> Retouradres

De minister van Binnenlandse Zaken en
Koninkrijksrelaties

Commissie Elektronisch
stemmen in het
stemlokaal

Datum 4 februari 2015
Betreft antwoorden op nadere vragen over elektronisch stemmen en tellen in het stemlokaal

Geachte heer Plasterk,

Op 16 september 2014 heeft u vijf nadere vragen gesteld aan de commissie Elektronisch stemmen in het stemlokaal (verder in deze brief als "de commissie" aangeduid). Alle leden van de commissie hebben zich bereid verklaard om uw vragen zo snel als mogelijk zou zijn te beantwoorden. Daartoe heeft de commissie op 22 september 2014 haar werkzaamheden weer hervat. Het rapport dat aan u is aangeboden op 18 december 2013 is uiteraard het vertrekpunt voor het beantwoorden van uw vragen. De commissie heeft ook nu weer enkele deskundigen geraadpleegd. Deze brief bevat de antwoorden op uw vragen. In de bijlage bij deze brief wordt bij sommige antwoorden nog een nadere toelichting gegeven. Gaarne is de commissie bereid om de antwoorden mondeling nader toe te lichten.

Beantwoording van de vragen

Vraag 1, 3 en 4

1. Deelt u het oordeel dat een beveiligingsprofiel van EAL[1] 5 of 6 tot gevolg heeft dat zowel de apparatuur als de programmatuur voor de stemprinter en stemmenteller specifiek moeten worden ontworpen en ontwikkeld? Zou dat het geval zijn, hoe duidt de commissie dan de gevolgen hiervan voor de complexiteit van het ontwerp- en ontwikkelingstraject van de stemprinter en stemmenteller?
3. Deelt u het oordeel dat de ontwikkeling van de stemprinter en stemmenteller (uitgaande van een beveiligingsprofiel van EAL 5 of 6) waarschijnlijk langer dan 1,5 jaar kan gaan duren? Kan de commissie een inschatting maken van de doorlooptijd voor de ontwikkeling en de certificering?

[1] EAL staat voor: Evaluation Assurance Level.

4. Kan de commissie een inschatting maken van de kosten van de stemprinter en de stemmenteller indien wordt uitgegaan van de aanname dat deze systemen niet kunnen worden samengesteld uit standaard componenten?

Antwoorden

De commissie heeft in haar rapport geconcludeerd dat vanwege de (beveiligings) maatregelen die zij wenselijk acht voor een Common Criteria[2] (CC) certificering een beveiligingsprofiel (EAL-niveau) van minimaal 5[3] zal moeten worden gehanteerd. Daarbij is aangetekend dat mogelijk voor de stemprinter een ander EAL-niveau gehanteerd zou moeten worden dan voor de stemmenteller. In bijlage 8[4] bij het rapport van de commissie wordt uitgegaan van EAL 6 voor de stemprinter en EAL 5 voor de stemmenteller.

De EAL-niveaus geven aan tegen welk niveau van dreigingen een systeem moet zijn beveiligd. De EAL-niveaus lopen van 1 tot en met 7. Hieronder wordt per EAL-niveau een duiding gegeven van instanties/personen die in staat worden geacht om een aanval uit te voeren op het betreffende niveau. Een certificering tegen dat niveau maakt het onwaarschijnlijk dat een dergelijke aanval zal kunnen slagen.

- **EAL 7 en 6: dreigingniveau hoog/high**

Beschermd tegen de kennis en mogelijkheden van een civiel beveiligingslab of een georganiseerde groep hackers of een universitair team gespecialiseerd in de technologie die wordt gebruikt in het product.

- **EAL 5: dreigingniveau matig/moderate**

Beschermd tegen de kennis en mogelijkheden van beveiligingsexperts (door leken "hackers" genoemd, hoewel sommige "hackers" mogelijk een hoger deskundigheidsniveau hebben).

- **EAL 4: dreigingniveau hoger dan basaal/enhanced basic**

Beschermd tegen de kennis en mogelijkheden van personen die beschikken over IT-vaardigheden op een bepaald technologisch gebied, maar niet gespecialiseerd zijn in het zoeken naar kwetsbaarheden.

