Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres

De Voorzitter van de Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA Den Haag

www.rijksoverheid.nl
www.facebook.com/minbzk
www.twitter.com/minbzk

Kenmerk
2015-0000083934

Uw kenmerk

Datum 13 februari 2015
Betreft elektronisch stemmen en tellen in het stemlokaal

Inleiding

In maart 2014[1] heeft de Tweede Kamer het standpunt van het kabinet ontvangen over het rapport van de commissie Onderzoek elektronisch stemmen in het stemlokaal (verder als commissie Van Beek aangeduid). Daarin is gesteld dat het kabinet de technische, organisatorische en financiële haalbaarheid van de voorstellen die de commissie heeft gedaan ging onderzoeken. Dat is de afgelopen periode ook gebeurd waarbij de eisen voor de beveiliging van de stemprinter en stemmenteller centraal hebben gestaan. Gaandeweg is mij duidelijk geworden dat de commissie Van Beek van een aantal eisen niet in beeld heeft gebracht wat het behelst om de betreffende eisen toe te passen. Daarom heb ik op in het Algemene Overleg van 11 september 2014[2] aan uw Kamer gemeld dat ik voornemens was de commissie Van Beek een aantal nadere vragen te stellen.

De commissie Van Beek is op 22 september 2014 begonnen aan de beantwoording van mijn nadere vragen. Op 4 februari j.l. heeft de commissie Van Beek de antwoorden aan mij aangeboden. De antwoorden treft u als bijlage bij deze brief aan.

Beveiliging en kosten

De antwoorden die de commissie Van Beek heeft gegeven op mijn nadere vragen bevestigen mijn beeld dat de afwegingen met betrekking tot de eisen waaraan de stemprinter en stemmenteller moeten voldoen complex zijn. Dat geldt in het bijzonder voor het vraagstuk ten aanzien van de beveiliging. Specifiek gaat het daarbij om de vraag tegen welk risicoprofiel de beveiliging bestand moet zijn.

[1] TK 2013-2014, 33 829 nr. 3
[2] Algemeen Overleg van 11 september 2014, TK 2014-2015, 33 829 nr. 5

Naar mijn mening heeft de commissie een juiste keuze gemaakt door als uitgangspunt te nemen dat het papieren proces bij het stemmen en het elektronisch tellen van de (papieren) stembiljetten leidend moet zijn. Door dat uitgangspunt te hanteren zou het zo moeten zijn dat een fout (mogelijk als gevolg van manipulatie) werkende stemprinters en stemmentellers niet onopgemerkt blijft. Immers de kiezer kan controleren of op het geprinte stembiljet de keuze staat die hij/zij heeft willen maken. Door een controle uit te voeren op de juistheid van de elektronisch getelde stembiljetten kan aan het licht komen dat de telling niet juist is. Het is uiteraard goed dat er maatregelen zijn om de fouten te detecteren, maar als die fouten op de verkiezingsdag zelf aan het licht komen is er dan niets aan te doen. Werkt de stemprinter niet correct en geldt dat voor veel of alle van de stemprinters dan zal het stemmen moeten worden gestaakt. Wordt gedetecteerd dat de stemmentellers niet correct werken dan zullen de stembiljetten handmatig worden geteld. Dit zijn risico's die, als ze zich op de verkiezingsdag voordoen, een grote impact kunnen hebben op het verloop van een verkiezing.

Meer in het algemeen speelt de vraag, die ook door de commissie Van Beek in haar antwoorden wordt geadresseerd, of het acceptabel kan zijn dat personen en/of groeperingen, buiten de verkiezingen om, kunnen aantonen dat de stemprinter en stemmenteller mogelijk niet adequaat zijn beveiligd. In 2006 is dat gebeurd met de stemcomputers die toen werden gebruikt. In een TV-uitzending is toen in beeld gebracht hoe de programmatuur van de stemcomputer kon worden gemanipuleerd, omdat er geen beveiligingsmaatregelen waren getroffen om dat te voorkomen. Dat heeft toen geleid tot de discussie over de betrouwbaarheid van de stemcomputers.

Het is naar mijn mening voorwaardelijk voor een besluit om de stemprinter en stemmenteller in te voeren dat er een breed gedragen consensus bestaat over de risico's die aanvaardbaar zijn. Er moet dus consensus zijn over de wijze waarop deze systemen beveiligd moeten zijn. Zonder een breed draagvlak is het risico te groot dat de betrouwbaarheid van de stemprinter en stemmenteller onderwerp van discussie is en blijft. Dat is niet goed voor het vertouwen dat er moet zijn in de systemen.

Het beveiligingniveau blijkt van grote invloed te zijn op de kosten van de stemprinter en stemmenteller. De commissie Van Beek heeft in haar antwoorden de bandbreedte van de kosten (150 à 250 mln Euro voor de investering en 6 à 10 mln Euro extra per verkiezing) niet verder kunnen preciseren. Er is wel geconstateerd dat er kostenposten zijn die niet zijn meegenomen in de ramingen die in haar rapport zijn vermeld. De commissie Van Beek is van mening dat er nu geen preciezere ramingen mogelijk zijn vanwege het grote aantal onzekere factoren, onder meer omdat er nog op fundamentele onderdelen verder moet worden gespecificeerd.

Hoe verder

Ik ben nog steeds van mening dat de invoering van de stemprinter en stemmenteller meerwaarde kan hebben voor de toegankelijkheid bij het stemmen en voor het tellen van de stembiljetten. Anderzijds moet ik constateren dat de invoering van deze ICT-systemen vele complexe vraagstukken kent en met onzekerheden is omgeven. Dat vraagt een zorgvuldige afweging.

Met de commissie Van Beek ben ik van mening dat, gelet op de mogelijke meerwaarde, het de moeite waard is om een volgende stap te zetten door nu eerst na te gaan of het mogelijk is om de onzekerheden weg te nemen en de complexiteit te verminderen. De aanname daarbij is dat het dan ook mogelijk zal zijn om (veel) preciezer te ramen wat de kosten zullen zijn. De commissie adviseert dat het ministerie van BZK de specificaties uitwerkt voor de stemprinter en de stemmenteller. Dat lijkt mij een nuttig voorstel. Waarbij ik het wel essentieel vind dat bij die uitwerking ook steeds getoetst wordt dat er breed draagvlak bestaat voor de specificaties. Ik heb het voornemen daarvoor, zoals ook door de commissie Van Beek is geadviseerd in haar rapport, een groep van (externe) deskundigen samen te stellen die kennis hebben van de relevante ICT-terreinen en van het openbaar bestuur. Ik zeg uw Kamer toe om u eind mei 2015 te informeren over de voortgang.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,

dr. R.H.A. Plasterk

> 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 eis 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 geteelde 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.

De voorzitter van de commissie Elektronisch stemmen in het stemlokaal

W.I.I. van Beek

Bijlage bij de brief aan de minister van Binnenlandse Zaken en Koninkrijksrelaties

Inhoudsopgave

Bijlagen:

- Vragen die zijn gesteld aan verschillende experts ten aanzien van het beveiligingsniveau en Common Criteria certificering
- Uitwerking van de controle van elektronisch getelde stembiljetten

1. Beveiligingsniveau: stelsel van Common Criteria en EAL-niveaus

De commissie heeft zich voor de beantwoording van de nadere vragen van de minister van BZK nader verdiept in het stelsel van de Common Criteria (CC). In dat kader hebben leden van de commissie gesproken met deskundigen op dit terrein. De vragen die aan deze deskundigen zijn gesteld en de antwoorden die zijn ontvangen zijn aan dit document gehecht. Eveneens is aan dit document gehecht een beschrijving op hoofdlijnen van het CC-stelsel.

Dilemma's

Om misbruik van de stemprinter en stemmenteller te voorkomen wordt door de commissie een combinatie van technische maatregelen en procedures voorgesteld die het mogelijk zou moeten maken om misbruik te voorkomen dan wel om misbruik te detecteren.

De maatregelen die gericht zijn op de detectie zullen, als de detectie werkt (en het systeem dus doet wat het moet doen), zichtbaar maken dat er misbruik is gepleegd of dat er een vermoeden daarvan bestaat. Als dat gebeurt tijdens een verkiezing of na een verkiezing dan zal dat tot de nodige commotie leiden. Immers onmiddellijk is dan de vraag aan de orde of de stemprinter en/of stemmenteller nog vertrouwd kunnen worden. Vindt de detectie voorafgaand aan de verkiezing plaats dan kan, mits daarvoor een wettelijke grondslag bestaat, de verkiezing worden uitgesteld. Dat zal evenwel ook heel wat consequenties kunnen hebben.

De goede werking van het voorgestelde concept (techniek + procedure), waarvan detectie van misbruik of het vermoeden daarvan een essentieel kenmerk is, leidt derhalve tot een hogere kans op significante (politieke) problemen bij de organisatie van de verkiezingen. In het verleden, ten tijde dat de stemmachines in gebruik waren, was dat risico er niet of veel kleiner omdat maatregelen om misbruik te detecteren ontbraken. Er waren immers alleen functionele eisen voor de stemmachines vastgesteld.

Gelet op de voorgeschiedenis van het dossier elektronisch stemmen, maar ook de in algemene zin kritische opstelling in Nederland ten aanzien van de beveiliging van ICT-systemen, mag verwacht worden dat allerlei (capabele) personen en groeperingen gemotiveerd zullen zijn om de robuustheid van de stemprinter en stemmenteller onder de loep te nemen en om te proberen om aan te tonen dat deze systemen niet goed beveiligd zijn. De hogere complexiteit van het concept van de stemprinter en stemmenteller ten opzichte van het huidige proces met het papieren stembiljet dat handmatig wordt geteld, leidt tot een grotere kans op dergelijke aanvallen (waarbij het doel van de aanval niet een succesvolle manipulatie van het kiesproces is, maar een succesvolle poging van de manipulatie van het systeem). Zouden dergelijke aanvallen slagen dan is de vraag hoe lang het vertrouwen in de stemprinter en/of stemmenteller in stand kan blijven.

