Van stembus naar uitslag: gegevensintegriteit verkiezingsproces

Scriptie

Maarten Engberts

M.engberts@student.ru.nl

Versie 1.0, juli 2011

Supervisors:

prof. dr. B.P.F. (Bart) Jacobs
prof. dr. ir. Th.P. (Theo) van der Weide

Afstudeernummer: 153 IK

Radboud Universiteit Nijmegen

Samenvatting

Voorafgaand aan de afschaffing van stemcomputers in 2007 is er in de publieke opinie veel discussie geweest over het gebruik van de stemcomputer. De actiegroep 'Wij vertrouwen stemcomputers niet' toonde aan dat het gebruik van de stemcomputer geen recht deed aan een aantal eisen voor het verkiezingsproces, zoals de voorwaarde 'stemgeheim'. Na de afschaffing van de stemcomputer heeft de Kiesraad besloten om het programma OSV te laten ontwikkelen, wat staat voor 'Ondersteunende Software Verkiezingen'. OSV wordt onder andere door het plaatselijk stembureau, het hoofdstembureau en het centrale stembureau gebruikt om verkiezingsuitslagen vast te leggen en door te sturen naar een bovenliggend stembureau.

De verkiezingsuitslagen worden binnen OSV vastgelegd in een XML-bestand. Na het vaststellen van de uitslag wordt er binnen OSV een proces-verbaal aangemaakt, evenals een XML-bestand. Op het proces-verbaal staan de verkiezingsuitslagen per partij en per kandidaat. Het proces-verbaal bevat tevens een hashcode van het XML-bestand. Het proces-verbaal wordt afgedrukt en ondertekend door de aanwezige leden van het stembureau waar OSV op dat moment gebruikt wordt. Het XML-bestand wordt gebruikt om verkiezingsuitslagen in te lezen in een ander deelprogramma van OSV. Het XML-bestand, dat gezamenlijk met het afgedrukte proces-verbaal per USB-stick van bijvoorbeeld het plaatselijk stembureau naar het hoofdstembureau wordt vervoerd, kan tussentijds eenvoudig met een tekstverwerker aangepast worden. Van het gemanipuleerde XML-bestand kan een nieuwe hashcode berekend worden. Als deze gemanipuleerde verkiezingsuitslagen worden ingeleverd bij het hoofdstembureau of bij het centrale stembureau, zijn er weinig middelen om fraude met verkiezingsuitslagen op te merken, aangezien OSV enkel een onbeschermde hashcode als authenticatiemiddel gebruikt om eventuele manipulatie van XML-bestanden op te merken.
Een bijkomend probleem zijn de beperkte echtheidskenmerken van processen-verbaal waardoor het voor kwaadwillenden eenvoudig is om gegevens op het proces-verbaal zoals hashcodes en verkiezingsuitslagen te manipuleren.
Om deze problemen te beheersen is er gekozen om de nadruk te leggen op detectie van manipulatie. Maatregelen ter bevordering van detectie van manipulatie doen meer recht aan de transparantie van het verkiezingsproces dan andere beveiligingsmaatregelen zoals volledige versleuteling van verkiezingsuitslagen. Om tussentijdse manipulatie van verkiezingsuitslagen in XML-bestanden op te merken, kan ervoor gekozen worden om hashcodes op processen-verbaal te ondertekenen. Hiervoor wordt asymmetrische cryptografie gebruikt, waardoor iedereen een ondertekende hashcode kan controleren op authenticiteit. In geval van manipulatie is het voor het hoofdstembureau of het centrale stembureau eenvoudig om fraude op te merken. Processen-verbaal worden van meer echtheidskenmerken voorzien om het manipuleren van verkiezingsuitslagen op processen-verbaal moeilijker te maken. Methoden als asymmetrische cryptografie bieden voor de toekomst mogelijkheden om XML-bestanden met daarin verkiezingsuitslagen aan te bieden aan het centrale stembureau via onbeveiligde communicatiekanalen zoals e-mail en internet. Ook kan er voor gekozen worden om de XML-bestanden voor iedereen beschikbaar te maken door deze bestanden op een internetpagina te plaatsen.
Een alternatief voor asymmetrische cryptografie is het verzenden van (de hashcode op) het proces-verbaal via een beveiligd kanaal naar het bovenliggende stembureau. Faxapparaten zijn veelgebruikte middelen om documenten op een veilige wijze te verzenden. De ontvangende partij heeft met een gefaxt proces-verbaal altijd vergelijkingsmateriaal ten opzichte van het ontvangen proces-verbaal dat persoonlijk wordt verstuurd. In geval van manipulatie van het XML-bestand en het papieren proces-verbaal kunnen medewerkers van bijvoorbeeld het centrale stembureau de ontvangen documenten vergelijken met het gefaxte proces-verbaal.

Inhoudsopgave

Samenvatting 2

Inhoudsopgave 3

Verklarende woordenlijst 5

1 Inleiding 6

1.1 Aanleiding en doel onderzoek 7

1.2 Scope: na sluiting van het stembureau 7

1.3 Methode 10

2 Achtergrond 12

2.1 Tijdslijn 12

2.2 Eisen aan het verkiezingsproces 13

2.3 Huidige situatie 14

2.4 Ondersteunende Software Verkiezingen 14

3 Bevindingen bij stembureaus en OSV 19

3.1 Bevindingen bij het lokale stembureau 19

3.2 Bevindingen bij het hoofdstembureau 22

3.3 Bevindingen bij het centraal stembureau 23

3.4 Bevindingen binnen OSV 25

3.5 Conclusie en samenvatting 45

4 Risico analyse 46

4.1 Inventaris 46

4.2 Gevonden kwetsbaarheden 47

4.3 Gevonden risico's 49

4.4 Conclusie 51

5 Methoden voor risicobeheersing 52

5.1 Afwegingen 53

5.2 Focusgebieden 53

5.3 Van lokaal stembureau naar plaatselijk stembureau: processen-verbaal 54

5.4 Van plaatselijk stembureau naar centraal stembureau: processen-verbaal en vastgelegde verkiezingsuitslagen in OSV 54

5.5 De implementatie van de hashfunctie sha256/512 65

6 Conclusies en aanbevelingen 66

6.1 OSV in de toekomst 66

6.2 Evaluatie onderzoek en slotwoord 66

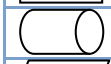
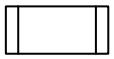
7 Bronnen en referenties 67

8 Bijlagen 69

8.1 ORM model 69

8.2 Schema OSV 70

Verklarende woordenlijst

Omschrijving	Uitleg
Alice (A)	Alice kan een medewerkster zijn van een lokaal stembureau, een plaatselijk stembureau, een hoofdstembureau of het centrale stembureau.
Bob (B)	Bob kan een medewerkster zijn van een lokaal stembureau, een plaatselijk stembureau, een hoofdstembureau of het centrale stembureau.
Trudy (T)	Trudy is een kwaadwillend persoon die erop uit is om te frauderen met vastgelegde verkiezingsuitslagen. Trudy kan als kwaadwillend persoon tevens medewerkster zijn van een lokaal stembureau, een plaatselijk stembureau of een hoofdstembureau.
Server (S)	De centrale fileserver met daarop XML-bestanden met vastgelegde verkiezingsuitslagen die afkomstig zijn uit OSV.
Client (C)	Een werkstation waarop gegevens van een proces-verbaal ingevoerd kunnen worden. De ingevoerde gegevens worden op de server (S) geplaatst.
OSV	Ondersteunende Software Verkiezingen
Sha1(document x)	Een hashcode van document x
PKI	Public Key Infrastructure
$Sign_{Alice}$(sha-1(document x))	De hashcode van document x is ondertekend door Alice
$Sign_{Bob}$(sha-1(document x))	De hashcode van document x is ondertekend door Bob
Firmware	Software dat is ingebouwd in een computer om de computer een aantal opdrachten te laten uitvoeren.
	Eén document
	Verzameling van meerdere documenten
	Proces
	Digitale opslag (database)
	Digitale opslag (bestand)
	Een systeem: dit kunnen meerdere processen zijn. Het programma ‘P4 HSB’ kan bijvoorbeeld worden aangeduid als ‘systeem’.

