Hoofdstuk 1 Inleiding

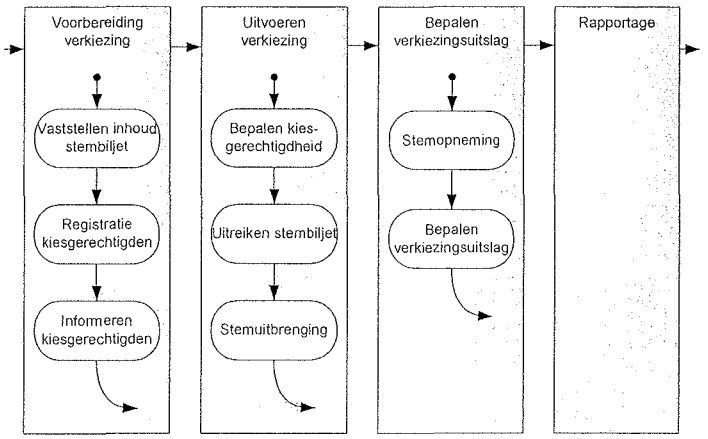
1.1. Uitgangspunt

Dit document heeft betrekking op de realisatie van een internetstemsysteem dat kan worden ingezet voor nationale verkiezingen in het Nederlandse publieke domein, specifiek ten behoeve van Nederlanders in het buitenland[1].

Als generiek model van het kiesproces wordt het volgende referentiemodel gebruikt. Daarin staan de (meest) cruciale stappen in het stemproces centraal. Deze stappen zijn:

- het vaststellen van de kiesgerechtigdheid;
- het identificeren van de kiezer
- het uitbrengen van de stem;
- de stemopneming/vaststellen van de uitslag.

In onderstaande figuur is het referentiemodel van het kiesproces weergegeven.



1.2. Opzet

In hoofdstuk 2 wordt, zowel grafisch als tekstueel, een aantal mogelijke systeemcomponenten en rollen onderscheiden. Vervolgens wordt in hoofdstuk 3 een beschrijving van het proces waarvan in een internetstemsysteem gebruik wordt gemaakt, gegeven, bezien vanuit een aantal relevante rollen. Tenslotte worden in hoofdstuk 4 de functionele eisen geformuleerd, opgehangen aan de in hoofdstuk 2 en 3 beschreven systeemcomponenten, rollen en het proces.

1.3 Definities

De navolgende definities worden in dit document gebruikt:

- Stemproces: procedure, bezien vanuit de kiezer, startend bij het toegang verkrijgen tot het internetstemsysteem en eindigend bij de bevestiging van het systeem aan de kiezer dat deze met succes een stem heeft uitgebracht.
- Stemopneming: het openen van de stembus en het tellen van de geldige stemmen.
- Stemtoken: authenticatiemiddel waarmee de kiezer toegang krijgt tot het Internetstembureau. Het stemtoken maakt onderdeel uit van de stembescheiden die aan de kiezer worden verstrekt.

[1] Op basis van het adviesrapport van de Commissie Inrichting verkiezingsproces. Ten aanzien van dit advies zal nog een kabinetsstandpunt te worden opgesteld. (stand van zaken d.d. 1 november 2007).

1.4 Versiebeheer [verwijderen uit openbare versie]

Versie	Input ontvangen	Van wie	Verwerkt d.d. door wie
0.3	23 augustus 2007		
0.5	28 augustus 2007		
0.6	31 augustus 2007		
0.8	10, 11 september 2007		
0.9	13 september		
0.10	17 september		
0.11	20 september		
0.12	20, 21 september		
0.13	25 september		
0.14	26 september		
0.15	27 september		
0.20	28 september		
0.21	9 oktober		
0.22	18 oktober		
0.23	1 november		
0.24	5 november		
0.25	7 november		
0.26	7 november		

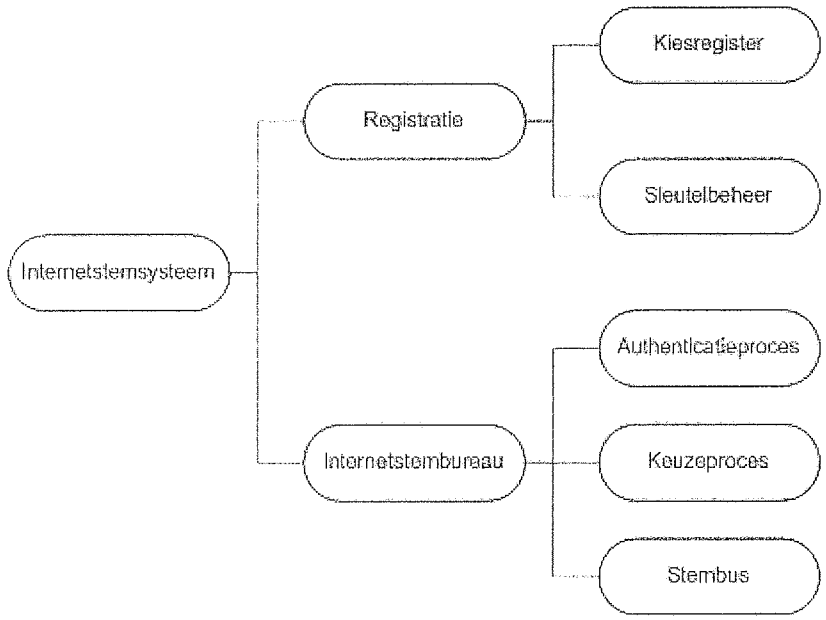
Hoofdstuk 2 Systeemcomponenten en rollen

2.1 Inleiding

In de onderstaande afbeelding worden, op een abstract niveau, diverse mogelijke systeemcomponenten van een internetstemsysteem onderscheiden. Deze systeemcomponenten worden vervolgens beschreven, gevolgd door de beschrijving van enkele generieke rollen binnen het internetstemsysteem.

Het hier gemaakte onderscheid tussen de verschillende systeemcomponenten en rollen is niet bedoeld om richting te geven aan de daadwerkelijke fysieke architectuur van een internetstemsysteem; het onderscheid wordt aangegeven om de betreffende functionaliteit zo duidelijk mogelijk te kunnen specificeren. Er is bewust gekozen voor een hoog abstractieniveau in deze beschrijving zodat geen of in elk geval zo weinig mogelijk inhoudelijke oplossingen worden voorgeschreven.

Aan de systeemcomponenten en rollen worden in hoofdstuk 4 functionele systeemeisen gekoppeld.



2.2. Systeemcomponenten

Internetstemsysteem - Het globale alomvattende technische systeem, bestaande uit onder andere software en hardware, servers, verbindingen, etc. Binnen het internetstemsysteem kunnen de volgende componenten onderscheiden worden:

Registratie – Het deel van het internetstemsysteem waar de registratie van kiezers voor een verkiezing plaatsvindt. Hierbinnen valt ook de creatie en distributie van de stembescheiden die kiezers toegang geven tot het internetstembureau. Registratie omvat het Kiesregister en het Sleutelbeheer:

- **Kiesregister** – Het Kiesregister bevat de persoons- en adresgegevens van alle kiezers. Het Kiesregister houdt bij welke personen kiesgerechtigd zijn voor een verkiezing en welke van hen zich ook werkelijk hebben geregistreerd voor een bepaalde verkiezing.

