Algemeen beveiligingsplan
Kiezen op Afstand

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Versie 1.0

Status definitief

november 2006

INHOUDSOPGAVE

1. Inleiding 1

2. Beveiligingseisen Kiezen op Afstand 2

2.1 Stemdienst Kiezen op Afstand 2

2.2 Stemsysteem 3

2.3 Beveiligingsdoelstelling 4

2.4 Eisen stemdienst 4

2.4.1 Waarborgen 4

2.4.2 Aanbevelingen Raad van Europa 5

2.5 Uitwerking wettelijke waarborgen 6

2.5.1 Stemgeheim 6

2.5.2 Uniciteit 6

2.5.3 Kiesgerechtigdheid 7

2.5.4 Integriteit 7

2.5.5 Controleerbaarheid 7

2.5.6 Hertelbaarheid 8

2.5.7 Toegankelijkheid 8

2.5.8 Transparantie 8

3. Beveiligingsorganisatie 10

3.1 Inleiding 10

3.2 Uitgangspunten 10

3.3 Eindverantwoordelijkheid BZK 11

3.4 Fasen 11

3.5 Functies in de beveiligingsorganisatie 11

3.5.1 Organogram beveiligingsorganisatie 12

3.5.2 Beveiligingsfunctionaris BZK 13

3.5.3 Programmamanagement BZK/KOA 13

3.5.4 Beveiligingspecialist BZK/KOA 14

3.5.5 Ontwikkelaars 15

3.5.6 Beheerders van het stemsysteem 15

3.5.7 Contactpersoon / securitymanager Waterschapshuis 16

3.5.8 Contactpersoon / securitymanager SURFnet 16

3.5.9 Toezichthouder stembureau 17

3.6 Beveiligingsincidenten en escalatie 17

4. Risicoanalyse 18

5. Beveiligingsmaatregelen 19

5.1 Maatregelen proces en organisatie 19
5.1.1 Functiescheiding 19
5.1.2 Beveiligingsorganisatie 20
5.1.3 Productie stembescheiden 20
5.1.4 Sleutelgeneratie en –beheer 21
5.1.5 Toegang documentatie en software stemdienst 21
5.1.6 Vernietigen informatie 22
5.1.7 Beveiligd uitwisselen van informatie 22
5.1.8 Voorlichting en instructie 22
5.1.9 Procedure vervangende stempakketten 22
5.1.10 Registratie alle bevindingen en handelingen 23
5.1.11 Beheerprocedures 23

5.2 Maatregelen stemsysteem 24
5.2.1 Systeemtesten 24
5.2.2 Systeemmaatregelen 24
5.2.3 Maatregelen stemserver 25
5.2.4 Fysieke beveiliging 26
5.2.5 Uitwijk 26

5.3 Maatregelen infrastructuur 27
5.3.1 Fysieke beveiliging 27
5.3.2 Uitwijk 27
5.3.3 Beveiligd netwerk 27

Bijlage A Aanbevelingen Raad van Europa 2004/462a 28

1. Inleiding

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) heeft voor de vervroegde Tweede Kamer verkiezingen in november 2006 een stemdienst laten ontwikkelen ten behoeve van een experiment waarbij de kiesgerechtigden die vanuit het buitenland kunnen stemmen de (aanvullende) mogelijkheid krijgen per internet te stemmen.

Voor dit experiment wordt gebruik gemaakt van een stemsysteem dat in 2004 in opdracht van het Hoogheemraadschap van Rijnland is ontwikkeld en met succes gebruikt is bij de Waterschapsverkiezingen van Rijnland en den Dommel. Het stemsysteem, Rijnland Internet Election System genaamd (RIES), is aangepast om gebruikt te kunnen worden bij een Tweede Kamerverkiezing.

Verkiezingen zijn in Nederland met vele wettelijke waarborgen omgeven die in de Kieswet met de daarbij behorende uitvoeringsregelgeving zijn verankerd. De waarborgen waaraan verkiezingen moeten voldoen gelden onverkort voor de verkiezing waar de stemdienst ingezet zal worden. Gelet op het feit dat de Kieswet thans niet voorziet in het stemmen per internet is daarvoor een aparte wettelijke grondslag gecreëerd middels de Experimentenwet Kiezen op Afstand.

In het voorliggend algemene beveiligingsplan worden de beveiligingseisen ten aanzien van de stemdienst, de beveiligingsorganisatie, risicoanalyse en de beveiligingsmaatregelen beschreven van het experiment Kiezen op Afstand 2006.

2. Beveiligingseisen Kiezen op Afstand

2.1 Stemdienst Kiezen op Afstand

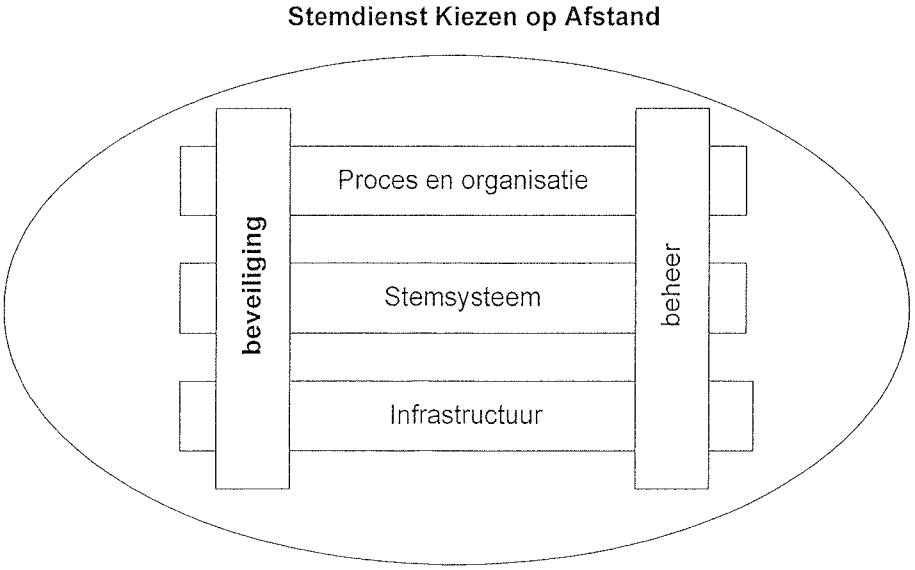
De stemdienst wordt door het Ministerie van BZK als dienst afgenomen van het Waterschapshuis. Het Waterschapshuis is de gemeenschappelijke ICT uitvoeringsorganisatie van de Waterschappen. Met het Waterschapshuis (en het hoogheemraadschap van Rijnland als octrooihouder) is hiertoe een samenwerkingsconvenant gesloten. Voor de uitvoering maakt het Waterschapshuis gebruik van externe partijen, waaronder de ontwikkelaars van het stemsysteem en SURFnet.

Als onderdeel van het samenwerkingsconvenant tussen het Ministerie van BZK en het Waterschapshuis is een Service Level Agreement opgesteld waarin de kwaliteitsnormen voor de dienstverlening zijn vastgelegd. In de Service Level Agreement is verwezen naar een gedetailleerde AO-beschrijving.

De volledige stemdienst Kiezen op Afstand bestaat uit drie domeinen. Dit zijn de domeinen:

1. Proces en organisatie;
2. Stemsysteem (RIES);
3. Infrastructuur.

Beveiliging maakt een integraal deel uit van de stemdienst en komt dan ook terug in alle drie de domeinen.



Figuur 1: Stemdienst schematisch

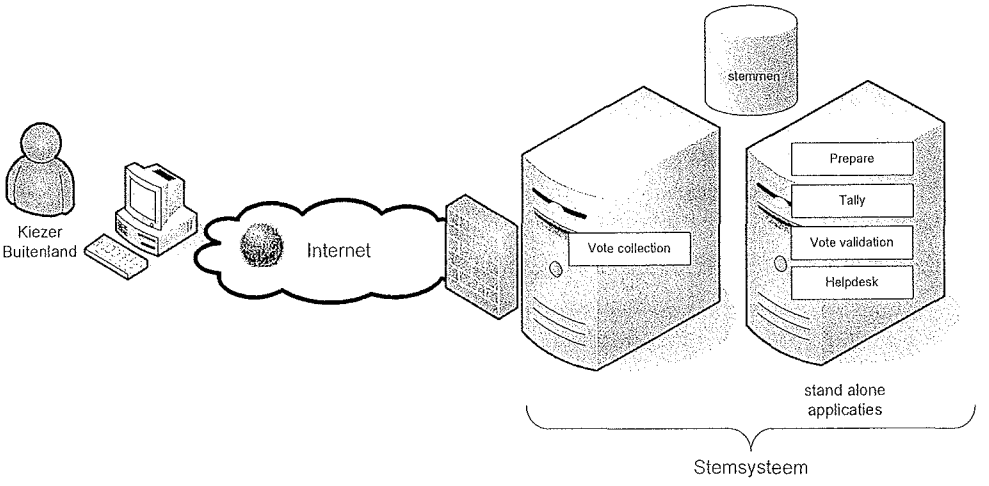
2.2 *Stemsysteem*

Het stemsysteem is intern opgedeeld in de volgende vijf delen:

1. Voorbereiding (prepare);
2. Stemvenster (vote collection);
3. Stemopname (tally);
4. Stemcontrole (vote validation);
5. Helpdesk.

De applicaties voorbereiding, stemvenster, stemcontrole en Helpdesk zijn stand alone applicaties, welke niet verbonden zijn aan het Internet.

Het stemsysteem is schematisch weergegeven in onderstaande figuur 2.



Figuur 2: Stemsysteem schematisch

2.3 Beveiligingsdoelstelling

De beveiligingsdoelstelling voor het experiment Kiezen Op Afstand is het waarborgen van de betrouwbaarheid van de stemdienst en daarmee de integriteit van de verkiezing.

2.4 Eisen stemdienst

2.4.1 Waarborgen

De stemdienst dient te voldoen aan de volgende wettelijke waarborgen zoals die voortvloeien uit de kieswet, het kiesbesluit, de Experimentenwet Kiezen op Afstand, het experimentenbesluit Kiezen op afstand en alle ministeriële regelgeving.