1 Inleiding

Eerlijk verlopen verkiezingen zijn van groot belang voor het functioneren van de democratie. Via verkiezingen worden de volksvertegenwoordigers door de bevolking zelf gekozen. Daardoor heeft de bevolking van een land directe invloed op de besluitvorming op het hoogste niveau in het land. Nederlanders gaan naar een stembureau om daar aan te geven op welke kandidaat van een bepaalde partij zij stemmen. Sinds 2007 worden wederom stembiljetten gebruikt om stemgerechtigden hun stem te laten uitbrengen. Alle kandidaten die zich verkiesbaar gesteld hebben staan met hun naam en woonplaats gerangschikt per partij afgedrukt op een stembiljet. De kiezer (de persoon die stemrecht heeft) mag maximaal één hokje bij de naam van een kandidaat markeren en deponeert het ingevulde stembiljet in een verzegelde stembus. Na sluitingstijd van het stemlokaal wordt de stembus met de daarin alle (ingevulde) stembiljetten geopend en worden de stemmen geteld op partijniveau en op kandidaat-niveau. Daarna wordt de uitslag op een proces-verbaal genoteerd. Dit proces-verbaal wordt van het lokale stembureau naar het plaatselijke stembureau gebracht. Naast het invullen van een stembiljet zijn er in het verleden meerdere methoden geweest om stemmen vast te leggen. Gedurende de periode 1993 – 2007 kon de kiezer in de meeste gemeenten gebruik maken van een stemcomputer.[1] Deze stemcomputers werden geleverd door de firma Nedap en de uitgeverij SDU. Het voordeel van deze stemcomputers was dat ingevoerde stemmen na sluitingstijd van het stembureau automatisch geteld konden worden. In de beginjaren van het gebruik van deze stemcomputers zag men vooral de gemakken van de stemcomputers. De laatste jaren van de periode waarin deze stemcomputers gebruikt werden, groeide de kritiek op het functioneren van deze stemcomputers. Het scherm met daarop de namen van de kandidaten op de stemcomputer van de uitgeverij SDU bleek vanaf enkele tientallen meters afgeluisterd te kunnen worden door de compromitterende straling die het scherm van de stemcomputer veroorzaakte. Door dit probleem werd er niet aan de voorwaarde ‘stemgeheim’ voldaan. De actiegroep ‘Wij vertrouwen stemcomputers niet’ in [STN07] toonde aan dat het gebruik van de stemcomputer van Nedap ook risico’s met zich meebracht: de software op de chips in de stemcomputer kon aangepast worden. De actiegroep toonde dit aan door andere software op de stemcomputer van Nedap te installeren zodat er een schaakspel mee gespeeld kon worden. De achterliggende gedachte hiervan was dat als men een schaakspel op de stemcomputer kan spelen, men ook frauduleus stemmen kan tellen.

Het Ministerie van Binnenlandse Zaken heeft een adviescommissie ingesteld om het verkiezingsproces in beeld te brengen. Er zijn voorstellen gedaan voor verbetering of verandering van het verkiezingsproces die voldoen aan een aantal eisen. Deze eisen hebben onder andere toepassing op het vrije karakter van de verkiezingen, het stemgeheim, de transparantie en de uitvoerbaarheid van de verkiezingen. In het door de Adviescommissie inrichting Verkiezingsproces uitgegeven rapport ‘Stemmen met vertrouwen’ [BZK07] is veel aandacht gegaan naar de automatisering rond het verkiezingsproces. Onder andere naar aanleiding van de presentatie van dit rapport is het gebruik van de stemcomputer afgeschaft.

Naar aanleiding van de adviezen van de Adviescommissie inrichting Verkiezingsproces heeft de Staatsecretaris van Binnenlandse Zaken en Koninkrijksrelaties besloten om software te laten ontwikkelen ter ondersteuning van gedeelten van het verkiezingsproces [KSR10b]. De Kiesraad heeft in overleg met de Vereniging Nederlandse Gemeenten besloten om het programma OSV (Ondersteunende Software Verkiezingen) te ontwikkelen. Het programma OSV is ontwikkeld als administratieve ondersteuning voor de kandidaatstelling, het vaststellen van de uitslag van de verkiezingen en de zetelverdeling die volgt op de verkiezingsuitslag [KSR10].

[1] Als men zou spreken over een ‘stemmachine’ spreekt men van een apparaat dat alleen datgene kan doen waarvoor het ontworpen was: stemmen vastleggen en tellen. Nu aangetoond is dat de machine ook gebruikt kan worden om er schaakspelletjes mee te spelen, kan men beter spreken van een computer, omdat een computer voor meerdere variërende doeleinden ingezet kan worden.

Het programma OSV wordt gebruikt om onder andere verkiezingsuitslagen door te geven van het plaatselijk stembureau naar het hoofdstembureau en van het hoofdstembureau naar het centrale stembureau.
In het programma OSV worden stemtotalen op plaatselijk, hoofd –en op centraal stembureauniveau ingevoerd. De verkiezingsuitslagen worden binnen OSV opgeslagen op een server. Ook hier kan men spreken van digitale opslag van stemtotalen, net zoals bij de stemcomputers van SDU en Nedap. Als het gebruik van OSV vergeleken wordt met de problemen rond de stemcomputer van Nedap, mogen er vragen gesteld worden over de integriteit en authenticiteit van deze opgeslagen verkiezingsuitslagen binnen OSV.

1.1 Aanleiding en doel onderzoek

Het verkiezingsproces in Nederland voorafgaand aan de afschaffing van de stemcomputers in 2007 veel in het nieuws geweest. De meeste aandacht was hierbij gevestigd op de problemen rond het gebruik van stemcomputers waarbij voorwaarden voor de verkiezingen zoals het stemgeheim en de controleerbaarheid niet gewaarborgd konden worden. Naar aanleiding van het rapport van de Adviescommissie inrichting Verkiezingsproces [BZK07] is het programma OSV ontwikkeld als administratieve ondersteuning van het verkiezingsproces. In het rapport 'Stemmen met vertrouwen' dat is uitgebracht door de Adviescommissie inrichting Verkiezingsproces [BZK07] is er veel aandacht uitgegaan naar digitale hulpmiddelen. De klassieke hulpmiddelen zoals het proces-verbaal hebben van de Adviescommissie inrichting Verkiezingsproces weinig tot geen aandacht gekregen. Daarom wordt er in dit onderzoek aandacht besteed aan de integriteit van verkiezingsuitslagen die genoteerd zijn op een proces-verbaal. De Kiesraad claimt dat verkiezingsuitslagen die door het hoofdstembureau in OSV vastgelegd zijn niet meer veranderd kunnen worden [KSR08]. De authenticiteit van gegevens wordt bewaakt door middel van een hashcode. Hier wordt verder op ingegaan in hoofdstuk 2.4.2.1: De beveiliging van hashcodes binnen OSV.
Het hoofdzakelijke doel van dit onderzoek is om de gegevensstromen binnen het verkiezingsproces te onderzoeken vanuit het perspectief van de informatiebeveiliging. Hierbij gaat het om de integriteit van de vastgelegde verkiezingsuitslagen. Deze verkiezingsuitslagen worden digitaal opgeslagen binnen OSV en daarnaast worden deze verkiezingsuitslagen vastgelegd op een proces-verbaal. Om na te gaan of de integriteit van vastgelegde verkiezingsuitslagen kan worden gewaarborgd zullen eerst alle risico's van het vastleggen van de verkiezingsuitslagen op een proces-verbaal en het digitaal opslaan van verkiezingsuitslagen in OSV worden geïdentificeerd. Daarna zal er onderzoek gedaan worden hoe deze risico's beheerst kunnen worden. Tot slot zal er een aanbeveling gedaan worden welke (digitale) hulpmiddelen of procedures er beschikbaar zijn of ontwikkeld moeten worden om de risico's van (digitaal) opgeslagen verkiezingsuitslagen te beheersen. Hiervoor wordt een risicoanalyse uitgevoerd.

