Deloitte.

Ministerie van Binnenlandse Zaken *en* Koninkrijksrelaties

Eindrapport

Quick scan

Methodiek teststemmen

Bij Kiezen op afstand

Uitgebracht aan:

Directeur Constitutionele Zaken en Wetgeving
van het Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

Intern kenmerk BZK: 2006-326609

28 september 2006

Van: Auditdienst BZK
Deloitte Enterprise Risk Services

28 september 2006

Inhoudsopgave

1 Inleiding

Op 22 november 2006 vinden de Tweede Kamerverkiezingen plaats. Tijdens deze verkiezingen wordt een experiment gehouden met stemmen via internet voor Nederlandse kiezers die in het buitenland wonen of werken. Doel van stemmen via internet is het vergroten van het stemgemak voor de kiezers. Het stemmen per brief blijft ook mogelijk. De kiezers in het buitenland moeten van tevoren aangeven hoe zij willen stemmen: via internet of per brief.

In dit kader is het project Kiezen Op Afstand (KOA) opgezet. Het stemmen via internet vindt plaats onder verantwoordelijkheid van het Ministerie van BZK. Politiek verantwoordelijk is de Minister voor BVK.

Voor de uitvoering van stemmen via internet wordt gebruik gemaakt van de dienstverlening van 'Het Waterschapshuis'. 'Het Waterschapshuis' is een stichting met als doel het bevorderen van samenwerking op het gebied van ICT tussen de waterschappen. Voor de waterschapsverkiezingen van 2004 en 2005 heeft 'Het Waterschapshuis' in samenwerking met een aantal externe partijen RIES ontwikkeld en ten behoeve van de Tweede Kamerverkiezingen is RIES aangepast in RIES-KOA.

Ten behoeve van het kunnen garanderen van een adequate dienstverlening stelt 'Het Waterschapshuis' als eis dat zij tijdens de verkiezingen in het operationele systeem gebruik kan maken van zogenaamde 'teststemmen'. Dit houdt in dat een set van teststemcodes – maximaal 75 stuks – wordt aangemaakt, waarvan een deel wordt gebruikt om de performance en beschikbaarheid te bewaken en een deel mogelijkerwijze (maar met een redelijke waarschijnlijkheid) handmatig kan worden ingezet bij een eventuele calamiteit.

Vanuit haar verantwoordelijkheid voor het integere verloop van de verkiezingen stuit deze handelswijze voor het ministerie van BZK op bezwaren. Naast het risico van frauduleus gebruik van de testmethodiek voor het manipuleren van de verkiezingsuitkomsten, bestaat volgens haar ook het risico dat in de publieke opinie deze handelswijze als onbetrouwbaar wordt aangemerkt. Tegen deze achtergrond is een quick scan op de methodiek testenstemmen gevraagd aan de Auditdienst van het ministerie van BZK in combinatie met een onafhankelijke externe partij, Deloitte.

2 Managementsamenvatting

Door 'Het Waterschapshuis' is een testmethodiek rondom het stemmen via internet voorgesteld waarbij gebruik wordt gemaakt van teststemmen in de operationele omgeving gedurende de verkiezingen. In opdracht van de Directie Constitutionele Zaken en Wetgeving is aan de Auditdienst in combinatie met Deloitte gevraagd om te onderzoeken of deze werkwijze niet op een gespannen voet staat met de kwaliteitswaarborgen[1] die gedefinieerd zijn voor het experiment Kiezen Op Afstand. Naar aanleiding hiervan hebben de Auditdienst en Deloitte een quick scan uitgevoerd met de volgende vraagstelling: "*Zijn in opzet de risico's voor de kwaliteit van de uitvoering van het stemproces via internet die ontstaan als gevolg van het gebruik van de voorgestelde testmethodiek, in voldoende mate afgedekt door beheersingsmaatregelen?*".

Het onderzoek heeft zich expliciet gericht op die onderdelen van het stemproces via internet die rechtstreeks gerelateerd zijn aan de voorgestelde testmethodiek met teststemmen. Onze beschrijvingen en conclusies hebben betrekking op de stand van zaken per 28 september 2006.

De uitkomst van de quick scan is dat de in opzet getroffen technische beheersingsmaatregelen een goede basis leggen voor de beheersing van de additionele risico's die ontstaan als gevolg van het gebruik van de voorgestelde testmethodiek. De bijbehorende procedurele maatregelen, zoals vastgelegd in de administratieve organisatie (AO), zijn in opzet nog in onvoldoende mate uitgewerkt, vastgelegd en geformaliseerd. Ons totaaloordeel is op dit moment dan ook dat in opzet de additionele risico's voor de kwaliteit van de uitvoering van het stemproces via internet die ontstaan als gevolg van het gebruik van de voorgestelde testmethodiek in onvoldoende mate zijn afgedekt door beheersingsmaatregelen.

Onze belangrijkste aanbeveling is de procedures rondom de voorgestelde testmethodiek en de werkinstructies verder uit te werken en hierbij expliciet te beschrijven op welke wijze de technische controlemogelijkheden in samenhang gebruikt moeten worden en hoe de uitkomsten van controles vastgelegd moeten worden. Daarbij hebben de procedures voor de voorbereiding van de stemming, zoals het aanmaken en bewaren van de cryptosleutels, ons inziens hoge prioriteit, aangezien deze:

- op zeer korte termijn moeten worden uitgevoerd;
- essentieel zijn voor het waarborgen van de kwaliteit van het gehele stemproces.

Deze aanbeveling sluit aan op de werkzaamheden die op dit moment binnen het project plaatsvinden voor het uitwerken en vaststellen van de administratieve organisatie. Wij hebben concrete aanbevelingen voor procedures opgenomen in hoofdstuk 5 van dit rapport.

---

[1] Voor de invulling van de kwaliteitscriteria wordt verwezen naar hoofdstuk 3.

3 Kwaliteitscriteria en algemene inherente risico's

3.1 Kwaliteitscriteria

De kwaliteit van het stemproces via internet wordt beoordeeld aan de hand van de vereiste waarborgen die in de volgende tabel opgenomen zijn. Deze zijn afkomstig uit het functioneel ontwerp RIES-KOA (versie 0.3.6) en worden geacht in voldoende mate de wettelijke eisen die voor het stemproces via internet gelden, weer te geven. Verder is de definitie van het kwaliteitsaspect controleerbaarheid uitgebreid om te waarborgen dat achteraf de werking vastgesteld kan worden.