1. Stemgeheim: het moet onmogelijk zijn om een verband te leggen tussen een kiezer en een uitgebrachte stem;
2. Uniciteit: iedere kiesgerechtigde mag precies één stem uitbrengen, welke precies één keer meegeteld moet worden bij de stemopneming;
3. Kiesgerechtigdheid: alleen stemmen van kiesgerechtigde personen mogen worden verwerkt;
4. Integriteit: de stemdienst (systeem in brede betekenis, dus met inbegrip van de organisatorische en procedurele aspecten, stemsysteem en technische infrastructuur) dient correct te werken en de uitkomst mag niet beïnvloedbaar zijn anders dan door het uitbrengen van rechtmatige stemmen;
5. Controleerbaarheid: de controleerbaarheid wordt ondermeer bepaald door het genereren van de verantwoordingsinformatie die wettelijk is voorgeschreven;
6. Hertelbaarheid: conform de wettelijke vereisten dient het mogelijk te zijn de uitgebrachte stemmen opnieuw te tellen.
7. Toegankelijkheid: kiesgerechtigden moeten zoveel mogelijk in staat worden gesteld om deel te nemen aan het verkiezingsproces;
8. Transparantie: de kiezer moet het stemproces kunnen begrijpen en vertrouwen

2.4.2 Aanbevelingen Raad van Europa

Naast de wettelijke waarborgen in de kieswet zijn de 112 aanbevelingen van de Raad van Europa voor "e-voting" 2004/462a voor Kiezen op Afstand als leidraad gehanteerd. Over het overgrote deel voldoet Kiezen op Afstand aan deze aanbevelingen. In het document "Compliance to requirements of CoE" heeft het Ministerie van BZK zich verantwoord over waar de stemdienst niet voldoet aan de aanbevelingen van de Raad van Europa.

De Raad van Europa heeft aanbevelingen opgesteld ten aanzien van:

1. Wettelijke standaarden;
2. Operationele standaarden;
3. Techniek.

De aanbevelingen van de Raad van Europa zijn bijgevoegd in Bijlage A.

2.5 Uitwerking wettelijke waarborgen

In de hierna volgende paragrafen worden de wettelijke waarborgen ten aanzien van de stemdienst nader uitgewerkt. Voor iedere waarborg wordt op hoofdlijnen aangegeven op welke wijze de stemdienst Kiezen op Afstand hieraan voldoet. De beveiligingsmaatregelen worden meer in detail beschreven in hoofdstuk 5.

2.5.1 Stemgeheim

Het moet onmogelijk zijn om een verband te leggen tussen een kiezer en een uitgebrachte stem. De gegevens die nodig zijn voor het uitbrengen van een stem bestaan uit twee delen: de identificerende gegevens van de kiezer en de kandidaat waarop hij zijn stem wil uitbrengen. De identificerende gegevens worden gebruikt om de kiesgerechtigdheid te controleren aan de hand van een kiezerregister en om in dit register vast te leggen dat de kiezer gestemd heeft; de stem dient gedeponeerd te worden in het elektronische equivalent van de stembus.
Het KoA systeem dient dus zo te worden opgezet dat de uitgebrachte stem en de persoonsgegeven niet meer te reconstrueren valt.

De kiezer is in de stemdienst alleen bekend onder een uniek en anoniem nummer. De generatie van deze nummers wordt door een van BZK onafhankelijke derde partij gedaan in een 'gesloten' proces. De identificatie van de kiezer gaat via een stemcode, welke in datzelfde proces is gegenereerd. De stemcode wordt per post toegezonden en wordt vervolgens gebruikt om de stem te versleutelen. De stem wordt via Internet verzonden via een versleutelde verbinding. De stemdienst bepaalt zonder de persoonsgegevens van de kiezer of de stem komt van een vooraf als kiesgerechtigd aangemerkte kiezer. Het ministerie van BZK ziet expliciet toe op de productie van de stembescheiden. Verder zijn aanvullende maatregelen genomen om te voorkomen dat de stemdienst gegevens vasthoud waaruit direct of indirect de identiteit van de kiezer uit kan worden afgeleid.

2.5.2 Uniciteit

Iedere kiesgerechtigde mag precies één geldige stem uitbrengen, welke precies één keer meegeteld moet worden bij de stemopneming.

Voordat de stemperiode begint krijgt iedere kiezer een unieke stemcode waarmee de kiezer zijn stem kan uitbrengen. De stemdienst controleert voorafgaand aan het uitbrengen van een stem of een kiezer reeds eerder gestemd heeft. Als dit het geval is geeft de stemdienst hiervan een signalering. De kiezer kan vervolgens toch zijn stem (nogmaals) uitbrengen.

De stemdienst is zo ontworpen dat mochten er toch meerdere stemmen binnenkomen van één kiezer, er volgens de in de Experimentenbesluit vastgelegde telregels achteraf wordt bepaald welke stemmen geldig zijn. Als een kiezer – al dat niet bewust – twee keer stemt en dezelfde stem uitbrengt wordt deze slechts eenmaal als geldige stem meegeteld. Als een kiezer twee maal verschillend stemt wordt de stem ongeldig verklaard en niet meegeteld in de uitslag. Er wordt niet geteld tijdens de stemperiode; tellen is een aparte proces dat na sluiten van de stemming plaats vindt.

2.5.3 *Kiesgerechtigdheid*

Alleen stemmen van kiesgerechtigde personen mogen worden verwerkt.
Deze waarborg draait om de identificatie van kiezers. De stemdienst gaat er van uit dat de kiezer wordt geïdentificeerd met een stemcode die door de stemdienst wordt toegekend.

Of een kiezer kiesgerechtigd is wordt vastgesteld door de gemeente Den Haag. Middels procedures wordt zeker gesteld dat alleen aan deze kiezers een stemcode wordt verzonden. De stemcode is dusdanig ontworpen dat de kans op het raden van een geldige stemcode en vervolgens deponeren van een geldige stem zeer klein is (1 op 2^{56}).

2.5.4 *Integriteit*

Het stemsysteem (systeem in brede betekenis, dus met inbegrip van de organisatorische en procedurele aspecten) dient correct te werken en de uitkomst mag niet beïnvloedbaar zijn anders dan door het uitbrengen van rechtmatige stemmen.

Deze eis noemt twee belangrijke aspecten van de stemdienst: correcte werking en de onmogelijkheid om de stemdienst onrechtmatig te beïnvloeden.
Correcte werking is afhankelijk van meerdere factoren: correct functioneren van de stemdienst, correcte werking van de infrastructuur, een correcte bediening van het stemsysteem en naleving van de procedures. De correcte werking kan vooral worden aangetoond door intensief testen.

Het niet onrechtmatig beïnvloedbaar zijn van de stemming kan weer onderscheiden worden in twee aspecten: verdediging tegen aanvallen van buitenaf en tegen aantasting van de integriteit van binnen uit. Het bijzondere karakter van de stemdienst vereist wel dat er ook regelmatig wordt gecontroleerd of de maatregelen effectief zijn. Dit wordt geborgd door een combinatie van technische en organisatorische maatregelen. Aantasting van de integriteit van binnenuit wordt voorkomen door de opzet van de organisatie en door technische maatregelen.

De integriteit van de stemdienst hangt overigens niet alleen af van de functionele opzet van de stemdienst, maar ook van de integriteit van het personeel. De integriteit van de stemdienst zal daarom aanvullend met organisatorische en procedurele maatregelen worden bewaakt. De medewerkers van het Waterschapshuis en SURFnet die een uitvoerende (beheer)taak hebben bij de verkiezing worden door de AIVD op B-niveau gescreend.

2.5.5 *Controleerbaarheid*

De controleerbaarheid wordt ondermeer bepaald door het genereren van de verantwoordingsinformatie die wettelijk is voorgeschreven.

Daarnaast is als uitgangspunt gehanteerd dat het systeem gedetailleerd moeten vastleggen welke handelingen er op de stemdienst worden uitgevoerd door het stembureau, door medewerkers van de stemdienst en door de kiezers (met als randvoorwaarde uiteraard dat deze vastleggingen het stemgeheim niet in gevaar mag brengen). De stemdienst biedt aan de kiezer en aan derden vergaande controle-

mogelijkheden om te bepalen of de stemmen zijn ontvangen en of de stemmen juist zijn geteld.

2.5.6 Hertelbaarheid

Conform de wettelijke vereisten dient het mogelijk te zijn de uitgebrachte stemmen opnieuw te tellen. Het bestand met de ontvangen stemmen is beschikbaar om later gebruikt te worden bij een hertelling.

Bij het experiment Kiezen op Afstand wordt achteraf het volledig stembestand en een referentiebestand openbaar gemaakt, waardoor iedere burger – met enige inspanning – een telling en een controle op de telling kan uitvoeren. De Radbout Universiteit zal onafhankelijk van het stembureau ook een telling uitvoeren met behulp van het stembestand en het referentiebestand.

2.5.7 Toegankelijkheid

Kiesgerechtigden moeten zoveel mogelijk in staat worden gesteld om deel te nemen aan het verkiezingsproces. Deze eis is zo geïnterpreteerd dat de manier waarop de stemdienst wordt opgezet geen technische belemmeringen mag opwerpen voor de kiezers. Om deze reden heeft het Ministerie van BZK gekozen om de stemdienst te baseren op standaard webbrowsertechnolgie. De stemdienst is zondanig ontworpen dat hij werkt met een de meeste gebruikte webbrowsers. Hierdoor kan de webapplicatie gebruikt kan worden op vrijwel iedere computer met Internettoegang.

Een tweede aspect van toegankelijkheid is dat de stemdienst vriendelijk in het gebruik en laagdrempelig is. Hiermee is vanaf het begin in het ontwerp van het stemsysteem rekening mee gehouden. Het stemsysteem voldoet zo ver mogelijk aan de door de overheid opgestelde webrichtlijnen[1].Vanwege de strenge (beveiligings-)eisen die gesteld worden aan een stemdienst, kan de huidige stemdienst niet aan alle webrichtlijnen voldoen.