1.2 Scope: na sluiting van het stembureau

De scope van dit onderzoek is gericht op de gebeurtenissen, procedures en omstandigheden die invloed kunnen hebben op de integriteit van vastgelegde verkiezingsuitslagen. Alle gebeurtenissen rond het vastleggen van de namen van de kandidaten, het aanmaken van de verkiezingsdefinitie, het versturen van stempassen, het stemmen zelf en het tellen van stemmen vallen buiten de scope van dit onderzoek. Het onderzoek betreft derhalve wat er plaatsvindt vanaf het moment van sluiting van het stembureau.
Het vastleggen van verkiezingsuitslagen op een proces-verbaal en in OSV, mede als het transport van vastgelegde verkiezingsuitslagen valt wel binnen de scope van dit onderzoek. Vanaf het moment dat verkiezingsuitslagen worden vastgelegd speelt de integriteit van vastgelegde verkiezingsuitslagen een rol.

Hieronder is per verkiezingsonderdeel vastgesteld of het betreffende onderdeel binnen de scope van dit onderzoek valt. Ook wordt per onderdeel het bijbehorende programma van OSV vastgesteld.

Verkiezingsonderdeel	Scope?	OSV-onderdeel
Kandidaatstelling politieke partijen	Nee	OSV P1
Onderzoek kandidatenlijsten	Nee	OSV P2
Vaststellen kandidatenlijsten	Nee	OSV P3
Versturen stemkaarten	Nee	
Inbrengen stemmen	Nee	
Tellen stemmen	Nee	
Versturen proces-verbaal van lokaal stembureau naar plaatselijk stembureau	Ja	
Samenvoegen en versturen verkiezingsuitslagen op plaatselijk stembureauniveau Versturen proces-verbaal van plaatselijk stembureau naar hoofdstembureau	Ja Ja	OSV P4 PSB
Samenvoegen en versturen verkiezingsuitslagen op hoofdstembureauniveau	Ja	OSV P4 HSB
Versturen proces-verbaal van hoofdstembureau naar centraal stembureau	Ja	
Samenvoegen en versturen verkiezingsuitslagen op centraal stembureauniveau	Ja	OSV P4 CSB
Zetelberekening	Nee	OSV P5

Tabel 1: scope

1.2.1 Soorten verkiezingen

Het hele verkiezingsprotocol zoals beschreven in de Nederlandse Kieswet bevat een omvangrijke hoeveelheid regels en afspraken, van het registreren van verkiesbare personen tot het installeren van nieuw gekozen kandidaten. In Nederland worden voor de volgende vertegenwoordigende organen verkiezingen georganiseerd:

- Gemeenteraad
- Provinciale Staten
- Europees Parlement
- Tweede Kamer

De opzet van de verkiezing kan per onderdeel verschillen; zo speelt het centrale stembureau bij de Gemeenteraadsverkiezingen en bij de Provinciale verkiezingen een andere rol dan bijvoorbeeld de Tweede Kamerverkiezingen en de verkiezingen voor het Europese Parlement. Bij de Provinciale Statenverkiezingen wordt de definitieve zetelberekening per provincie berekend. Bij de Tweede Kamerverkiezingen wordt de definitieve zetelberekening voor het hele land door het Centrale

Stembureau in Den Haag berekend. In de tabel hieronder staan per onderdeel volgens [KSR10b] de rollen beschreven van het lokale stembureau, het hoofdstembureau en het centrale stembureau.

	Lokaal stembureau	Hoofdstembureau	Centraal Stembureau	Opmerkingen
Gemeenteraadsverkiezingen	• Vastleggen uitslagen op partij –en op kandidaat-niveau	• Vaststellen stemtotalen per kieskring • Standaard taken*	• Vervult de rol van het hoofdstembureau	Elke gemeente vormt één kieskring
Provinciale/Eerste Kamerverkiezingen	• Vastleggen uitslagen op partij –en op kandidaat-niveau	• Vaststellen stemtotalen per kieskring • Standaard taken*	• Vervult de rol van het hoofdstembureau, behalve als een provincie uit meerdere kieskringen bestaat.	Elke provincie heeft één of meerdere kieskringen. Eén centraal stembureau per provincie.
Europese Parlementsverkiezingen	• Vastleggen uitslagen op partij –en op kandidaat-niveau	• Vaststellen stemtotalen per kieskring	• Vaststellen verkiezingsuitslag • Beoordeling geldigheid kandidatenlijsten • Standaard taken*	Eén kieskring voor Nederland
Tweede Kamerverkiezingen	• Vastleggen uitslagen op partij –en op kandidaat-niveau	• Vaststellen stemtotalen per kieskring	• Vaststellen verkiezingsuitslag • Standaard taken*	Eén of meerdere kieskringen per provincie (19 in totaal)

Tabel 2: soorten verkiezingen

*De standaard taken van het Centraal Stembureau volgens [KSR10b] zijn:

- registratie van namen (aanduidingen) van politieke partijen;
- beoordeling van de geldigheid van lijstencombinaties;
- nummering van de kandidatenlijsten

Het programma OSV is ingericht om op een flexibele wijze met deze verschillende soorten verkiezingen om te gaan. Meer details staan beschreven in hoofdstuk 3.4.1: Hiërarchische structuur OSV.

1.2.2 Kieskringen

Nederland is onderverdeeld in kieskringen. Het aantal kieskringen verschilt per verkiezingssoort. Zo zijn er bij Tweede Kamerverkiezingen 19 kieskringen, waarvoor geldt dat er in een provincie minimaal één kieskring is. Provincies zoals Groningen, Drenthe en Friesland hebben allemaal één kieskring, maar de provincie Zuid Holland is opgedeeld in 4 kieskringen. De gedachte hierachter is om de spreiding van de regionale kandidaten te bevorderen. [2]

[2] http://nl.wikipedia.org/wiki/Evenredige_vertegenwoordiging

Bij de Europese Parlementsverkiezingen bestaat heel Nederland uit precies één kieskring en bij de Provinciale Statenverkiezing bestaat elke provincie uit precies één of meerdere kieskringen, net zoals bij de Tweede Kamerverkiezingen.
Voor Gemeenteraadsverkiezingen heeft elke gemeente of deelgemeente één kieskring.

Er worden in Nederland ook waterschapsverkiezingen georganiseerd. De waterschapsverkiezingen worden hier buiten beschouwing gelaten om dat de opzet van deze verkiezingen anders georganiseerd is: kiezers krijgen stembiljetten thuis gestuurd en kunnen deze indienen per post of er kan gestemd worden via internet [WTR08].

Gedurende dit onderzoek wordt ingegaan op de volgende onderdelen:

- De gegevensintegriteit van vastgelegde verkiezingsuitslagen
    - Op een proces-verbaal
    - In OSV

1.3 Methode

Voorafgaand aan dit onderzoek is er studie gedaan naar de huidige situatie van het verkiezingsproces. De nadruk is gelegd op het gebruik van processen-verbaal en OSV om verkiezingsuitslagen te vervoeren. Tijdens deze voorstudie is er een inventarisatie opgemaakt van de procedures rond het vastleggen van verkiezingsuitslagen. Naar aanleiding van deze procedures zijn er een aantal hypothesen opgesteld waarin wordt beschreven welke mogelijke zwakke punten invloed kunnen uitoefenen op de integriteit van vastgelegde verkiezingsuitslagen. De hypothesen vormden een grondslag voor een aantal interviews bij het lokale stembureau, het hoofdstembureau en de Kiesraad. Deze interviews hadden tot doel om de gestelde hypothesen te valideren. De gevalideerde hypothesen en de rapportages van de interviews en de praktijkstudie van OSV worden beschreven in hoofdstuk 3: Bevindingen.
Het model zoals beschreven is in hoofdstuk 1.3.3 ‘Werkstroomdiagram’ geeft aan dat er een relatie is tussen de interviews bij het lokale stembureau en de interviews bij het hoofdstembureau. Deze interviews volgen elkaar op om zo de waarnemingen die gedaan zijn bij het lokale stembureau waar nodig te valideren bij het hoofdstembureau. In geval van twijfel over de correctheid van deze validatie kan besloten worden om ook nog contact op te nemen met een ander lokaal stembureau. De waarnemingen die gedaan zijn bij het lokale stembureau en het hoofdstembureau worden tot slot gevalideerd door een interview met de Kiesraad.