Term	Verklaring
Stemgeheim	Het is onmogelijk om een verband te leggen tussen een Kiezer en een uitgebrachte stem, ter waarborging van de vertrouwelijkheid van de stem
Uniciteit	Iedere Kiesgerechtigde kan precies één keuze-wilsuitdrukking uitbrengen, welke precies één keer als stem meegeteld wordt bij de stemopneming
Kiesgerechtigdheid	Alleen stemmen van kiesgerechtigde personen worden geregistreerd als geldige stem
Integriteit	De uitkomst is niet beïnvloedbaar anders dan door het uitbrengen van rechtmatige stemmen
Controleerbaarheid	Het systeem genereert de verantwoordingsinformatie die wettelijk is voorgeschreven en waarmee achteraf de werking van het systeem vastgesteld kan worden
Hertelling	Conform de wettelijke vereisten is een hertelling mogelijk
Toegankelijkheid	Kiesgerechtigden moeten zoveel mogelijk in staat worden gesteld om deel te nemen aan het verkiezingsproces. De mededeling van de Europese Commissie inzake de toegankelijkheid van websites van de overheid en de inhoud daarvan dient hierbij in acht te worden genomen.
Transparantie voor de Kiezer	De Kiezer moet het stemproces kunnen begrijpen en vertrouwen

3.2 Inherente risico's

Het teststemmechanisme brengt een aantal inherente risico's met zich mee die mede aanleiding zijn geweest voor de uitvoering van deze quick scan. Onder inherente risico's verstaan wij in dit kader de bruto risico's, dat wil zeggen de risico's die onlosmakelijk verbonden zijn aan het proces. Daarbij is nog geen rekening gehouden met getroffen maatregelen. Het risico na rekening gehouden te hebben met de getroffen maatregelen, noemen wij het restrisico of het netto risico.

De volgende inherente risico's hebben wij onderkend:

- Het eerste inherente risico betreft het niet voldoen aan de kwaliteitscriteria uniciteit, kiesgerechtigdheid en integriteit. Dit is het geval als het teststemmechanisme een persoon, die al dan niet kiesgerechtigd is, in staat stelt om een (additionele) stem uit te brengen die één of meerdere keren meetelt bij de stemopneming.

- Het tweede inherente risico is dat niet wordt voldaan aan de criteria controleerbaarheid en hertelling, doordat tijdens en / of na afloop van de stemming niet kan worden vastgesteld of het gebruik van het teststemmechanisme betrouwbaar functioneert/ heeft gefunctioneerd. Wij beschouwen (de mogelijkheid tot) hertelling hierbij als een onderdeel van de controleerbaarheid.

- Het derde inherente risico is dat niet wordt voldaan aan het kwaliteitscriterium 'Transparantie voor de Kiezer', doordat de controleerbaarheid niet op orde is of de kiezer onvoldoende (betrouwbare) informatie krijgt om zelf de controles te kunnen uitvoeren.

In hoofdstuk 5 zijn deze algemene inherente risico's verder uitgewerkt voor de verschillende stappen in het proces stemmen via internet. Per risico is vervolgens geïnventariseerd welke beheersingsmaatregelen getroffen zijn en is een conclusie getrokken over de mate waarin deze risico's door maatregelen zijn afgedekt, het restrisico.

4 Begrippenkader

4.1 Relatie stemcode, technische stem en ontvangstbevestiging

Via de post ontvangt de kiezer een unieke stemcode. Met deze stemcode is hij in staat deel te nemen aan het stemmen via internet. Daartoe voert de kiezer de stemcode in op www.internetstembureau.nl waarna hij de partij en de kandidaat selecteert. Vervolgens wordt de stem via internet verzonden.

Als de stem juist ontvangen en in de stembus opgenomen is, dan ziet de kiezer zijn technische stem aan de hand waarvan achteraf gecontroleerd kan worden of de uitgebrachte stem in de uitslag is opgenomen. Ook krijgt de kiezer op zijn scherm een ontvangstbevestiging waarmee hij achteraf, indien nodig, kan bewijzen dat hij een stem heeft uitgebracht.

4.2 Teststemmechanisme

Het teststemmechanisme in RIES-KOA biedt de mogelijkheid om zowel voor als tijdens de stemperiode de werking van de internetstemdienst te verifiëren. Het mechanisme maakt gebruik van teststemmen die in technisch opzicht vrijwel gelijk zijn aan reguliere stemmen. De doelstelling van het teststemmechanisme is zoveel mogelijk (end-to-end) de systeemonderdelen te gebruiken die ook in het reguliere stemproces worden toegepast, om op deze wijze een zo goed mogelijk beeld te kunnen geven van de werking van het operationele systeem.

Er zijn drie mogelijkheden om teststemmen uit te brengen:

Soort teststem	Omschrijving
Monitor	De beheerder van het webapplicatiedeel van RIES-KOA (Surfnet) brengt geautomatiseerd elke vijf minuten een teststem uit om vast te stellen of de stemdienst beschikbaar is. Hiervoor krijgt SurfNet één teststem. Een op deze manier uitgebrachte teststem wordt niet in de registratie van uitgebrachte stemmen – de stemdatabase – opgenomen en kan opnieuw gebruikt worden. Wel wordt de uitgebrachte monitor-teststem in de logbestanden opgenomen. Ook genereert RIES-KOA een (constante) ontvangstbevestiging.
/test	Via deze functie kan een persoon die beschikt over een geldige stemcode (bijvoorbeeld een teststemcode), het stemproces grotendeels simuleren en op deze wijze bijvoorbeeld de kandidatenlijst in RIES-KOA valideren. Voor de werking is een via "/test" uitgebrachte stem gelijk aan een monitor-teststem. De uitgebrachte stem wordt niet in de registratie van uitgebrachte stemmen, maar wel in het logbestand opgenomen, kan hergebruikt en er wordt ook een constante ontvangstbevestiging gegenereerd.

Soort teststem	Omschrijving
Echte test	Met een teststemcode wordt handmatig een stem uitgebracht. Deze teststem wordt in de stemdatabase opgenomen en er wordt een reguliere ontvangstbevestiging gegenereerd. Deze ontvangstbevestiging kan worden vergeleken met een eerder in de testomgeving verkregen ontvangstbevestiging waarmee zekerheid kan worden verkregen over de geladen cryptosleutel (ReceiptKey) in de stemomgeving.

5 Risico's, maatregelen en conclusie

In dit hoofdstuk worden de risico's en de getroffen maatregelen beschreven. Op basis hiervan wordt vastgesteld in welke mate de risico's zijn afgedekt en welke aanvullende maatregelen aanwezig zouden moeten zijn.