2.5.8 Transparantie

De kiezer moet het stemproces kunnen begrijpen en vertrouwen.Voor de individuele kiezer leidt dit tot eisen aan de gebruikersinterface, die eenvoudig en eenduidig moet zijn en aan moet sluiten bij het stemproces waarmee hij vertrouwd is. Het stemsysteem moet dusdanig transparant zijn dat de kiezer de werking van het stemproces goed begrijpt. Experts die zich met elektronisch stemmen bezighouden moeten toegang hebben tot uitgebreidere informatie. Op basis hiervan zijn zij in staat om zich een oordeel te vormen over de transparantie van de stemdienst.

Het stemsysteem is zodanig ontworpen dat kiezers zelf kunnen controleren of hun stem is ontvangen en juist is meegenomen. Deze controle kan door iedereen, dus expliciet ook door de kiezer, en geheel met openbaar beschikbare middelen en functies plaatsvinden. Gecontroleerd kan worden:

- Of er een plausibel verband is tussen het aantal kiesgerechtigden en de gepubliceerde referentie-informatie;

[1] De webrichtlijnen zijn, bij Ministerieel besluit van 30 juni 2006, sinds 1 september 2006 verplicht voor alle nieuwe overheidsinternetsites.

- Of de stemcode van de kiezer inderdaad leidt tot een stem van zijn keuze, gegeven de informatie in de gepubliceerde referentiebestanden;
- Of er ongeautoriseerde wijzigingen zijn aangebracht in de gepubliceerde bestanden;
- Of de eigen (unieke technische) stem van de kiezer is opgenomen in de gepubliceerde ontvangen (unieke technische) stemmen en dus is meegeteld in de uitslag;
- Welke stemmen als ongeldig zijn aangemerkt;
- Of de totaal tellingen juist zijn;
- Of de stemmen aan de juiste kandidaat zijn toegewezen;
- Of een stem door een kiezer tijdig is ingeleverd en ontvangen. Hiertoe wordt de ontvangstbevestiging door de onafhankelijke Scheidsrechter gecontroleerd.

De helpdesk opent na de stemming een speciaal voor dit doel opgezette website (www.internetstembureau.nl/stemcontrole) waar kiezers en anderen de benodigde documenten kunnen vinden om de stemcontrole uit te voeren. Op deze website wordt uitgelegd hoe de stemcontrole werkt en hoe te handelen bij een geconstateerd probleem.

3. Beveiligingsorganisatie

3.1 Inleiding

Voor het programma Kiezen op Afstand is een beveiligingsorganisatie ingericht die de taak heeft om de beveiligingsmaatregelen te ontwerpen, de maatregelen hetzij zelf te implementeren hetzij toe te zien op de implementatie door derden en daarnaast de taak heeft om toe te zien op de naleving van de maatregelen. In dit hoofdstuk wordt deze beveiligingsorganisatie gedefinieerd.

3.2 Uitgangspunten

Voor het ontwerpen, implementeren en beheren van de beveiligingsmaatregelen is een beveiligingsorganisatie noodzakelijk. Het Ministerie van BZK heeft een beveiligingsorganisatie voorzien die voldoet aan de hierna volgende uitgangspunten.

3.2.1.1 Functiescheiding

De beveiligingsorganisatie moet zodanig worden ingericht dat er sprake is van voldoende functiescheiding. Deze functiescheiding is zodanig dat één functionaris niet in staat kan zijn om één van de waarborgen in gevaar te brengen.
Bevoegdheden worden zodanig toebedeeld dat elke persoon alleen de strikt noodzakelijke bevoegdheden verkrijgt. Het Ministerie van BZK gaat uit van een strikte functiescheiding waarbij precies is gedefinieerd welke rollen er worden gedefinieerd, welk taken en bevoegdheden zijn gekoppeld aan een rol, en welke rollen aan welke personen zijn toebedeeld.

3.2.1.2 Integriteit

De personen die betrokken zijn bij het ontwerpen van de stemdienst, bij het implementeren van het ontwerp en bij het beheren daarvan dienen integer te zijn. Dat wordt onder meer geconcretiseerd door AIVD-screaning te laten doen en door het ondertekenen van geheimhoudingsverklaringen. De personen die handelingen kunnen verrichten op de stemdienst worden bij besluit van de minister voor Bestuurlijke Vernieuwing en Koninkrijksrelaties aangewezen.

3.2.1.3 Vier-ogen principe

Het zogenaamde vier-ogenprincipe wordt toegepast om te verzekeren dat personen die op grond van hun rol bepaalde bevoegdheden hebben daar geen misbruik van maken.

3.3 Eindverantwoordelijkheid BZK

In de beveiligingsorganisatie is het Ministerie van BZK eindverantwoordelijk. In de beveiligingsorganisatie worden functieprofielen opgesteld. Voor elk van deze functieprofielen zijn de verantwoordelijkheden, taken en bevoegdheden vastgelegd voor de verschillende fasen van het project.

3.4 Fasen

Er wordt onderscheid gemaakt naar vier fasen:

1. **Ontwikkeling**. In deze fase wordt de stemdienst ontworpen, gebouwd en getest. Deze fase is gestart bij aanvang van het project en loopt tot de fase voorbereiding.
2. **Voorbereiding**. In deze fase worden de voorbereidende handelingen getroffen om de stemdienst in operationele status te brengen. Deze fase eindigt zodra de finale schouw is afgerond. De stemdienst-applicatie is dan in de status 'voorbereiding' gebracht.
3. **Stemperiode**. In deze fase is de stemdienst inclusief haar organisatie operationeel. De stemperiode start zodra het stembureau de stemming opent en eindigt zodra het stembureau de stemming sluit.
4. **Na stemming**. Deze fase start vanaf het moment dat de stemming gesloten is en eindigt op een nader te bepalen tijdstip.

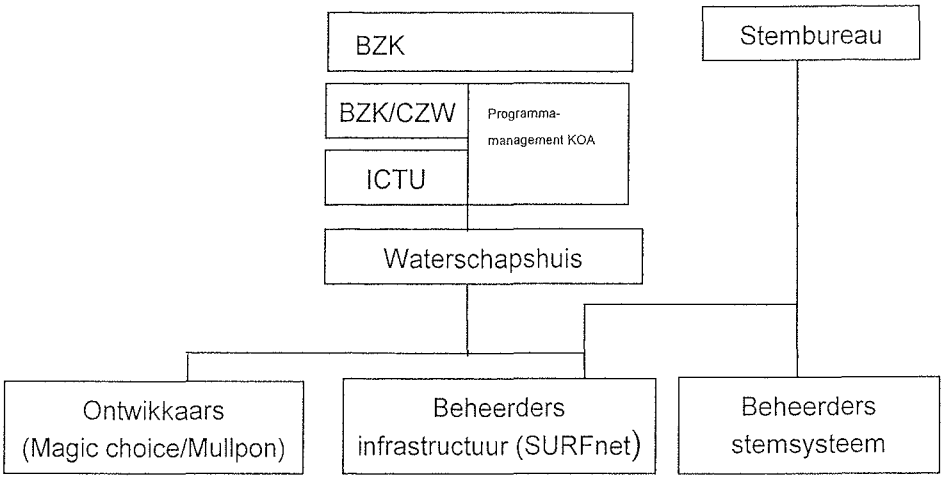
3.5 Functies in de beveiligingsorganisatie

In de beveiligingsorganisatie worden de volgende acht functies onderscheiden:

1. Beveiligingsfunctionaris BZK;
2. Programmamanagement BZK/KOA;
3. Beveiligingsspecialist BZK/KOA;
4. Ontwikkelaars stemsysteem Mullpon/Magic choice;
5. Beheerders van het stemsysteem;
6. Contactpersoon / Security manager Waterschap;
7. Contactpersoon / Security manager SURFnet;
8. Toezichthouder namens stembureau.

De verantwoordelijkheden, taken en bevoegdheden van de verschillende beveiligingsfuncties worden in de hierna volgende paragrafen nader beschreven. Hierbij wordt opgemerkt dat uitsluitend de beveiligingsgerelateerde taken zijn opgenomen. Voor een volledig overzicht van de verantwoordelijkheden, taken en bevoegdheden van alle betrokkenen wordt verwezen naar de door BZK/KOA opstelde AO-beschrijving.

3.5.1 Organogram beveiligingsorganisatie



De Gemeente Den Haag registreert de kiesgerechtigden voor het Kiezen op Afstand en bepaalt de kiesgerechtigheid. Het programma Kiezen op Afstand heeft hiertoe een convenant gesloten waarin de wederzijdse verantwoordelijkheden, taken en bevoegdheden staan beschreven. De Gemeente Den Haag maakt geen onderdeel uit van de beveiligingsorganisatie.

Het Print Service Bureau heeft een uitvoerende taak in het stemproces in het kader van het printen van de stembescheiden. Zij wordt aangestuurd door het programmamanagement KOA die als taak heeft toezicht te houden op de geleverde diensten. Het Print Service Bureau maakt geen deel uit van de beveiligingsorganisatie.

Het stembureau opereert volledig onafhankelijk en heeft een zeer belangrijke rol in de beveiligingsorganisatie. Het stembureau houdt toezicht op het volledige stemproces en de juiste werking van de stemdienst. Gesignaleerde beveiligingsincidenten moeten bij het stembureau worden gemeld, waarna het stembureau besluit over te nemen maatregelen.

3.5.2 *Beveiligingsfunctionaris BZK*

Deze functie is onverenigbaar met andere functies.

Verantwoordelijkheid

- Eindverantwoordelijk voor de algehele beveiliging van Kiezen op Afstand

Taken

In onderstaande tabel is weergegeven in welke fase welke taak uitgevoerd moet worden (aangegeven met JA).

	Ontwikkeling	Voorbereidin	Stemperiode	Na stemming
Toezien op alle handelingen van de securitymanagers	Ja	Ja	Ja	Ja
Rapporteren aan de minister en stembureau in geval van beveiligingsincidenten	Ja	Ja	Ja	Ja
Goedkeuren beveiligingsorganisatie		Ja		

Bevoegdheden

- Bepalen welke personen in beheer- en beveiligingsorganisatie mogen plaatsnemen;
- Ontnemen van autorisaties aan personen in de beheer- en beveiligingsorganisatie;
- Geven van aanwijzingen t.a.v. beveiligingsmaatregelen;
- Inzage recht in logboeken, logfiles en systemen.