- **EAL 3 en lager: dreigingniveau basaal/basic**

Beschermd tegen de kennis en mogelijkheden van personen die geen specifieke vaardigheden of kennis bezitten en zich alleen richten op algemeen bekende kwetsbaarheden, of in aanvulling daarop willekeurige pogingen doen om kwetsbaarheden te vinden. Als het gaat om Internet-technologie vallen bijvoorbeeld

[2] Common Criteria for Information Technology Security Evaluation (afgekort als Common Criteria of CC) is een internationale standaard (ISO/IEC 15408) voor de certificering van de beveiliging van computers.
[3] Pagina 46 van het rapport van de commissie.
[4] Pagina 163 van de rapportage functionele, technische en beveiligingseisen.

de zogenaamde "script-kiddies" in deze categorie, ofwel personen die gebruik maken van gepubliceerde hulpmiddelen voor de aanval op kwetsbaarheden zonder deze kwetsbaarheden noodzakelijkerwijs te begrijpen. De bijlage bij deze brief bevat een uiteenzetting van de verschillende beveiligingsniveaus met de daarbij behorende dreigingprofielen.

Het is inderdaad zo, u duidt daarop in uw brief, dat het ontwerpen en ontwikkelen van systemen die aan een EAL-niveau 5 of hoger moeten voldoen complexer zal zijn dan het ontwerpen en ontwikkelen van systemen die daar niet aan moeten voldoen. Het moeten voldoen aan een EAL-niveau 5 of hoger vergt namelijk een ontwerp- en ontwikkelingstraject dat veel nauwgezetter moet verlopen dan gangbaar is. De grotere complexiteit ontstaat ook omdat mogelijk niet of maar in beperkte mate gebruik gemaakt zal kunnen worden van standaard componenten.

Deskundigen verschillen enigszins van mening over de mate waarin wel of niet gebruik gemaakt zal kunnen worden van standaard componenten. Deskundigen uit de hoek van de organisaties die systemen evalueren in het kader van een CC-certificering achten het theoretisch mogelijk dat standaard componenten gebruikt zouden kunnen worden, maar de kans wordt klein geacht dat dit in de praktijk ook zal lukken. De reden daarvoor is dat de meeste standaard componenten niet zijn ontwikkeld om aan de beveiliging te voldoen die nodig is voor een EAL-niveau 5 en hoger. Het gebruik van standaard componenten is ook problematisch omdat een EAL-niveau 5 en hoger vergt dat de systemen volledig en gedetailleerd zijn gedocumenteerd. Dergelijke documentatie bestaat doorgaans niet van standaard componenten. Andere deskundigen afkomstig van bedrijven die systemen ontwikkelen, waaronder ook de apparatuur voor die systemen, achten de kans groter dat op onderdelen standaard componenten te gebruiken zijn.

De commissie deelt uw inschatting dat de ontwikkeling van de stemprinter en stemmenteller zeker 1,5 jaar zal duren en als de stemprinter en stemmenteller gecertificeerd moeten worden tegen een EAL-niveau van 5 of hoger zeker langer dan 1,5 jaar. Hoeveel langer kan de commissie niet bepalen. Ook de door de commissie geraadpleegde deskundigen kunnen dat niet precies zeggen, maar deze deskundigen zijn wel van mening dat dan het waarschijnlijk zal gaan om een doorlooptijd van meerdere jaren.

In haar rapport heeft de commissie reeds opgemerkt dat er te veel onzekerheden zijn om de kosten van de invoering en het gebruik van de stemprinter en stemmenteller nauwkeurig te bepalen[5]. Daarom is in het rapport een ruime marge aangehouden voor zowel de aanschafkosten (€ 150 à € 250 miljoen) als voor de structurele kosten per verkiezing (€ 6 à € 10 miljoen per verkiezing).

[5] Pagina 82 van het rapport van de commissie.

De commissie heeft zich in haar rapport van december 2013 gebaseerd op de raming van kosten van standaard componenten. Indien de stemprinter en stemmenteller zouden moeten voldoen aan een CC-certificering tegen een EAL-niveau van 5 of 6 dan zal, zoals blijkt uit het antwoord op vraag 1, het gebruik van standaard componenten niet of maar in beperkte mate mogelijk zijn.
De consultatie van deskundigen wijst uit dat bij een EAL-niveau van 5 en hoger er niet alleen maatwerk nodig zal zijn vanwege het niet kunnen gebruiken van standaard componenten. Het hele systeemontwerp zelf voor de stemprinter en stemmenteller zal maatwerk moeten zijn waarbij een groter aantal ontwikkel-iteraties nodig zal zijn. Dit heeft een kostenverhogend effect. Hoeveel duurder de stemprinters en stemmentellers dan zullen worden kan de commissie niet zeggen. Ook de geraadpleegde CC-deskundigen kunnen hiervan geen onderbouwde inschatting geven.