5.1 Voorbereiden stemming

5.1.1 Inherente risico's

De volgende inherente risico's[2] als gevolg van het teststemmechanisme onderkennen wij voor de fase "Voorbereiden stemming":

Fase/ Subfase	Kwaliteitscriteria								Inherent risico a.g.v. methodiek teststemmen
Voorbereiden verkiezingen	St[3]	Un	Kg	In	Ct	Ht	Tg	Tr	
Genereren sleutels en stemcodes		X	X	X	X			X	Er worden te veel of te weinig teststemcodes aangemaakt.
Aanmaken referentiebestand		X	X	X	X			X	Aangemaakte teststemcodes komen niet juist of niet volledig in de (verantwoordings-) overzichten.
Productie en verzending stembescheiden/ Beheren teststem-bescheiden		X	X	X	X			X	Stembescheiden benodigd voor het uitbrengen van teststemmen raken verloren of raken bekend.
Helpdesk		X	X	X	X			X	Teststemcodes worden omgezet naar reguliere stemcodes.
		X	X	X	X			X	Reguliere stemcodes worden omgezet naar teststemcodes.

[2] Voor de definitie van inherent risico verwijzen wij naar de eerste alinea van § 3.2.
[3] Voor de betekenis van de verschillende kwaliteitscriteria verwijzen wij naar § 3.1.

Fase/ Subfase	Kwaliteitscriteria								Inherent risico a.g.v. methodiek teststemmen
Voorbereiden verkiezingen	St[3]	Un	Kg	In	Ct	Ht	Tg	Tr	
Algemeen					X			X	De burger heeft onvoldoende informatie om voor zichzelf vast te stellen of in deze fase goed met teststemcodes is omgegaan.

5.1.2 Maatregelen

Om deze risico's af te dekken zijn beheersingsmaatregelen nodig. In onderstaande tabel geven wij aan welke maatregelen in opzet al getroffen zijn en welke nog tenminste aanvullend getroffen moeten worden:

Inherent risico a.g.v. methodiek teststemmen	Beheersingsmaatregelen
Er worden te veel of te weinig teststemcodes aangemaakt.	Getroffen maatregelen: 1. Het is technisch mogelijk de sleutel die nodig is voor het genereren van de stemcodes (Kgenvoterkey), te verdelen, bijvoorbeeld deels in beheer (op CD) bij het project en deels bij 'Het Waterschapshuis' (wachtwoord), waardoor het vier-ogen-principe op het aanmaken van de stemcodes gewaarborgd kan worden. 2. RIES-KOA maakt automatisch na het genereren van de stemcodes een verwerkingsverslag aan. 3. Met behulp van de "Reference Table Integrity Validation Tool" (RTI-VT) kan vastgesteld worden hoe de stemcodes in het referentiebestand over de verschillende stemcategorieën zijn verdeeld. 4. Het referentiebestand wordt gepubliceerd op internet en de hashwaarde hierover wordt gepubliceerd in de Staatscourant. Aanvullend te treffen maatregelen: 5. De verschillende delen van de sleutel worden verdeeld over TPPI en BZK. In § 3.4 van de AO ("Genereren stemcodes") is dit op hoofdlijnen uitgewerkt. Verder zijn ons geen eenduidige procedureafspraken ten aanzien van het transport, beheer en gebruik van de verschillende delen van de sleutel medegedeeld. 6. In de procedures waarover § 3.9 van de AO ("Generatie referentiebestanden voor stemming"), § 5 ("Stemcontrole") en § 7.4 ("Vervangende stembescheiden uitreiken") gaan, wordt het

Inherent risico a.g.v. methodiek teststemmen	Beheersingsmaatregelen
	referentiebestand gegenereerd, gebruikt respectievelijk aangepast. Hierin worden geen maatregelen beschreven die waarborgen dat iedere keer als het referentiebestand gebruikt wordt, vastgesteld wordt met RTI-VT dat het aantal teststemcodes niet is gewijzigd. Ook anderszins is ons niet eenduidig bekend geworden welke procedureafspraken op dit punt gemaakt zijn. 7. In § 3.4 van de AO ("Genereren stemcodes") wordt geen melding gemaakt van de controle en aftekening van het verwerkingsverslag. Ook zijn ons hierover geen eenduidige procedureafspraken medegedeeld. 8. Ons is medegedeeld dat changemanagementprocedures worden afgesproken die waarborgen dat alleen de geautoriseerde RIES-KOA-software wordt gebruikt. Voor zover ons bekend is geworden, zijn voor de invulling hiervan echter nog geen concrete afspraken gemaakt.
Aangemaakte teststemcodes komen niet juist of niet volledig in de (verantwoordings-) overzichten.	Getroffen maatregelen: 9. Op de (verantwoordings-) overzichten naar aanleiding van het genereren van de stemcodes worden aangemaakte teststemcodes afzonderlijk genoemd. 10. De source code waarmee data voor de (verantwoordings-) overzichten aangemaakt worden, is en wordt door een onafhankelijk bureau (CIBIT) gereviewed. Aanvullend te treffen maatregelen: 11. Ten aanzien van de configuratietabellen waarin de opmaak en samenstelling van de (verantwoordings-) overzichten is opslagen, zijn ons geen adequate beheersprocedures medegedeeld. 12. Voor de changemanagementprocedures wordt verwezen naar hetgeen is opgemerkt onder punt 8.
Stembescheiden benodigd voor het uitbrengen van teststemmen raken verloren of raken bekend.	Te treffen maatregelen: 13. Ons zijn geen eenduidige procedureafspraken medegedeeld over hoe omgegaan zal worden (bij verdelen, ontvangen, opslaan, vrijgeven, openen, inventariseren etc. van de teststembescheiden) met de stembescheiden waarop de teststemcodes staan.
Teststemcodes worden omgezet naar reguliere stemcodes.	Getroffen maatregelen: 14. In het functioneel ontwerp is geen functionaliteit beschreven voor het omzetten van teststemcodes naar reguliere stemcodes. 15. Door de onafhankelijke code reviewer is vastgesteld dat geen code aanwezig is voor het omzetten van teststemcodes naar reguliere stemcodes.