- **Sleutelbeheer** – Sleutelbeheer is de component waarbinnen voorafgaand aan de verkiezingen de cryptografische sleutels worden aangemaakt die door kiezers gebruikt worden om tijdens de verkiezing toegang te krijgen tot het internetstembureau om daar hun stem uit te brengen. Sleutelbeheer heeft ook als taak het beheren van deze sleutels om revocatie en vervanging mogelijk te maken.

Internetstembureau – Het internetstembureau is de systeemcomponent waartoe de kiezer gedurende de verkiezing toegang krijgt en waarbinnen de kiezer een keuze maakt en die keuze in de stembus kan deponeren. Binnen het internetstembureau kunnen de volgende componenten worden onderscheiden:

- **Authenticatieproces** – Het authenticatieproces is de digitale ingang van het internetstembureau, waar wordt bepaald welke kiezers toegang krijgen tot de andere onderdelen van het internetstembureau.
- **Keuzeproces –** Het keuzeproces is waar de kiezer het overzicht van kandidaten te zien krijgt en een keuze kan maken.
- **Stembus** – De stembus is waar alle uitgebrachte stemmen worden bewaard en op basis waarvan de telling van de stemmen plaatsvindt.

2.3 Rollen

In het stemproces zelf, de voorbereiding en nadien, kunnen verschillende rollen worden onderscheiden. Zoals dat ook geldt voor de systeemcomponenten, zijn de rollen illustratief en kan aan de hand ervan met name het uitgangspunt van functiescheiding gedemonstreerd worden.

Er zijn enkele organisaties die rollen hebben die direct overlappen met bepaalde systeemcomponenten. Om nodeloze complicatie te voorkomen wordt voor de organisaties en de componenten in die gevallen dezelfde naam gebruikt:

- **Kiesregister** – De organisatie die verantwoordelijk is voor de kiesregistercomponent.
- **Sleutelbeheer** – De organisatie die verantwoordelijk is voor de sleutelbeheercomponent.
- **Internetstembureau** – De organisatie van het internetstembureau wordt gevormd door de voorzitter en de leden van het stembureau en is verantwoordelijk voor het toezicht op de componenten binnen het internetstembureau.

Verder zijn er enkele rollen die betrekking hebben op meerdere componenten.

- **Ontwikkelaar –** Omvat alle partijen die verantwoordelijk zijn voor de ontwikkeling van het internetstemsysteem of delen daarvan.
- **Beheerder –** Omvat alle partijen die verantwoordelijk zijn voor het technisch beheer van het internetstemsysteem of delen daarvan.
- **Waarnemer -** Onafhankelijke waarnemers van het verkiezingsproces. Zien toe op het correcte verloop van de verkiezing.
- **Kiezer -** De Nederlandse burger die zijn stem wenst uit te brengen door middel van het internetstemsysteem.
- **Opdrachtgever** - De nationale autoriteit die verantwoordelijkheid draagt voor het internetstemsysteem. Naast het opdrachtgeverschap in de richting van de leverancier van het internetstemsysteem, heeft deze ook een aantal meer operationele taken in de voorbereiding van, tijdens en na afloop van de verkiezing.

Hoofdstuk 3 Procesbeschrijving

3.1 Inleiding

Dit hoofdstuk geeft een korte procesbeschrijving op hoofdlijnen, bezien vanuit de verschillende onderscheiden rollen. Er is bewust gekozen voor een hoog abstractieniveau in deze beschrijving zodat zo weinig mogelijk inhoudelijke oplossingen worden voorgeschreven.

Opdrachtgever
De opdrachtgever is tijdens de ontwikkeling van het internetstemsysteem, c.q. de aanpassing van een bestaand internetstemsysteem, betrokken. Hij wordt door de ontwikkelaar in de gelegenheid gesteld zich een beeld te vormen van de mate waarin wordt voldaan aan de eisen zoals die zijn gesteld aan de ontwikkeling. In de registratie- en de daaropvolgende verkiezingsperiode is de opdrachtgever bij alle cruciale stappen en processen betrokken.

Ontwikkelaar
De ontwikkelaar ontwerpt en bouwt een internetstemsysteem, c.q. past een bestaand systeem aan, aan de hand van de door de opdrachtgever geformuleerde eisen en wensen en/of volgens voorgeschreven normen, etc. Op basis van begrijpelijke en actuele documentatie houdt de ontwikkelaar de opdrachtgever op de hoogte.

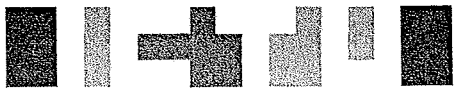
Kiesregister
Deze organisatie ontvangt verzoeken van kiezers om te mogen stemmen via het internetstemsysteem en beoordeelt, mede op basis van controle in het Kiesregister, de kiesgerechtigheid van de burger en neemt daarover een besluit. Wanneer een kiezer kiesgerechtigd is bevonden, zorgt het kiesregister in samenwerking met de sleutelbeheer-autoriteit ervoor dat de kiezer zijn stemtoken ontvangt, waarmee deze tezijnertijd toegang tot het internetstembureau krijgt.

Sleutelbeheer
Deze onafhankelijke organisatie genereert, al dan niet samen met andere betrokken actoren, sleutels die nodig kunnen zijn in het verkiezingsproces en daaraan voorafgaande fasen. Hieronder vallen bijvoorbeeld de stembescheiden die kiezers toegang geven tot het internetstembureau en de digitale certificaten en sleutels die de verschillende partijen gebruiken. De sleutelbeheer-autoriteit draagt er in samenwerking met de kiesregister-autoriteit zorg voor dat kiesgerechtigden hun stemtoken ontvangen.

Beheerder
De beheerder voert het technisch beheer uit van (de verschillende componenten van) het internetstemsysteem voorafgaand aan en tijdens de verkiezing, waarbij er afspraken zijn over uit te voeren beheertaken met enerzijds de Opdrachtgever en anderzijds de Stembureauleden (tijdens de verkiezing).

Kiezer
Een Nederlands burger die in het buitenland verblijft wordt geattendeerd op, of wenst uit eigener beweging te gaan stemmen via, een internetstemsysteem bij een aangekondigde verkiezing. De kiezer meldt zich aan bij het Kiesregister en dient een aanvraag in om zijn stem te kunnen uitbrengen via een internetstemsysteem. Na controle van de kiesgerechtheid van de burger in het Kiesregister, ontvangt deze van het Sleutelbeheer een stemtoken, waarmee hij toegang kan verkrijgen tot het stembureau binnen het internetstemsysteem.

