterhouseCoopers	-	25 november 2008
29	Calamiteitenplannen: – calamiteitenbestrijdingsplan Villa DM – calamiteitenbestrijdingsplan Het Waterschapshuis – calamiteitenbestrijdingsplan Callcenter – calamiteitenbestrijdingsplan MIDEX – calamiteitenbestrijdingsplan Kieskompas – calamiteitenbestrijdingsplan TNT Post – calamiteitenbestrijdingsplan Service Point – calamiteitenbestrijdingsplannen RR Donnelley	-	-	-
30	Calamiteitenplan Waterschapsverkiezingen 2008	-		22 oktober 2008
31	Draaiboek initalisatie	Het Waterschapshuis	-	11 september 2008