Inherent risico a.g.v. methodiek teststemmen	Beheersingsmaatregelen
	16. Ten aanzien van de "Reference Table Integrity Validation Tool" wordt verwezen naar punt 3. 17. Met behulp van de "RIES Integriteits Controle Referentiedata" (RICOR) kan de hashwaarde van het referentiebestand vastgesteld worden. 18. Iedereen kan zelfstandig vaststellen dat het gepubliceerde referentiebestand de enig juiste is door de hashwaarde te vergelijken met de waarde die is gepubliceerd in de Staatscourant en vervolgens vaststellen hoeveel teststemcodes er bestaan. Aanvullend te treffen maatregelen: 19. Voor het gebruik van RTI-VT wordt verwezen naar hetgeen is opgemerkt onder punt 6. 20. Er zijn ons geen procedures kenbaar gemaakt die waarborgen dat iedere keer als het referentiebestand gebruikt wordt, vastgesteld wordt dat de berekende hashwaarde overeenkomt met de gepubliceerde hashwaarde. 21. Ons is niet bekend geworden dat na afloop van de stemming gecontroleerd wordt of de status in het definitieve referentiebestand van de teststemmen juist is.
Reguliere stemcodes worden omgezet naar teststemcodes.	Voor de meeste beheersingsmaatregelen verwijzen wij naar de getroffen en nog te treffen maatregelen (nummers 14 tot 20), plus: 22. Na afloop van de verkiezingen kunnen kiezers zelf controleren of de door hen uitgebrachte stem heeft meegeteld in de einduitslag en daarmee zeker weten dat hun reguliere stemcode niet is omgezet naar een teststemcode.
De burger heeft onvoldoende informatie om voor zichzelf vast te stellen of in deze fase goed met teststemcodes is omgegaan.	Getroffen maatregelen: 23. Op internet wordt het referentiebestand volledig gepubliceerd, zodat de burger kan vaststellen hoeveel teststemcodes zijn gegenereerd. 24. In de Staatscourant wordt de hashwaarde over het referentiebestand gepubliceerd, zodat de burger zelfstandig kan vaststellen dat het gepubliceerde referentiebestand juist is door de gepubliceerde waarde te vergelijken met de door hem zelf berekende hashwaarde. Aanvullend te treffen maatregelen: 25. Aan de burger wordt helder uitgelegd hoe hij zelfstandig kan vaststellen dat (in opdracht van) het stembureau goed is omgegaan met de teststemcodes.

5.1.3 Conclusie

Gelet op de maatregelen waarvan de opzet in de vorige paragraaf is beschreven, worden ten aanzien van de eerder onderkende specifieke risico's de volgende conclusies getrokken:

Inherent risico a.g.v. methodiek teststemmen	Conclusie[4]
Er worden te veel of te weinig teststemcodes aangemaakt.	Deels afgedekt
Aangemaakte teststemcodes komen niet juist of niet volledig in de (verantwoordings-) overzichten.	Deels afgedekt
Stembescheiden benodigd voor het uitbrengen van teststemmen raken verloren.	Deels afgedekt
Teststemcodes worden omgezet naar reguliere stemcodes.	Deels afgedekt
Reguliere stemcodes worden omgezet naar teststemcodes.	Deels afgedekt
De burger heeft onvoldoende informatie om voor zichzelf vast te stellen of in deze fase goed met teststemcodes is omgegaan.	Deels afgedekt

Motivering:
Aan het technisch aspect van het stemproces via internet is in opzet voldoende aandacht besteed. Omdat een aantal essentiële procedures nog niet (volledig) is afgesproken, vastgelegd en geformaliseerd (zie hiervoor de maatregelen die in de vorige paragraaf zijn onder het kopje "Te treffen maatregelen") is de conclusie dat de risico's slechts gedeeltelijk zijn afgedekt. Ook ontbreekt een eenvoudige beschrijving hoe de burger zelfstandig kan vaststellen dat (in opdracht van) het stembureau goed is omgegaan met de teststemcodes.

---

[4] Voor de betekenis van de conclusie wordt verwezen naar fase 4 in bijlage II.

5.2 Uitbrengen stemmen

5.2.1 Inherente risico's

De volgende inherente risico's als gevolg van het teststemmechanisme zijn voor de fase "Uitbrengen stemmen" te onderkennen:

Fase/ Subfase	Kwaliteitscriteria								Inherent risico a.g.v. methodiek teststemmen
Uitbrengen stemmen	**St**	**Un**	**Kg**	**In**	**Ct**	**Ht**	**Tg**	**Tr**	
Uitgifte teststemcodes/ Uitbrengen (test-) stem					X			X	Ten onrechte worden teststemmen met de teststemcodes uitgebracht.
					X			X	Uitgebrachte teststemmen komen niet juist of niet volledig in de (verantwoordings-) overzichten.
		X	X	X	X			X	Uitgebrachte teststemmen worden omgezet naar uitgebrachte reguliere stemmen.
		X	X	X	X			X	Uitgebrachte reguliere stemmen worden omgezet naar uitgebrachte teststemmen.
Algemeen					X			X	De burger heeft onvoldoende informatie om voor zichzelf vast te stellen of in deze fase goed met teststemcodes is omgegaan.

5.2.2 Maatregelen

Om deze risico's af te dekken zijn beheersingsmaatregelen nodig. In onderstaande tabel geven wij aan welke maatregelen in opzet al getroffen zijn en welke nog tenminste aanvullend getroffen moeten worden:

Inherent risico a.g.v. methodiek teststemmen	Beheersingsmaatregelen
Ten onrechte worden teststemmen met de	Nog te treffen maatregelen: Een procedure waarin is beschreven hoe om te gaan met de

Inherent risico a.g.v. methodiek teststemmen	Beheersingsmaatregelen
teststemcodes uitgebracht.	stembescheiden waarop de teststemcodes staan, is ons niet medegedeeld. Hierin dient ingegaan te worden op de administratie van teststemcodes, het uitbrengen van teststemmen en de controlemaatregelen hier om heen.
Uitgebrachte teststemmen komen niet juist of niet volledig in de (verantwoordings-) overzichten.	Verwezen wordt naar het risico "Aangemaakte teststemcodes komen niet juist of niet volledig in de (verantwoordings-) overzichten." in § 5.1.2.
Uitgebrachte teststemmen worden omgezet naar uitgebrachte reguliere stemmen.	Aan de uitgebrachte technisch stem kan niet vastgesteld worden of een reguliere of een teststemcode is gebruikt. Hiervoor moet het gepubliceerde referentiebestand van alle technische stemmen gebruikt worden. Voor het omzetten van een uitgebrachte teststem moet in het referentiebestand de status van de stemcode aangepast worden. Daarom wordt voor relevante beheersingsmaatregelen voor dit risico verwezen naar de maatregelen bij het eerdere risico "Teststemcodes worden omgezet naar reguliere stemcodes." in § 5.1.2.
Uitgebrachte reguliere stemmen worden omgezet naar uitgebrachte teststemmen.	Idem, verwezen wordt naar risico "Reguliere stemcodes worden omgezet naar teststemcodes." in § 5.1.2.
De burger heeft onvoldoende informatie om voor zichzelf vast te stellen of in deze fase goed met teststemcodes is omgegaan.	<u>Getroffen maatregelen:</u> 1. De kiezer kan achteraf vaststellen dat de door hem uitgebrachte stem niet als teststem in de uitslag is opgenomen. 2. In de gepubliceerde lijst met uitgebrachte technische stemmen kan de burger vaststellen hoeveel teststemmen en op welke kandidaten teststemmen zijn uitgebracht. 3. De juistheid van de gepubliceerde lijst met uitgebrachte technische stemmen kan de burger controleren door deze te combineren met het referentiebestand van de technische stemmen. <u>Nog te treffen maatregelen:</u> 4. Aan de burger wordt helder uitgelegd hoe hij zelfstandig kan vaststellen dat (in opdracht van) het stembureau goed is omgegaan met de teststemcodes.