In de periode dat de verkiezing bezig is en dus het internetstemsysteem actief, krijgt de kiezer vanaf de computer van de kiezer, na authenticatie met zijn stemtoken, toegang



tot het internetstembureau. De kiezer maakt zijn keuze aan de hand van het overzicht van kandidaatlijsten en bevestigt deze. Zijn stem wordt in de stembus gedeponeerd.

Stembureau
De voorzitter en de leden van het stembureau houden tijdens de verkiezing toezicht op het verloop ervan op basis van de aan hen toegekende wettelijke bevoegdheden. Het stembureau opent en sluit de verkiezing, concreet het Internetstembureau, en is verantwoordelijk voor de stemopneming.

Waarnemer
Een onafhankelijke waarnemer ziet toe op het correcte verloop van het verkiezingsproces, alsmede op de voorbereiding en de nasleep daarvan.

Hoofdstuk 4 Systeemeisen

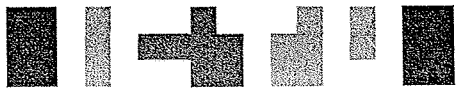
4.1 Inleiding

Dit hoofdstuk beschrijft ten eerste een aantal generieke waarborgen waarin het internetstemsysteem moet voorzien. In het tweede deel van dit hoofdstuk wordt ingegaan op de functionele systeemeisen waaraan het internetstemsysteem moet voldoen. Deze functionele eisen kunnen kortheidshalve worden beschouwd als een uitwerking van de genoemde generieke waarborgen.

4.2 Generieke waarborgen

De volgende generieke waarborgen vloeien voort uit de Grondwet, de Kieswet en internationale verdragen en zijn overgenomen uit het adviesrapport van de commissie Korthals Altes. Zij vormen het kader waarbinnen meer specifieke eisen en wensen aan een internetstemsysteem kunnen worden geformuleerd.

Transparantie	Het verkiezingsproces moet zo zijn ingericht dat het helder van structuur en opzet is, zodat in beginsel iedereen inzicht in de structuur ervan kan hebben. Er zijn in het verkiezingsproces geen geheimen. Vragen moeten beantwoord kunnen worden; de antwoorden moeten controleerbaar en verifieerbaar zijn.
Controleerbaarheid	Het verkiezingsproces moet objectief controleerbaar zijn. De controle-instrumenten kunnen, afhankelijk van de vorm van stemmen waartoe wordt besloten, verschillen. Het systeem moet in staat zijn om, zonder dat de privacy in gevaar komt, aan te tonen dat voldaan is aan de gestelde eisen.
Stemgeheim	Het moet onmogelijk zijn om een verband te leggen tussen de identiteit van de persoon die de stem uitbrengt en de inhoud van de uitgebrachte stem. Het proces moet zodanig zijn ingericht dat het onmogelijk is de kiezer te laten aantonen hoe hij of zij heeft gestemd.
Stemvrijheid	Het stemsysteem moet waarborgen dat een kiesgerechtigde in volledige vrijheid, vrij van beïnvloeding, zijn stem kan uitbrengen
Uniciteit	Iedere kiesgerechtigde mag, gegeven het Nederlandse kiesstelsel, precies één stem uitbrengen per verkiezing, die precies één keer meegeteld mag worden bij de stemopneming.
Kiesgerechtigdheid	Het stemsysteem dient er voor te zorgen dat alleen kiesgerechtigde personen aan de verkiezing deel kunnen nemen.
Integriteit	Het stemsysteem dient foutloos te werken en de uitkomst mag niet beïnvloedbaar zijn anders dan door het uitbrengen van rechtmatige stemmen.
Toegankelijkheid	Elke persoon die kiesgerechtigd is moet zoveel mogelijk in staat worden gesteld om deel te nemen in het verkiezingsproces.



4.3 Eisen

In deze sectie worden de eisen aan het internetstemsysteem weergegeven. Paragrafen **A** tot en met **E** bevatten eisen die op het internetstemsysteem als geheel van toepassing zijn. Paragrafen **F** tot en met **I** bevatten eisen die gekoppeld zijn aan de afzonderlijke in het tweede hoofdstuk geïntroduceerde systeemcomponenten.

A. Eisen aan de ontwikkeling van het internetstemsysteem

A.1	Ontwikkeling (Standaard)	De ontwikkeling en het onderhoud van het internetstemsysteem dienen conform ISO 12207 of een vergelijkbare kwaliteitstandaard te geschieden. *ISO 12207 beschrijft de complete levensloop van een softwareproduct, beginnend als conceptueel idee, gevolgd door de ontwikkeling, de documentatie, het testen, het gebruik en het onderhoud, afsluitend met het beëindigen van het gebruik van het product.* *Een standaard als ISO 12207 biedt een bepaalde mate van kwaliteitsgarantie in het ontwikkeltraject.*
A.2	Ontwikkeling (Documentatie en versiebeheer)	Het internetstemsysteem dient voorzien te zijn van actuele, volledige en duidelijke documentatie. Tevens wordt aan versiebeheer (van software én documentatie) gedaan.
A.3	Ontwikkeling (Beveiliging)	Beveiliging dient een integraal onderdeel te zijn van de levenscyclus (ontwikkeling, testen, onderhoud) van het internetstemsysteem. Hierbij zou NIST Special Publication 800-64 als leidraad kunnen dienen. *NIST Special Publication 800-64 beschrijft onder andere het gebruik van risico analyse, beveiligingseisen, testen, certificatie en audits.*
A.4	Ontwikkeling (Open standaarden)	Het internetstemsysteem maakt zoveel mogelijk gebruik van open standaarden. *In overeenstemming met het actieplan "Nederland open in verbinding" van het kabinet, wordt het gebruik van open standaarden nagestreefd.* *Een voorbeeld van een open standaard in de context van internetstemmen is EML (Election Markup Language).*
A.5	Ontwikkeling (Open source)	De broncode van het internetstemsysteem dient publiekelijk raadpleegbaar te zijn. *Er zijn verschillende manieren om dit te realiseren. Het internetstemsysteem kan bijvoorbeeld ontwikkeld worden onder een Open Source Software licentie (zoals bijvoorbeeld Linux) waarbij derden de broncode niet alleen kunnen inzien maar ook mogen hergebruiken. Er kan ook gekozen worden om broncode slechts publiekelijk ter inzage te geven onder een specifieke licentie waarbij hergebruik van de broncode uitgesloten is. Een dergelijke constructie wordt toegepast bij ondermeer de encryptie pakketten PGP en Cryptophone.*

A.6	Ontwikkeling (Levensduur)	De ontwikkeling van het internetstemsysteem dient er op gericht te zijn dat het internetstemsysteem tenminste 10 jaar wordt gebruikt en gedurende die tijd zal moeten worden onderhouden en doorontwikkeld. *Nationale verkiezingen worden gemiddeld niet meer dan eens per jaar gehouden. Een internetstemsysteem zal dus meerdere jaren gebruikt moeten kunnen worden om de investering te verantwoorden.*