Vereist beveiligingsniveau opnieuw overwogen

Uw vragen over het beveiligingsprofiel en het antwoord daarop zijn voor de commissie aanleiding geweest om wederom te doordenken wat de gewenste beveiligingsprofielen voor de stemprinter en de stemmenteller zouden moeten zijn.

De opzet die de commissie voorziet voor het proces om een stembiljet te printen en het papieren stembiljet elektronisch te tellen, is er op gericht dat er vertrouwen kan ontstaan en behouden kan blijven in de tijdens de verkiezingen gebruikte programmatuur en apparatuur. Dat vertrouwen moet worden ontleend aan de volgende fundamenten:

- Het papieren proces is leidend. De kiezer zelf kan controleren of zijn/haar keuze voor een verkiezing correct op het stembiljet is geprint. Door middel van (handmatige) steekproefsgewijze controle wordt vervolgens vastgesteld dat de stembiljetten juist elektronisch zijn geteld. Voor programmatuur en apparatuur gelden robuuste beveiligingeisen. Eisen die onderhouden moeten worden, waarbij externe deskundigen nadrukkelijk een rol dienen te spelen. Als de eisen aanpassing behoeven zal dat moeten leiden tot aanpassingen in de stemprinter en stemmenteller;
- De stemprinter en stemmenteller moet CC-gecertificeerd worden waardoor onafhankelijke deskundigen vaststellen (evalueren) dat aan de eisen wordt voldaan.

In de literatuur[6] is de stelling te vinden dat een stemsysteem zonder leidend papieren proces het niveau EAL 6 of 7 zou moeten hebben. Als er een leidend papieren proces is, zoals het geval is in het concept van de commissie, dan kan volgens de betreffende auteur het EAL-niveau omlaag. Welk EAL-niveau wordt gekozen hangt af van de risico's die afgedekt moeten worden.

De commissie heeft in haar rapport met betrekking tot het vraagstuk van de compromitterende straling geconcludeerd dat ook het risico afgedekt moet zijn dat personen zullen willen bewijzen dat het mogelijk is een aanval succesvol uit te voeren met als doel aan te tonen dat ze in technische zin er in kunnen slagen "af te luisteren" welke keuze er met de stemprinter is gemaakt[7]. De vraag is of het wenselijk c.q. noodzakelijk is om deze redenering ook te hanteren voor alle risico's ten aanzien van de beveiliging. Met andere woorden: moet worden voorkomen dat personen kunnen aantonen dat ze de stemprinter en stemmenteller kunnen manipuleren? Als dat risico moet worden afdekt dan is bescherming tegen een "moderate attack potential" (corresponderend met EAL-niveau 5) het aangewezen niveau. Uitdrukkelijk wordt er op gewezen dat het slagen van een dergelijke aanval niet hoeft te betekenen dat de integriteit van de uitslag van een verkiezing daadwerkelijk in het geding is. Als de kiezers het geprinte stembiljet goed controleren én als de controle van de elektronisch getelde stembiljetten adequaat is dan zou het immers zo moeten zijn dat een manipulatie wordt ontdekt voordat de uitslag van de verkiezing wordt vastgesteld.

Ten aanzien van het risico dat het stemgeheim bedreigd zou kunnen worden omdat de keuze van de kiezer in de stemprinter zou worden opgeslagen wil de commissie u een nadere toelichting geven. Voorkomen moet worden dat deze els verkeerd wordt geïnterpreteerd.

De commissie heeft in haar rapport de eis geformuleerd dat de keuze van de kiezer niet mag worden opgeslagen in de stemprinter. Daarbij is vermeld dat dit vastgesteld moet worden in het certificeringtraject en bij testen. De rapporten hierover moeten openbaar zijn, zodat de kiezer kan controleren dat de keuze niet in de stemprinter wordt opgeslagen. De commissie wijst erop dat om de keuze van de kiezer te kunnen printen (voor korte duur) een tijdelijke vorm van opslag niet te vermijden is. Na het printen van de keuze moet echter, met gebruikmaking van de verwijdertechnieken die gangbaar zijn, de keuze gewist worden. Het is desondanks mogelijk dat in de stemprinter sporen van de keuze achterblijven. Het moet

---

[6] http://people.csail.mit.edu/rivest/pubs/RW06.pdf. Ron Rivest: "On the notion of "software Independence" in voting systems". Ron Rivest, 2006. Hij is een Amerikaans wiskundige en informaticus. Hij is gespecialiseerd in cryptografie en is (mede-)ontwerper van verschillende algoritmes op dit gebied. Daarnaast is hij bekend om zijn algemene werk op het gebied van algoritmen in de theoretische informatica. Hij is werkzaam als hoogleraar informatica aan de faculteit Elektrotechniek en Informatica bij het Massachusetts Institute of Technology.
[7] Pagina 29 van het rapport van de commissie.

naar de mening van de commissie onmogelijk zijn om, anders dan met forensische middelen en technieken, bij deze sporen te kunnen komen.