5.2.3 Conclusie

Gelet op de maatregelen waarvan de opzet in de vorige paragraaf is beschreven, worden ten aanzien van de eerder onderkende specifieke risico's de volgende conclusies getrokken:

Inherent risico a.g.v. methodiek teststemmen	Conclusie
Ten onrechte worden teststemmen met de teststemcodes uitgebracht.	**Deels afgedekt**
Uitgebrachte teststemmen komen niet juist of niet volledig in de (verantwoordings-) overzichten.	**Deels afgedekt**
Uitgebrachte teststemmen worden omgezet naar uitgebrachte reguliere stemmen.	**Deels afgedekt**
Uitgebrachte reguliere stemmen worden omgezet naar uitgebrachte teststemmen.	**Deels afgedekt**
De burger heeft onvoldoende informatie om voor zichzelf vast te stellen of in deze fase goed met teststemcodes is omgegaan.	**Deels afgedekt**

Motivering:
Aan het technisch aspect van het stemproces via internet is in opzet voldoende aandacht besteed. Omdat een aantal essentiële procedures nog niet (volledig) is afgesproken, vastgelegd en geformaliseerd is de conclusie dat de risico's slechts gedeeltelijk zijn afgedekt. Ook ontbreekt een eenvoudige beschrijving hoe de burger zelfstandig kan vaststellen dat (in opdracht van) het stembureau goed is omgegaan met de teststemcodes.

5.3 Tellen stemmen

5.3.1 Inherente risico's

De volgende inherente risico's als gevolg van het teststemmechanisme zijn voor de fase "Tellen stemmen" te onderkennen:

Fase/ Subfase	Kwaliteitscriteria								Inherent risico a.g.v. methodiek teststemmen
Tellen stemmen	S t	U n	K g	I n	C t	H t	T g	T r	
Voorbereiding tellen stemmen				X	X	X		X	De integriteit van de stemgegevens wordt aangetast bij de overdracht van de stemservers naar de machines waarop de verwerking met de Tally-software plaatsvindt.
		X	X	X	X			X	Een onjuist of niet integer referentiebestand wordt gebruikt als invoer voor de Tally-software.
Tellen stemmen		X	X	X	X			X	Uitgebrachte teststemmen worden als reguliere stem in de uitslag opgenomen.
		X	X	X	X			X	Uitgebrachte reguliere stemmen worden als teststem in de uitslag opgenomen.
					X	X			Aangemaakte teststemcodes komen niet juist of niet volledig in de (verantwoordings-) overzichten.
Algemeen					X	X		X	De burger heeft onvoldoende informatie om voor zichzelf vast te stellen of in deze fase goed met uitgebrachte teststemmen is omgegaan.

5.3.2 Maatregelen

Om deze risico's af te dekken zijn beheersingsmaatregelen nodig. In onderstaande tabel geven wij aan welke maatregelen in opzet al getroffen zijn en welke nog tenminste aanvullend getroffen moeten worden:

Inherent risico a.g.v. methodiek teststemmen	Beheersingsmaatregelen
De integriteit van de stemgegevens wordt aangetast bij de overdracht van de stemservers naar de machines waarop de verwerking met de Tally-software plaatsvindt.	Getroffen maatregelen: 1. Ons is medegedeeld dat de stemgegevens via een beveiligde VPN-verbinding worden opgehaald. 2. Het stembureau houdt toezicht op het ophalen van het bestand met de ontvangen stemmen van de stemservers. Het bestand wordt direct op meerdere CD-ROM's gebrand, waarvan er één aan het stembureau wordt gegeven (AO § 4.8.1). Aanvullend te treffen maatregelen: 3. Een procedure waarin is beschreven dat per stemserver het uitvoerverslag wordt aangesloten op het ontvangen bestand, is ons niet medegedeeld.
Een onjuist of niet integer referentiebestand wordt gebruikt als invoer voor de Tally-software.	Getroffen maatregelen: 4. Voor het gebruik van RTI-VT wordt verwezen naar hetgeen is opgemerkt onder punt 6 in § 5.1.2. 5. Voor het gebruik van "RIES Integriteits Controle Referentiedata" (RICOR) wordt verwezen naar hetgeen is opgemerkt onder punt 17 in § 5.1.2. 6. Iedereen kan zelfstandig het telproces uitvoeren en vaststellen dat het gepubliceerde referentiebestand is gebruikt als basis voor het tellen van de stemmen op basis van de op Internet gepubliceerde stemmen. Aanvullend te treffen maatregelen: 7. Over het gebruik van RTI-VT en RICOR in het telproces zijn ons geen procedure-afspraken medegedeeld (zie ook punt 6 en 20 uit § 5.1.2).
Uitgebrachte teststemmen worden als reguliere stem in de uitslag opgenomen.	Om teststemmen te tellen als reguliere, geldige stem moeten óf de statuswaarden in het gepubliceerde referentiebestand gewijzigd worden óf de gebruikte software aangepast zijn. Voor een opsomming van de beheersingsmaatregelen rondom de statuswaarden in het referentiebestand wordt verwezen naar de maatregelen behorende bij het risico "Teststemcodes worden omgezet naar reguliere stemcodes" in § 5.1.2. Voor de beheersingsmaatregelen ten aanzien van de gebruikte software wordt verwezen naar punt 8.

Inherent risico a.g.v. methodiek teststemmen	Beheersingsmaatregelen
Uitgebrachte reguliere stemmen worden als teststem in de uitslag opgenomen.	Idem, verwezen wordt naar risico "Reguliere stemcodes worden omgezet naar teststemcodes." in § 5.1.2.
Aangemaakte teststemcodes komen niet juist of niet volledig in de (verantwoordings-) overzichten.	Verwezen wordt naar risico "Aangemaakte teststemcodes komen niet juist of niet volledig in de (verantwoordings-) overzichten." in § 5.1.2.
De burger heeft onvoldoende informatie om voor zichzelf vast te stellen of in deze fase goed met uitgebrachte teststemmen is omgegaan.	Getroffen maatregelen: 8. De kiezer kan achteraf vaststellen dat de door hem uitgebrachte stem niet als teststem in de uitslag is opgenomen. 9. De juistheid van het telproces kan de burger vervolgens volledig zelfstandig controleren aan de hand van de gepubliceerde lijst met alle uitgebrachte technische stemmen, het gepubliceerde, definitieve referentiebestand en de in de Staatscourant gepubliceerde hashcode. Aanvullend te treffen maatregelen: 10. Aan de burger wordt helder uitgelegd hoe hij zelfstandig kan vaststellen dat (in opdracht van) het stembureau goed is omgegaan met de teststemcodes.