1.3.1 Iteratieve methode

Interviews worden na het afnemen hiervan direct vastgelegd in rapportages. Deze rapportage ligt ten grondslag aan de risicoanalyse. Zodra er een mogelijke bedreiging of een risico is gevonden, worden deze vastgelegd volgens een ORM-model (zie hoofdstuk 8.1). Als na aanleiding van een vervolginterview blijkt dat waarnemingen niet overeenkomen doordat ze bijvoorbeeld verkeerd geïnterpreteerd zijn, kunnen gegevens nog gewijzigd worden. Als alle waarnemingen en hypothesen gevalideerd zijn, kunnen de kwetsbaarheden, bedreigingen en risico’s op het gebied van de integriteit van vastgelegde verkiezingsuitslagen formeel vastgelegd worden.

1.3.2 Formele vastlegging

Alle gevonden kwetsbaarheden, bedreigingen en risico’s die invloed kunnen hebben op de integriteit van vastgelegde verkiezingsuitslagen worden op een formele manier vastgelegd zodat daaruit onderlinge relaties van elkaar kunnen worden afgeleid. De structuur van dit model is afgeleid van

'Information security based on ISO 27001/27002'.[3] Deze structuur is ook beschreven in een ORM model zoals te vinden is in hoofdstuk 8.1: ORM model.

1.3.3 Werkstroomdiagram

In dit diagram wordt de aanpak van dit onderzoek weergegeven zoals dit is beschreven in hoofdstuk 1.3: Methode.

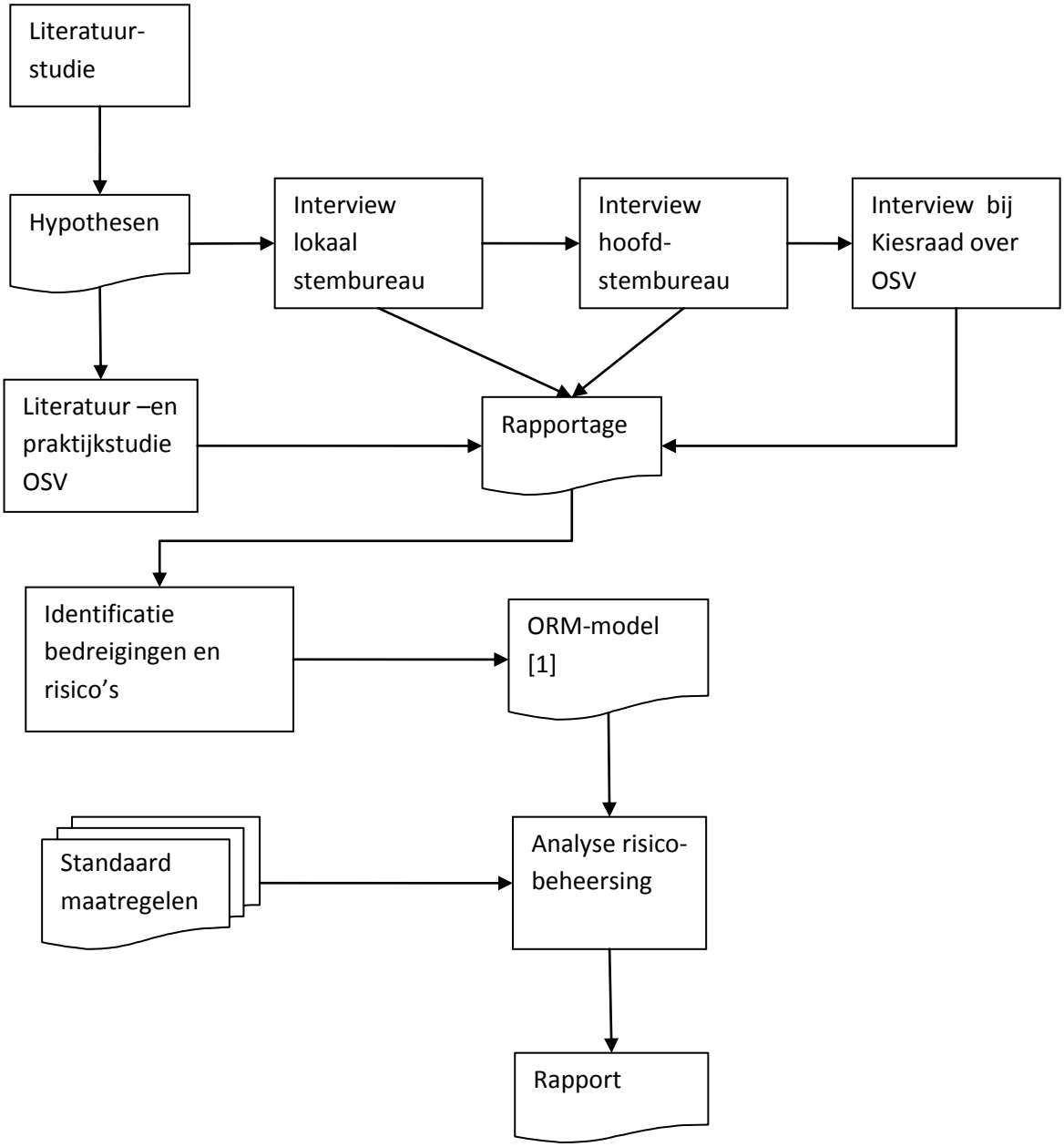


Diagram 1: werkstroom onderzoek

[1] Zie hoofdstuk 8.1: "ORM model" (pagina 69)

[3] http://www.sos.cs.ru.nl/applications/courses/sio2009/

2 Achtergrond

2.1 Tijdslijn

In deze paragraaf is een tijdslijn beschreven van alle gebeurtenissen vanaf het moment dat er problemen geconstateerd werden met het gebruik van de stemcomputer tot en met de Provinciale Statenverkiezingen van 2 maart 2011.

Datum/periode	Gebeurtenis
4 oktober 2006	De actiegroep 'Wij vertrouwen stemcomputers niet' toont aan dat er risico's zijn op het gebied van integriteit en transparantie bij het gebruik van stemcomputers van Nedap en SDU. [4]
30 oktober 2006	De minister van Bestuurlijke vernieuwing en Koninkrijksrelaties schaft het gebruik van de SDU stemcomputer af i.v.m. de compromitterende straling.
22 november 2006	Tweede Kamerverkiezingen. Vastleggen van stemmen met behulp van Nedap stemcomputers en met stembiljetten.
19 december 2006	Instelling commissie 'Commissie Besluitvorming Stemcomputers'
18 januari 2007	Instelling commissie 'Adviescommissie inrichting Verkiezingsproces'
Maart 2007 (na Provinciale Statenverkiezing)	De staatssecretaris van Binnenlandse zaken besluit om het gebruik van alle overgebleven (Nedap) stemcomputers af te schaffen.
7 maart 2007	Provinciale Statenverkiezingen. Vastleggen van stemmen met behulp van Nedap stemcomputers aangevuld met stembiljetten.
27 september 2007	De 'Adviescommissie inrichting Verkiezingsproces' brengt het rapport 'Stemmen met vertrouwen' uit.
1 oktober 2007	De rechter oordeelt in een definitieve uitspraak dat er tijdens de Tweede Kamerverkiezingen van 2006 geen stemcomputers gebruikt hadden mogen worden. [5]
Zomer 2008 Oktober 2008	Openbare aanbestedingsprocedure OSV. De aanbesteding is opgezet door de Kiesraad. Toewijzing ontwikkeling OSV aan IVU Traffic Technologies uit Duitsland
4 juni 2009	Europese Parlementsverkiezingen. Vastleggen stemmen met behulp van

[4] http://wijvertrouwenstemcomputersniet.nl/Televisie

[5] De Kiesraad bevestigde dat het hier ging om een definitieve uitspraak. Hier zou men nu niets meer aan kunnen doen.

	stembiljetten. Vastleggen verkiezingsuitslagen m.b.v. OSV.
3 maart 2010	Gemeenteraadsverkiezingen. Vastleggen stemmen met behulp van stembiljetten. Vastleggen verkiezingsuitslagen m.b.v. OSV.
9 juni 2010	Tweede Kamerverkiezingen. Vastleggen stemmen met behulp van stembiljetten. Vastleggen verkiezingsuitslagen m.b.v. OSV.
24 november 2010	Gemeenteraadsverkiezingen in enkele gemeenten in verband met gemeentelijke herindelingverkiezingen. Vastleggen stemmen met behulp van stembiljetten. Vastleggen verkiezingsuitslagen m.b.v. OSV.
2 maart 2011	Provinciale Statenverkiezingen. Vastleggen stemmen met behulp van stembiljetten. Vastleggen verkiezingsuitslagen m.b.v. OSV.