De commissie hecht er ook aan om te memoreren dat het kunnen achterhalen van de keuze van een kiezer in de stemprinter (nog) niet betekent dat het stemgeheim zal zijn doorbroken. Daarvoor moet immers nog de identiteit van de kiezer achterhaald kunnen worden. Op de stemprinter zelf is dat niet mogelijk, omdat de stemprinter geen identificerende gegevens over de kiezer opslaat.

De commissie heeft ook de gelegenheid genomen om een verdere uitwerking te laten maken van de methode om te controleren of de papieren stembiljetten correct elektronisch zijn geteld. De commissie heeft professor dr. E. Wit van de Universiteit Groningen gevraagd om voorstellen te doen voor de uitwerking. Het rapport van professor Wit is als bijlage bij deze brief gevoegd.

Het werk van professor Wit laat zien dat een steekproefsgewijze controle mogelijk is. Het rapport gaat er van uit dat het genereren van de lijsten met de te controleren stembiljetten centraal getrokken wordt. Elk stembureau krijgt gesloten enveloppen met daarin de lijsten van de te controleren stembiljetten. Nadat de stembiljetten elektronisch zijn geteld wordt de enveloppe geopend en de steekproef uitgevoerd.

De commissie is zich er van bewust dat het controleproces van de elektronisch getelde papieren stembiljetten het nodige zal vergen van de organisatie van de verkiezing. In de wet- en regelgeving zal de controlemethode en de wijze waarop die moet worden geïmplementeerd heel zorgvuldig moeten worden uitgewerkt. Tenslotte wijst de commissie erop dat de processen-verbaal van de stembureaus zo snel als mogelijk nadat ze zijn opgemaakt dienen te worden gepubliceerd zodat eenieder die dat wil zelf kan controleren dat de optelling van de uitgebrachte stemmen op de lijsten en kandidaten vertrouwd kan worden. Dit is nodig omdat de methode van professor Wit niet voorziet in een controle van de juiste optelling van de getelde stembiljetten, maar louter op de controle of de stemmenteller juist heeft geïnterpreteerd wat er op individuele stembiljetten staat.

Politiek zal een keuze gemaakt moeten worden omtrent de foutmarge die geaccepteerd wordt ten aanzien van de werking van de stemmenteller. Hoe meer zekerheid er gewenst wordt omtrent de betrouwbaarheid van de controle hoe groter het aantal getelde stembiljetten dat zal moeten worden gecontroleerd. Het rapport van professor Wit geeft de bouwstenen aan de hand waarvan de politiek deze keuze kan maken.

Concluderend ten aanzien van vraag 1, 3 en 4

De hiervoor gegeven antwoorden laten zich samenvatten in onderstaande tabel:

EAL-niveaus	Complexiteit, doorlooptijd en kosten	Afgedekt dreiging-niveau volgens CC
1 t/m 3	**Complexiteit:** vergelijkbaar met een gangbaar ICT-project (inclusief de daarbij behorende risico's en onzekerheden). **Doorlooptijd**: ca 1,5 jaar te rekenen vanaf het moment dat de opdracht aan een leverancier is gegeven. **Kosten** binnen de bandbreedte die de commissie in haar rapport heeft genoemd dwz: investering 150-250 mln Euro. Extra kosten per verkiezing: 6 à 10 mln Euro.	Basic/Basaal
4	**Complexiteit:** vergelijkbaar met een gangbaar ICT-project indien grotendeels gebruik kan worden gemaakt van standaard componenten. Is dat voor een deel niet mogelijk dan complexer vanwege maatwerk aan apparatuur en programmatuur. **Doorlooptijd**: afhankelijk van hoeveelheid maatwerk aan apparatuur en programmatuur. Waarschijnlijk langer dan bij EAL 1 t/m 3. **Kosten:** als de hoeveelheid maatwerk beperkt kan blijven dan zullen kosten waarschijnlijk aan de bovenkant van de bandbreedte liggen die de commissie in haar rapport heeft genoemd.	Hoger dan basaal/Enhanced basic
5 en 6	**Complexiteit:** heel complex vanwege noodzakelijk maatwerk aan apparatuur en programmatuur. Alleen technisch haalbaar met leverancier die ervaring heeft met ontwikkeling van systemen die CC-gecertificeerd zijn tegen EAL-4 of hoger. **Doorlooptijd**: mogelijk jaren meer dan bij EAL 1 tot en met 4. **Kosten:** Zeker hoger dan bij EAL 1 t/m 4. Hoeveel hoger niet te ramen.	EAL 5: Matig /Moderate EAL-6: Hoog/High