3.5.3 *Programmamanagement BZK/KOA*

Verantwoordelijkheid

- Verantwoordelijk voor inrichting en werking van de beveiligingsorganisatie Kiezen op Afstand;
- Verantwoordelijk voor werking beveiligingsmaatregelen Kiezen op Afstand;
- Verantwoordelijk voor sleutelbeheer Kiezen op Afstand.

Taken

In onderstaande tabel is weergegeven in welke fase welke taak uitgevoerd moet worden (aangegeven met JA).

	Ontwikkeling	Voorbereidin	Stemperiode	Na stemming
Opstellen beveiligingsplan	Ja			
Uitvoeren risicoanalyse stemdienst	Ja			
Testen en eindschouw stemsysteem	Ja	Ja		
Goedkeuren van configuratie stemdienst en configuratie bevriezen		Ja	Ja	Ja

Opstellen instructies / aanwijzing en aan de partijen over te nemen beveiligingsmaatregelen	Ja	Ja	Ja	Ja
Rapporteren aan beveiligingsfunctionaris BZK in geval van beveiligingsincidenten	Ja	Ja	Ja	Ja
Aanmelden personen voor antecedentenonderzoek AIVD				
Opdracht geven voor beveiligingsonderzoeken stemsysteem	Ja			
Inhoudelijke controle aangeleverde lijsten met KOA-kiezers door Gemeenten Den Haag		Ja		
Beheer vervangende stempakketten		Ja	Ja	Ja
Toezien op Print Service Bureau dat stembiljetten print		Ja		
Toezien dat Print Service Bureau informatie vernietigd		Ja		
Toezien op veilig versturen van registratielijsten kiezers (k10) van gemeente Den Haag naar BZK/KOA		Ja		
Toezien op veilig versturen van registratielijsten kiezers (k10) van BZK/KOA naar beheerders van het stemsysteem		Ja		
Sleutelbeheer Kiezen op Afstand		Ja	Ja	Ja
Toezien dat beheerders van het stemsysteem op de juiste wijze de stemcodes genereert		Ja	Ja	
Toezien dat stemcodelijst (c10) op een veilige manier wordt verstuurd naar Print Service Bureau		Ja	Ja	

Bevoegdheden

- Besluiten over wel/niet implementeren van aanbevelingen die door leveranciers en adviseurs worden gedaan.
- Ontnemen van autorisaties aan personen in de beheer- en beveiligingsorganisatie;
- Geven van aanwijzingen t.a.v. beveiligingsmaatregelen;
- Inzage recht in logboeken, logfiles en systemen.

3.5.4 Beveiligingspecialist BZK/KOA

Taken

In onderstaande tabel is weergegeven in welke fase welke taak uitgevoerd moet worden (aangegeven met JA).

	Ontwikkeling	Voorbereidin	Stemperiode	Na stemming
Adviseren programmamanagement BZK/KOA	Ja	Ja	Ja	Ja
Toezien op werking beveiligingsmaatregelen en risico's signaleren	Ja	Ja	Ja	Ja
Incidenten rapporteren aan programmamanagement BZK/KOA	Ja	Ja	Ja	Ja
Operationeel contact met beveiligingsfunctionarissen			Ja	

overige partijen				

3.5.5 *Ontwikkelaars*

Verantwoordelijkheid

- Voor implementeren van beveiligingsmaatregelen in het stemsysteem

Taken

In onderstaande tabel is weergegeven in welke fase welke taak uitgevoerd moet worden (aangegeven met JA).

	Ontwikkeling	Voorbereidin	Stemperiode	Na stemming
Beveiligingsmaatregelen op de juiste wijze implementeren in het stemsysteem	Ja			
Risico's signaleren en rapporteren tijdens ontwikkeling stemsysteem	Ja			

3.5.6 *Beheerders van het stemsysteem*

Verantwoordelijkheid

- Verantwoordelijk voor operationele bediening van het stemsysteem gedurende Kiezen op Afstand

Taken

In onderstaande tabel is weergegeven in welke fase welke taak uitgevoerd moet worden (aangegeven met JA).

	Ontwikkeling	Voorbereidin	Stemperiode	Na stemming
Sleutels aanmaken samen met Ministerie van BZK		Ja		
Rapporteren aan stembureau in geval van beveiligingsincidenten			Ja	
Beveiligingsmaatregelen nemen in opdracht van stembureau			Ja	
Stemsysteem 24 uur per dag monitoren			Ja	

Bevoegdheden

Tijdens de stemperiode hebben de beheerders van het stemsysteem geen bevoegdheden. Zij werken volledig in opdracht van het stembureau.

3.5.7 *Contactpersoon / securitymanager Waterschapshuis*

Verantwoordelijkheid

- Verantwoordelijk voor operationele beveiliging van het stemsysteem voor Kiezen op Afstand

Taken

In onderstaande tabel is weergegeven in welke fase welke taak uitgevoerd moet worden (aangegeven met JA).

	Ontwikkeling	Voorbereidin	Stemperiode	Na stemming
Rapporteren programmamanagement ICTU/KOA in geval van beveiligingsincidenten	Ja	Ja		Ja
Rapporteren aan stembureau in geval van beveiligingsincidenten			Ja	
Contactpersoon SURFnet	Ja	Ja	Ja	Ja
Toezicht houden op handelingen SURFnet	Ja	Ja	Ja	Ja

3.5.8 *Contactpersoon / securitymanager SURFnet*

Verantwoordelijkheid

- Verantwoordelijk voor de technische en fysieke beveiliging van de infrastructuur voor Kiezen op Afstand

Taken

In onderstaande tabel is weergegeven in welke fase welke taak uitgevoerd moet worden (aangegeven met JA).

	Ontwikkeling	Voorbereidin	Stemperiode	Na stemming
Rapporteren securitymanager Waterschapshuis in geval van beveiligingsincidenten	Ja	Ja		Ja
Rapporteren aan stembureau in geval van beveiligingsincidenten			Ja	
Adviseren over beveiliging infrastructuur in geval van beveiligingsincidenten	Ja	Ja	Ja	Ja
Implementeren van infrastructurele beveiligingsmaatregelen	Ja	Ja	Ja	Ja
Implementeren fysieke beveiligingsmaatregelen lokaties Kiezen op Afstand	Ja	Ja	Ja	Ja
Opstellen calamiteitenplan infrastructuur	Ja			

Bevoegdheden
Tijdens de stemperiode heeft SURFnet geen bevoegdheden. Zij werkt volledig in opdracht van het stembureau.

3.5.9 Toezichthouder stembureau

Verantwoordelijkheid
- Verantwoordelijk voor het juist verloop van de verkiezingen Kiezen op Afstand

Taken
In onderstaande tabel is weergegeven in welke fase welke taak uitgevoerd moet worden (aangegeven met JA).

	Ontwikkeling	Voorbereidin	Stemperiode	Na stemming
Toezien op een veilige werken Kiezen op Afstand			Ja	
Toezien op het gebruik/misbruik van teststemmen			Ja	
Maatregelen nemen in geval van beveiligingsincidenten tijdens stemming			Ja	
Indien noodzakelijk: rapporteren van beveiligingsincidenten aan Minister			Ja	

3.6 Beveiligingsincidenten en escalatie

In geval van beveiligingsincidenten treedt een escalatieprocedure in werking. Deze procedure staat nader beschreven in de door het Ministerie van BZK opgestelde AO-procedure.

4. Risicoanalyse

In het kader van het experiment Kiezen op Afstand 2006 is door het Ministerie van Binnenlandse Zaken een uitgebreide risicoanalyse uitgevoerd. Het doel van de risicoanalyse was de belangrijkste risico's van de stemdienst in kaart brengen. Voor het inventariseren en rangschikken van de risico's is gebruik gemaakt van meerdere invalshoeken. De gehanteerde invalshoeken zijn:

- Risico's per processtap van de stemdienst;
- Politiek-bestuurlijke risico's;
- Organisatorische risico's;
- Juridische risico's;
- Technische / Operationele risico's.

Voor elk risico is de waarschijnlijkheid van het optreden ingeschat en zijn mogelijke (preventieve en correctieve) maatregelen benoemd. Voor de risico's wordt inhoudelijk verwezen naar de risicoanalyse Kiezen op Afstand. Op basis van deze risicoanalyse zijn de beveiligingsmaatregelen genomen die beschreven zijn in hoofdstuk 5 van dit algemeen beveiligingsplan Kiezen op Afstand.

5. Beveiligingsmaatregelen

Dit hoofdstuk beschrijft op hoofdlijnen de beveiligingsmaatregelen die zijn genomen bij het experiment Kiezen op Afstand. De maatregelen zijn geclusterd naar de in hoofdstuk 2 beschreven drie dimensies, proces & organisatie, stemsysteem en infrastructuur.

5.1 Maatregelen proces en organisatie

Het volledige verloop van het stemproces is gedetailleerd beschreven in de AO-procedure. In deze paragraaf worden de relevante beveiligingsmaatregelen op hoofdlijnen beschreven.

5.1.1 Functiescheiding

Binnen het gehele stemproces is bijzondere aandacht voor functiescheiding. Dit komt tot uitdrukking in de volgende maatregelen:

- Voor de generatie van de sleutels voor de stemdienst zijn verschillende partijen betrokken. Iedere partij heeft een eigen deel van de sleutel. Zie voor een nadere toelichting paragraaf 5.1.3 over sleutelbeheer.
- De generatie van de stemcodes gebeurt door een andere organisatie dan het Ministerie van Binnenlandse zaken, om zo te voorkomen dat BZK een relatie kan leggen tussen kiezers en de stemcodes.
- Voor de stemming wordt er een onafhankelijk orgaan ingesteld (stembureau) die toezicht houdt op het verloop van de stemming.
- Het technisch beheer op de infrastructuur wordt uitgevoerd door een andere organisatie dan de bediening van het stemsysteem.
- Binnen het stemproces is een uitgebreide AO-beschrijving opgesteld waarin gedetailleerd staat beschreven welke verantwoordelijkheden, taken en bevoegdheden de verschillende actoren hebben in het stemproces.
- De notaris houdt een aantal specifieke documenten en sleutelmateriaal in depot.
- Er is een scheidsrechter (onafhankelijke deskundige) die bevoegd is om een oordeel te vellen over ingediende bezwaarschriften van kiezers. De scheidsrechter voert bij een klacht een feitenonderzoek uit. Op basis van zijn bevindingen brengt de scheidsrechter advies uit aan het Centraal stembureau.