Tabel 3: tijdslijn

2.2 Eisen aan het verkiezingsproces

Sinds 2007 wordt er tijdens verkiezingen bij lokale stembureaus opnieuw gebruik gemaakt van stembiljetten. Na studie van de Adviescommissie inrichting Verkiezingsproces [BZK07] voldoet deze manier van het registreren van stemmen het meest aan de in de kieswet gestelde eisen. De Adviescommissie inrichting Verkiezingsproces heeft in [BZK07] de volgende eisen gesteld waaraan het verkiezingsproces moet voldoen:

1. **Transparantie**: Het verkiezingsproces moet zo zijn ingericht, dat het helder van structuur en opzet is, zodat in beginsel iedereen inzicht in de structuur ervan kan hebben. Er zijn in het verkiezingsproces geen geheimen. Vragen moeten beantwoord kunnen worden; de antwoorden moeten controleerbaar en verifieerbaar zijn.
2. **Controleerbaarheid**: Het verkiezingsproces moet objectief controleerbaar zijn. De controle-instrumenten kunnen, afhankelijk van de vorm van stemmen waartoe wordt besloten, verschillen.
3. **Integriteit**: Het verkiezingsproces moet correct verlopen en de uitkomst mag niet beïnvloedbaar zijn anders dan door het uitbrengen van rechtmatige stemmen.
4. **Kiesgerechtigdheid**: Alleen kiesgerechtigde personen mogen aan de verkiezing deelnemen.
5. **Stemvrijheid**: Iedere kiesgerechtigde moet bij het uitbrengen van zijn of haar stem zijn of haar keuze in alle vrijheid, vrij van beïnvloeding, kunnen bepalen.
6. **Stemgeheim**: Het moet onmogelijk zijn om een verband te leggen tussen de identiteit van de persoon die de stem uitbrengt en de inhoud van de uitgebrachte stem. Het proces moet zodanig zijn ingericht, dat het onmogelijk is de kiezer te laten aantonen hoe hij of zij gestemd heeft.
7. **Uniciteit**: Iedere kiesgerechtigde mag, gegeven het Nederlandse kiesstelsel, één stem per verkiezing uitbrengen, die bij de stemopneming precies één keer meegeteld mag en moet worden.
8. **Toegankelijkheid**: Kiesgerechtigden moeten zoveel mogelijk in de gelegenheid gesteld worden om direct deel te nemen aan het verkiezingsproces. Indien dat onmogelijk is, moet de mogelijkheid openstaan om indirect – door het verlenen van een volmacht – aan de verkiezing deel te nemen.

2.3 Huidige situatie

Na sluitingstijd van het lokale stembureau worden stembiljetten geteld. Eerst worden de stembiljetten op partijniveau geteld, waarna de uitslag op partijniveau doorgebeld wordt naar het plaatselijke stembureau ter indicatie. Daarna worden alle stembiljetten geteld op kandidaat-niveau. Tenslotte wordt de uitslag genoteerd op een proces-verbaal en het proces-verbaal wordt ondertekend door alle aanwezige leden in het stembureau. Het proces-verbaal wordt gezamenlijk met o.a. de ingevulde stembiljetten naar het plaatselijk stembureau gebracht (zie ook hoofdstuk 3: Bevindingen).
Het plaatselijk stembureau telt de uitslagen van alle ontvangen processen-verbaal bij elkaar op en de resultaten worden ingevoerd in OSV. Het programma OSV maakt een XML-bestand aan met daarin de verkiezingsuitslagen op plaatselijk stembureauniveau. Daarnaast maakt OSV ook een afdrukbaar proces-verbaal aan. Het proces-verbaal met daarop de uitslagen bevat tevens de hashcode van het XML-bestand. Het proces-verbaal wordt afgedrukt en ondertekend door de aanwezige leden. Het XML-bestand wordt per USB-stick gezamenlijk met het afgedrukte proces-verbaal naar het hoofdstembureau gebracht. Daar wordt het XML-bestand in OSV ingelezen.
Het hoofdstembureau telt alle uitslagen van de plaatselijke stembureaus bij elkaar op. OSV maakt ook nu weer een XML-bestand en een proces-verbaal aan dat naar het centrale stembureau gestuurd kan worden.

2.4 Ondersteunende Software Verkiezingen

De Kiesraad heeft de regie gehad tijdens het ontwikkelen van het programma OSV. Het programma OSV is ontwikkeld als administratieve ondersteuning voor de kandidaatstelling, het vaststellen van de uitslag van de verkiezingen en de zetelberekening die volgt op de verkiezingsuitslag. Na een openbare Europese aanbestedingsprocedure in de zomer van 2008 werd in oktober 2008 door de Kiesraad de ontwikkeling van OSV toegewezen aan IVU Traffic Technologies uit Duitsland. Voor een goed verloop van deze aanbesteding werd er een Beschrijvend Document opgesteld met daarin 100 voorwaarden waar het programma OSV aan moet voldoen [KSR10b]. Dit document is gebaseerd op een aantal eisen die de Staatssecretaris van Binnenlandse zaken en Koninkrijksrelaties heeft opgesteld (zie hoofdstuk 3.4.2.1: De eisen van de Staatssecretaris aan OSV). Het programma is open source en maakt gebruik van open standaarden, waardoor vastgelegde uitslagen en berekeningen voor de zetelverdeling te verifiëren zijn. Het programma OSV wordt gebruikt door de Kiesraad om de verkiezingsdefinitie naar politieke partijen op te sturen. Politieke partijen gebruiken OSV om kandidaat-lijsten op te sturen naar de hoofdstembureaus. Ook gebruikt de Kiesraad OSV om de geldigheid van de door politieke partijen aangeleverde kandidaat-lijsten te beoordelen op geldigheid. Deze kandidaat-lijsten ontvangt de Kiesraad van de hoofdstembureaus. De Kiesraad gebruikt OSV ook om goedgekeurde kandidaat-lijsten op te sturen naar hoofdstembureaus en naar drukkerijen voor het afdrukken van stembiljetten. Tot slot gebruiken de hoofdstembureaus en het centraal stembureau OSV om verkiezingsuitslagen uit te wisselen en om processen-verbaal aan te maken die nodig zijn om de uitslag van verkiezingen op stembureauniveau vast te stellen. De redenen volgens Kiesraad in [KSR10b] om het programma OSV voor verkiezingen te gebruiken zijn:

- De grote hoeveelheid te verwerken informatie;
- De vereiste betrouwbaarheid;
- De termijn van enkele dagen waarbinnen de verkiezingen definitief moet zijn vastgesteld.