Concluderend zou kunnen worden gesteld dat een hoog niveau van (openbaar gemaakte) gedocumenteerde beveiliging van de stemprinter en stemmenteller deze motivatie om de hiervoor genoemde aanvallen uit te voeren kan reduceren waardoor de kans op commotie en verminderd vertrouwen afneemt.

Wat zijn de Common Criteria (CC)

De Common Criteria [CC] vormen een instrument voor het evalueren en beoordelen van de informatiebeveiliging van ICT-producten en -systemen. Voor het beoordelen wordt gebruik gemaakt van de documentatie van de ICT-producten en het ICT-systeem. Tevens worden testen op de ICT-producten en het ICT-systeem uitgevoerd.

De CC zijn het resultaat van inspanningen van deskundigen om criteria voor evaluatie van ICT-beveiling te ontwikkelen die gebruikt zouden kunnen worden in internationaal verband. Aan de CC liggen meerdere reeds ontwikkelde criteria ten grondslag zoals bestaande Europese, Amerikaanse en Canadese criteria (respectievelijk ITSEC, TCSEC en CTCPEC).

De structuur van CC biedt flexibiliteit bij het specificeren van beveiligde ICT-producten en -systemen. Opdrachtgevers, leveranciers en andere partijen kunnen de beveiligingsfunctionaliteit van een ICT-product en ICT-systemen specificeren in een beschermingsprofiel en het niveau voor de evaluatie bepalen, gebruikmakend van een gedefinieerde set van zeven oplopende EAL's (Evaluation Assurance Levels), van EAL1 t/m EAL7.

Bij het definiëren van de beveiliging moeten allereerst de dreigingen worden geïnventariseerd waartegen de ICT-producten en -systemen beschermd moeten worden. De CC bevat een catalogus aan eisen die kunnen worden gebruikt om het gewenste beveiligingsniveau te realiseren. Met gebruikmaking van deze catalugus wordt het zogenaamde Protection Profile (PP) opgesteld. Bij het opstellen van het PP wordt systematisch vastgesteld of voor elke geïdentificeerde dreiging afdoende maatregelen getroffen kunnen worden. De specifieke invulling van de maatregelen wordt uitgeschreven in het Security Target (ST).

EAL-niveaus[1]

De CC bevat een reeks gedefinieerde niveaus. Om te voldoen aan specifieke doelstellingen, kan een niveau worden uitgebreid met één of meerdere aanvullende onderdelen uit een hoger niveau (de zogenaamde "plus"). Om ervoor te zorgen dat systemen voldoen aan de vereisten van deze niveaus, moeten ze zijn ontworpen en ontwikkeld met de intentie om aan die vereisten te voldoen.

EAL1 is het instapniveau. Tot EAL-niveau 4 worden de vereisten strenger en meer gedetailleerd, maar worden geen zeer gespecialiseerde technieken op het gebied van beveiligingsengineering vereist. EAL1-4 kunnen over het algemeen worden gebruikt voor de modificatie van reeds bestaande producten en systemen. Boven niveau EAL4 wordt een toenemende mate van toepassing vereist van gespecialiseerde technieken op het gebied van beveiligingsengineering.

Evaluatie en certificering

De evaluatie bestaat uit een beoordeling van de vereiste documentatie over en van de ICT-producten en het ICT-systeem en uit testen die de evaluator uitvoert. De evaluator moet geaccrediteerd zijn bij een van de instanties die bevoegd zijn om te certificeren.

[1] Zie voor nadere informatie de website van het Common Criteria Portal, waar een meer uitgebreide beschrijving staat van de zeven EAL-niveaus. Zie daarvoor het volgende document: http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R4.pdf (hoofdstuk 8).

De evaluator controleert dat de documentatie over het ICT-product en -systemen aan de CC-vereisten voldoet. De evaluator beoordeelt, als dat volgt uit het betreffende EAL-niveau, de testrapportages van de ontwikkelaar. Daarbij wordt nagegaan of de uitgevoerde testen dekkend zijn. Hier past wel een kanttekening. Volgens de CC moet de ontwikkelaar alleen in functionele zin de beveiliging testen. Penetratietesten hoeft de ontwikkelaar zelf niet te doen. Penetratietesten worden door de evaluator uitgevoerd. Pas als de ontwikkeling van het systeem is afgerond start de evaluator met de testen. De evaluator moet aan de certificerende instantie vooraf voorleggen welke testen er zullen worden uitgevoerd. De certifcerende instantie beoordeelt of die testen, voor het betreffende EAL-niveau dekkend zijn.

Hieronder wordt, op grote hoofdlijnen, weergegeven welke testen de evaluator uitvoert. De intensiviteit, zowel wat betreft de middelen als wat betreft de tijdsduur, verschilt per EAL-niveau. Hoe hoger het niveau, hoe intensiever en diepgaand de testen worden uitgevoerd en hoe langer ze duren.

EAL-niveau	Wat test de evaluator	Afgedekt dreigingniveau/attack potential vlgs CC
1	De gebruikersfuncties worden getest voor zover de evaluator die belangrijk vindt voor de beveiliging. Voert penetratietesten uit uitsluitend om na te gaan of het te evalueren product cq systeem bestand is tegen op internet gepubliceerde kwetsbaarheden.	Dreigingniveau: Basaal/Basic EAL 1 tot en met 3 bieden bescherming 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 internettechnologie vallen bijv. de zgn. "script-kiddies" in deze categorie, ofwel personen die gebruik maken van gepubliceerde hulpmiddelen voor de aanval op kwetsbaarheden zonder deze kwetsbaarheden noodzakelijkerwijs te begrijpen.
2 en 3	Beveiliginggerelateerde gebruikersfuncties worden getest. Dezelfde penetratietesten worden uitgevoerd als bij EAL 1. Naast de gepubliceerde kwetsbaarheden wordt ook getest op kwetsbaarheden die de evaluator heeft geïdentificeerd bij het beoordelen van de documentatie die de leverancier levert van het product cq systeem.	Dreigingniveau: Basaal/Basic Idem als bij EAL 1.
4	Gebruikersfuncties worden getest. Dezelfde penetratietesten worden uitgevoerd als bij EAL 1 t/m 3. Daarenboven wordt ook getest op kwetsbaarheden die de evaluator heeft geïdentificeerd bij de beoordeling van de broncode van het product cq systeem.	Dreigingniveau: Hoger dan basaal/Enhanced basic EAL 4 biedt bescherming 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-niveau	Wat test de evaluator	Afgedekt dreigingniveau vlgs CC
5	Gebruikersfuncties worden getest. Dezelfde penetratietesten worden uitgevoerd als bij EAL 1 t/m 4. Omdat bij dit niveau er veel meer gedetailleerde documentatie moet worden gemaakt van het product cq systeem heeft de evaluator ook veel meer kennis omtrent het systeem en de mogelijke kwetsbaarheden daarvan waarop dan ook getest wordt.	Dreigingniveau: Matig/Moderate EAL 5 biedt bescherming tegen de kennis en mogelijkheden van beveiligingsexperts (door leken "hackers" genoemd, hoewel sommige "hackers" mogelijk een hoger deskundigheidsniveau hebben).
6	Zie EAL 5. Bij EAL 6 geldt dat het product cq systeem met gebruikmaking van semi-formele methoden moet zijn ontworpen en ontwikkeld, met uitzondering van belangrijke aspecten van de beveiliging en de relatie daarvan met het gedrag van het product cq systeem. Die aspecten moeten met gebruikmaking van formele methoden zijn ontworpen en ontwikkeld. Waar gebruik is gemaakt van formele methoden biedt dat de mogelijkheid om op wiskundige wijze de correcte werking vast te stellen.	Dreigingsniveau: Hoog/High EAL 6 biedt bescherming 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.

De evaluator zal, gerelateerd aan het EAL-niveau van de certificering, uiteraard steeds proberen om bij het testen na te gaan of het systeem bestand is tegen de meest actuele dreigingen die hij kan vinden. Mede daardoor bestaat het risico dat bij de testen door de evaluator een kwetsbaarheid in het systeem wordt ontdekt. In dat geval zal de leverancier aanpassingen moeten verrichten aan het systeem om de kwetsbaarheid weg te nemen. Dit risico bestaat overigens ook als er voor gekozen wordt geen CC-certificering uit te laten voeren. Het is namelijk ondenkbaar dat de opdrachtgever (in casu de overheid) in het kader van de acceptatie van de systemen geen beveiligingstesten, waaronder penetratietesten, laat uitvoeren.

De certificering zelf geschiedt door de instanties die bevoegd zijn tot het afgeven van het certificaat. Het resultaat is een certificaat waarin het bereikte waarborgingsniveau van de beoordeling (EAL) wordt vermeld en een bijbehorend certificeringsrapport waarin een samenvatting wordt gegeven van de uitkomst van de certificering.

2. Nadere uitwerking van de methode voor de controle van de elektronisch geteelde stembiljetten

In haar rapport heeft de commissie geadviseerd om steekproefsgewijs een deel van de elektronisch geteelde papieren stembiljetten te controleren. Dit is een van de fundamenten onder het concept van de commissie waarin het papieren proces leidend is. Voor de beantwoording van de nadere vragen heeft de commissie door professor dr. E.C. Wit van de Rijksuniversiteit Groningen

aanvullend werk laten verrichten aan de methode die zou kunnen worden gebruikt voor deze controle. Het rapport van professor Wit is als bijlage bij dit document gevoegd. Een centraal element van de methode is de risicomarge die gehanteerd moet worden. Het hanteren van een risicomarge is nodig omdat er fouten bij het elektronisch tellen, net al bij handmatig tellen, niet kunnen worden uitgesloten. Het rapport van professor Wit bevat de bouwstenen om te kunnen bepalen welke marge er voor de controle aangehouden kan worden. Hoe kleiner de marge hoe meer stembiljetten er gecontroleerd moeten worden.