De ontwikkelorganisatie en de beheerders die het stemsysteem tijdens de stemperiode bedienen staan beiden onder contract van het Waterschaphuis. De ontwikkelorganisatie en de beheerders bestaan uit dezelfde personen. Dit is vanuit functiescheiding perspectief in principe niet gewenst. Gezien de vervroeging van de verkiezingen van mei 2007 naar november 2006 was het niet meer mogelijk een andere organisatie op te leiden om het stemsysteem tijdens de stemperiode te bedienen. Om het risico van belangenverstrengeling of fraudeleus handelen te verkleinen is een aantal aanvullende maatregelen genomen:

1) De personen die handelingen kunnen verrichten op de stemdienst worden bij besluit van de minister voor Bestuurlijke Vernieuwing en Koninkrijksrelaties aangewezen.
2) De ontwikkelaars en beheerders van de stemdienst ondergaan een veiligheidsonderzoek;
3) 24 uurs toezicht op het handelen door het stembureau, waarbij het stembureau wordt bijgestaan door een adviesteam met deskundigheid op het vlak van ICT, de stemdienst en het kiesrecht.;
4) Het "bevriezen" van het stemsysteem na acceptatie;
5) Een broncode onderzoek door een onafhankelijke instantie om na te gaan of de stemdienst ongewenste functionaliteit bevat;
6) De ontwikkelaars na acceptatie geen mogelijkheden meer geven het systeem te wijzigen;
7) Controle bij het starten van de stemdienst of het stemsysteem gelijk is aan het systeem dat "bevroren" is na acceptatie.
8) Het gebruik van test validatietransacties gedurende de stemperiode mag alleen plaatsvinden na instemming van het stembureau

5.1.2 Beveiligingsorganisatie

Alle beveiligingsfuncties met bijbehorende verantwoordelijkheden, taken en bevoegdheden zijn vastgelegd. In de beveiligingsorganisatie zijn de rapportagelijnen beschreven in geval van calamiteiten en beveiligingsincidenten. Alle personen die betrokken zijn bij de stemdienst hebben een geheimhoudingsverklaring getekend. Voor een overzicht van de beveiligingsorganisatie wordt verwezen naar hoofdstuk 4 Beveiligingsorganisatie.

5.1.3 Productie stembescheiden

De productie van de stembescheiden wordt uitgevoerd door het Print Service Bureau. Alvorens over te gaan tot het drukken en personaliseren van de stembescheiden doet het Print Service bureau een totaalcontrole. De stembescheiden bestaan uit een vensterenvelop, een brief (tevens adresdrager), een stemkaart met stemcode en een handleiding. Op de stemkaart wordt een barcode gedrukt die correspondeert met een adres van een kiezer. De stemcodes zitten in een speciale envelop, waardoor de stemcode niet vanaf de buitenkant van de envelop is te lezen en altijd zichtbaar is wanneer de envelop is opengemaakt door derden.

De juiste stemkaart wordt vervolgens automatisch bij de juiste brief gevoegd. Ter controle wordt er om de 100 kiezers een test-stembescheidenpakket geproduceerd. Deze worden aan het einde van de productie ter controle opengemaakt. Als bij controle blijkt dat de verkeerde stemkaart bij de verkeerd brief is gevoegd, dan worden alle 99 voorgaande stembescheiden vernietigd en opnieuw geproduceerd.

Het Ministerie van BZK houdt op gezette momenten toezicht op de productie en verzending en controleert of:

- Voor alle kiezers stembescheiden zijn gedrukt;
- Alle stembescheiden tijdig zijn verzonden;
- Al het uitval en afval-materiaal is vernietigd;
- Er geen bestanden zijn achtergebleven bij het Print Service Bureau.

5.1.4 Sleutelgeneratie en –beheer

In het stemsysteem worden drie cryptografische sleutels gebruikt:

- Masterkey; de sleutel voor interne werking van het stemsysteem;
- GenVoterkey; de sleutel waarmee de stemcodes worden gegenereerd;
- Receiptkey; de sleutel waarmee de ontvangstbewijzen worden gegenereerd.

Op de generatie en beheer van de cryptografische sleutels is functiescheiding toegepast. De delen van waaruit de sleutel is gegenereerd is verdeeld over verschillende partijen. In beide gevallen is het een samenstel van twee personen van BZK/KOA en twee beheerders van het stemsysteem.

De Masterkey en de Genvoterkey worden gegenereerd op basis van een tweetal passphrases van het Ministerie van BZK (ieder tussen 16 en 64 karakters lang) en een passphrase van de beheerders van de stemsysteem. De diverse passphrases worden onderling geheim gehouden en bewaard in sealbags. Bij de generatie van de sleutels zijn zowel mensen van BZK/KOA als de beheerders van het stemsysteem aanwezig. De Masterkey wordt uiteindelijk gecontroleerd overgebracht naar het operationele systeem.

Alle (onder)delen van de sleutels worden, voor zover niet in gebruik op het operationele systeem, apart bewaard in sealbags (in een kluis). De kluissleutel is bij een andere functionaris in beheer. Bij gebruik van het sleutelmateriaal wordt dit in het register opgetekend (zowel in de kluis als op de sealbags). Al het sleutelmateriaal wordt steeds simultaan op een tweetal PC's gegenereerd en de uitkomsten worden vergeleken, om eventuele cryptografische fouten uit te sluiten.

De Genvoterkey wordt alleen gebruikt tijdens de voorbereiding van de verkiezingen ten behoeve van het genereren van de stemcodes en het verwerken van de helpdesk mutaties van de vervangende stempakketten.
Alleen tijdens deze momenten wordt de sleutel uit de kluis gehaald en overhandigd aan de beheerders van het stemsysteem. Het gebruikt vindt plaats onder toezicht van BZK/KOA. Na afloop wordt de sleutel weer in een sealbag in de kluis gelegd.

De Genvoterkey wordt onder toezicht van het Ministerie van BZK en de notaris vernietigd voorafgaand aan de verkiezingen, na het sluiten van de helpdesk en het verwerken van de helpdeskmutaties.

De Receiptkey ontstaat tijdens generatie van de Masterkey. Een kopie van de sleutel wordt in beheer gegeven bij de notaris, ten behoeve van eventuele geschillen na afloop van de verkiezingen die door de 'scheidsrechter' moeten worden beoordeeld.

5.1.5 Toegang documentatie en software stemdienst

Vanuit oogpunt van transparantie naar de burger heeft het Ministerie van BZK het beleid om zo veel mogelijk informatie over Kiezen op Afstand openbaar te maken. Alle publieke informatie staat vermeld op de uitgebreide informatiewebsite. Het deel van functionele en technische documentatie dat niet openbaar is gemaakt, is uitsluitend toegankelijk voor geautoriseerde (project)medewerkers van het project Kiezen op Afstand. De stemsoftware die op de server staat is uitsluitend aanwezig in beveiligde

KOA/SURFnet/Waterschap ruimten. De "browsersoftware" op basis van javascript die gebruikers nodig hebben om gebruik te maken van de stemdienst, is op iedere werkplek raadpleegbaar.

5.1.6 Vernietigen informatie

Binnen het proces worden alle elektronische gegevensbestanden en sleutels van de stemdienst die niet meer strikt noodzakelijk zijn binnen het proces onder toezicht van het Ministerie van BZK vernietigd. Dit is onder andere het geval in de volgende situaties:

- De gegenereerde sleutels voor de stemdienst worden vernietigd;
- Na generatie van het bestand C10 (met kiezersgegevens en stemcodes door diegene die de stemdienst bedienen) wordt het bestand via een gecontroleerd transport verzonden naar het Print Service Bureau. Als het bestand lijst goed ontvangen is wordt de lijst bij de beheerders van het stemsysteem vernietigd.
- Na het drukken van de stemcodes door het Print Service Bureau wordt het bestand met kiezers en stemcodes vernietigd;
- Vervangende stempakketten worden als zij niet meer noodzakelijk zijn vernietigd.
- De door de Gemeente Den Haag aangeleverde lijst met kiesgerechtigden wordt na het drukken in depot gegeven bij de notaris en vervolgens vernietigd.

5.1.7 Beveiligd uitwisselen van informatie

Alle informatie die tussen de verschillende partijen wordt uitgewisseld, waaronder het kiezersbestand, stemcodebestand en kandidatenbestand, worden beveiligd uitgewisseld. In geval van fysieke bestanduitwisseling zal gebruik worden gemaakt van speciale "tamper proof" enveloppen die uniek genummerd zijn. Bestanden worden niet elektronisch uitgewisseld.

5.1.8 Voorlichting en instructie

De kiesgerechtigden worden uitgebreid voorgelicht over het gebruik van de stemdienst. Ook worden ze gewezen op risico's en de maatregelen die ze zelf daarbij kunnen nemen. Dit gebeurt zowel via de stemapplicaties, de informatiewebsite als met een gebruikshandleiding. Als kiezers nog aanvullende vragen hebben kunnen ze contact opnemen met de helpdesk.