Het programma OSV bestaat volgens [KSR10] uit meerdere onderdelen:

- Programma 0: Aanmaken verkiezingsdefinitie
- Programma 1: Aanmaken kandidatenlijsten
- Programma 2: Onderzoek kandidatenlijsten

- Programma 3: Vaststellen kandidatenlijsten
- Programma 4: Invoeren en samenvoegen stemtotalen
- Programma 5: Zetelverdeling en vaststelling uitslag

2.4.1 OSV en het gebruik van een stemcomputer

Het gebruik van OSV als ondersteunend middel rond de verkiezingen roept vragen op. Binnen OSV worden verkiezingsuitslagen digitaal vastgelegd in het elektronische geheugen van de computer. Het digitaal opslaan van verkiezingsuitslagen gebeurde ook bij de oude stemcomputers van de fabrikant Nedap en van de uitgever SDU. Als een kiezer op een stemcomputer een stem invoerde, werd deze stem weggeschreven in het geheugen van de stemcomputer. De vastgelegde stemmen in het geheugen van de stemcomputer konden na sluiting van het stembureau snel geteld worden. De stemcomputers van beide fabrikanten zijn afgeschaft. De firmware van de stemcomputer van Nedap was door Nedap zelf ontwikkeld en de broncode was geheim. De stemcomputer van uitgever SDU was een gewone pc waarop via een aanraakscherm stemmen weggeschreven konden worden. Het was voor kiezers, stembureauleden en andere waarnemers niet te controleren of de firmware die werd gebruikt in de stemcomputers authentiek was [OSC07]. De actiegroep 'Wij vertrouwen stemcomputers niet' toonde aan dat de firmware op de chip van de Nedap-stemcomputer te manipuleren was, door de chips met de firmware van Nedap te verwisselen voor chips waar heel andere firmware op stond. De actiegroep kreeg het op deze manier voor elkaar om, in plaats van stemmen te tellen, een schaakspelletje te installeren op de stemcomputer van Nedap.[6] En als men een schaakspel kan installeren, kan men ook software ontwikkelen om stemmen op een frauduleuze manier weg te schrijven [STN06]. De stemcomputer van de uitgever SDU was afgeschaft vanwege problemen met tempest straling: ingevoerde stemmen waren met speciale apparatuur op enkele tientallen meters afstand van de stemcomputer nog uit te lezen, waardoor er niet voldaan is aan de voorwaarde 'stemgeheim' [OSC07].
In het programma OSV worden verkiezingsuitslagen dia via processen-verbaal van lokale stembureaus afkomstig zijn door het plaatselijk stembureau digitaal vastgelegd in het geheugen van een centrale computer. Deze in OSV vastgelegde verkiezingsuitslagen worden door de centrale stembureau gebruikt voor het vaststellen van de definitieve uitslag van de verkiezingen en voor de zetelberekening. Kan de integriteit van deze digitaal vastgelegde verkiezingsuitslagen in OSV wel gegarandeerd worden? Vastgelegde verkiezingsuitslagen in OSV worden voorzien van een hashcode om eventuele tussentijdse wijzigingen in de verkiezingsuitslagen op te merken. Een hashcode is, mits deze op een correcte wijze wordt toegepast, een middel om de authenticiteit van gegevens te waarborgen.

[6] http://wijvertrouwenstemcomputersniet.nl/other/es3b-en.pdf

2.4.2 Integriteit vastgelegde verkiezingsuitslagen binnen OSV

Na afloop van het tellen van stemmen brengt een medewerker of de voorzitter van het lokale stembureau het proces-verbaal naar het plaatselijk stembureau (of naar het hoofdstembureau). Medewerkers van het plaatselijk stembureau zorgen ervoor dat de gegevens van verkiezingsuitslagen op gemeenteniveau worden ingevoerd in OSV. Vastgelegde verkiezingsuitslagen in OSV worden volgens de standaard EML opgeslagen. EML staat voor Election Markup Language. De Kiesraad in [KSR08] beschrijft dit proces als volgt:

> *"Gemeenten, hoofdstembureaus en centrale stembureaus zijn de belangrijkste gebruikers van de software ter ondersteuning van de berekening en vaststelling van de verkiezingsuitslag. De resultaten van de verkiezingen op stembureauniveau worden bij de gemeenten na afloop van de verkiezingen in de software ingevoerd. Vervolgens kunnen alle processen-verbaal worden aangemaakt die bij gemeente, hoofdstembureau en centraal stembureau nodig zijn voor de vaststelling van de uitslag (modellen I 1, I 4, I 9, I 10, I 12-1, I 12-2, N 11, O 3, P 22-1 en P 22-Aan het eind van het proces kunnen de benoemingsbrieven worden uitgedraaid.*
> *De gegevens die worden uitgewisseld tussen de verschillende gebruikers zijn gestructureerd volgens een internationale standaard, genaamd EML (Election Markup Language; EML is een vorm van XML specifiek voor verkiezingen) versie 5.0. De bestanden zijn niet versleuteld en dus leesbaar voor iedereen die ze ontvangt. Nadat het proces-verbaal is vastgesteld, kunnen bestanden niet meer worden gewijzigd. Dit kan worden gecontroleerd met behulp van een zogenaamde hashcode. De software kan worden gebruikt op gangbare versies van Windows, Linux en Mac OS/X."*

De Kiesraad claimt hier dat verkiezingsuitslagen niet meer gewijzigd kunnen worden omdat dit gecontroleerd kan worden door middel van een hashcode. Het is in het bovenstaande citaat niet beschreven waar deze hashcode wordt opgeslagen. Iedereen kan een hashcode van een bepaald document berekenen, omdat het benodigde hash-algoritme openbaar is.

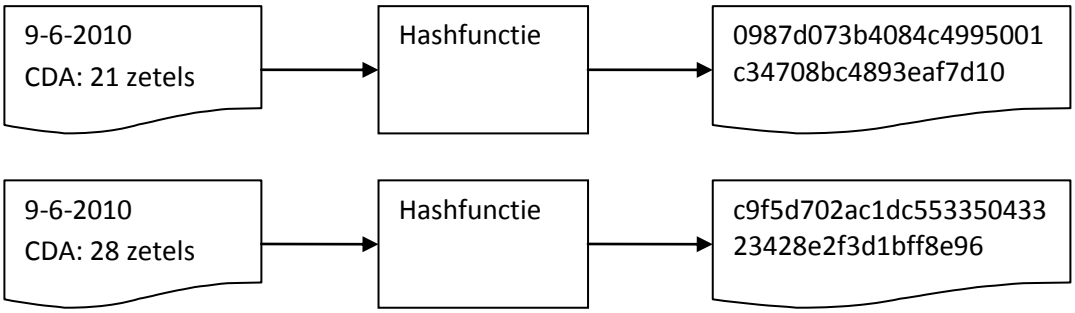


Diagram 2: de mogelijkheid van hashcodes

Een hashfunctie maakt van een tekst van een willekeurige lengte een code met een 160 bits (sha-1) vaste lengte.[7] Als in de bron één of meerdere karakters worden vervangen, verandert de hele hashcode, zie diagram 2. Bij het gebruik van de hashfunctie gelden er een aantal regels:

- Het is praktisch onmogelijk om een berekende hashcode weer om te zetten naar de brontekst (one-wayness);
- Het is praktisch onmogelijk om van de hashcode van document 1 een ander document (document 2) te vinden waarvan de hashcode van document 2 gelijk is aan de hashcode van document 1 (collision resistance).

[7] http://en.wikipedia.org/wiki/Sha-1

Een hashcode kan een middel zijn om te controleren of de inhoud van een document authentiek is. De authenticiteit van een document kan worden gecontroleerd door een zelf berekende hashcode van het ontvangen document te vergelijken met de van tevoren (door de auteur van het document) vastgelegde hashcode van het document. Als de beide hashcodes overeenkomen, mag men ervan uitgaan dat de inhoud van het document authentiek is.