B. Eisen aan de performance van het internetstemsysteem

B.1	Performance (Capaciteit)	Het internetstemsysteem dient voldoende capaciteit te kunnen bieden voor een verkiezing waarin tenminste een miljoen kiezers hun stem uitbrengen in een aaneengesloten periode van 3 dagen met een voorafgaande, enkele weken durende registratieperiode. *De cijfers zijn gebaseerd op de doelgroep kiesgerechtigden buiten Nederland bij een Tweede Kamer verkiezing.*
B.2	Performance (Schaalbaarheid)	Het internetstemsysteem moet schaalbaar zijn om rekening te houden met een eventuele toekomstige groei van de doelgroep. *Het uitbreiden van de capaciteit van het systeem dient mogelijk te zijn zonder aanpassing van de software. Het opschalen van de gebruikte hardware en infrastructuur dient voldoende te zijn.*
B.3	Performance (Beschikbaarheid)	Het internetstemsysteem dient een beschikbaarheid van 99.9% per dag te kunnen leveren tijdens een verkiezing en 99% per dag tijdens de voorgaande registratieperiode. *Dit houdt een maximale downtime van anderhalve minuut per dag tijdens de verkiezing en 15 minuten per dag tijdens de registratiefase in.* *Hoewel de beschikbaarheid ook afhankelijk is van de exploitatie van het systeem, dient tijdens het ontwikkelen rekening te worden gehouden met de gewenste beschikbaarheid zodat dit geen bottleneck is.*
B.4	Performance (Responstijden)	Het internetstemsysteem dient adequate responstijden te bieden aan de gebruikers. *Adequaatheid dient te worden aangetoond door de leverancier op basis van gebruikerstesten.*

C. Eisen aan de toegankelijkheid van het internetstemsysteem

C.1	Toegankelijkheid (Stemgemak)	Het internetstemsysteem moet begrijpelijk en eenvoudig te gebruiken zijn voor kiezers. Het systeem moet dusdanig intuïtief zijn, dat een onervaren computergebruiker bij zijn eerste gebruik van het internetstemsysteem zonder hulp zijn stem kan uitbrengen.
C.2	Toegankelijkheid (Browsers en	Het internetstemsysteem dient bruikbaar te zijn voor kiezers die gebruik maken van de populaire versies van verschillende

	Operating Systems)	browsers (Internet Explorer, Mozilla Firefox) en operating systems (Windows, Mac OS, Linux). *Als definitie van populair kan een marktaandeel van tenminste 5% gehanteerd worden.*
C.3	Toegankelijkheid (Buitenland)	Bij de ontwikkeling van het systeem en met name de keuze van de gebruikte cryptografische technieken moet er naar gestreefd worden het gebruik van het internetstemsysteem voor zo min mogelijk personen te beperken. De clientzijde van de stemapplicatie bestaat slechts uit een standaard internet browser en het gebruik van crypto in het stemsysteem is beperkt tot de standaard crypto (https). *Verschillende landen hanteren wettelijke restricties op het gebruik van cryptografie door particulieren. Dergelijke restricties kunnen tot gevolg hebben dat in bepaalde landen het gebruik van het internetstemsysteem juridische problemen oplevert.*
C.4	Toegankelijkheid (Webrichtlijnen)	Het internetstemsysteem moet zoveel mogelijk voldoen aan de Webrichtlijnen voor de overheid. *De Webrichtlijnen zijn te vinden op webrichtlijnen.overheid.nl*
C.5	Toegankelijkheid (Burger Service Code)	Het internetstemsysteem moet zoveel mogelijk voldoen aan de 10 punten van de BurgerServiceCode. *De BurgerServiceCode is te vinden op www.burger.overheid.nl/wat_wij_doen/burgerservicecod*
C.6	Toegankelijkheid (Web Accessibility Initiative)	Het internetstemsysteem moet zoveel mogelijk voldoen aan de richtlijnen van het Web Accessibility Initiative. *Het WAI streeft toegankelijkheid voor gehandicapten na. De richtlijnen zijn te vinden op www.w3.org/WAI.*

D. Eisen aan de controleerbaarheid van het internetstemsysteem

D.1	Controleerbaarheid (Codereview)	Voor de verkiezing dient de werking van het internetstemsysteem op codeniveau volledig geverifieerd en gecertificeerd te kunnen worden door partijen die door de Opdrachtgever worden gekozen.
D.2	Controleerbaarheid (Actieve code)	Tijdens de verkiezing dient controleerbaar te zijn dat het actieve internetstemsysteem inderdaad gelijk is aan de vooraf gecontroleerde code. *Waarnemers moeten kunnen verifiëren dat op servers de goede programmatuur draait, kiezers moeten kunnen verifiëren dat code die op de pc van de kiezer wordt uitgevoerd authentiek is.*
D.3	Controleerbaarheid (Statusinformatie)	Het Internetstembureau, de Opdrachtgever en de beheerders hebben, ieder vanuit hun eigen (wettelijke) rol, gedurende het hele verkiezingsproces de beschikking over actuele informatie betreffende het functioneren van het internetstemsysteem. *Hier gaat het bijvoorbeeld om de belasting van de servers en het aantal kiezers dat aan het stemmen is.*

D.4	Controleerbaarheid (Waarschuwingen)	Het internetstemsysteem dient de eigen toestand en beschikbare statusinformatie zelf constant te analyseren om aanvallen en andere problemen te detecteren. In het geval van problemen dient het systeem door middel van een alarmeringsmechanisme betrokken verantwoordelijken te kunnen waarschuwen.
D.5	Controleerbaarheid (Waarnemers)	Het internetstemsysteem dient functionaliteit te bezitten om het onafhankelijke waarnemers mogelijk te maken tijdens een verkiezing aspecten van de verkiezing te observeren.
D.6	Controleerbaarheid (Proces-verbaal)	Het internetstemsysteem genereert de wettelijk voorgeschreven verantwoordingsinformatie, onder andere ten behoeve van het proces-verbaal van het internetstembureau.
D.7	Controleerbaarheid (Logging)	Alle gebeurtenissen in het internetstemsysteem dienen te worden gelogd om controle/audit op een later moment mogelijk te maken. Er mag echter geen informatie bewaard worden die, op zichzelf of in combinatie met andere informatie, kan leiden tot een schending van het stemgeheim. Het loggingmechanisme is gescheiden van, en niet te beïnvloeden door, de rest van het internetstemsysteem en is beschermd tegen wijziging en verwijdering van gegevens.