5.1.9 Procedure vervangende stempakketten

De Helpdesk van het programma Kiezen op Afstand kan aan kiezers vervangende stembescheiden verstrekken als de kiezer deze is kwijtgeraakt of als de kiezer zijn stembescheiden niet per post heeft ontvangen. Omdat het uitreiken van vervangende stembescheiden vanuit beveiligingsperspectief een gevoelig proces is, is hiervoor een uitbreide procedurebeschrijving opgesteld met diverse waarborgen. De helpdesk identificeert de kiezer aan de hand van gegevens die ten tijde van registratie zijn opgegeven en een kopie van het identiteitsbewijs.
De beheerders van het stemsysteem en het stembureau worden door de Helpdesk op de hoogte worden gesteld van de vervangende stembescheiden die zijn uitgereikt. De oude stembescheiden worden vervolgens ongeldig gemaakt en de nieuw uitgereikte set geactiveerd in de stemdienst. Voor een nadere uitwerking van de procedure

vervangende stembescheiden wordt verwezen naar de AO-beschrijving Kiezen op Afstand.
De vervangende stembescheiden zijn in een kluis opgeslagen. De applicatie waarmee de stembescheiden ongeldig gemaakt kunnen worden staat op een beveiligde PC in een fysieke beveiligde kamer.

5.1.10 Registratie alle bevindingen en handelingen

Gedurende de periode stemperiode leggen de beheerders van het stemsysteem, het stembureau en het adviesteam alle handelingen, bevindingen, communicatie, vragen en de reactie daarop vast in een logboek.

5.1.11 Beheerprocedures

Voor de stemdienst zijn diverse beheerprocedures opgesteld waaronder voor backup en recovery in geval van calamiteiten. Deze procedures betreffen alle partijen, waaronder Het Ministerie van BZK, Waterschapshuis, de beheerders van het stemsysteem en SURFnet. Deze beheerprocedures zijn opgenomen in de AO-procedure welke is afgestemd met alle betrokkenen.

5.2 Maatregelen stemsysteem

5.2.1 Systeemtesten

Het stemsysteem wordt vooraf aan diverse testen onderworpen, waaronder:

a) Functionele testen: biedt de stemdienst de geëiste functionaliteit?
b) Performance testen: is de verwerkingscapaciteit van de stemdienst voldoende en hoe wat is het gedrag bij extreme belasting?
c) Penetratietest: is de stemdienst bestand tegen inbraakpogingen?
d) Broncode onderzoek: bevat de stemdienst ongewenste functionaliteit?
e) Accessibility test: voldoet de stemdienst aan de toegankelijkheidsrichtlijnen?
f) Browser compatibility test: werkt de stemdienst correct op verschillende typen browsers (Internet Explorer, Opera, Firefox, Safari etc.) en op verschillende platforms?
g) Beheertesten: werken de backup mechanismen, werken herstelmaatregelen indien een component uitvalt?
h) Sessie met vertegenwoordigers van politieke partijen om de optimale weergave van lijsten en kandidaten te bepalen
i) Integrale ketentest. Werken alle onderdelen van het systeem ook in samenhang met elkaar juist.
j) Usability-test. Onderzoek onder eindgebruikers naar de gebruikersvriendelijkheid van het systeem.
k) Eindschouw: Eindcontrole door het Ministerie van BZK voor het in productie aan van de stemdienst. Tijdens de finale schouw worden reservekopieën gemaakt van alle programmatuur, databases, configuratiebestanden en overige instellingen van de stemdienst. Na de schouw mag het stemsysteem niet meer worden gewijzigd.

5.2.2 Systeemmaatregelen

Het stemsysteem voorziet in de volgende set van systeemmaatregelen:

- Het systeem genereert met behulp van cryptografische software en een softwarematige sleutel een unieke stemcode per kiesgerechtigde;
- De stemcode is dusdanig lang dat de kans op het raden van een geldige stemcode zeer klein is;
- Alleen kiesgerechtigden met een stemcode kunnen een geldige stem uitbrengen in het systeem;
- Het systeem heeft de mogelijkheid tot stemcontrole door de kiezer;
- Iedereen kan de uitslag berekenen. De benodigde informatie wordt gepubliceerd op een website en controle waarden worden gepubliceerd in de Staatcourant. De Radboud Universiteit zal de uitslag herberekenen, m.b.v. de openbare informatie;
- De stem wordt versleuteld uitgewisseld tussen computer van de kiezer en de stemdienst zodat de versleutelde stem niet door derden onderschept kan worden;
- De kiezer heeft de mogelijkheid de authenticiteit van de stemdienst op basis van een PKIoverheid certificaat kunnen controleren;

- Er is een scheiding in het stemsysteem voor de verschillende stemfasen;
- Er zijn offline beheersystemen;
- De communicatie tussen de kiezer en het systeem vindt plaats zonder dat er voor elke kiezer een sessie in stand gehouden wordt.
- Kiezers moeten een vooraf bepaalde volgorde van schermen doorlopen om een stem uit te kunnen brengen. Indien de kiezer de stem niet uitbrengt kan hij opnieuw de stemcode invoeren en alsnog de stem uitbrengen.
- Het systeem houdt niet centraal bij in welke stap in het proces de kiezer zich bevindt. Deze statusinformatie blijft hierdoor op de computer van de kiezer.
- Het systeem doet geen lokale opslag van gevoelige informatie. Er wordt geen informatie vastgehouden op het systeem in cookies;
- Pagina's worden niet als tijdelijke bestanden opgeslagen;
- Het systeem zorgt ervoor dat de stempagina's niet direct adresseerbaar zijn en dat deze hierdoor niet door zoekmachines doorzocht kunnen worden;
- De stemdienst is dubbel uitgevoerd op meerdere niveaus;
- Het systeem heeft monitor/testfunctionaliteiten;
- Het systeem heeft backupfunctionaliteiten;
- De stem wordt versleuteld opgeslagen, zonder vermelding van de kiezeridentificatie;
- Het is niet mogelijk in het systeem de stemcode terug te relateren aan de persoonsgegevens van de kiezer. De sleutel rekent namelijk slechts één kant op;
- Het systeem heeft de mogelijkheid tot het generen van (wettelijke) verantwoordingsinformatie;
- Het systeem is voorzien van controle- en registratiemechanismen;
- Het systeem heeft voldoende capaciteit om piekbelasting aan te kunnen.

5.2.3 Maatregelen stemserver

De volgende maatregelen zijn getroffen ten aanzien van de stemserver. De maatregelen voor de technische infrastructuur worden nader beschreven in paragraaf 5.3.

- De stemserver is dubbel uitgevoerd;
- De stemservers staan op twee geografisch verschillende beveiligde lokaties;
- De opstelling staat opgesteld in een in afgesloten serverkast (specifiek voor dit doel in gebruik) in centrale serverruimte met stringent toegangs- en sleutelbeheer;
- De apparatuur wordt beheerd door SURFnet en valt onder beheerbeleid van SURFnet (o.a. monitoring en bewaking infrastructuur 24 uur/dag, gespecialiseerd personeel beheert fysieke lokatie, diverse toegangsmaatregelen en beleid worden bijgesteld aan de geldende normen).
- Drie speciaal aangewezen systeembeheerders in dienst van SURFnet beheren het systeem.
- De stemserver en apparatuur hebben dubbele uitgevoerde stroomvoorziening waarvan minimaal 1 groep voorzien is van no-break stroomvoorziening of een UPS.
- Een inbraaksysteem maakt onderdeel uit van het stemsysteem;

- Een speciale onderdeel van het systeem maakt vastleggingen van diverse componenten. Indien calamiteiten daartoe aanleiding geven kan besloten worden extra informatie vast te leggen;
- Op de internetverbinding is een firewall aanwezig met strikte firewall-instellingen.
- Het gebruik van de stemdienst is uitsluitend mogelijk via een versleutelde verbinding waarvoor een hardwarematige 'cryptocard' in gebruik is.
- Handmatige bediening server op lokatie is niet mogelijk zonder herstart van de stemserver. De bedieningsconsole van de stemserver is softwarematig uitgeschakeld;
- Iedere statuswijziging van de server genereert een melding op de beheerconsoles;
- Backup van de database en logfiles worden lokaal op het systeem opgeslagen. Er is geen verbinding met een externe backupsysteem;
- Backupbestanden worden regelmatig m.b.v. de beheerstations off-site opgehaald en opgeslagen;
- De stemservers zijn bij diverse soorten defecten met beperkte inspanning in de oorspronkelijke staat te herstellen met beschikbare standaardcomponenten en originele installatie-media en -procedures.

5.2.4 Fysieke beveiliging

Het beheer van het stemsysteem wordt uitgevoerd op een lokatie van het Hoogheemraadschap Rijnland. Het Hoogheemraadschap Rijnland is dan ook verantwoordelijk voor de fysieke beveiliging van het pand en heeft hiervoor standaard beveiligingsmaatregelen getroffen.

- De normale huisregels (en ontruimingsplan) van Hoogheemraadschap Rijnland gelden 24 uur per dag (bijv. bezoekers worden begeleid van en naar de deur);
- Beveiligingspersoneel tijdens de verkiezingsperiode is 24 uur per dag aanwezig;
- Er is een bemande receptie tijdens kantooruren. Buiten kantooruren is er geen toegang zonder een key-card;
- De opstelling van het stembureau en beheersystemen is aanwezig in af te sluiten ruimten;
- Er is alleen toegang voor herkenbaar personeel (badge en identificatie en registratie bij aanvang dienstperiode);
- Tijdens verkiezingsperiode wordt een logboek bijgehouden;
- Kluizen zijn beschikbaar voor gevoelige informatie.

Het Hoogheemraadschap Rijnland heeft een eigen beveiligingsplan informatievoorziening waarin onder andere de toegangscontrole, beveiligde computerruimten en beveiliging van de apparatuur nader staan beschreven.

5.2.5 Uitwijk

De bediening en beheer van het stemsysteem wordt uitgevoerd in een speciaal beveiligde ruimte. Hier zijn passende maatregelen getroffen onder andere tegen stroomonderbreking, brand- en waterschade. Het Hoogheemraadschap Rijnland heeft in geval van calamiteiten een calamiteitenplan beschikbaar. In geval van een zeer ernstige calamiteit kan worden uitgeweken naar een beschikbare uitwijklokatie. De

lokatie is minimaal voorzien van middelen (zoals netwerkverbinding) om in de behoefte te voorzien.

5.3 Maatregelen infrastructuur

Het Waterschapshuis heeft de technische infrastructuur voor het aanbieden en beheren van het Voting Window deel van Kiezen op Afstand contractueel uitbesteed aan SURFnet. SURFnet is dan ook integraal verantwoordelijk voor de beveiliging van dit deel van de KOA-infrastructuur.