3. Aantal stemprinters per stemlokaal

In haar rapport is de commissie van het volgende uitgegaan:

- 10.000 stembureaus en gemiddeld 1.000 kiezers per stembureau;
- Eén stemprinter per stembureau en 2.500 reserve stemprinters voor het geval op de dag van de verkiezing een stemprinter als gevolg van gebreken moet worden vervangen;
- Bij meervoudige verkiezingen wordt op 1 stembiljet de keuze voor 1 verkiezing geprint.

De commissie heeft in haar rapport onderkend dat bij meervoudige verkiezingen mogelijk niet zou kunnen worden volstaan met 1 stemprinter per stemlokaal. Gezien de beperkte tijd die beschikbaar was voor de werkzaamheden van de commissie en de complexiteit van het vraagstuk is aan deze constatering verder geen uitwerking gegeven.

Naar aanleiding van de nadere vragen die de minister van BZK heeft gesteld, is alsnog verder onderzocht hoeveel stemprinters daadwerkelijk nodig zouden kunnen zijn per stemlokaal. Het is duidelijk dat meervoudige verkiezingen een feit zijn. In ieder geval zullen de verkiezingen van provinciale staten en de besturen van de waterschappen in de toekomst (te beginnen in 2015) op 1 dag plaatsvinden. Daarnaast moet er rekening mee worden gehouden dat in de toekomst op 1 dag mogelijk meerdere raadgevende referenda worden gehouden dan wel een of meerdere referenda in combinatie met een (andere) verkiezing.

Voor het onderzoek is gebruik gemaakt van de tijdmetingen die het ministerie van BZK heeft laten uitvoeren bij testen in 2012 en tijdens de herindelingverkiezingen op 19 november 2014. Deze tijdmetingen laten zien dat een kiezer gemiddeld 30 seconden bezig is om het huidige stembiljet in te vullen en dat de leden van de stembureaus er gemiddeld 30 seconden over doen om de kiezer te voorzien van zijn/haar stembiljet.

Verder is gebruik gemaakt van gegevens van de gemeente Rotterdam over de tijdstippen waarop kiezers hun stem hebben uitgebracht bij de verkiezing voor de gemeenteraad in maart 2014. Hieruit is op te maken dat ca 30% van de kiezers in de laatste drie uur (dus tussen 18.00 en 21.00 uur) hun stem uitbrengen.

<u>Scenario's</u>

De stemprinter die de commissie voor ogen heeft is nog niet uitgespecificeerd. Er zijn daarbij nog vele keuzes te maken, bijvoorbeeld met betrekking tot de wijze van activering, maar ook ten aanzien van de interface die zal worden ontwikkeld om de kiezer een keuze te laten maken en het stembiljet te printen. Er zijn verder geen referentiegegevens beschikbaar van een stemprinter in andere landen. Zouden die er zijn, dan is het overigens maar de vraag in hoeverre die gegevens bruikbaar zouden kunnen zijn, gelet op de verschillen die er bestaan tussen landen ten aanzien van het kiesstelsel.

Om toch een inschatting te kunnen maken van het aantal noodzakelijke stemprinters heeft de commissie een drietal scenario's opgesteld. Voor deze scenario's gelden de volgende uitgangspunten:

- De scenario's gaan uit van meervoudige verkiezingen, te weten van 3 verkiezingen die tegelijk plaatsvinden (twee lijstverkiezingen en een (landelijk) raadplegend referendum).

- De kiezer activeert zelf de stemprinter. Dit is overeenkomstig het rapport van de commissie. In de navolgende berekening is ervan uitgegaan dat de kiezer één token per verkiezing meekrijgt. Daarom is een keer 5 seconden geschat voor het activeren.

- Er wordt geen rekening mee gehouden dat een deel van de kiezers (tussen de 10 à 15% van de kiezers) ook 1 of 2 volmachtstemmen uitbrengt. Aangenomen mag worden dat het (mede) uitbrengen van een volmachtstem minder tijd in beslag neemt dan het uitbrengen van een eigen stem. Deze tijdswinst zal naar schatting echter beperkt blijven tot 10 à 20% per volmachtstem. Dit resulteert in 1-3% tijdwinst over het geheel. Dit is voor dit moment te verwaarlozen.

- Er wordt geen rekening mee gehouden dat sommige kiezers audio-ondersteuning nodig zullen hebben om de stemprinter te gebruiken. Er is geen inschatting te maken van het aantal kiezers dat deze ondersteuning nodig zal hebben.

- De kiezer kiest zelf de volgorde van de twee verkiezingen en het referendum.
- Het aantal interactieve stappen per verkiezing is minimaal.

- Tijd tussen opdracht tot printen en daadwerkelijk printen alsook de tijdsduur van het printen zelf zijn minimaal.

- Voor elke verkiezing wordt een afzonderlijk stembiljet aangemaakt.

- Het stembiljet wordt geprint na iedere keuze.

- Controleren van het stembiljet gebeurt door de kiezer bij de stemprinter, dus in het stemhokje.

De drie scenario's worden aangeduid met:

a. Minimaal;
b. Nominaal;
c. Maximaal.

Deze scenario's representeren een bandbreedte, waarbij de variatie met name bepaald wordt door de menselijke handelingen. Dat wil zeggen dat de technische aspecten (activeren, printen) in elk van de scenario's gelijk is, maar de handelingen die de kiezer verricht variëren.

Handeling	**Minimaal** tijd (sec)	**Nominaal** tijd (sec)	**Maximaal** tijd (sec)
Stemhokje binnengaan	2,5	2,5	2,5
Activeren	5	5	5
Keuze lijstverkiezing 1	15	20	25
Print lijstverkiezing 1	5	5	5
Controleren lijstverkiezing 1	5	7,5	10
Keuze lijstverkiezing 2	15	20	25
Print lijstverkiezing 2	5	5	5
Controleren lijstverkiezing 2	5	7,5	10
Keuze referendum	2,5	5	7,5
Print referendum	5	5	5
Controleren referendum	2,5	5	7,5
Stemhokje uitgaan	2,5	2,5	2,5
Totaal aantal seconden	70	90	110

Berekening aantal stemprinters per stemlokaal

Voor de berekening van het aantal stemprinters worden de volgende uitgangspunten gehanteerd:

a. De capaciteitsbehoefte (aantal verkiezingen, belangstelling) kan per verkiezing variëren, maar het aantal stemprinters moet toereikend zijn voor de piek. Dit betekent dat bij bepaalde verkiezingen sprake kan zijn van overcapaciteit, aangezien het aantal stemprinters zich niet per verkiezing laat bepalen. Deze worden voor een bepaalde periode waarin verschillende verkiezingen (met verschillende behoeften) plaatsvinden, verworven.

b. De spreiding over de dag is niet gelijk, met pieken tijdens het eerste openingsuur en de laatste drie uren van de dag. De capaciteit moet toereikend zijn voor deze pieken, met dien verstande dat de wachttijden niet langer zouden mogen moeten zijn dan men nu gewend is (en kennelijk niet tot problemen leidt). Op grond van metingen door gemeente Rotterdam wordt ervan uitgegaan dat tijdens piekuren 10% van de kiezers de stem uitbrengt, dus 100 per uur.

In onderstaand overzicht is de volgende berekening gemaakt:

a. Hoeveel kiezers kunnen in een uur met gebruikmaking van de stemprinter hun stem uitbrengen.
b. De capaciteitsbehoefte gegeven de piek (10% van de kiezers).
c. Hoeveel stemprintercapaciteit is nodig (b delen door a).
d. Benodigd aantal stemprinters.

	Minimaal	Nominaal	Maximaal
Aantal kiezers per uur	51	40	33
Benodigde piek capaciteit	100	100	100
Aantal stemprinters op piek	1,9	2,5	3,1
Benodigd aantal stemprinters	2	3	3

4. Kosten

De commissie heeft in haar rapport al opgemerkt dat er te veel onzekerheden zijn om de kosten van de invoering en het gebruik van de stemprinter en stemmenteller precies te kunnen ramen. Daarom is in het rapport een ruime marge aangehouden voor zowel de investeringskosten als voor de meerkosten per verkiezing.

Bij het beantwoorden van de nadere vragen heeft de commissie er kennis van genomen dat er kostenposten zijn die niet zijn meegenomen in de ramingen. In de tijd die beschikbaar was voor het beantwoorden van de nadere vragen was het niet mogelijk om zinvol nader onderzoek te doen om de ramingen te corrigeren. Overigens is het maar de vraag of, als er wel meer tijd zou zijn geweest, een dergelijk onderzoek bruikbare resultaten zou hebben opgeleverd. Er zijn namelijk te veel onzekere factoren, onder meer omdat er nog op vele onderdelen keuzes moeten worden gemaakt en verder gespecificeerd.

Vragen en antwoorden die zijn gesteld aan en gegeven door deskundigen op het terrein van de Common Criteria

Vraag 1
Wat is het gangbare proces om het juiste EAL-niveau te kunnen bepalen?

Antwoord
De klassieke weg om dit vast te stellen is door te bepalen wat het potentieel is van de aanvaller waartegen de systemen moeten zijn beveiligd met inachtneming van de mate waarin vertrouwd kan worden op de omgeving waarin de stemprinter en stemmenteller zullen worden gebruikt. Gelet op het belang dat verkiezingen vertegenwoordigen zou voor de stemprinter en de stemmenteller uitgegaan moeten worden van een "high attack potential" aanvaller. Dat plaatst de systemen gelijk in het domein van de EAL 6 (high attack potential). EAL 5 gaat immers uit van een "enhanced moderate attack potential". Verder kan er niet vanuit worden gegaan dat er beschermende maatregelen zijn te nemen die uitsluiten dat een iemand met een "high attack potential" de beschikking krijgt over een stemprinter of stemmenteller. Die persoon of organisatie zou dan kunnen aantonen dat de beveiliging niet voldoet. Dat kan potentieel politiek en maatschappelijk leiden tot verlies aan vertrouwen in de betrouwbaarheid van de stemprinter en stemmenteller. Het bieden van bescherming tegen een dergelijke aanval is een lastige taak. Er kunnen echter in deze context bijvoorbeeld inbraakdetectie methoden worden gebruikt die bescherming bieden tegen een bedreiging. Een alternatieve benadering zou zijn om te kijken naar de details van elke EAL en te beslissen of elk aspect dat is vervat in een EAL relevant is of niet.