Uiteindelijk is het een politieke afweging welk risico wel of niet aanvaardbaar is. Als het kabinet het acceptabel vindt dat personen die al dan niet deskundig zijn, bijvoorbeeld op basis van gepubliceerde documentatie over de stemprinter en stemmenteller, in het openbaar beweren danwel aantonen dat de beveiliging tekort schiet dan zou een lager beveiligingsprofiel gekozen kunnen worden. Er moet dan wel de politieke bereidheid bestaan om, als deze situatie zich voordoet, te verdedigen dat dit risico bewust is ingecalculeerd doordat wordt vertrouwd op zowel de controle die de kiezer moet uitvoeren (op de juiste werking van de stemprinter) als op de steekproefsgewijze controle van de elektronisch getelde stembiljetten. Of dit voldoende zal zijn om het vertrouwen in de stemprinter en/of stemmenteller niet te laten eroderen kan de commissie niet zeggen. Dat zal in de praktijk moeten blijken.

Vraag 2

Indien het juist is dat een deel van de stemprinters na gebruik bij één of meerdere verkiezingen niet meer zal voldoen aan de norm voor de compromitterende straling, dan zal een steekproefsgewijze tempestmeting alleen er toe leiden dat een gedeelte van de stemprinters die niet meer voldoen wordt hersteld. Bij een volgende verkiezing zullen dan stemprinters in gebruik zijn die niet aan de norm voldoen. Is in dat geval in alle stemlokalen het stemgeheim op gelijke wijze gewaarborgd?

Antwoord

De commissie heeft in haar rapport van december 2013 onderkend dat de stemprinter na gebruik bij een verkiezing mogelijk niet meer zal voldoen aan de NATO-norm. Dat is de reden geweest waarom de commissie heeft geadviseerd periodiek een deel van de stemprinters opnieuw te meten.

De commissie veronderstelt dat deze periodieke metingen positief zullen uitvallen, dat wil zeggen dat de meting zal uitwijzen dat de stemprinter nog aan de norm voldoet. Deze aanname is gebaseerd op de gedachte dat de tempest maatregelen die worden getroffen zo robuust zullen zijn dat vervoer en gebruik geen effect zullen hebben op de effectiviteit van de maatregelen. Of deze aanname in de praktijk waargemaakt kan worden kan de commissie niet met zekerheid zeggen. Daarvoor zouden er testen moeten worden gedaan met stemprinters waarbij het werkelijke gebruik (inclusief het vervoer, deconfigureren, etc.) wordt gesimuleerd. Er kan dan ook worden bekeken of er zinvolle fysieke controles (aan de behuizing) mogelijk zijn om te bepalen of een stemprinter mogelijk niet meer aan de norm zal voldoen.

De enige weg om het risico verder te beperken waar u in uw vraag op doelt, te weten dat niet zeker is dat het stemgeheim in alle stemlokalen even goed gewaarborgd is als niet zeker is of de stemprinter die wordt gebruikt aan de NATO-norm voldoet, is om voor elke verkiezing alle stemprinters weer opnieuw te meten en waar nodig te herstellen zodat aan de norm wordt voldaan. Maar zelfs dan is het risico niet weg. Immers door het vervoer (na de meting) kan het voorkomen dat een stemprinter niet meer voldoet aan de norm. De commissie beveelt daarom (en ook vanwege de kosten) niet aan om voor elke verkiezing alle stemprinters opnieuw te meten.

De commissie betreurt het dat er geen andere normen zijn voor (compromitterende) straling dan de CE-markering en de NATO-norm. De CE-markering is te basaal[8]. Gelet hierop kan niet anders dan de NATO-norm gehanteerd worden om de stemprinter te beschermen tegen het "afluisteren" van de stemkeuze.