5.3.1 Fysieke beveiliging

Alle infrastructuur voor de stemdienst Kiezen op Afstand is dubbel uitgevoerd in twee housing lokaties binnen het SURFnet-netwerk. Deze lokaties staan in Nijmegen en Amsterdam. De housing lokaties staan onder 24 uurs toezicht en hebben zodanige fysieke en logische toegangsbeveiliging dat onbevoegden geen toegang hebben tot de Kiezen op Afstand infrastructuur. Op de lokaties zijn daarnaast maatregelen getroffen tegen stroomonderbreking, brand- en waterschade. SURFnet heeft in geval van calamiteiten een calamiteitenplan beschikbaar.

5.3.2 Uitwijk

Zoals hierboven beschreven is het stemsysteem redundant uitgevoerd op twee verschillende lokaties. Dit betekent dat als één lokatie uitvalt de stemdienst voor de kiezers volledig blijft doordraaien. De Voting Window applicatie houdt, middels een synchronisatiemechanisme dat via het afgeschermde deel van de infrastructuur loopt, de statustabellen van de servers, waarin wordt bijgehouden of een kiezer al heeft gestemd, synchroon.

5.3.3 Beveiligd netwerk

De Kiezen op Afstand infrastructuur staat in een speciaal beveiligd netwerk met per lokatie een publiek segment naar de Voting Window applicatie en een afgeschermd beheersegment. Alle netwerksegmenten zijn logisch gescheiden van de rest van het SURFnet-netwerk. Alle netwerksegmenten zijn middels access-lijsten afgeschermd voor niet geautoriseerd netwerkverkeer. Alle server-componenten en beheerstations zijn middels host-based firewalls afgeschermd voor niet geautoriseerd verkeer (ook intern). De communicatie van de kiezer naar het KOA-netwerk is versleuteld met zowel hardware encryptie als software encryptie. Als de hardware encryptie uitvalt neemt de softwarematige encryptie het over. Een klein aantal aangewezen SURFnet-beheerders kunnen uitsluitend via het speciaal beveiligd beheernetwerk en met dedicated beheerstations de infrastructuur beheren. Communicatie tussen beheerstations (zowel die van de SURFnet-beheerders als de beheerders van de stemdienst) en servers wordt extra beveiligd door gebruik te maken van end-to-end-encryptie. De beheerders werken met unieke beheeraccounts en de activiteiten van de beheerders worden geregistreerd. Vanaf deze beheeromgeving is het niet mogelijk stemmen uit te brengen. De database is afgeschermd middels rolspecifieke wachtwoorden.De SURFnet infrastructuur is gedimensioneerd op een zeer hoge piekbelasting. De infrastructuur en de operationele conditie van de stemdienst wordt voor en tijdens de stemperiode continu gemonitord.

Bijlage A Aanbevelingen Raad van Europa 2004/462a

Legal standards

Principals

I. Universal suffrage
1. The voter interface of an e-voting system shall be understandable and easily usable.
2. Possible registration requirements for e-voting shall not pose an impediment to the voter participating in e-voting.
3. E-voting systems shall be designed, as far as it is practicable, to maximise the opportunities that such systems can provide for persons with disabilities.
4. Unless channels of remote e-voting are universally accessible, they shall be only an additional and optional means of voting.
II. Equal suffrage
5. In relation to any election or referendum, a voter shall be prevented from inserting more than one ballot into the electronic ballot box. A voter shall be authorised to vote only if it has been established that his/her ballot has not yet been inserted into the ballot box.
6. The e-voting system shall prevent any voter from casting a vote by more than one voting channel.
7. Every vote deposited in an electronic ballot box shall be counted, and each vote cast in the election or referendum shall be counted only once.
8. Where electronic and non-electronic voting channels are used, there shall be a secure and reliable method to aggregate all votes and to calculate the correct result.
III. Free suffrage
9. The organisation of e-voting shall secure the free formation and expression of the voter's opinion and, where required, the personal exercise of the right to vote.
10. The way in which voters are guided through the e-voting process shall be such as to prevent their voting precipitately or without reflection.
11. Voters shall be able to alter their choice at any point in the e-voting process before casting their vote, or to break off the procedure, without their previous choices being recorded or made available to any other person.
12. The e-voting system shall not permit any manipulative influence to be exercised over the voter during the voting.
13. The e-voting system shall provide the voter with a means of participating in an election or referendum without the voter exercising a preference for any of the voting options, e.g. to cast a blank vote.
14. The e-voting system shall indicate clearly to the voter the fact that the vote has been cast successfully and the fact that the whole voting procedure has been completed.
15. The e-voting system shall prevent the changing of a vote once that vote has been cast.
IV. Secret suffrage
16. E-voting shall be organised in such a way as to exclude at any stage of the voting procedure and, in particular, at voter authentication, anything that would endanger the

secrecy of the vote.
17. The e-voting system shall secure that votes in the electronic ballot box and votes being counted have been made and remain anonymous, and that it is not possible to reconstruct a link between the vote and the voter.
18. The e-voting system shall be so designed that the expected number of votes in any electronic ballot box will not allow the result to be linked to individual voters.
19. Measures shall be taken to ensure that the information needed during electronic processing cannot be used to breach the secrecy of the vote.

Procedural safeguards

I. Transparency
20. Member states shall take steps to ensure that voters understand and have confidence in the e-voting system in use.
21. Information on the functioning of an e-voting system shall be made publicly available.
22. Voters shall be provided with an opportunity to practise any new method of e-voting before and separately from the moment of casting an electronic vote.
23. Any observers, to the extent permitted by law, shall be able to be present to observe and comment on the e-elections, including the establishing of the results.
II. Verifiability and accountability
24. The components of the e-voting system shall be disclosed, at least to the competent electoral authorities, as required for verification and certification purposes.
25. Before any e-voting system is introduced, and at appropriate intervals thereafter, and in particular after any changes are made to the system, an independent body, appointed by the electoral authorities, shall verify that the e-voting system is working correctly and that all the necessary security measures have been taken.
26. There shall be the possibility for a recount. Other features of the e-voting system that may influence the correctness of the results, shall be verifiable.
27. The e-voting system shall not prevent the partial or complete re-run of an election or a referendum.
III. Reliability and security
28. The member state's authorities shall ensure the reliability and security of the e-voting system.
29. All possible steps shall be taken to avoid the possibility of fraud or unauthorised intervention affecting the system during the whole voting process.
30. The e-voting system shall contain measures to preserve the availability of its services during the e-voting process. It shall resist, in particular, malfunction, breakdowns or denial of service attacks.
31. Before any e-election or e-referendum takes place, the competent electoral authority shall satisfy itself that the e-voting system is genuine and operates correctly.
32. Only persons appointed by the electoral authority shall have access to the central infrastructure, the servers and the election data. There shall be clear rules established for such appointments. Critical technical activities shall be carried out by teams of at least two. The composition of the teams shall be regularly changed. As far as possible, such activities shall be carried out outside election periods.
33. While an electronic ballot box is open, any authorised intervention affecting the system shall be carried out by teams of at least two persons, be the subject of a report, and be able to be monitored by representatives of the competent electoral

authority and any election observers.
34. The e-voting system shall maintain the availability and integrity of the votes. It shall also maintain the confidentiality of the votes and keep them sealed until the counting process. If stored or communicated outside controlled environments, the votes shall be encrypted.
35. Votes and voter information shall remain sealed as long as the data is held in a manner where they can be associated. Authentication information shall be separated from the voter's decision at a pre-defined stage in the e-election or e-referendum.

Operational standards

Notification

36. Domestic legal provisions governing an e-election or e-referendum shall provide for clear timetables concerning all stages of the election or referendum, both before and after the election or referendum.
37. The period in which an electronic vote can be cast shall not begin before the notification of an election or a referendum. Particularly with regard to remote e-voting, the period shall be defined and made known to the public well in advance of the start of voting.
38. The voters shall be informed, well in advance of the start of voting, in clear and simple language, of the way in which the e-voting will be organised, and any steps a voter may have to take in order to participate and vote.

Voters

39. There shall be a voters register which is regularly updated. The voter shall be able to check, as a minimum, the information which is held about him/her on the register, and request corrections.
40. The possibility of creating an electronic register and introducing a mechanism allowing online application for voter registration and, if applicable, for application to use e-voting, shall be considered. If participation in e-voting requires a separate application by the voter and/or additional steps, an electronic, and, where possible, interactive procedure shall be considered.
41. In cases where there is an overlap between the period for voter registration and the voting period, provision for appropriate voter authentication shall be made.

Candidates

42. The possibility of introducing online candidate nomination could be considered.
43. A list of candidates that is generated and made available electronically shall also be publicly available by other means

Voting

44. It is particularly important, where remote e-voting takes place while polling stations are open, that the system shall be so designed that it prevents any voter from voting more than once.
45. Remote e-voting may start and/or end at an earlier time than the opening of any polling station. Remote e-voting shall not continue after the end of the voting period at polling stations.
46. For every e-voting channel, support and guidance arrangements on voting procedures shall be set up for, and be available to, the voter. In the case of remote e-voting, such arrangements shall also be available through a different, widely available communication channel.
47. There shall be equality in the manner of presentation of all voting options on the device used for casting an electronic vote.

48. The electronic ballot by which an electronic vote is cast shall be free from any information about voting options, other than that strictly required for casting the vote. The e-voting system shall avoid the display of other messages that may influence the voters' choice.
49. If it is decided that information about voting options will be accessible from the e-voting site, this information shall be equally presented.
50. Before casting a vote using a remote e-voting system, voters' attention shall be explicitly drawn to the fact that the e-election or e-referendum in which they are submitting their decision by electronic means is a real election or referendum. In case of tests, participants shall have their attention drawn explicitly to the fact that they are not participating in a real election or referendum and shall - when tests are continued at election times - at the same time be invited to cast their ballot by the voting channel(s) available for that purpose.
51. A remote e-voting system shall not enable the voter to be in possession of a proof of the content of the vote cast.
52. In a supervised environment, the information on the vote shall disappear from the visual, audio or tactile display used by the voter to cast the vote as soon as it has been cast. Where a paper proof of the electronic vote is provided to the voter at a polling station, the voter shall not be able to show it to any other person nor take this proof outside of the polling station.