E. Eisen aan de beveiliging van het internetstemsysteem

E.1	Beveiliging (Standaard)	Leidraad bij de ontwikkeling van het internetstemsysteem dient te zijn dat het systeem voldoet aan de eisen die gesteld worden in de Code voor Informatiebeveiliging (ISO 27001 en ISO 27002). *De Code voor Informatiebeveiliging stelt primair eisen aan een organisatie. De organisatie die betrokken zijn bij de ontwikkeling en exploitatie van het stemsysteem dienen deze Code als richtlijn te hanteren.*
E.2	Beveiliging (Protection Profile)	Leidraad bij de ontwikkeling van het internetstemsysteem dient te zijn dat het systeem voldoet aan de eisen die gesteld worden in het in ontwikkeling zijnde Protection Profile voor remote electronic voting. *Momenteel is een volgens de Common Criteria (ISO/IEC 15408) opgesteld Protection Profile voor remote electronic voting in ontwikkeling in de academische wereld. Ontwikkelingen op dit gebied dienen te worden gevolgd en de bruikbaarheid in de context van deze eisen dient te worden geanalyseerd.*
E.3	Beveiliging (Functiescheidin g)	Het internetstemsysteem onderscheidt verschillende rollen. De verschillende rollen hebben verschillende rechten in het internetstemsysteem. Personen dienen geauthenticeerd te worden om een rol te kunnen uitoefenen en mogen slechts één rol hebben binnen het systeem. *De bij de inleiding van deze eisen aangegeven rolverdeling kan als initiële leidraad dienen. De exacte rolverdeling dient nader te worden vastgesteld tijdens het ontwikkelingsproces.*
E.4	Beveiliging (Gezamenlijke	Handelingen waarvoor (onder andere wettelijk) is vastgelegd dat ze meerdere personen vergen, dienen alleen uit te voeren

	handelingen)	te zijn door de benodigde personen in gezamenlijkheid nadat zij zijn geauthenticeerd.
E.5	Beveiliging (Vooruitgang)	Het internetstemsysteem moet zo ontworpen zijn dat het mogelijk is de gebruikte beveiligingstechnieken (zoals cryptografie) aan te passen aan vooruitgang op dit gebied, zonder dat dit ingrijpende veranderingen in de rest van het systeem vergt.
E.6	Beveiliging (Toekomstbestendig)	Het internetstemsysteem dient zo te zijn ontworpen dat, mocht in de toekomst de tijdens een verkiezing gebruikte cryptografie worden gebroken, dit niet kan leiden tot het breken van het stemgeheim op basis van publiek gemaakte informatie. *Bijvoorbeeld: het openbaar maken van versleutelde bestanden waarin de link tussen kiezers en stemmen aanwezig is, is dus geen optie.*
E.7	Beveiliging (Backup data)	Omdat eventuele storingen in het internetstemsysteem niet mogen leiden tot verlies van data, moet er tijdens de exploitatie een live backup worden bijgehouden van alle data. *Het moet bijvoorbeeld onmogelijk zijn dat een storing halverwege een verkiezing als gevolg heeft dat de tot dan toe uitgebrachte stemmen verloren gaan.*
E.8	Beveiliging (Redundantie)	Het internetstemsysteem dient volledig redundant te kunnen worden opgezet. Het uitvallen van één onderdeel van het systeem mag nooit leiden tot een onderbreking van de dienst. *Alhoewel het werkelijk redundant uitvoeren een onderdeel van de exploitatie is, moet het systeem zo ontwikkeld worden dat de mogelijkheid bestaat.*
E.9	Beveiliging (Denial of Service)	Het internetstemsysteem dient bestand te kunnen worden gemaakt tegen Distributed Denial of Service aanvallen. *Alhoewel dit primair een zaak is van de exploitatie (servers, infrastructuur) van het systeem, is het van belang dat bij het ontwerpen rekening wordt gehouden met dit type aanval.*
E.10	Beveiliging (Vijandige omgeving)	Het internetstemsysteem dient bruikbaar te zijn in een omgeving die als vijandig kan worden aangemerkt (met spyware/virussen geïnfecteerde computers van kiezers), zonder dat dit kan leiden tot problemen zoals manipulatie van de stem of schending van het stemgeheim.
E.11	Beveiliging (Vijandige infrastructuur)	Het internetstemsysteem dient de communicatie tussen zichzelf en de pc van de kiezer afdoende te kunnen beveiligen om de integriteit, authenticiteit en geheimhouding van de communicatie via een ongecontroleerde infrastructuur (het internet) te garanderen.
E.12	Beveiliging (Integriteit data)	De integriteit van data in het internetstemsysteem moet gecontroleerd kunnen worden, zowel voor, tijdens als na de verkiezing. *Het gaat hierbij bijvoorbeeld om het kunnen vaststellen dat de actieve kandidatenlijst de originele is en niet gewijzigd is, bijvoorbeeld door cryptografische hashes van de bestanden te controleren.*

E.13	Beveiliging (Interne fraude)	Het dient onmogelijk te zijn voor betrokkenen bij de exploitatie van het internetstemsysteem om de verkiezing te beïnvloeden, bijvoorbeeld door stemmen te wijzigen, te verwijderen of toe te voegen, of het stemgeheim te breken.

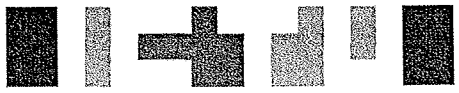
F. Eisen aan de component Registratie van het internetstemsysteem

Het registreren van kiezers en het verspreiden van het stemtoken (bijvoorbeeld cryptografische toegangsgegevens) dat toegang verleent tot het internetstembureau zal onderdeel moeten zijn van het internetstemsysteem. Over dit onderdeel bestaat nog veel onzekerheid. Deze splitst zich onder andere toe op de volgende punten:

- **Nationale of regionale registratie.** Op dit moment is de registratie van buiten Nederland gevestigde Nederlanders verspreid over de Nederlandse gemeentes. Het ICTU project *Registratie Niet Ingezetenen* (RNI) ontwikkelt een nationaal register van deze groep Nederlanders. In de context van dit internetstemsysteem zou een dergelijk register zeer nuttig zijn. Het is echter onzeker wanneer dit register voltooid zal zijn.
- **Papier of digitaal.** In de *Kiezen Op Afstand* (KOA) experimenten in 2004 en 2006 vond registratie van kiezers en het opsturen van stembescheiden plaats via de post. Dit zou echter ook volledig via internet kunnen plaatsvinden. De keuze tussen papier en digitaal is nog niet gemaakt.
- **Authenticatie.** Een cruciaal punt is hier de wijze van authenticatie van kiezers. De papieren vorm van authenticatie is traditioneel het opsturen van een kopie van het paspoort. Digitale authenticatie zou kunnen plaatsvinden op basis van DigiD en dan bij voorkeur met behulp van de in ontwikkeling zijnde *elektronische Nederlandse identiteitskaart* (eNIK). Het is echter onzeker wanneer de eNIK bruikbaar en voldoende verspreid zal zijn in de doelgroep.
- **Actieve of passieve registratie.** De keuze dient gemaakt te worden of kiezers zich actief op eigen initiatief dienen te registreren voor een verkiezing, of dat zij automatisch ingeschreven worden en bericht krijgen.
- **Wijze van stemmen.** Het is essentieel dat kiezers naast de mogelijkheid tot stemmen via internet ook de mogelijkheid hebben om te kiezen voor stemmen per post. Dit roept echter de vraag op of kiezers voor de verkiezing één van de twee methoden moeten kiezen, of dat zij voor beiden stembescheiden ontvangen en tijdens de verkiezing de keuze pas maken.
- **Scope.** Alhoewel het opzetten van een kiesregister niet binnen de scope van deze opdracht valt, is het gebruiken van de informatie binnen dat kiesregister wel deel van een internetstemsysteem. De scheiding tussen de twee is niet eenvoudig. Het bruikbaar maken van de kiesregisters voor direct gebruik van de gegevens door het internetstemsysteem kan aanpassingen vergen in de opzet van de kiesregisters.