Beide benaderingen worden ook vaak gecombineerd. In eerste instantie leidt de algemene beslissing over het aanvalspotentieel tot een basale EAL. Vervolgens wordt elk aspect van de EAL bekeken en aangevuld (of verwijderd) waar nodig geacht. Dit leidt vaak tot de tussenliggende niveaus van EAL X +.

Vraag 2
Is gebruik van standaardcomponenten mogelijk bij een EAL-niveau van 5 en 6?

Antwoord
Het is een bijna onmogelijke opgave om gebruik te kunnen maken van standaardcomponenten. Allereerst omdat de meeste standaardcomponenten niet ontwikkeld zijn om bestand te zijn tegen een "high attack potential" aanval. Daarnaast moet bij EAL 5 en 6 nauwgezet worden gedocumenteerd hoe de apparatuur en de programmatuur precies is samengesteld, hoe het is gefabriceerd en hoe het werkt. Dat is bij de ontwikkeling van standaardcomponenten niet gebeurd. Voor een EAL 5 of 6 certificering zou voor de betreffende componenten dat werk alsnog gedaan moeten worden. Het risico is groot dat de leverancier er niet goed in slaagt en daardoor dus ook niet door de certificering komt.

Gewezen wordt op de ervaringen met de certificering van betaalautomaten. In het verleden werden voor deze systemen weinig of geen standaardcomponenten gebruikt en was als gevolg hiervan de beveiliging van een hoog niveau. Door allerlei commerciële ontwikkelingen zijn leveranciers daarvan afgestapt en worden er standaardcomponenten gebruikt. Als gevolg hiervan is bij certificeringstrajecten vastgesteld dat het beveiligingsniveau lager is en de betaalautomaten gevoeliger zijn geworden voor dreigingen.

Voor de stemprinter is, zo heeft de commissie Van Beek geoordeeld, cruciaal dat de keuze die de kiezer maakt niet wordt opgeslagen nadat die keuze is geprint. Dit is met standaardcomponenten naar alle waarschijnlijkheid niet te realiseren. Immers van standaardcomponenten is niet beschreven hoe ze precies werken en waar, wanneer, wat wordt opgeslagen.

Hierbij dient te worden vermeld dat deze beperkingen alleen gelden voor de aspecten van de apparaten die relevant zijn voor de beveiliging. Wanneer standaard hardware of software wordt gebruikt in delen van het apparaat die niet relevant zijn voor de beveiliging, dan richt de beoordeling zich niet op deze delen. Een standaard CPU (zonder enige vorm van crypto) is een voorbeeld van een dergelijk generiek onderdeel. Gewoonlijk wordt aangenomen dat deze onderdelen betrouwbaar zijn, zonder dat gedetailleerde informatie over die componenten beschikbaar dient te zijn. De beslissing wat wel of niet relevant is voor de beveiliging is niet makkelijk te nemen en leidt derhalve tot discussies.

Vraag 3
Wat is het verschil tussen EAL 4, 5 en 6?

Antwoord
Tot EAL-niveau 4 worden de vereisten steeds strenger en meer gedetailleerd, maar worden geen zeer gespecialiseerde technieken op het gebied van beveiligingsengineering vereist. EAL1-4 kunnen over het algemeen worden gebruikt voor de modificatie van reeds bestaande producten en systemen. Boven niveau EAL4 wordt een toenemende mate van toepassing vereist van gespecialiseerde technieken op het gebied van beveiligingsengineering. Om ervoor te zorgen dat systemen voldoen aan de vereisten van deze niveaus, moeten ze zijn ontworpen en ontwikkeld met de intentie om aan die vereisten te voldoen.

Een EAL4-evaluatie biedt, naast EAL3, een analyse die wordt ondersteund door een volledige specificatie van de interface, een beschrijving van het modulaire basisontwerp van de TOE (Target of Evaluation) en een subset van de implementatie. Het testen wordt ondersteund door een analyse van de kwetsbaarheid (waarbij ook gebruik wordt gemaakt van de implementatie-representatie), waarmee de weerstand wordt aangetoond tegen aanvallers met een aanvalspotentieel dat hoger is dan basaal. Waarborging wordt ook geboden via aanvullend geautomatiseerd configuratiemanagement.

EAL5 is van toepassing wanneer een hoge mate van onafhankelijk gewaarborgde beveiliging is vereist, met een robuuste aanpak van de ontwikkeling. Een EAL5-evaluatie biedt, naast EAL4, een analyse die wordt ondersteund door een modulair ontwerp van de beveiligingsfuncties van de TOE. Waarborging wordt aangevuld met een semi-formele presentatie van het ontwerp, een gestructureerde architectuur, uitgebreid configuratiemanagement van de TOE en een onafhankelijke, methodische analyse van de kwetsbaarheid waarmee de weerstand wordt aangetoond tegen aanvallers met een matig aanvalspotentieel.

Een EAL6-evaluatie biedt, naast EAL5, aanvullende waarborging door middel van een formeel model van het beveiligingsbeleid van de TOE en een semi-formele presentatie van de functionele specificatie en het ontwerp van de TOE (Target of Evaluation). De onafhankelijke, methodische analyse van de kwetsbaarheid toont de weerstand aan tegen aanvallers met een hoog aanvalspotentieel.

Samenvattend: het verhogen van het waarborgingsniveau zorgt ervoor dat de maatregelen die worden toegepast vollediger zijn (de controles gaan van een subset naar een volledige set). Dit leidt ook tot het gebruik van meer (semi)-formele methoden. Met name het gebruik van (semi)-formele methoden heeft een aanzienlijke invloed op zowel de ontwikkeling van het product als de evaluatie ervan.

Vraag 4
Kunnen procedurele maatregelen meetellen als beveiligingsmaatregelen in een evaluatie voor EAL 5 en 6?

Antwoord
Het Common Criteria-systeem gaat uit van de veronderstelling dat het product cq systeem dat moet worden geëvalueerd (TOE) werkt binnen een specifieke omgeving die bijdraagt aan de beveiligingskenmerken van het totale product cq systeem. Dat zou een probleem kunnen vormen voor de stemprinter en stemmenteller, aangezien men slechts een zeer beperkt vertrouwen kan hebben in de omgeving. Dat probleem begint al bij de ontwikkelaar. Uitgaande van het stelsel van de Common Criteria zou de ontwikkelaar vertrouwd moeten worden.

Echter voor het verkiezingsproces is dat al een stap te veel. Ook de ontwikkelaar kan een dreiging opleveren voor de integriteit van de systemen. Het complicerende hier is de politiek/ maatschappelijke context. De systemen moeten niet alleen beveiligd zijn tegen daadwerkelijke dreigingen, maar ook tegen het feit dat er personen en/of groeperingen kunnen zijn die zich inzetten om aan te tonen dat de systemen bedreigd kunnen worden. Dat maakt deze casus extra complex. Dit leidt tot een situatie waarin de klassieke maatregelen van een Common Criteria-beoordeling niet voldoende zijn, maar mogelijk moeten worden aangevuld met specifieke eisen binnen of buiten de Common Criteria-beoordeling.

Vraag 5
Zou met procedurele maatregelen een lager niveau dan EAL 5 of 6 kunnen volstaan?

Antwoord
Zie het antwoord op vraag 4. Het stelsel van Common Criteria kent de mogelijkheid om een EAL niveau te kiezen (bijvoorbeeld EAL 4) en vervolgens (als zogenaamde "plussen") een aantal maatregelen van toepassing te verklaren uit de hogere niveaus (bijvoorbeeld EAL 5 en/of 6). Procedurele maatregelen, zoals bijvoorbeeld een visuele controle van een (relatief klein) deel van de elektronisch getelde papieren stembiljetten is een maatregel op basis waarvan zou kunnen worden geoordeeld dat de TOE een minder hoog beveiligingsniveau zou kunnen hebben. De vraag die dan beantwoord moet worden is hoe groot de kans is dat met een dergelijke visuele controle van een (relatief klein) deel van de elektronisch getelde papieren stembiljetten daadwerkelijk kan worden opgespoord dat stemmentellers niet correct hebben gewerkt. Als de kans daarop niet groot is, dan zou nog steeds sprake moeten zijn van een "high attack potential".

Ook een visuele controle door de kiezer van diens geprinte stemkeuze kan niet als dekkend worden beoordeeld, omdat zeker niet alle kiezers die controle zullen uitvoeren. Zou het voorkomen dat de stemprinter iets anders geprint heeft dan de keizer heeft beoogd en dit is reproduceerbaar dan zal wederom het vertrouwen in de betrouwbaarheid van de stemprinter in het geding zijn.

De beveiligingsmaatregelen die worden geboden door de TOE en de maatregelen die worden geboden door de omgeving dienen met zorg te worden vastgesteld. Hierbij dient niet de vraag leidend te zijn hoe de last van het certificeringsproces kan worden beperkt. Leidend voor de te nemen beveligingsmaatregelen moet een diepgaande analyse van de dreigingen zijn.

Vraag 6
Is het mogelijk en haalbaar om een stemprinter en stemmenteller te ontwikkelen die voldoet aan EAL 5 of 6?

Antwoord
Ja, mits de leverancier die deze systemen gaat ontwikkelen ervaring heeft met het ontwikkelen van producten van een niveau van EAL 4 of hoger. Er bestaat een aanzienlijk risico dat de ontwikkeling en evaluatie/certificering zal mislukken indien een leverancier die ervaring niet heeft.

Vraag 7
Hoeveel tijd moet gerekend worden voor de ontwikkeling van een stemprinter en stemmenteller op EAL 5 of 6 niveau?

Antwoord
Meer dan een jaar moet verwacht worden. Het hangt onder meer af van de specificaties van de systemen en van de ervaring van de leverancier en tenslotte van de ervaring van de evaluator. Van EAL 1 tot en met 4 neemt de extra inspanning voor het toepassen van de CC nog lineair toe, vanaf niveau 5 neemt die extra inspanning exponentieel toe dankzij het gebruik van (semi)formele methodes.