5.3.3 Conclusie

Gelet op de maatregelen waarvan de opzet in de vorige paragraaf is beschreven, worden ten aanzien van de eerder onderkende specifieke risico's de volgende conclusies getrokken:

Inherent risico a.g.v. methodiek teststemmen	Conclusie
De integriteit van de stemgegevens wordt aangetast bij de overdracht van de stemservers naar de machines waarop de verwerking met de Tally-software plaatsvindt.	**Deels afgedekt**
Uitgebrachte teststemmen worden als reguliere stem in de uitslag opgenomen.	**Deels afgedekt**
Uitgebrachte reguliere stemmen worden als teststem in de uitslag opgenomen.	**Deels afgedekt**

Inherent risico a.g.v. methodiek teststemmen	Conclusie
Aangemaakte teststemcodes komen niet juist of niet volledig in de (verantwoordings-) overzichten.	**Deels afgedekt**
De burger heeft onvoldoende informatie om voor zichzelf vast te stellen of in deze fase goed met uitgebrachte teststemmen is omgegaan.	**Deels afgedekt**

Motivering:
Aan het technisch aspect van het stemproces via internet is in opzet voldoende aandacht besteed. Omdat een aantal essentiële procedures nog niet (volledig) is afgesproken, vastgelegd en geformaliseerd is de conclusie dat de risico's slechts gedeeltelijk zijn afgedekt. Ook ontbreekt een eenvoudige beschrijving hoe de burger zelfstandig kan vaststellen dat (in opdracht van) het stembureau goed is omgegaan met de teststemcodes.

Auditdienst BZK
Auditmanager,

Deloitte Accountants B.V.

Bijlage I: Onderszoeksverantwoording

Teamsamenstelling

Het onderzoek is uitgevoerd door Auditdienst in combinatie met de Deloitte. Het onderzoeksteam bestaat uit de volgende personen:

Rol	Persoon
Verantwoordelijk auditmanager vanuit AD BZK	
Verantwoordelijk partner vanuit Deloitte	
Auditor BZK	
Auditor Deloitte	

Fasering

Fase 1: Kennisvergaring

Doel van de eerste fase is het verkrijgen van het beeld van het verloop van het stemproces in het algemeen en de teststemmethodiek in het bijzonder. Dit beeld dient zo volledig mogelijk te zijn, omdat op basis hiervan in de volgende fase de risicoanalyse plaatsvindt, alsmede de inventarisatie van de opzet van de beheersingsmaatregelen.

In dit kader hebben wij de volgende documentatie ontvangen:

- Functioneel ontwerp RIES-KOA versie 0.3.6 datum 3 oktober 2006
- Administratieve organisatie internetstemmen kiezen op afstand, versie 25 september 2006
- Master test plan Kiezen Op Afstand, versie 0.27, datum 4 augustus 2006, concept
- Bijlage I, Uitkomsten acceptatietesten – geen datum
- Beoordeling KOA, Een beoordeling van de integriteit van "Kiezen op Afstand", versie 11 september 2006
- Risicoanalyse controlemechanismen RIES-KOA, datum 29 augustus 2006
- Cryptographic architecture for RIES-2008 and RIES-KOA, datum 7 juli 2006, versie 0.9 draft
- Brief Waterschapshuis aan BZK van 18 september 2006, onderwerp validatie transactie
- Bijlage 3, Werking stemcontrole, geen datum
- RIES – Internet Voting in Action, Institute for Computing and Information Sciences Radboud University Nijmegen.
- Handleiding Stemmen via internet
- Proces en Interactie Model, experiment met Internetstemmen bij vervroegde TK verkiezingen 2006, datum 2 augustus 2006, versie 0.3 concept
- Samenwerkingsconvenant ministerie BZK Rijnland en Het Waterschapshuis D10
- Diverse testrapportages RIES_KOA

- Voorbeelden uitvoerbestanden volledig stemtraject RIES-KOA
- Relevante onderdelen uit de JAVA code van RIES-KOA, o.a. verwerking statusinformatie in Tally
- Voorbeelden van proces-verbaal

Uit deze documentatie hebben wij ons een eerste beeld gevormd van het proces dat tijdens de interviews met betrokkenen (fase 3) is voltooid.

Voor de uitkomsten van deze fase, een beschrijving op hoofdlijnen voor zover relevant voor de quick scan, is opgenomen in bijlage II.

Fase 2: Uitvoeren globale risicoanalyse

Op basis van de geldende kwaliteitscriteria en informatie over het stemproces via internet is een risicoanalyse uitgevoerd specifiek gericht op het gebruik van de te hanteren methodiek van teststemmen. Bij de risicoanalyse is in deze fase afgezien van reeds getroffen maatregelen. Alle deze inherente risico's zijn benoemd, zowel algemeen (hoofdstuk 3.2) als specifiek per proces (§ 5.1.1, 5.2.1 en 5.3.1).

Fase 3: Inventarisatie opzet maatregelen

Om de inherente risico's uit de vorige fase te mitigeren zijn diverse beheersingsmaatregelen getroffen. Voor zover bekend uit de documentatie zijn deze geïnventariseerd. Verder zijn in deze fase interviews gehouden met de volgende personen om de inventarisatie van de opzet van de maatregelen binnen de kaders van de onderzoeksvraag zo volledig mogelijk te maken:

- programmamanager ICTU;
- testcoördinator KOA;
- testmanager KPMG;
- code reviewer CIBIT Consultants;
- architect RIES, MullPon;
- Projectmanager Elektronische Dienstverlening;
- technical consultant SurfNet.

Per geïdentificeerd inherent risico (eindproduct fase 2) zijn de geïnventariseerde beheersingsmaatregelen vastgelegd (§ 5.1.2, 5.2.2 en 5.3.2). Op feitelijke juistheid is bijlage II afgestemd met de geïnterviewden.

Fase 4: Analyse

Aan de hand van de verkregen informatie is tijdens de 4e fase vastgesteld in welke mate de risico's in opzet zijn afgedekt door de voorziene beheersingsmaatregelen en op basis hiervan zijn restrisico's geïdentificeerd.