De bovenstaande issues maken het specificeren van eisen voor het deel van het internetstemsysteem dat de registratie van kiezers verzorgt een complexe zaak. De onderstaande eisen vormen een poging enige richting te geven.

F.1	Registratie (Samenwerking)	Het Kiesregister controleert de kiesgerechtigdheid van kiezers, het Sleutelbeheer verstrekt op basis van die informatie de sleutels die toegang geven tot de stemdienst. In samenwerking, maar ieder met een duidelijk gescheiden taak, dienen zij kiesgerechtigden toegang te kunnen geven tot de stemdienst.
F.2	Registratie (Scheiding	Het Kiesregister is de enige partij in het verkiezingsproces die de persoonsgegevens van kiezers mag bezitten. Het



	gegevens)	Sleutelbeheer is de enige partij die de cryptografische toegangsgegevens mag bezitten die kiezers gebruiken om toegang tot het internetstembureau te krijgen. Er mag geen enkele partij binnen het internetstemsysteem zijn die de beschikking heeft over beide gegevens.
F.3	Registratie (Anonimisering)	Identificerende gegevens van de kiezer zoals zijn IP adres mogen niet bij het Sleutelbeheer beschikbaar zijn of beschikbaar gemaakt kunnen worden. *Er zou bijvoorbeeld voor gekozen kunnen worden een reverse proxy toe te voegen die het verkeer van de kiezer anonimiseert voor het naar het sleutelbeheer gaat.*
F.4	Registratie (Revocatie)	Wanneer een kiezer zijn door het Sleutelbeheer verstrekte toegangsgegevens kwijt raakt, of deze niet langer geheim zijn, moet het mogelijk zijn de originelen ongeldig te maken en nieuwe gegevens te verstrekken.
F.5	Registratie (Technologie)	Het internetstemsysteem moet flexibel genoeg zijn om authenticatie van kiezers, registratie van kiezers, en het verstrekken van toegangsgegevens tot het internetstembureau zowel via de post als via internet te kunnen ondersteunen. *Afhankelijk van de ontwikkelingen die buiten dit project vallen zal voor de papieren of digitale variant gekozen moeten worden. Het internetstemsysteem zal, tot de keuze gemaakt is rekening moeten houden met verschillende mogelijkheden.*
F.6	Registratie (Koppeling met authenticatie)	Het Sleutelbeheer verschaft de cryptografische toegangsgegevens die bij het Internetstembureau in het authenticatieproces moeten worden gecontroleerd. Het internetstemsysteem moet dus een koppeling tussen deze twee componenten bevatten. *Hier kan zowel gekozen worden voor een offline oplossing, waar alle benodigde gegevens voor het begin van een verkiezing door het sleutelbeheer aan de authenticatiecomponent worden geleverd, als een online oplossing waar de authenticatiecomponent tijdens de verkiezing deze gegevens kan opvragen bij het sleutelbeheer wanneer ze benodigd zijn.*

G. Eisen aan de component Internetstembureau - Authenticatieproces van het internetstemsysteem

G.1	Authenticatie (Kiesrecht)	Het authenticatieproces controleert op basis van gegevens die zijn verkregen van het sleutelbeheer of een kiezer toegang mag krijgen tot het Internetstembureau. Alleen kiesgerechtigden krijgen toegang. *De kiesgerechtigden hebben van het sleutelbeheer een stemtoken ontvangen dat ze vervolgens gebruiken om zich te authenticeren bij het internetstembureau.*
G.2	Authenticatie (Uniciteit)	Kiezers mogen slechts één keer hun stem uitbrengen. Als een kiezer zijn stem succesvol heeft uitgebracht, krijgt hij geen verdere toegang meer tot het Internetstembureau.

G.3	Authenticatie (Herhaald authenticeren)	Mocht een kiezer het stemmen onderbreken voordat hij zijn stem succesvol heeft uitgebracht, dan moet deze kiezer opnieuw geauthenticeerd kunnen worden om alsnog zijn stem uit te brengen. *Het kan voorkomen dat een kiezer zelf besluit om op een later moment te stemmen of tijdens het stemmen door technische problemen de verbinding met het internetstemsysteem verliest. In dat geval moet de kiezer op een later moment alsnog toegang kunnen krijgen.*
G.4	Authenticatie (Brute Force)	Het moet praktisch onmogelijk zijn om door middel van een brute force aanval geldige toegangsgegevens te raden. Het authenticatieproces dient detectiemechanismen te bevatten die brute force aanvallen kunnen ontdekken en melden. *De te doorzoeken ruimte van mogelijke toegangsgegevens moet ruimschoots groot genoeg zijn om het raden van geldige toegangsgegevens praktisch onmogelijk te maken binnen de tijdspanne van een verkiezing, zelfs als een aanvaller grote hoeveelheden resources ter beschikking heeft.*
G.5	Authenticatie (Anonimisering)	Identificerende gegevens van de kiezer zoals zijn IP adres dienen niet binnen het Internetstembureau beschikbaar te zijn of beschikbaar gemaakt te kunnen worden. *Er zou voor gekozen kunnen worden om voor het authenticatieproces een reverse proxy toe te voegen die het verkeer van de kiezer anonimiseert voor het naar het internetstembureau gaat.*

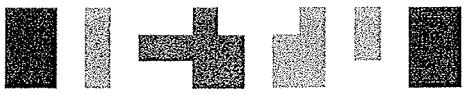
H. Eisen aan de component Internetstembureau – Keuzeproces van het internetstemsysteem

H.1	Keuze (Type verkiezing)	Het internetstemsysteem ondersteunt in ieder geval alle typen verkiezingen die in de Nederlandse Kieswet zijn opgenomen. Verder ondersteunt het systeem het houden van referenda. De keuze van het type verkiezing en veranderingen in een type dienen in het systeem te kunnen worden verwerkt door middel van configuratie, zonder dat aanpassing van de software nodig is.
H.3	Keuze (Neutraliteit)	Alle partijen en kandidaten worden op een identieke en neutrale manier gerepresenteerd. Op de schermen is geen enkele andere informatie weergegeven dan noodzakelijk voor het uitbrengen van een stem. Ieder kiezer krijgt in het keuzeproces een identieke opmaak van de schermen.
H.4	Keuze (Uniciteit)	Een kiezer mag per vraagstuk waarvoor hij zich mag uitspreken slechts één keer zijn stem uitbrengen.
H.5	Keuze (Bevestiging)	Om een definitieve keuze te maken, moet een kiezer zijn stem expliciet bevestigen. Het internetstemsysteem waarborgt dat de stem van de kiezer goed wordt weergegeven en dat het ook deze stem is die in de stembus belandt.
H.6	Keuze (Wijzigen)	Tot het moment van de bevestiging mag de kiezer zijn stem nog wijzigen of het stemproces afbreken, zonder dat zijn keuze op enige manier wordt vastgelegd.