De vragen rond het gebruik van hashcodes spelen hoofdzakelijk bij het OSV-onderdeel P4, waarbij verkiezingsuitslagen worden ingevoerd in OSV. In deze onderdelen van OSV worden uitslagen van verkiezingen zelf vastgelegd, waarbij een hashcode berekend moet worden. Bij de programma-onderdelen P1, P2 en P3 worden hashcodes door de Kiesraad zelf berekend. De Kiesraad publiceert deze hashcode op de website van de Kiesraad. Als een stembureau of een politieke partij een cd-rom van de Kiesraad met daarop verkiezingsbestanden of het programma OSV ontvangt, is het de bedoeling dat de ontvanger van de cd-rom eerst de authenticiteit van de cd-rom vaststelt. De ontvanger berekent een hashcode van de inhoud van de cd-rom en vergelijkt deze berekende hashcode met de hashcode die op de site van de Kiesraad staat. Komen deze beide hashcodes overeen, dan kan men ervan uitgaan dat de inhoud van de cd-rom legitiem is. Bestanden in de programma-onderdelen P1, P2 en P3 worden op lokale werkstations gegenereerd. Op datzelfde moment worden ook de hashcodes vastgelegd en gepubliceerd. Een bestand met verkiezingsdefinities die bestemd voor politieke partijen, zijn voor alle politieke partijen hetzelfde. Verkiezingsuitslagen die in de programma's P4 en P5 worden vastgelegd verschillen per stembureau. Deze gegevens kunnen dus niet van te voren gevalideerd worden. Een bijkomend feit is dat de verkiezingsuitslagen binnen OSV P4 opgeslagen worden op een centrale server. Dit is niet het geval bij de programma-onderdelen P1, P2 en P3. Een overzicht van de onderdelen van OSV en het bijbehorende focusgebied van het verkiezingsproces staat in hoofdstuk 1.2: 'Scope: na sluiting van het stembureau'.

2.4.2.1 De beveiliging van hashcodes binnen OSV

Het genoemde citaat in hoofdstuk 2.4.2: 'Integriteit vastgelegde verkiezingsuitslagen binnen OSV' wekt misschien verwarring op. De claim dat bestanden niet meer gewijzigd kunnen worden doordat dit te zien zou zijn aan de hashcode, lijkt onwaarschijnlijk. Als een kwaadwillende een document onderschept en dat document wil aanpassen, moeten er twee zaken aangepast worden: het betreffende document zelf en de bijbehorende hashcode. Het is voor een buitenstaander niet moeilijk om een hashcode van een document te berekenen, aangezien het hash-algoritme openbaar is. Als een kwaadwillende de verkiezingsuitslag wil aanpassen, hoeft hij alleen een hashcode te berekenen van het document dat hij zelf veranderd heeft. De (valse) verkiezingsuitslag met de bijbehorende hashcode kan vervolgens worden doorgestuurd of deze valse verkiezingsuitslag kan teruggezet worden op de originele locatie nadat de echte verkiezingsuitslagen gewist zijn. De ontvanger zal controleren of de hashcode correspondeert met de inhoud van de vastgelegde verkiezingsuitslag. De inhoud van het bericht zal door de ontvanger als valide beschouwd worden, omdat iedereen bij een verkiezingsuitslag een hashcode kan genereren.
Gegevens zoals verkiezingsuitslagen die binnen OSV uitgewisseld worden, hoeven vanwege het open en transparante karakter van de verkiezingen niet geheim te zijn. Wel moet gegarandeerd worden dat de gegevens authentiek zijn. Het meesturen van een hashcode kan hierbij helpen, maar met de bovenstaande claim dat bestanden met daarin de verkiezingsuitslagen door middel van de hashcode niet veranderd kunnen worden schiet tekort, zeker als in de beschrijving van OSV [KSR08] het volgende staat:

"De bestanden zijn niet versleuteld en dus leesbaar voor iedereen die het ontvangt."

Om integriteit te garanderen, is het noodzakelijk dat de meegestuurde hashcode ondertekend wordt. Een alternatief is dat de hashcode van de verkiezingsuitslagen op een beveiligde locatie wordt opgeslagen. Het opslaan van een hashcode op een andere locatie kan problemen opleveren op het gebied van transparantie: de gegevens van verkiezingsuitslagen moeten openbaar zijn. Een kwaadwillende (man-in-the-middle) kan wel een hash berekenen van een bestand met daarin vastgelegde verkiezingsuitslagen, maar het is niet mogelijk om een ondertekend document te maken, aangezien er dan een (geheime) sleutel nodig is. De verzender van het document ondertekent het document met zijn eigen geheime sleutel. De ontvanger kan het document valideren met behulp van de openbare sleutel van de afzender. [8]

2.4.2.1.1 Praktijksituatie

Hieronder staat schematisch de communicatie beschreven die plaats vindt als er een bestand met verkiezingsuitslagen wordt gestuurd door Alice (medewerkster hoofdstembureau) naar Bob (medewerker centraal stembureau). In het protocol hieronder probeert de kwaadwillende Trudy gegevens te manipuleren. De inhoud van dit protocol is gebaseerd op hoofdstuk 2.4.2.1: De beveiliging van hashcodes binnen OSV.

Regelnr	Verzender	Bericht	Ontvanger
1	Alice	• 9-6-2010 D66 24 zetels • SHA-1(9-6-2010 D66 24 stemmen)	Trudy
2	Trudy	• 9-6-2010 D66 38 zetels • SHA-1(9-6-2010 D66 38 stemmen)	Bob

Protocol 1: Trudy onderschept en manipuleert een bericht dat door Alice is verstuurd naar Bob

In het bovenstaande protocol probeert Alice een document met daarin de verkiezingsuitslag van de partij D66 te versturen naar Bob. Ze verstuurt het document gezamenlijk met de niet-ondertekende hashcode van het document. Trudy is een kwaadwillend persoon die de uitslagen wil manipuleren en onderschept het document dat door Alice is verstuurd voordat het aankomt bij Bob (zie regel 1). Trudy verandert de inhoud door D66 een paar extra stemmen te geven en ze berekent een nieuwe hashcode naar aanleiding van de gemanipuleerde inhoud en stuurt het document en de nieuwe hashcode door naar Bob (zie regel 2). Bob zal bij ontvangst controleren of de hashcode overeen correspondeert met de inhoud van het document.
De opzet van Trudy zal slagen, aangezien Bob niet over middelen beschikt om na te gaan of de hashcode gemanipuleerd is.

[8] http://en.wikipedia.org/wiki/Asymmetric_key_algorithm

3 Bevindingen bij stembureaus en OSV

In dit hoofdstuk worden alle gebeurtenissen en elementen beschreven die gedurende dit onderzoek waargenomen zijn. De informatie die relevant was voor dit onderzoek is verkregen door middel van literatuurstudie, interviews en bevindingen in de praktijk.

3.1 Bevindingen bij het lokale stembureau

Op 24 november 2010 waren er in een aantal gemeenten in Nederland gemeentelijke herindelingverkiezingen. Deze verkiezingen boden voor dit onderzoek een gelegenheid om lokale waarnemingen te verrichten om na te gaan hoe verkiezingsuitslagen werden vastgelegd op processen-verbaal. Op deze dag is in Maarssen een bezoek gebracht aan een lokaal stembureau. Hier is gesproken met een aantal leden en de voorzitter van dit lokale stembureau. Voorafgaand aan dit bezoek is er een telefonische afspraak gemaakt. Tijdens dit telefoongesprek is ook verzocht of er waarnemingen verricht konden worden op het hoofdstembureau in Maarssen om na te gaan hoe verkiezingsuitslagen vastgelegd worden in het programma OSV. Dit verzoek werd geweigerd omdat het vastleggen van verkiezingsuitslagen 'een secuur proces was waar veel aandacht voor nodig was. Daarom mag hierbij geen publiek aanwezig zijn.' Deze weigering is opmerkelijk: het hele verkiezingsproces moet volgens de Adviescommissie inrichting Verkiezingsproces [BZK07] 'objectief controleerbaar' zijn. Bij het lokale stembureau zijn de volgende gebeurtenissen waargenomen:

- Na sluiting stembureau: de gevulde stembus wordt geopend. Alle ingevulde stembiljetten worden gesorteerd per partij. Per partij worden alle stemmen opgeteld en deze stemmen worden telefonisch doorgegeven aan het plaatselijke stembureau ter indicatie.
- Vervolgens worden de stemmen op kandidaat-niveau geteld. Per partij wordt vervolgens per kandidaat geturfd hoeveel stemmen er zijn. Een voorbeeld van een document waarop dit wordt bijgehouden:

Lijst 1: CDA

Naam kandidaat	**Aantal in cijfers**	**5**	**10**	**15**
Maxime Verhagen	14	~~////~~	~~////~~	////
Joop Atsma	9	~~////~~	////	
Hans Hillen	7	~~////~~	//	
…				
…				
Totaal	75			

In deze lijst staat een voorbeeldpopulatie. In werkelijkheid staan hier namen van lokale kandidaten.