Vraag 8
Geef een toelichting op het aanvalsniveau dat bij een EAL hoort.

Antwoord
Om het dreigingsniveau te kunnen bepalen waartegen een systeem moet zijn beveiligd maakt de CC gebruik van een classificatiemethode waarbij aan een bepaalde aanval een bepaald aantal "punten" wordt toegekend. De volledige methode wordt beschreven in bijlage "B.4 Calculating attack potential". Een aanval met een cijfer tussen de 20 en 24 wordt bijvoorbeeld geclassificeerd als "Hoog". Dit betekent dat een aanvaller met aanvalspotentieel "hoog" in staat wordt geacht deze te kunnen uitvoeren, maar een aanvaller met aanvalspotentieel "matig" of lager niet. Hierbij dient te worden opgemerkt dat wat betreft de betrokken factoren, het aanvalspotentieel van een aanvaller afhankelijk kan zijn van een specifieke combinatie van deskundigheid en apparatuur. Een laboratorium gespecialiseerd in bepaalde aanvallen op internetprotocollen en -toepassingen kan bijvoorbeeld een hoog aanvalspotentieel hebben met betrekking tot webservers maar geen hoog aanvalspotentieel met betrekking tot aanvallen op smartcards.

Hieronder is samengevat weergegeven welk aanvalspotentieel aan een EAL wordt toegekend. De beschrijving van het aanvalspotentieel verwijst hier altijd naar het niveau van een aanvaller waartegen de TOE bestand moet zijn. Met andere woorden: Voor een aanvaller op dit niveau mag het NIET mogelijk zijn om een aanval uit te voeren op de mogelijk resterende kwetsbaarheden.

- **EAL 7 en 6: Hoog/High**

Een civiel beveiligingslab of een georganiseerde groep hackers of een universitair team gespecialiseerd in de technologie die wordt gebruikt in het product.

- **EAL 5: Matig/Moderate**

Beveiligingsexperts (door leken "hackers" genoemd, hoewel sommige "hackers" mogelijk een hoger deskundigheidsniveau hebben).

- **EAL 4: Hoger dan basaal/Enhanced basic**

Personen die beschikken over IT-vaardigheden op een bepaald technologisch gebied, maar niet gespecialiseerd zijn in het zoeken naar kwetsbaarheden.

- **EAL 3 en lager: Basaal/basic**

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 internettechnologie vallen bijvoorbeeld 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.

Vragen die zijn gesteld en antwoorden die zijn gegeven door deskundigen op het terrein van de ontwikkeling van apparatuur

Vraag 1
Hoe ziet een ontwikkeltraject waarbij (ook) hardware moet worden ontworpen en ontwikkeld in elkaar? Wat moet, in de vorm van eisen, bekend zijn voordat begonnen kan worden met ontwerpen en ontwikkelen van hardware?

Antwoord:
In wezen niet anders dan bij een "regulier systeemontwikkeltraject". Dat wil zeggen dat de opdrachtgever idealiter op functioneel niveau specificeert wat er moet worden ontwikkeld en welke randvoorwaarden gelden. De leverancier vertaalt die specificaties en maakt, waar de specificaties dat toestaan, nadere keuzes. Idealiter zou je willen dat het specificeren van de eisen door de opdrachtgever in samenspraak kan plaatsvinden met de leveranciers.

Het ontwerp- en ontwikkeltraject van complexe hardware/software-systemen verloopt in het algemeen het beste als de opdrachtgever continu betrokken is in het proces. Een co-development verhoogt in dit soort projecten de kans op succes. Zo is het vaak bij het analyseren van de eisen door de opdrachtnemer zinvol om de achterliggende gedachte van een eis te kennen. Bepaalde eisen kunnen grote impact hebben op kosten en/of complexiteit, terwijl het achterliggende doel ook op andere manieren behaald kan worden. Dit tegen lagere kosten of een eenvoudiger concept.

Een goede dialoog met de opdrachtgever is dus zinvol om een kosteneffectieve en de minst complexe oplossing te realiseren met behoud functionaliteit. Daarom wordt erop geattendeerd dat het van belang is om voorzichtig te zijn in het formuleren van de specificaties. De slag die het Ministerie en de Commissie nu maken in de vertaling van het gekozen kiesproces naar functionele eisen is vooral van groot belang in het opstellen van een passend Protection Profile, omdat dat immers de impact op de Common Criteria evaluatie heeft. Als voorbeeld wordt genoemd: niet specificeren "alles moet worden verwijderd uit het geheugen", maar "uit het geheugen moet de informatie over de keuze van de kiezer worden verwijderd". Verder is van belang wanneer de keuze van de kiezer verwijderd moet worden. Is dat onmiddellijk nadat de kiezer de keuze heeft gemaakt of kan dat later zijn. Verder is aangegeven dat in een gecombineerd ontwikkeltraject met software en hardware er kruisverbanden liggen tussen de keuzes in de hardware en de software. Het aanpassen van de eisen en ontwerpkeuzes na de initiële designfase kunnen van grote invloed zijn. Dit kan leiden tot inefficiëntie en vertragingen.

Een onderwerp waar relatief veel over gesproken is in het overleg, is het wissen van het geheugen op de stemprinter. Het verwijderen van keuzen uit geheugens van de stemprinter kan bijvoorbeeld door meermaals overschrijven van het geheugen of door de stroom van componenten met geheugen af te halen. Geheugen wissen door stroom van componenten af te halen werkt echter alleen voor tijdelijk geheugen en niet voor permanent geheugen, zoals een harde schijf of flash memory. Daarnaast moet de stroom er lang genoeg afgehaald worden, zodat zeker is dat alle sporen van hetgeen is opgeslagen zijn verdwenen. Het op geautomatiseerde wijze afschakelen van de stroom van een component vergt maatwerk aan de component. Die "functionaliteit" is namelijk niet standaard. Het is de vraag of dit een geaccepteerde methode is volgens de Common Criteria evaluatoren, wat weer afhangt van de verwoording van de eis tot wissen van het geheugen in het Protection Profile.

Daarnaast zal het tijd duren voordat de component, nadat deze is aangezet, weer operationeel is. Gezien voorgaande consequenties zal het overschrijven van het geheugen veelal simpeler zijn, mits de werking van het gebruik van het geheugen is gedocumenteerd. Als dit allemaal in ogenschouw wordt genomen, dan is het aannemelijk te concluderen dat overschrijven van geheugen veelal simpeler zal zijn, mits precies is gedocumenteerd hoe het geheugen wordt gebruikt. Het is niet waarschijnlijk dat dit laatste bij standaardcomponenten het geval zal zijn.

De verwachting is dat aan- en uitzetten van componenten, gezien het aantal keer dat een stemprinter voor het maken van een stemkeuze wordt gebruikt (rond de 1000 per verkiezing), geen significante invloed zal hebben op de levensduur. Vanzelfsprekend zal dit in de componentkeuze geverifieerd moeten worden.

Vraag 2
Heeft het feit dat de hardware wordt ontwikkeld gevolgen voor de ontwikkeling van de software waar de hardware gebruik van gaat maken? Gedacht zou kunnen worden aan gevolgen voor de te hanteren ontwerpmethode, de te gebruiken ontwikkelomgeving, de te gebruiken programmeertalen, de wijze van testen, de te gebruiken testhulpmiddelen en het proces van het installeren van de software op de hardware.

Antwoord:
Neen. De wijze waarop de software wordt ontwikkeld en getest is niet anders dan bij standaard elektronica die ingekocht wordt. Wel zal om aan de Common Criteria eisen te kunnen voldoen gewerkt moeten worden met een volgens Common Criteria geaccepteerde of accepteerbaar te maken programmeertaal en ontwikkelomgeving. Voor de goede orde is het daarbij goed om te melden dat windows/android/java en andere veelgebruikte commerciële omgevingen vrijwel per definitie niet geschikt zijn om te gebruiken om een te certificeren systeem op te baseren ivm EAL5/6-eisen. Datzelfde geldt voor de typische hardware waar dit soort systemen op draait, zoals intel- en AMD-processoren. (Waarbij de kanttekening gemaakt moet worden dat daar waar de hardware component niet kritisch is voor de beveiliging, dit wel een standaard component mag zijn. Het is aan de evaluatoren om uiteindelijk te bepalen of een systeem onderdeel kritisch is voor de beveiliging of niet.) Hieronder valt dat de evaluator inzage moet hebben in alle programmatuur. Het gebruikmaken van standaard programmabibliotheken is lastig in dit geval. Een aantal programmeertalen en -compilers zou voor de hand kunnen liggen om te gebruiken, zoals assembly, de programmeertaal van de processor ook wel machine taal genoemd, C of C++. Maar deze lijst is niet uitputtend.

Naast de taal en compiler is de grootste impact van Common Criteria certificering op de systeemontwikkeling dat er veel meer eisen gesteld worden aan het ontwerpproces en de ontwerpers in termen van documentatie, screening en locatie.
Overigens is in het (denkbeeldige) geval dat er met standaard hardware gewerkt zou gaan worden geen grote kostenbesparing te verwachten in het gehele traject, omdat het samengestelde systeem van hardware en software, uiteindelijk als geheel ontworpen, ontwikkeld en gecertificeerd zal moeten worden.

Vraag 3
Wat zijn de gevolgen ten aanzien van de doorlooptijd, de kosten en de risico's voor een ontwikkelingstraject van een systeem als voor delen of voor het geheel van dat systeem de hardware moet worden ontworpen en ontwikkeld?