Results

53. The e-voting system shall not allow the disclosure of the number of votes cast for any voting option until after the closure of the electronic ballot box. This information shall not be disclosed to the public until after the end of the voting period.
54. The e-voting system shall prevent processing information on votes cast within deliberately chosen sub-units that could reveal individual voters' choices.
55. Any decoding required for the counting of the votes shall be carried out as soon as practicable after the closure of the voting period.
56. When counting the votes, representatives of the competent electoral authority shall be able to participate in, and any observers to observe, the count.
57. A record of the counting process of the electronic votes shall be kept, including information about the start and end of, and the persons involved in, the count.
58. In the event of any irregularity affecting the integrity of votes, the affected votes shall be tabulated as such.

Audit

59. The e-voting system shall be auditable.
60. The conclusions drawn from the audit process shall be applied in future elections and referendums.

Technical Requirements

The design of an e-voting system shall be underpinned by a comprehensive assessment of the risks involved in the successful completion of the particular election or referendum. The e-voting system shall include the appropriate safeguards, based on this risk assessment, to manage the specific risks identified. Service failure or service degradation shall be kept within pre-defined limits.

Accessibility

61. Measures shall be taken to ensure that the relevant software and services can be used by all voters and, if necessary, provide access to alternative ways of voting.
62. Users shall be involved in the design of e-voting systems, particularly to identify constraints and test ease of use at each main stage of the development process.
63. Users shall be supplied, whenever required and possible, with additional facilities, such as special interfaces, or other equivalent resources, such as personal

assistance. User facilities shall comply as much as possible with the guidelines set out in the Web Accessibility Initiative (WAI).
64. Consideration shall be given, when developing new products, to their compatibility with existing ones, including those using assistive technologies for people with disabilities.
65. The presentation of the voting options shall be optimised for the voter.

Interoperability

66. Open standards shall be used to ensure that the various technical components or services of an e-voting system, possibly derived from a variety of sources, interoperate.
67. At present, the Election Mark-up Language (EML) standard is such an open standard and in order to guarantee interoperability, EML shall be used whenever possible for e-election and e-referendum applications. The decision of when to adopt EML is a matter for member states. The EML standard valid at the time of adoption of this Recommendation, and supporting documentation are available on the Council of Europe website.
68. In cases which imply specific election or referendum data requirements, a localisation procedure shall be used to accommodate these needs. This would allow for extending or restricting the information to be provided, whilst still remaining compatible with the generic version of EML. The recommended procedure is to use structured schema languages and pattern languages.

Systems Operation
(for the central infrastructure and clients in controlled environments)

69. The competent electoral authorities shall publish an official list of the software used in an e-election or e-referendum. Member states may exclude from this list data protection software for security reasons. At the very least it shall indicate the software used, the versions, its date of installation and a brief description. A procedure shall be established for regularly installing updated versions and patches of the relevant protection software. It shall be possible to check the state of protection of the voting equipment at any time.
70. Those responsible for operating the equipment shall draw up a contingency procedure. Any backup system shall conform to the same standards and requirements as the original system.
71. Sufficient backup arrangements shall be in place and permanently available to ensure that voting proceeds smoothly. The staff concerned shall be ready to intervene rapidly according to a procedure drawn up by the competent electoral authorities.
72. Those responsible for the equipment shall have procedures to ensure that during the polling period the voting equipment and its use satisfy requirements. The backup services shall be regularly supplied with monitoring protocols.
73. Before each election or referendum, the equipment shall be checked and approved in accordance with a protocol drawn up by the competent electoral authorities. The equipment shall be checked to ensure that it complies with specifications. The findings shall be submitted to the competent electoral authorities.
74. Any technical operations shall be subject to a formal change control procedure. Any critical changes to key equipment shall be announced.
75. Key e-election or e-referendum equipment shall be located in a secure area and that area shall, throughout the election or referendum period, be guarded against interference of any sort and from anyone. During the election or referendum period a physical disaster recovery plan shall be in place. Furthermore, any data retained after the election or referendum period shall be stored securely.
76. Where incidents that could threaten the integrity of the system occur, those responsible for operating the equipment shall immediately inform the competent electoral authorities, who will take the necessary steps to mitigate the effects of the

incident. The level of incident which shall be reported shall be specified in advance by the electoral authorities.

Security
General Requirements
(referring to pre-voting, voting, and post-voting stages)

77. Technical and organisational measures shall be taken to ensure that no data will be permanently lost in the event of a breakdown or a fault affecting the e-voting system.
78. The e-voting system shall maintain the privacy of individuals. Confidentiality of voters registers stored in or communicated by the e-voting system shall be maintained.
79. The e-voting system shall perform regular checks to ensure that its components operate in accordance with its technical specifications and that its services are available.
80. The e-voting system shall restrict access to its services, depending on the user identity or the user role, to those services explicitly assigned to this user or role. User authentication shall be effective before any action can be carried out.
81. The e-voting system shall protect authentication data so that unauthorized entities cannot misuse, intercept, modify, or otherwise gain knowledge of authentication data or part of it. In uncontrolled environments, authentication based on cryptographic mechanisms is advisable.
82. Identification of voters and candidates in a way that they can unmistakably be distinguished from other persons (unique identification) shall be ensured.
83. E-voting systems shall generate reliable and sufficiently detailed observation data so that election observation can be carried out. The time at which an event generated observation data shall be reliably determinable. The authenticity, availability and integrity of the data shall be maintained.
84. The e-voting system shall maintain reliable synchronised time sources. The accuracy of the time source shall be sufficient to maintain time marks for audit trails and observations data, as well as for maintaining the time limits for registration, nomination, voting, or counting.
85. Electoral authorities have overall responsibility for compliance with these security requirements which shall be assessed by independent bodies.

Requirements in Pre-Voting Stages
(and for data communicated to the voting stage)

86. The authenticity, availability and integrity of the voters registers and lists of candidates shall be maintained. The source of the data shall be authenticated. Provisions on data protection shall be taken into account.
87. The fact that candidate nomination and, if required, the decision of the candidate and/or the competent electoral authority to accept a nomination has happened within the prescribed time limits shall be ascertainable.
88. The fact that voter registration has happened within the prescribed time limits shall be ascertainable.

Requirements in the Voting Stage
(and for data communicated to post-election stages)

89. Data communicated from the pre-voting stage (e.g. voters registers and lists of candidates) shall be maintained in integrity. Data-origin authentication shall be carried

out.
90. It shall be ensured that the e-voting system presents an authentic ballot to the voter. In the case of remote e-voting, the voter shall be informed about the means to verify that a connection to the official server has been established and the authentic ballot been presented.
91. The fact that a vote has been cast within the prescribed time limits shall be ascertainable.
92. Sufficient means shall be provided to ensure that the systems that are used by the voters to cast the vote can be protected against influence that can modify the vote.
93. Residual information holding the voter's decision or the display of the voter's choice shall be destroyed after the vote has been cast. In the case of remote e-voting, the voter shall be provided with information on how to delete, where that is possible, from the device used to cast the vote.
94. The e-voting system shall at first ensure that a user who tries to vote is eligible to vote. The e-voting system shall authenticate the voter and shall ensure that only the appropriate number of votes per voter is cast and stored in the electronic ballot box.
95. The e-voting system shall ensure that the voter's choice is accurately represented in the vote and that the sealed vote enters the electronic ballot box.
96. After the end of the e-voting period, no voters shall be allowed to gain access to the e-voting system. However the acceptance of electronic votes into the electronic ballot box shall remain open for a sufficient period of time to allow for any delays in the passing of messages over the e-voting channel.

Requirements in Post-Voting Stages

97. The integrity of data communicated from the voting stage (e.g. votes, voters registers, lists of candidates) shall be maintained. Data-origin authentication shall be carried out.
98. The counting process shall accurately count the votes. The counting of votes shall be reproducible.
99. The e-voting system shall maintain the availability and integrity of the electronic ballot box and the output of the counting process as long as required.

Audit

General

100. An audit system shall be designed and implemented as part of the e-voting system. Audit facilities shall be present on different levels of the system: logical, application, and technical.
101. End-to-end auditing of an e-voting system shall include recording, providing monitoring facilities, providing verification facilities. Audit systems with the features set out in sections II – V below shall therefore be used to meet these requirements.

Recording

102. An audit system shall be open, comprehensive, and actively report on potential issues and threats.
103. An audit system shall record times, events and actions, including: a.) all voting related information, including number of eligible voters, number of votes cast, number of invalid votes, counts and recounts. b.) any attacks on the operation of the e-voting systems and its communications infrastructure; c.) system failures, and malfunctions and other aspects of system compromise.

Monitoring

104. An audit system shall provide the ability to oversee the election or referendum and to verify that the results and procedures are in accordance with the applicable legal provisions.
105. Disclosure of the audit information to unauthorised persons shall be prevented.
106. An audit system shall maintain voter anonymity at all times.

Verifiability

107. An audit system shall provide the ability to cross check and verify the correct operation of the e-voting system and the accuracy of the result, detecting voter fraud and proving all counted votes are authentic and all votes have been counted.
108. An audit system shall provide the ability to verify that an e-election or e-referendum has complied with the applicable legal provisions, the aim being to verify that the results are an accurate representation of the authentic votes.

Other

109. An audit system shall be protected against attacks which may corrupt, alter or lose records in the audit system.
110. Member states shall take adequate steps to ensure that the confidentiality of any information obtained by any person while carrying out auditing functions is guaranteed.

Certification

111. Member states shall introduce certification processes that allow for any ICT (Information and Communication Technology) component to be tested and certified as being in conformity with the technical requirements described in this Recommendation.
112. In order to enhance international co-operation and avoid duplication of work, member states shall consider whether their respective agencies shall join, if they have not done so already, relevant international mutual recognition arrangements such as the European Co-operation for Accreditation (EA), the International Laboratory Accreditation Cooperation (ILAC) and the International Accreditation Forum (IAF) and other bodies of a similar nature.