H.7	Keuze (Afronding)	Het keuzeproces moet duidelijk aangeven dat met succes een stem is uitgebracht en dat daarmee de procedure voor de kiezer is voltooid.
H.8	Keuze (Vastlegging stem)	De keuze van een kiezer dient op geen enkele andere manier te worden vastgelegd dan in zijn stem die in de stembus terecht komt.
H.9	Keuze (Bewijs stem)	Het moet onmogelijk zijn om een verband te leggen tussen de identiteit van een kiezer en de inhoud van zijn stem. Een stemgerechtigde mag daarom geen overdraagbaar bewijs van de inhoud van zijn stem krijgen van het internetstemsysteem. *Het internetstemsysteem mag kiezers de mogelijkheid bieden om te controleren dat hun stem is meegeteld, mits de inhoud van de stem niet te controleren is.*

I. Eisen aan de component Internetstembureau – Stembus van het internetstemsysteem

I.1	Stembus (Stemmen toevoegen)	Het is uitsluitend via het officiële kiesproces mogelijk om een stem aan de stembus toe te voegen.
I.2	Stembus (Uitgebrachte stemmen)	Wanneer een stem via het officiële kiesproces is uitgebracht en in de stembus terecht is gekomen, kan deze op geen enkele wijze meer gewijzigd, noch verwijderd worden.
I.3	Stembus (Sluiting)	Na het sluiten van de toegang tot het internetstembureau, hebben kiezers die zich reeds hebben geauthenticeerd maar nog geen stem hebben uitgebracht nog enkele minuten om het stemproces te voltooien.
I.4	Stembus (Telling)	Het openen van de stembus vergt de samenwerking van de leden van het Internetstembureau. Het openen van de stembus start het tellen van de uitgebrachte stemmen door het internetstemsysteem.
I.5	Stembus (Uniciteit)	Bij de stemmentelling wordt iedere geldige stem precies één keer meegeteld.
I.6	Stembus (Uitslag)	De uitslag moet uiterlijk 10 minuten na het openen van de stembus en het starten van de telling door het internetstemsysteem bij de leden van het internetstembureau bekend zijn.
I.7	Stembus (Hertelling)	Er dient, conform wettelijke vereisten, een hertelling van de stemmen te kunnen worden uitgevoerd op basis van de oorspronkelijke ten tijde van de sluiting van de stembus in de stembus aanwezige stemmen.
I.8	Stembus (Geen tussentijdse uitslag)	De internetstemdienst dient niet toe te staan dat een tussentijdse stand van zaken voor wat betreft de inhoud van de uitgebrachte stemmen in de stembus gegenereerd kan worden.



J. Juridische eisen omtrent het internetstemsysteem

Algemeen

J.1	Waarborgen verkiezingsproces	Leverancier dient te allen tijde de door de Commissie Korthals Altes[2] geformuleerde waarborgen in acht te nemen bij de ontwikkeling van het internetstemsysteem. Leverancier zal tot genoegen van Opdrachtgever moeten beschrijven hoe aan deze waarborgen zal worden voldaan en tot welke gevolgen dat eventueel leidt.
J.2	Kwaliteitsbewaking / audit	Opdrachtgever behoudt zich het recht voor om op elk moment tijdens de uitvoering van de Overeenkomst deze uitvoering door auditors te laten toetsen[3]. Leverancier is verplicht het personeel van Opdrachtgever toegang te verlenen tot de plaats waar de werkzaamheden ten behoeve van de overeengekomen diensten worden verricht. Dit om na te gaan of er in voldoende mate is voorzien in de overeengekomen veiligheidsmaatregelen. Eventueel toepasselijke overheidsvoorschriften dienen in het contract te worden geïncorporeerd.

Eigendom

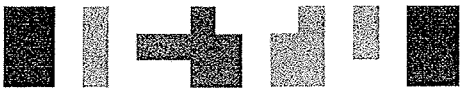
J.3	IE-rechten	Opdrachtgever wil in staat zijn zonder beperkingen op het gebied van IE-rechten, het internetstemsysteem in te voeren, al dan niet door daartoe Leverancier en/of concurrerende derden in te schakelen.
J.4	Overdracht[4]	Alle intellectuele en industriële (eigendoms-)rechten ten aanzien van het internetstemsysteem (inclusief FO, TO, documentatie, materialen e.d.) berusten bij Opdrachtgever. *Alternatief: open source[5], in welk geval:* • *De broncode van de software vrij beschikbaar en adequaat gedocumenteerd dient te zijn* • *Het mogelijk moet zijn om aanpassingen of bewerkingen aan de software aan te brengen of aan te laten brengen door een derde partij*
J.5	Octrooi	Eventueel aanwezige octrooien ten aanzien van het internetstemsysteem worden overgedragen aan Opdrachtgever, dan wel vormen geen belemmering voor gebruik door Opdrachtgever.
J.6	Vrijwaring	Leverancier verklaart dat de programmatuur geen rechten van derden schendt en dat Opdrachtgever door Leverancier wordt gevrijwaard tegen de gevolgen van een inbreuk op

[2] Zie pagina 7 van dit document.
[3] Zie ook pagina 87 van het adviesrapport van de Commissie Korthals Altes
[4] In lijn met de Algemene Voorwaarden voor het verstrekken van opdrachten door het ministerie van BZK tot het verrichten van diensten (AVODI-BZK).
[5] Zie pagina 34 van het adviesrapport van de Commissie Korthals Altes: "Alleen als de systemen volledig "open" zijn, bijvoorbeeld door het gebruik van opensource programmatuur, is er sprake van enige transparantie".

		intellectuele (eigendoms-)rechten van deze derden, zogenaamde persoonlijkheidsrechten alsmede aanspraken met betrekking tot know-how, ongeoorloofde mededinging e.d. daaronder begrepen, in verband met verveelvoudiging, openbaarmaking of gebruik van de (open source) software.
J.7	Overdracht materialen	Op de datum waarop een bepaalde fase in het project dient te zijn voltooid, zal Leverancier aan Opdrachtgever de in deze fase ontwikkelde componenten, alsmede alle andere gegevens, documentatie, technische ontwerpen, resultaten en instructies beschikbaar stellen. Leverancier zal tegelijkertijd de broncode van de terzake ontwikkelde programmatuur aan Opdrachtgever overdragen.