Vraag 5
Hoe groot acht de commissie de kans dat 1 stemprinter per stemlokaal zal volstaan, rekening houdend met meervoudige verkiezingen en rekening houdend met het feit dat het stemmen met het huidige stembiljet gemiddeld 28 seconden duurt en er in de stemlokalen nu meerdere stemhokjes staan? Indien de kans klein is, kan de commissie dan een inschatting maken van de extra kosten die daaruit voortvloeien voor de invoering van de stemprinter?

Antwoord

Voor het aantal benodigde stemprinters is de commissie uitgegaan van 10.000 stemprinters met daar bovenop ca 2.500 stemprinters om in te zetten als de systemen gebreken vertonen tijdens een verkiezing en vervangen moeten worden. Uitgaande van 10.000 stemlokalen is dat 1 stemprinter per stemlokaal. Onderkend is evenwel dat 1 stemprinter per stemlokaal problematisch zou kunnen zijn bij meervoudige verkiezingen[9]. De commissie heeft daar echter daaraan in het rapport geen gevolg aan verbonden.

Naar aanleiding van uw vraag heeft de commissie alsnog geprobeerd om na te gaan hoeveel stemprinters er per stemlokaal nodig zijn. Het is daarvoor nodig om uit te gaan van veronderstellingen, immers de stemprinter moet nog worden uitgespecificeerd. Alleen als dat werk is afgerond kan er met precisie worden vastgesteld hoe lang het zal duren om met de stemprinter een keuze te maken en het stembiljet te printen.

---

[8] De regelgeving waarop de CE-markering is gebaseerd heeft vooral betrekking op de veiligheids- en gezondheids- en milieuaspecten van de producten. Voor elektrische apparaten geldt bijvoorbeeld dat ze geen storende elektromagnetische straling mogen veroorzaken en ook niet gevoelig voor dergelijke straling mogen zijn.
[9] Pagina 73 van het rapport van de commissie.

Echter, ook al zou dat even lang duren als het invullen van het huidige stembiljet, dan is er meer dan 1 stemprinter nodig om de huidige wachttijden niet te laten oplopen. In het stemlokaal staan thans namelijk standaard 2 of 3 stemhokjes.

Om een berekening te maken heeft de commissie een drietal scenario's opgesteld die in de bijlage bij deze brief zijn beschreven. Op basis van deze scenario's constateert de commissie dat in de meeste stemlokalen zeker 2 stemprinters nodig zullen zijn. In een deel van de stemlokalen zullen 3 of meer stemprinters nodig zijn. Dit zijn de stemlokalen waar veel kiezers komen stemmen, zoals de stemlokalen in grote stations. In bijzondere stemlokalen, zoals mobiele stemlokalen, kan mogelijk 1 stemprinter volstaan.

De commissie kan niet precies uitrekenen wat de financiële gevolgen zullen zijn van het grotere aantal benodigde stemprinters. De commissie kan namelijk niet goed inschatten wat de invloed zal zijn van het grotere aantal op de stukprijs van de stemprinter.

Tot slot

De commissie kan zich voorstellen dat de onzekerheden omtrent de kosten zwaar wegen voor het kabinet. Bij een besluit over de invoering van de stemprinter en stemmenteller moet immers te overzien zijn wat de kosten zullen zijn.
De commissie zou het echter, vanwege de voordelen van het voorgestelde concept, betreuren indien het kabinet, vanwege de onzekerheden over de kosten, nu zou besluiten dat invoering van een stemprinter en stemmenteller niet haalbaar is.

De commissie kan zich daarom voorstellen dat het kabinet nu een "tussenbesluit" zou nemen, inhoudende dat het door de commissie aanbevolen concept door het ministerie van BZK verder zal worden uitgewerkt in concrete specificaties. Aan de hand van die specificaties zullen de kosten preciezer kunnen worden geraamd.

Met de specificaties kan dan ook een marktverkenning worden uitgevoerd waarin breed aan marktpartijen wordt gevraagd aan te geven of en zo ja, hoe invulling kan worden gegeven aan de specificaties en om marktpartijen in de gelegenheid te stellen inzicht te geven in de kosten.

Daarbij tekent de commissie nog aan dat als gekozen zou worden voor een financiering via het Gemeentefonds de investeringskosten niet in een keer opgebracht hoeven te worden. In dat geval zou volstaan kunnen worden met een structurele jaarlijkse toevoeging door het Rijk aan het Gemeentefonds van enkele tientallen miljoenen Euro's.

Datum
4 februari 2015

Kenmerk

De voorzitter van de commissie Elektronisch stemmen in het stemlokaal

W.I.I. van Beek