Antwoord:
De doorlooptijd die de commissie Van Beek heeft vermeld in het rapport (6 a 9 maanden) is niet reëel. Kijkend naar wat de systemen (stemprinter en stemmenteller) moeten kunnen is een doorlooptijd van minimaal 18 maanden te verwachten wanneer er geen CC eisen worden opgelegd. Wanneer er ook nog aan een CC EAL5 evaluatie moet worden voldaan is een doorlooptijd van enige jaren te verwachten. Voor het ontwerpproces van producten op EAL5/6 zijn moderne ontwikkeltechnieken als *Agile* en *Scrum* waarschijnlijk niet toepasbaar. In deze technieken wordt zeer flexibel omgegaan met o.a. wijzigingen in specificaties en documentatie. Voor EAL5/6 is juist een formele aanpak vereist en is dus een meer traditioneel waterval of V-model geschikt. Hierbij worden gestructureerd stap-voor-stap de functionele eisen in een aantal stappen vertaald in detail-eisen, waarna ze even gestructureerd worden omgezet in een product.

Vraag 4
Is het EAL-niveau waartegen de CC-evaluatie moet plaatsvinden van invloed op het antwoord op vraag 3? Zo ja, is dat te kwantificeren in tijd, kosten en risico's?

Antwoord:
Ja. Vanaf EAL niveau 5 moet er al rekening mee worden gehouden dat hardware, maar ook software, "op maat" gemaakt zal moeten worden om aan de CC eisen te kunnen voldoen. Hoe hoger het EAL-niveau, hoe stringenter de eisen aan het ontwerptraject, documentatie en testen zijn. Ook moet de evaluator meer doen tijdens het ontwerp-, ontwikkel- en testproces wat gaandeweg het traject waarschijnlijk zal leiden tot meer aanpassingen van het ontwerp en in de te ontwikkelen hardware. Concreet betekent dit dat naar mate het EAL niveau hoger wordt, er meer ontwikkeliteraties nodig zijn voordat het systeem succesvol gecertificeerd is.
Voor een harder antwoord op vragen 3 en 4 is meer onderzoek nodig. Een kosten- en tijdinschatting voor een dergelijk complex traject kan slecht gegeven worden zonder goed te doordenken wat eisen en oplossingen zijn.

Advies voor commissie Van Beek m.b.t. de statistische controle van de elektronische stemmenteller

Prof. dr. Ernst C. Wit
Hoogleraar Statistiek en Kansrekenen
JBI, Rijksuniversiteit Groningen

16 januari 2015

Samenvatting

De commissie Van Beek adviseert de invoering van een stemprinter waarmee de kiezer een keuze maakt voor een verkiezing en die de keuze print op een stembiljet. Het belangrijkste argument om de stemprinter in te voeren is het vergroten van de toegankelijkheid voor de kiezer (meer kiezers zouden dan zelfstandig kunnen stemmen). Daarnaast adviseert de commissie om een stemmenteller in te voeren om de papieren stembiljetten elektronisch te tellen. Het argument voor elektronisch tellen is dat het tellen dan sneller en waarschijnlijk nauwkeuriger zal kunnen verlopen dan het handmatig tellen van de stembiljetten.

De commissie wil dat de stemmenteller functioneel goed werkt en ook goed beveiligd is. Daarvoor heeft de commissie eisen geformuleerd. De commissie is echter van mening dat het niet voldoende is om te vertrouwen op die eisen. De commissie is van mening dat een controle op de juistheid van de elektronisch getelde stemmen onontbeerlijk is om vertrouwen te kunnen hebben op de juiste werking van de stemmenteller.

In deze notitie stellen we een Controllerende Toevalssteekproef voor die per stemmenteller een aantal stembiljetten en geregistreerde elektronische stemmen checkt of ze kloppen. We laten zien hoe de steekproefgrootte en acceptatiegrenzen het mogelijk maken om iedere foutenmarge met ieder gewenste betrouwbaarheid te kunnen detecteren. Afhankelijk van de eisen die gesteld worden, worden er per stemmenteller een specifiek aantal stemmen handmatig gecontrolleerd. Worden er geen afwijkingen gevonden, dan wordt de uitkomst van de elektronische stemmenteller overgenomen. Worden er een of meer afwijkingen gevonden, dan wordt de stembus handmatig geteld.

Een voorbeeld van de controlerende steekproef in actie

We beginnen dit stuk met een mogelijk scenario van de statistische toets in actie. Hiermee kan de impact van bepaalde begrippen worden gezien in een realistische context. De keuzes t.a.v. de statistische zekerheden die gemaakt worden, zijn slechts als voorbeeld bedoeld.

Stel, er wordt besloten om aan een individuele stemmenteller een foutenmarge van 3% toe te staan. Bovendien, als een stemmenteller een foutenmarge heeft die groter is dan 3%, dan moet dit met 95% betrouwbaarheid worden opgespoord. Op basis van deze twee getallen wordt er een steekproefgrootte van 50 voor de Controlerende Toets berekend (zie tabel 1): dit bestaat uit een controle van 50 stembiljetten en 50 stemregistraties. Via een randomiserend apparaat worden in totaal 100 controles uitgevoerd, bestaande uit het controleren op het bestaan en juistheid van 50 biljetten die elektronisch zijn geregistreerd, en het controleren op het bestaan en juistheid van 50 elektronische telregistraties van de papieren stembiljetten.

Stel, er wordt 1 foutieve registratie gevonden. Op dat moment kan niet met voldoende betrouwbaarheid worden gezegd dat de foutenmarge onder de 3% ligt (letterlijk: de kans op maximaal 1 fout in 100 controles als de foutenmarge al 3% is, is groter dan $100\% - 95\% = 5\%$). Op dat moment wordt er besloten om deze specifieke stemmenteller niet verder te gebruiken en om tot een handtelling over te gaan.

1 Inleiding

In 2007 heeft het kabinet besloten om het stemmen met stemmachines/stemcomputers niet meer toe te staan. Sindsdien wordt in Nederland met een rood potlood en papier gestemd en worden de stembiljetten handmatig geteld.

In opdracht van minister Plasterk van Binnenlandse Zaken en Koninkrijksrelaties heeft de commissie Van Beek in 2013 onderzocht of en hoe er (opnieuw) elektronisch gestemd kan worden. De commissie Van Beek concludeerde in zijn rapport "Elke stem telt" in december 2013 dat de tijd rijp is om weer elektronische apparatuur te gebruiken bij het stem- en telproces. De commissie stelt voor, in navolging van de commissie Korhals Altes, een stemprinter en stemmenteller in te voeren. In het concept van de commissie is de kiezer verantwoordelijk voor het controleren van het stembiljet, i.e., komt wat er geprint is overeen met wat de kiezer heeft willen kiezen? Het stembureau is in dit concept verantwoordelijk voor het controleren van de juiste werking van de stemmenteller.

Het kabinet heeft hier in maart 2014 op gereageerd door aan te kondigen de voorstellen van de commissie op de haalbaarheid te zullen onderzoeken. In september 2014 heeft minister Plasterk van Binnenlandse Zaken en Koninkrijksrelaties (BZK) de commissie Van Beek aanvullende vragen gesteld over het beveiligingsniveau, het invoeringstijdpad en de kosten van de stemprinter en stemmenteller die zij heeft geadviseerd in te voeren. De minister wil weten wat de gevolgen zijn van het door de commissie voorgestelde beveiligingsniveau van de stemprinter en de stemmenteller. Het gaat bijvoorbeeld om de complexiteit en risico's van het ontwikkelingstraject van de systemen, het geschetste invoeringstijdpad en

de kosten.

In november 2014 heeft de commissie Van Beek de ondergetekende benaderd om de haalbaarheid van een statistische controle van de stemmenteller te bestuderen. Dit document bevat een statistisch advies, waarbij formele juistheid, eenvoud & transparantie en practische haalbaarheid een belangrijke rol hebben gespeeld. Het stuk is echter beschrijvend van aard en de keuze welke foutenmarge en detectie kans gekozen zouden moeten worden, wordt overgelaten aan de commissie.

2 Controle van de stemmenteller

In de voorstellen van de commissie Van Beek worden er twee nieuwe componenten in het stemproces ingevoerd:

1. Allereerst wordt het stemmen met een rood potlood op een papieren stembiljet vervangen door het maken van een keuze op de stemprinter dat vervolgens een papieren stembiljet met daarop de gemaakte keuze uitprint. De kiezer deponeert vervolgens, net zoals nu, het papieren stembiljet in de stembus.

2. Na het sluiten van de stembus worden de papieren stembiljetten eerst uitgevouwen, gestapeld en vervolgens gescand met gebruikmaking van de stemmenteller. De stemmenteller moet op elk papieren stembiljet printen wat er gescand is. De stemmenteller genereert vervolgens een telresultaat waarin de gescande stemmen worden vermeld plus het totaal van de uitgebrachte stemmen per lijst en het totaal van de uitgebrachte stemmen per kandidaat. Ook vermeldt het telresultaat het aantal blanco uitgebrachte stemmen.

Het telresultaat van de stemmenteller zou in beginsel moeten overeenstemmen met het aantal toegelaten kiezers. Het aantal toegelaten kiezers bepaalt het stembureau door het aantal stempassen, kiezerspassen en schriftelijke volmachten op te tellen. Het aantal toegelaten kiezers en het aantal uitgebrachte stemmen (geldig plus ongeldig) moet gelijk zijn. Als het aantal niet gelijk is moet, conform de huidige regelgeving en telinstructie, het stembureau opnieuw tellen. Blijft ook na het opnieuw tellen er een verschil bestaan dan dient het stembureau in het proces-verbaal daar een verklaring voor te geven. De processen-verbaal van de stembureaus vormen de basis voor het centraal stembureau om de uitslag van de verkiezing te bepalen. Het centraal stembureau kan besluiten om een hertelling te laten uitvoeren in een, enkele of alle stembureaus.

Dit document gaat louter in op de controle van de met de stemmenteller getelde papieren stembiljetten. De vraag die we zullen beantwoorden in dit rapport kan als volgt worden geformuleerd:

> *Hoe kan door middel van handmatige steekproeven statistisch worden gecontroleerd dat de uitslag van de stemmenteller de juiste is, rekening houdend met de randvoorwaarden gesteld door het electoraal process?*

Het is bovendien van belang dat keuze voor de statistische methode zowel kan worden toegepast op gemeenteraadsverkiezingen (GR), provinciale statenverkiezingen (PV), Tweede Kamerverkiezingen (TK), verkiezing van de leden van het Europees Parlement (EP) en raadgevende referenda.