Daarbij wordt de volgende classificatie aangehouden:

Conclusie	Betekenis
Afgedekt	De opzet van de beheersingsmaatregelen is effectief en dekt in voldoende mate het onderkende inherente risico af.
Deels afgedekt	De opzet van de beheersingsmaatregelen is deels effectief en dekt in beperkte mate het onderkende inherente risico af. Verbeteringsmaatregelen zijn aanbevolen.
Niet afgedekt	De opzet van de beheersingsmaatregelen is niet effectief en dekt in onvoldoende mate het onderkende inherente risico af. Verbeteringsmaatregelen zijn noodzakelijk.

De mijlpaal van deze fase is een overzicht van de onderkende inherente risico's, de geïnventariseerde relevante beheeringsmaatregelen in opzet en de conclusie over de mate waarin de risico's hierdoor zijn afgedekt (§ 5.1.3, 5.2.3 en 5.3.3).

Fase 5: Oordeelsvorming en rapportage

In de laatste fase is op basis van de bevindingen van de voorafgaande fasen mondeling (presentatie directeur CZW op 3 oktober 2006) en schriftelijk antwoord gegeven op de gestelde onderzoeksvraag.

Bijlage II: Procesbeschrijving

Onderstaand is een deel van het totale proces stemmen via internet beschreven, voor zover relevant voor de quick scan teststemmethodiek.

1 Voorbereiden stemming

Voor zover relevant voor het onderzoek bestaat de fase "Voorbereiden stemming" uit de volgende subfasen:

- Genereren sleutels
- Genereren stemcodes
- Aanmaken referentiebestand
- Productie en verzending stembescheiden
- Helpdesk

1.1 Genereren sleutels

De kwaliteit van het stemmen via internet steunt in sterke mate op encryptietechnieken. Zo worden via encryptie (test-) stemcodes gegenereerd (Kgenvoterkey) en ook voor het genereren van de ontvangstbevestiging is een encryptiesleutel nodig.

Daarom start het proces – voor zover relevante voor het onderzoek – met het genereren van de sleutels. Omdat stemcodes geheim gehouden dienen te worden, moeten ook de gebruikte encryptiesleutels geheim gehouden worden.

Uit het Functioneel ontwerp van RIES en tijdens interviews is ons gebleken dat RIES-KOA werkt met verdeelde sleutels: de totale encryptiesleutel wordt verdeeld over verschillende media die worden beheerd door verschillende verantwoordelijken, zodat geen enkele partij zelfstandig over de sleutel kan beschikken.

1.2 Genereren stemcodes

Er zijn drie categorieën stemcodes te onderkennen:

1. Stemcodes voor de kiesgerechtigden;
2. Vervangende stemcodes die aan kiesgerechtigden worden verstrekt als de reguliere stemcode verloren is gegaan;
3. Stemcodes die nodig zijn voor het uitbrengen van een teststem.

Het genereren van deze drie categorieën stemcodes vindt plaats in hetzelfde proces.

Van de gemeente Den Haag wordt drie maal een zogenaamde K10-lijst ontvangen, met daarop alle kiesgerechtigden die in het buitenland wonen en/of werken en die hebben aangegeven via internet te willen stemmen. Op deze K10-lijst staan volgnummer en de NAW-gegevens van de kiesgerechtigden. Het volgnummer inclusief een aantal andere gegevens worden gebruikt om met een sleutel (Kgenvoterkey) voor iedere kiesgerechtigde een stemcode te genereren. Deze stemcode is uniek en is het enige dat een kiezer nodig heeft om een stem uit te kunnen brengen. Daarom dienen stemcodes zoveel mogelijk geheim gehouden te worden. Verder worden voor een percentage van de kiesgerechtigden vervangende stemcodes gegenereerd (K11-lijst) en per generatieslag 25 stemcodes (totaal 75) die gebruikt kunnen worden voor het uitbrengen van een teststem. De volgnummers van de vervangende stemcodes beginnen met '90' en voor de teststemmen begint met '99'. De gegevens op de K10-lijst, de vervangende codes en de teststemmen inclusief de stemcode vormen de C10-lijst, die verzonden wordt naar de drukker.

1.3 Aanmaken referentiebestand

Nadat voor de derde maal de stemcodes zijn gegenereerd, wordt op basis van de totale K10-lijst in combinatie met de definitieve lijst van kandidaten o.a. het referentiebestand aangemaakt:

- Allereerst worden alle mogelijke zogenaamde technische stemmen berekend: voor iedere mogelijke stem die met de stemcode uitgebracht kan worden. Deze technische stem bestaat uit twee delen:

Deel	Doel	Technische aanduiding	Wijze van berekening
Linkerdeel	De pseudo-identiteit van de kiezer n	VnPID	Het nummer van de stembus (BalBxId) wordt versleuteld met de stemcode (Kp)
Rechterdeel	De stem van pseudo-identiteit n op kandidaat x	VnCx	De kandidaatkeuze (Cx) wordt versleuteld met de stemcode (Kp)

- In hetzelfde proces worden vervolgens alle technische stemmen via een hashfunctie (MDC: Modification Detection Code) omgezet in een referentiewaarde, die ook bestaat uit een linker- (RnPID) en een rechterdeel (RnCm).

Deze referentiewaarden vormen samen het eerste referentiebestand. Dit bestand bestaat voor iedere stemcodereferentie uit een apart bestand, waarin via statussen voor iedere stemcodereferentie wordt aangegeven tot welke categorie deze stemcodereferentie en zijn mogelijke technische stemmen behoren. De statussen kunnen de volgende waarden hebben:

Betekenis	Statussen en statuswaarde		
	Vervangend	Verstrekt	Vervallen
Reguliere stemcode	0	0 1	0
Reguliere stemcode die later is geblokkeerd	0	1	1
Niet verstrekte vervangende stemcode	1	0	0
Verstrekte vervangende stemcode	1	1	0
Teststemcode	1	0	1
Niet geldige stemcode	0 1	0 1	1

Het referentiebestand wordt na wijziging op basis van gegevens van de helpdesk (zie § 1.6), gepubliceerd op internet en is essentieel bij de telling van de stemmen. Het is voldoende voor het wijzigen van de status van de stemcode (bijvoorbeeld van reguliere stemcode naar een vervallen stemcode, van teststemcode naar reguliere stemcode etc.) om de statuswaarde in het referentiebestand te wijzigen. Om te kunnen vaststellen dat het referentiebestand blijvend juist is, wordt een hashwaarde berekend en gepubliceerd in de Staatscourant.

1.4 Productie en verzending stembescheiden

Analoog aan de vorige subfase waarin de verschillende categorieën stemcodes gelijk werden behandeld, wordt ook in deze fase geen onderscheid gemaakt tussen reguliere, vervangende en teststemcodes.