Integriteit, beveiliging en geheimhouding

J.8	Garantie	Leverancier garandeert gedurende [zeven] jaar na Acceptatie dat het internetstemsysteem geen andere beveiligingsmaatregelen of -functies of voor het internetstemsysteem vreemde elementen bevat (zoals logic bombs, virussen, worms, etc.) dan die welke aan Opdrachtgever zijn bekendgemaakt.
J.9	Geen manipulatie	Leverancier garandeert gedurende [zeven] jaar na Acceptatie dat de resultaten van de verkiezingen die met het internetstemsysteem worden verworven 100% betrouwbaar zijn en dat deze niet gemanipuleerd en/of gewijzigd kunnen worden of anderszins kunnen worden gefrustreerd.
J.10	Geheimhouding	Leverancier zal strikte vertrouwelijkheid in acht nemen ten aanzien van de informatie over de organisatie van de Opdrachtgever, de functionele ontwerpen, de technische ontwerpen, de diverse componenten van het internetstemsysteem, de werking van de apparatuur, de bestanden, de apparatuur- en programmatuur en het internetstemsysteem in zijn geheel. Leverancier zal zijn personeel alsmede zijn onderaannemers c.q. leveranciers verplichten deze geheimhoudingsbepaling na te leven.
J.11	Personeel	Personeel van Leverancier dat betrokken is bij de uitvoering van de werkzaamheden, diens onderaannemers c.q. - leveranciers daaronder begrepen, voorzover die bij Opdrachtgever worden verricht, is verplicht door Opdrachtgever aangehouden beveiligingsprocedures in acht te nemen. Opdrachtgever is gerechtigd te vorderen dat van personeel alsmede onderaannemers c.q. -leveranciers, die door Leverancier bij de uitvoering van de Overeenkomst worden ingezet vooraf verklaringen omtrent het gedrag worden overlegd. Opdrachtgever is te allen tijde gerechtigd Personeel van Leverancier alsmede diens onderaannemers c.q. -



		leveranciers, die voor de uitvoering van de Overeenkomst zijn of zullen worden ingeschakeld, aan een veiligheidsonderzoek conform de bij de Opdrachtgever gebruikelijke regels te onderwerpen.

Garanties

[Let op: indien tot de verwerving van open source software wordt overgegaan, kunnen specifieke garanties op hun plaats zijn. Verwezen zij naar het handboek Open Source en Inkoop dat thans in de maak is (www.ososs.nl/node/65137]

J.12	Specifieke kenmerken stemproces	Leverancier garandeert dat de specifieke kenmerken van het stemproces zoals stemgeheim, betrouwbaarheid, controleerbaarheid en de wijze waarop de autorisatie van systemen en personen plaatsvindt, zullen worden gewaarborgd.
J.13	Overige overeenkomsten Leverancier	Leverancier garandeert dat de nakoming van de overeengekomen prestaties niet in strijd is met overige door of namens Leverancier gesloten overeenkomsten.

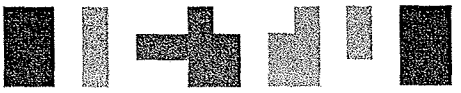
Onderhoud

[Let op: indien tot de verwerving van open source software wordt overgegaan, kunnen specifieke onderhoudsvoorwaarden op hun plaats zijn. Verwezen zij naar het handboek Open Source en Inkoop dat thans in de maak is (www.ososs.nl/node/65137]

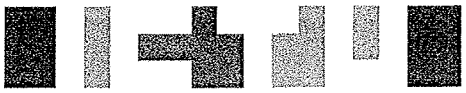
J.14	Garanties ten aanzien van de werking van het systeem	Leverancier garandeert gedurende [zeven] jaar na Acceptatie dat: 1. het internetstemsysteem ook bij piekbelasting de overeengekomen eigenschappen bevat, zoals vastgelegd in de Overeenkomst; 2. het internetstemsysteem efficiënt, deugdelijk en onderling samenhangend is ontworpen; 3. het internetstemsysteem geschikt is voor gebruik in samenhang met de door Opdrachtgever te gebruiken systeem en/of applicatie programmatuur en de overige bij de Opdrachtgever aanwezige apparatuur; 4. het internetstemsysteem zodanig is ontworpen dat door eenvoudige ingrepen de capaciteit en performance van het systeem kan worden uitgebreid. 5. het internetstemsysteem voldoet aan (internationale) technische normen.

Diversen

J.15	Aansprakelijkheid	Indien Leverancier toerekenbaar tekortschiet in de nakoming van zijn verplichting(en), is hij tegenover Opdrachtgever aansprakelijk voor vergoeding van de door Opdrachtgever geleden c.q. te lijden schade.



J.16	Verzekering	Leverancier dient zich adequaat te verzekeren voor de navolgende risico's: • wettelijke aansprakelijkheid • beroepsaansprakelijkheid
J.17	Change of control	Ontbindingsbevoegdheid voor Opdrachtgever indien de zeggenschap binnen (het consortium van) Leverancier wezenlijk wijzigt, welke van invloed is op de nakoming van de Overeenkomst.
J.18	Continuïteit	Bij het eindigen van de relatie tussen Opdrachtgever en Leverancier, zal Leverancier in goed overleg met Opdrachtgever de overeenkomst afwikkelen. Partijn zijn in dat geval gehouden al het redelijkerwijs mogelijke te doen om de continuïteit in de uitvoering van overheidstaken met betrekking tot het internetstemsysteem te verzekeren.
J.19	Opzegging door Opdrachtgever	Opdrachtgever is gerechtigd de overeenkomst tussentijds te beëindigen indien naar zijn redelijk oordeel ongewijzigde voortzetting van de overeenkomst niet langer opportuun is, bijvoorbeeld door veranderde politieke inzichten of indien Opdrachtgever van mening is dat de met dit project beoogde doelstellingen niet kunnen worden gerealiseerd.
J.20	Overig	Indien als gevolg van de aard van de aanbieding van Leverancier aanvullende bedingen dienen te worden overeengekomen, zullen deze bedingen in lijn zijn met het bovengenoemde en de positie van Opdrachtgever niet verzwakken.



4.4 Bronnen

Een selectie van de gebruikte bronnen.

- *Legal, operational and technical standards for e-voting*, Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 and explanatory memorandum, Council of Europe Publishing, http://www.coe.int/t/e/integrated_projects/democracy/02_activities/02_e-voting/01_Recommendation/
- *Stemmen met vertrouwen*, Adviescommissie inrichting verkiezingsproces, 27 september 2007, http://www.adviescommissieinrichtingverkiezingsproces.nl/aspx/download.aspx?file=/contents/pages/89904/advies.pdf
- Verslag van uitvoering experiment internetstemmen Tweede Kamerverkiezingen 2006, Project Kiezen op Afstand, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.
- Verslaglegging Project Kiezen op Afstand 2004, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.