2.1 Fouten in het telprocess

Op dit moment worden stemmen uitgebracht op een groot stembiljet dat met een rood potlood wordt ingekleurd. Bij het tellen van dit stembiljet worden fouten gemaakt. Er zijn meerdere oorzaken voor die fouten, zoals het formaat van het stembiljet, de vele kandidaten, de stappen die moeten worden doorlopen bij het tellen, etc. Er is geen onderzoeksmateriaal beschikbaar aan de hand waarvan zou kunnen worden vastgesteld of deze fouten al dan niet systematisch van aard zijn. Staatssecretaris Bijleveld-Schouten gaf destijds, naar aanleidingen van telfouten bij de gemeenteraadsverkiezingen in maart 2010, aan niet te weten wat de foutenmarge was in handmatige tellingen [Tweede Kamer].

Tegen deze achtergrond wordt nu voorgesteld om de papieren stembiljetten elektronisch te tellen door middel van een stemmenteller. De kwaliteitseisen aan deze stemmenteller zouden in beginsel moeten waarborgen dat de stemmenteller functioneel correct zal werken. Echter ook een correct werkende stemmenteller zal niet alle stembiljetten altijd correct tellen. Dat is inherent aan de scantechnologie. Daarnaast is er de dreiging dat de werking van de stemmenteller gemanipuleerd zou kunnen worden en dat de stemmenteller als gevolg daarvan niet correct de papieren stembiljetten verwerkt.

Aangezien de commissie transparantie en controleerbaarheid van het telproces voorstaat is het van belang dat er bij iedere verkiezing een onafhankelijke toets komt die vaststelt of de gebruikte stemmenteller correct de papieren stembiljetten heeft verwerkt. Het onderscheid of het hierbij gaat om gerichte manipulatie van buiten, een technisch mankement of een softwarefout, is in principe irrelevant voor dit document en zullen ieder gewoonweg als fout worden aangemerkt.

In principe kunnen er twee soorten fouten worden gemaakt:

1. Een uitgebrachte stem wordt door de stemteller ten onrechte aan een andere partij of een andere kandidaat toegewezen, of niet geregistreerd.

2. De stemmenteller telt een stem, waar nooit een stem is uitgebracht.

2.2 Toetsen op fouten

De persistentie van papier stembiljetten maakt het mogelijk om het resultaat van de stemming te toetsen op numerieke juistheid. Dit kan gebeuren voor een TK, EP, PV, GR en raadgevende referenda. Om de statistische toets schaalbaar te maken voor elk soort verkiezing over verschillende groottes van gemeenten kiezen wij in dit document ervoor om de kleinste eenheid, i.e. de individuele stemmenteller, het object van de toets te maken. Daar zijn in principe een aantal mogelijkheden voor. We bespreken hier twee mogelijke steekproef scenario's.

1. **Tellende Toets.** Een toevalssteekproef over de hele verkiezingseenheid met als doel om te controleren of de waargenomen stemratio's door de elektronische stemmenteller overeenstemmen met de ratio's in de handgetelde toets.

2. **Controlerende Toets.** Een toevalssteekproef over de hele verkiezingseenheid met als doel om te controleren of er fouten, zoals bijvoorbeeld beschreven in de vorige paragraaf, zijn gemaakt.

Het nadeel van de eerste soort van toets, i.e. de Tellende Toets, is dat de steekproefgrootte in principe afhangt van de relatieve fracties van de waargenomen stemmen door de elektronische stemmenteller. Dit maakt het fundamenteel onmogelijk om vooraf een steekproefgrootte vast te stellen, zonder extra aannames. Zulke aannames zijn natuurlijk wel mogelijk — bijvoorbeeld, als als stemeenheid het hele land wordt genomen in het geval van een TK verkiezing, dan zouden onder bepaalde aannames het mogelijk zijn om een steekproefgrootte vooraf te bepalen om de verdeling van de restzetel mogelijk te maken [Gill, 2013]. Het is echter erg lastig om aannames te maken die zowel voor TK of EP verkiezingen, en ook voor PV, GR of raadgevende referenda gelden.

De tweede soort van toets is conceptueel eenvoudiger. Het controleert enkel en alleen *of* en *hoeveel* fouten er zijn gemaakt door de stemmenteller. Dit kunnen fouten zijn zowel van de eerste (i.e. het toewijzen van stemmen aan de verkeerde of geen enkele partij of kandidaat) als tweede (i.e. het tellen van spookstemmen, d.w.z. stemmen waarvan geen overeenkomstig papieren stembiljet bestaat) soort zijn. Een nadeel van deze tweede soort toets dat het geen onderscheid maakt in de type fout die gemaakt wordt. Een systematische fout in de stemmenteller kan in principe niet worden onderscheiden van een willekeurige fout: een stemmenteller die eens in de 100 stembiljetten een willekeurige fout maakt is in de controlerende toets even goed als een stemmenteller die de stemmen van een kandaat met 1% van de stemmen systematisch aan een andere kandidaat toeschrijft.

Voorlopig hebben leden van de commissie Van Beek aangegeven (in een direct gesprek met ondergetekende, 7/11/2014) een Controlerende Toets te prefereren. Het is belangrijk om hierbij te realiseren dat de doorzichtigheid van een Controlerende Toets in bepaalde gevallen een grotere steekproefgrootte tot gevolg zal hebben, met name voor TK en EP verkiezingen — hoeveel groter hang af van de omstandigheden. Daartegenover staat dat de Controlerende Toets inherent eenvoudiger en inzichtelijker is dan een Tellende Toets.

2.3 Kansen op fouten

Er zijn drie kansen die in ogenschouw moeten worden genomen. In deze paragraaf leggen we uit wat deze drie kansen zijn en hoe zij de grootte en werking van de Controlerende Toets beinvloeden.

Staatssecretaris Bijleveld-Schouten heeft destijds aangegeven een foutenmarge van 0% na te streven [Tweede Kamer]. Dit streven is door de commissie Van Beek vertaald door hoge eisen aan de stemmenteller te stellen. Echter, om te weten of de stemmenteller ook werkelijk een foutenmarge van 0% haalt, zou iedere geregistreerde stem en ieder geprint stembiljet moeten worden gecontroleerd door de Controlerende Toets. Als men echter bereid is om een kleine foutenmarge toe te staan, dan hoeven niet alle biljetten te worden

gecontroleerd. De toegestane foutkans wordt vaak de *marge* genoemd. Het is belangrijk dat de hoogstwaarschijnlijk kleine foutenmarge die wordt nagestreefd door de makers van stemmenteller (en die gedeeltelijk inherent is aan de scantechnologie) wordt onderscheiden van de foutenmarge die de Controlerende Toets wordt geëist te detecteren. In dit stuk hebben we het over deze laatste kans

> **Foutenmarge (m).** De toegestane fractie van foutieve tellingen door de stemmenteller.[1]

Vanaf nu zullen we met uitdrukking "Stemmenteller OK" bedoelen dat de foutenmarge onder m ligt voor die individuele stemmenteller. Een stemmenteller waar iets mee mis is ("Stemmenteller fout") betekent een stemmenteller met foutenmarge boven de m. Als er een steekproef wordt genomen, waarna een beslissing volgt over het al dan niet goed werken van de stemmenteller, dan zijn er in principe vier mogelijke uitkomsten mogelijk, aangegeven in de volgende tabel.

	Steekproef	
	OK	verdacht
Stemmenteller OK	Goed	Fout 1
Stemmenteller fout	Fout 2	Goed

In tegenstelling tot het gebruikelijke hypothese toetsen, zoals gebruikt in de wetenschap of farmaceutische industrie, is de burger voornamelijk geïnteresseerd in de kans op de fout van de tweede soort, namelijk,

> **Kans op Fout 2 (β).** De waarschijnlijkheid dat de steekproef niet detecteert als er werkelijk iets mis is met de stemmenteller.

In principe zouden we graag deze kans zo klein mogelijk willen houden. Dat wil zeggen, als een bepaalde stemmenteller een foutenmarge heeft die hoger is dan m, dan zouden we dit zo graag met 100% zekerheid willen vaststellen. In principe zou dan de hele stembus met de hand gecontroleerd moeten worden in een Controlerende Toets. Als men bereid is om een foutenmarge die groter is dan m niet te detecteren met een kleine kans β, dan kan de omvang van de Controlerende Toets worden verkleind.

Een mogelijke uitkomst van de Controlerende Toets is dat de stemmenteller foutief *lijkt* te werken en dat derhalve de telling met de hand moet worden overgedaan. Natuurlijk is het onwenselijk om tot een handtelling over te gaan als de foutenmarge toch binnen de perken is gebleven zoals hij hierboven gesteld is. De mate van onwenselijkheid wordt beschreven de kans van de eerste soort:

> **Kans of Fout 1 (α).** De waarschijnlijkheid dat de steekproef zegt dat er iets mis is met de stemmenteller, terwijl dit niet het geval is.

[1] De werkelijke foutenmarge is de theoretische fout inherent aan de stemmenteller. Alleen als de Controlerende Steekproef erg groot is, komt deze overeen met de relatieve fractie van het aantal gedetecteerde fouten.

Hoewel het mogelijk is om pas over te gaan tot een volledige handtelling als de Controlerende Steekproef minimaal een bepaald aantal foutieve registraties heeft gevonden en op die manier de kans α beperkt te houden, heeft de commissie aangegeven om in het belang van eenvoud dit achterwege te willen laten.

3 Risicomijdende controlerende steekproef

In de voorafgaande paragraaf zijn drie kansen op fouten benoemd.

1. Ten eerste is er de mogelijke fysische fout van de stemmenteller zelf. Dat wil zeggen, de relatieve fractie m van stemmen die het verkeerd toewijst aan kandidaten en/of partijen *of* de relatieve fractie m van geregisteerde stemmen door de stemmenteller die niet overeenkomen met een fysiek stembiljet.