Voor alle drie de categorieën maakt de drukker de stembescheiden aan. Na aanmaken worden de normale stemcodes verzonden naar de kiesgerechtigden. De vervangende en de teststemcodes worden overgedragen aan het project KOA.

1.5 Beheren teststembescheiden

Nadat de teststembescheiden zijn ontvangen door het project KOA, worden deze opgeslagen. Ons is medegedeeld dat deze teststembescheiden door het project bewaard worden en, indien nodig, door het stembureau verstrekt worden om een teststem uit te brengen.

1.6 Helpdesk

Wanneer een kiesgerechtigde bij de helpdesk aangeeft zijn stembescheiden niet of niet goed te hebben ontvangen, verstrekt de helpdesk telefonisch, na controle van identiteit, een vervangende stemcode.

Tegelijkertijd zorgt de helpdesk ervoor dat de oorspronkelijke stemcode ongeldig en de verstrekte vervangende stemcodes geldig gemaakt kunnen worden. Daarvoor geeft de helpdesk het volgnummer van de kiesgerechtigde op de K10-lijst en het volgnummer van de vervangende stemcode op de K11-lijst door. Op basis van deze nummers kan met gebruik van de Kgenvoterkey het referentiebestand overeenkomstig worden aangepast. Dit is een van de meest gevoelige stappen aangezien het in deze stap in theorie ook mogelijk zou zijn de status van teststemmen te veranderen in reguliere stemmen.

Als gevolg van het (on-) geldig maken van de stemcodes wijzigt het referentiebestand en ook de hashwaarde ervan. Dit tweede referentiebestand wordt gepubliceerd op internet en de hashwaarde in de Staatscourant.

2 Uitbrengen stemmen

2.1 Uitgifte teststemcodes

Voor het uitbrengen van een teststem zijn de teststembescheiden nodig, die beheerd worden door het stembureau. Onder voorwaarden, zoals vastgelegd in het nog te formaliseren protocol, verstrekt het stembureau één teststemcode om de werking van het systeem te testen door het uitbrengen van één teststem.

2.2 Uitbrengen (test)stem

Het uitbrengen van een teststem gaat technisch volgens hetzelfde proces als het uitbrengen van een reguliere of vervangende stem. Voor het uitbrengen van een stem is alleen een geldige stemcode nodig. Op de website www.internetstembureau.nl geeft de kiezer de ontvangen stemcode in. Vervolgens dient een keuze gemaakt te worden voor de politieke partij of voor een blanco stem (=lijst 99). Indien gekozen is voor een politieke partij, dan moet vervolgens nog de kandidaat gekozen worden, waarna de kiezer zijn stem kan bevestigen.

Na bevestiging wordt in de webbrowser van de kiezer via een Java-script zijn stem versleuteld in een technische stem. Zoals aangegeven in § 1.3 bestaat de technische stem uit een linker- en een rechterdeel (VnPID respectievelijk VnCx). Beide delen worden door een Java-script in de browser van de gebruiker berekend en via een beveiligde SSL-verbinding verzonden.

Stemmen die zijn uitgebracht met een ongeldige stemcode, worden niet in de stembus opgeslagen. Ook teststemmen uitgebracht via "/test" of de monitorfunctie worden niet in de stembus opgenomen. Alle andere ontvangen stemmen, zowel van reguliere als van vervangende en teststemcodes worden wel in de stembus opgeslagen. Ook als een tweede stem met dezelfde stemcode wordt uitgebracht of als gestemd is op een niet-bestaande kandidaat, wordt de uitgebrachte stem opgeslagen. Controle op de geldigheid van een uitgebrachte stem vindt plaats tijdens de volgende fase, het tellen van de stemmen.

Dat een stem in de stembus is opgeslagen, ziet de kiezer via een melding op het scherm. Verder kan hij via een extra optie 'techniek' zijn uitgebrachte technische stem opslaan om te gebruiken na afloop van de verkiezingen bij de stemcontrole: de kiezer kan zelf controleren of zijn uitgebrachte (unieke) technische stem is opgenomen in de gepubliceerde lijst met uitgebrachte technische stemmen en dus is meegeteld in de uitslag.

Ook ziet de kiezer een ontvangstbevestiging (VotRecConCnt) op het scherm. Deze ontvangstbevestiging is de helft van het gehashte nummer van de stembus die vervolgens opnieuw is versleuteld met de uitgebrachte technische stem. Mocht na afloop van de verkiezingen bij de stemcontrole door de kiezer blijken dat de uitgebrachte stem niet voorkomt in de gepubliceerde lijst met uitgebrachte technische stemmen, dan kan de kiezer met de ontvangstbevestiging bewijzen dat hij wel gestemd heeft.

3 Tellen stemmen

In de fase "Tellen stemmen" vindt de stemopneming plaats, dat wil zeggen het tellen van de uitgebrachte geldige stemmen. De procedure hiervoor is in concept vastgelegd in § 4.8 van de AO. Als eerste start de stemopneming met het overbrengen van het bestand met de ontvangen (technische) stemmen van de stemservers naar twee laptops waarop de verdere verwerking plaatsvindt. De bestanden worden op meerdere CD-rom's gebrand waarvan er één aan het stembureau wordt gegeven. De tweede stap is dat de veilig gestelde stemmen worden verwerkt met de 'Tally'-software. De invoer voor de Tally-software bestaat uit de verzameling technische stemmen van de stemservers en het definitieve referentiebestand[5]. De Tally-software voert in relatie tot (test-) stemmen op hoofdlijnen de volgende acties uit:

- Inlezen van technische stemmen en versleuteling naar de referentiewaarde zoals dat wordt gebruikt in het referentiebestand; deze lijst met technische stemmen en hun referentiewaarde wordt gepubliceerd op internet;

---

[5] De concept-AO vermeldt dat een nieuw referentiebestand wordt gegenereerd op basis van de informatie over het uitgeven van vervangende stembescheiden ná afloop van de stemming. Tijdens de interviews is echter gebleken dat deze actie plaats vindt vóór de start van de stemming en hiervan zijn wij in de risico-analyse uitgegaan.

- Teststemmen zijn in het referentiebestand opgenomen met de statusinformatie: "vervangend = 1", "verstrekt = 0", en "vervallen = 1"; op basis van deze informatie herkent de Tally-software deze stemmen als teststemmen en worden de stemmen **niet** meegenomen in de uitslag van de stemming;
- Uitvoeren telling en produceren overzicht waarop ondermeer is aangegeven hoeveel teststemmen er zijn uitgebracht.

Vervolgens worden de resultaten van de telling overgedragen aan het stembureau dat op basis van deze gegevens het proces-verbaal kan opmaken.