2. Vervolgens zijn er twee statistische fouten, geassocieerd met de nauwkeurigheid met de steekproef, i.e.,

   (a) de non-detectie kans β dat de stemmenteller op basis van de steekproef ten onrechte goed functionerend wordt bevonden (fout 2);

   (b) de kans α dat de stemmenteller op basis van de steekproef ten onrechte foutief wordt bevonden (fout 1).

Door middel van grote Controlerende Steekproeven is het in principe mogelijk om een willekeurig kleine foutenmarge m van de stemmenteller te ontdekken met een willekeurige precisie $(1 - \beta)$. De commissie heeft besloten om ter wille van de eenvoud de kans α niet verder te willen controleren. Dit betekent dat zodra de Controlerende Steekproef een stemmenteller niet met precisie $1 - \beta$ kan zeggen dat de marge onder de m ligt, er automatisch zal worden besloten tot een handtelling.

De statistische techniek om deze fouten te beheersen is ontwikkeld en beschreven in Stark [2008], Lindeman and Stark [2012] en wordt de risicomijdende controletellingen genoemd. Het is toegepast in California en kan worden aangepast aan de Nederlandse situatie. Gill [2013] beschrijft een mogelijke toepassing van deze methodologie op landelijk TK niveau. In deze notitie geven we een beschrijving op het niveau van de individuele stemmenteller. In tegenstelling tot Stark [2008], Lindeman and Stark [2012] en Gill [2013] zullen wij de marge m in eerste instantie niet direct verbinden aan de uitslag van de verkiezingen, maar aan een acceptabel niveau voor een stemmenteller.

Het achterliggende idee van de risicomijdende controletellingen is om een steekproef ter grootte van n stembiljetten te doen en het aantal afwijkingen te tellen ten opzichte van de elektronische stemmenteller.[2] Vervolgens worden twee scenarios onderscheiden:

[2] De steekproefgrootte n volgt uit een gekozen combinatie van toegestane marge m, de toegestane non-detectie kans β *en* het aantal toegestane gevonden afwijkingen. Om de steekproefgrootte zo klein mogelijk te houden, zullen we geen enkele gedetecteerde afwijking toestaan in de steekproef.

- **Aantal afwijkingen = 0.** Het aantal afwijkingen van de controlerende steekproef ten opzichte van de elektronische uitslag is dusdanig klein, dat

  $$P(\text{aantal afwijkingen} = 0 \text{ terwijl foutenmarge stemmenteller} > m) \leq \beta,$$

  de kans dat er geen fouten worden waargenomen terwijl de stemmenteller net niet acceptabel presteert, klein is. Derhalve kan worden aangenomen dat de stemmenteller correct werkt. In dat geval zal de elektronische uitslag worden geaccepteerd en als zodanig worden doorgegeven aan een centrale instantie.

- **Aantal afwijkingen = C $\geq$ 1.** Het aantal afwijkingen van de controlerende steekproef ten opzichte van de elektronische uitslag is dusdanig groot, dat

  $$P(\text{aantal afwijkingen} \leq C \text{ terwijl foutenmarge stemmenteller} > m) > \beta,$$

  de kans dat er zo veel fouten worden waargenomen consistent is met een stemmenteller die niet acceptabel presteert. Derhalve wordt er — mogelijkerwijze foutief, maar voor de zekerheid — aangenomen dat de stemmenteller niet correct werkt, en zal er worden overgegaan op een handmatige telling van de hele stembus.

3.1 Toevalssteekproef

De gehele analyse is gebaseerd op het feit dat er zowel een *toevalssteekproef*[3] getrokken kan worden uit de stembiljetten als uit de elektronische stemuitdraai. Vanuit een practische standpunt stellen wij voor om de volgende procedure aan te houden:

1. Een centrale onafhankelijke instantie presenteert elk stembureau met een gesloten en verzegelde envelop met random gegenereerde volgnummers. Omdat stembureaus verschillende aantallen stemmen te verwerken krijgen worden er verschillende lijsten geleverd, waarbij de getrokken getallen variëren van 1 tot en met verscheidene maxima (e.g. 500, 750, 1000, 2000, 3000, 5000).[4]

2. Het stembureau kiest de envelop met random getallen dat behoort bij het kleinste maximale nummer dat groter is dan het aantal uitgebrachte stemmen. Iedere envelop bevat twee lijsten met getallen: een die hoort bij de fysieke stembiljetten en een die hoort bij de stemmenprinteruitdraai.

3. Er vinden twee type controles plaats: een controle van een aantal fysieke stembiljetten volgens de ene lijst en een controle van een aantal stemregistraties op de telstrook volgens de andere lijst. Het aantal controles voor iedere lijst is gelijk aan het aantal zoals gegeven in tabel 1.

[3]Wat ten alle tijden moet worden vermeden is om de keuze van de steekproef uit te voeren op een systematische wijze (bijvoorbeeld "elke tiende stembiljet") of willekeurige wijze (bijvoorbeeld "her en der wat stembiljetten controleren"). Deze wijze van sampelen speelt mogelijkerwijs een systematische fout in de kaart en bovendien invalideert alle probabilistische berekeningen die in deze notitie worden uitgevoerd.

[4]Het aantal stemmen dat per stembureau wordt uitgebracht kan enorm verschillen: van een paar honderd tot wel een paar duizend. De berekeningen hangen echter in geen enkele wijze af van het aantal uitgebrachte stemmen. Wel van belang is de grootte van de steekproef. De groter de steekproef, de groter de zekerheid over de werkelijke foutenmarge van de stemmenteller.

(a) Tellend vanaf het bovenste stembiljet worden precies die stembiljetten gecontroleerd die overeenkomen met de random nummers in de eerste lijst. Voor de controle van een fysiek stembiljet moet worden gekeken of de stem geregistreerd is en wel voor de juiste kandidaat en partij.

(b) Tellend van de bovenste stemregistratie worden precies die registraties gecontroleerd die overeenkomen met de random nummers in de tweede lijst. Bij elke telregistratie moet het corresponderende biljet in de stapel gezocht worden en de tekst op het biljet moet overeenkomen met de tekst op de telstrook.

4. Voor ieder van de twee controles geldt dat nummers op de lijst die groter zijn dan het totale aantal stembiljetten en elektronische registraties, respectievelijk, worden overgeslagen, net zo lang totdat de hele steekproef is vervuld.

In het onderstaande noemen we de steekproefgrootte n en definiëren de variabele,

T_n = aantal gevonden afwijkingen van stemmenteller t.o.v. steekproef ter grootte n.

Een afwijking is gedefinieerd als,

- een papieren stembiljet in de steekproef die niet geteld is door de stemmenteller.
- een papieren stembiljet in de steekproef die aan de verkeerde partij of kandidaat is toegekend. (Deze fout kan mogelijkerwijs worden geteld als twee afwijkingen, namelijk een fout bij de niet-gekozen partij/kandidaat en een fout bij de gekozen partij/kandidaat. Deze definitie wordt door Lindeman and Stark [2012] aangehangen. Wij zien het in deze notitie als een afwijking, met name omdat we in eerste instantie niet naar de effecten van de fout op de uitslag kijken, maar naar de foutenmarge van de stemmenteller zelf.)
- een elektronisch geregistreerde stem die niet voorkomt als papieren stembiljet.

3.2 Aanbevelingen voor steekproefgrootte

We precisieren nu de oorspronkelijke onderzoeksvraag als volgt:

> Hoe groot moet de steekproef zijn om er met kans $1-\beta$ zeker van te zijn dat een stemmenteller met foutenmarge m wordt gedetecteerd.

Om de steekproef zo klein mogelijk te houden, zal een stemmenteller alleen als betrouwbaar worden bestempeld als er in de steekproef geen afwijkingen worden gevonden. De totale steekproefgrootte kan worden bepaald via de volgende formule,

$$n = \frac{\log \beta}{\log(1-m)}.$$

Voor iedere afzonderelijk controle moet de steekproefgrootte door tweeë worden gedeeld en worden afgerond naar boven. In tabel 1 staan de noodzakelijke steekproefgroottes

voor ieder van de twee afzonderlijke controles, i.e. de controle van de stembiljetten en de controle van de elektronische registraties om een bepaalde detectie kans van een foutief functionerende stemmenteller te behalen. Bijvoorbeeld, als de steekproefgrootte gelijk is aan 50 van beide controles, dan is de kans 95% om een stemmenteller met foutenmarge van 3% te detecteren.

Referenties

R. Gill. Statistical audits for elections. In *Bijlagen "Elke Stem Telt"*, pages 243–260, 2013.

Mark Lindeman and Philip B Stark. A gentle introduction to risk-limiting audits. *IEEE Security and Privacy*, 10(5):42, 2012.

Philip B Stark. Conservative statistical post-election audits. *The Annals of Applied Statistics*, pages 550–581, 2008.

Tweede Kamer. *Verslag van Algemeen Overleg*, number 22 in 31 142, 13 april 2010.

marge m	detectie kans $1-\beta$	steekproef grootte
0.005	0.995	529
	0.990	460
	0.970	350
	0.950	299
	0.900	230
0.010	0.995	264
	0.990	230
	0.970	175
	0.950	150
	0.900	115
0.020	0.995	132
	0.990	114
	0.970	87
	0.950	75
	0.900	57
0.030	0.995	87
	0.990	76
	0.970	58
	0.950	50
	0.900	38
0.040	0.995	65
	0.990	57
	0.970	43
	0.950	37
	0.900	29
0.050	0.995	52
	0.990	45
	0.970	35
	0.950	30
	0.900	23
0.100	0.995	26
	0.990	22
	0.970	17
	0.950	15
	0.900	11

Tabel 1: De noodzakelijke steekproefgrootte voor zowel de controle van de stembiljetten als van de controle van de elektronische telregistraties om een stemmenteller met foutenmarge m met betrouwbaarheid $1-\beta$ te detecteren. Alleen steekproeven zonder waargenomen afwijkingen leiden tot acceptatie van de elektronische stemmentelling. Als er afwijkingen worden gevonden in een van de twee controles (of beiden) dan zal dit leiden tot een handtelling.