- Vervolgens wordt er op een pagina verslag opgemaakt van alle ingediende bezwaren, ongeldige stemkaarten en ongeldige stembiljetten.
- Daarna wordt er op een pagina de uitslag per partijniveau vermeld:

Uitslagen gemeenteraadsverkiezingen <naam stembureau, districtnummer>

CDA	122
PVDA	155
VVD	98
….	
…	
Totaal uitgebrachte geldige stemmen:	815
Blanco stemmen	5
Ongeldig	2
Totaal aantal stemmen	822

Tabel 4: een voorbeeld van proces-verbaal

3.1.1 Opmaak en vervoer proces-verbaal

Alle relevante gegevens omtrent de uitslag worden genoteerd op een proces-verbaal. Het proces-verbaal bestaat uit meerdere pagina's. Deze pagina's worden los in een tas per auto door één persoon vervoerd naar het hoofdstembureau.

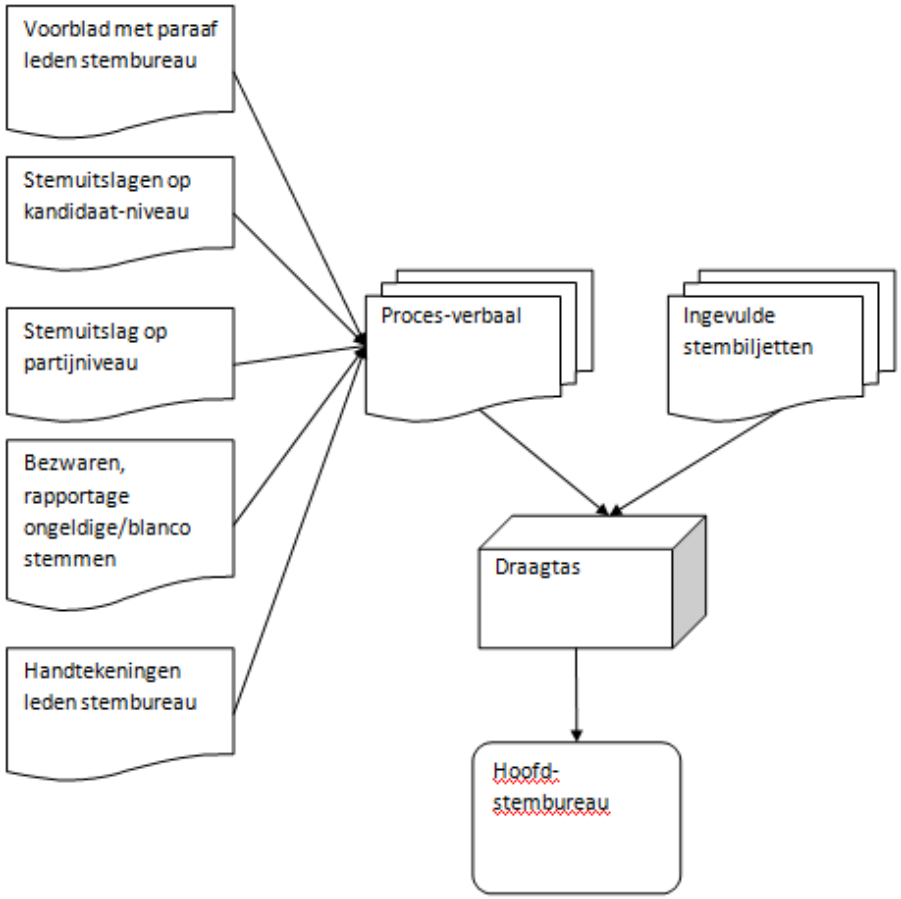


Diagram 3: samenstelling en transport proces-verbaal

- Alle aanwezige leden zetten hun handtekening op het laatste blad.
- Alle documenten samen vormen het proces-verbaal.
- Deze documenten worden niet aan elkaar gehecht.
- Het proces-verbaal is een sjabloon afgedrukt op A4 papier dat behalve de handtekeningen geen echtheidskenmerken bevat.
- Het proces-verbaal wordt gezamenlijk met alle ingevulde stembiljetten in een tas gedaan en door één persoon (per auto) naar het plaatselijke stembureau of het hoofdstembureau gebracht.

3.2 Bevindingen bij het hoofdstembureau

Op 5 januari 2011 is er opnieuw telefonisch contact geweest met het hoofdstembureau in Maarssen. Hierbij zijn een aantal aanvullende vragen gesteld naar aanleiding van de waarnemingen op het stembureau van 24 november 2010 in Maarssen. Uit dit gesprek is het volgende gebleken:

1. Een proces-verbaal dat is verzonden door een lokaal stembureau heeft geen echtheidskenmerken, behalve de handtekeningen die op de laatste pagina van het proces-verbaal staan.
2. Het is bijna niet op te merken als processen-verbaal tijdens transport vervalst worden. Er wordt vanuit gegaan dat deze documenten integer worden behandeld door de persoon die het proces-verbaal vervoert. Het hoofdstembureau gaat ervan uit dat de integriteit van het proces-verbaal tijdens het transport gewaarborgd is.

3.2.1 Processen-verbaal en de kieswet

De kieswet geeft terzake geen details over de invulling van de integriteit van het proces-verbaal tijdens het transport. De Kieswet[9] geeft in Afdeling 2, hoofdstuk O, artikel O3 en O4 de volgende details over (het transporteren van) het proces-verbaal:

- Artikel O 3:
  - Nadat alle werkzaamheden zijn beëindigd, wordt daarvan onmiddellijk proces-verbaal opgemaakt. Alle ingebrachte bezwaren worden in het proces-verbaal vermeld.
  - Het proces-verbaal wordt door alle aanwezige leden van het hoofdstembureau getekend.
  - Bij ministeriële regeling wordt voor het proces-verbaal een model vastgesteld.
  - Indien het de verkiezing betreft van de gemeenteraad of van provinciale staten van een provincie die één kieskring vormt, maakt het proces-verbaal deel uit van het proces-verbaal, bedoeld in artikel P 22.
- Artikel O4:
  - Tenzij het de verkiezing betreft van de gemeenteraad of van provinciale staten van een provincie die één kieskring vormt, doet de voorzitter terstond een afschrift van het proces-verbaal, bedoeld in artikel O 3, naar het centraal stembureau overbrengen en doet hij tegelijkertijd het proces-verbaal ter secretarie van de gemeente waar het hoofdstembureau is gevestigd, voor een ieder ter inzage leggen. De terinzagelegging wordt beëindigd, zodra over de toelating van de benoemden is beslist.
  - De voorzitter doet de processen-verbaal van de stembureaus, de opgave, bedoeld in artikel N 12, eerste lid, en, tenzij het de verkiezing betreft van de gemeenteraad of van provinciale staten van een provincie die één kieskring vormt, een afschrift van het proces-verbaal van de zitting van het hoofdstembureau terstond overbrengen aan het orgaan waarvoor de verkiezing plaats heeft.

[9] http://wetten.overheid.nl/BWBR0004627/AfdelingII/HoofdstukO/ArtikelO3/geldigheidsdatum_18-05-2011

Uit de Kieswet en uit de bevindingen bij het hoofdstembureau kan geconcludeerd worden dat er geen concrete maatregelen getroffen zijn om de integriteit van gegevens op het proces-verbaal te bewaken.

3.2.2 Protocol

Het onderstaande protocol beschrijft een situatie die op kan treden als een ondertekend proces-verbaal met daarop verkiezingsuitslagen van het lokale stembureau naar het hoofdstembureau wordt vervoerd. Trudy is een kwaadwillend persoon en tevens medewerkster van het lokale stembureau. Trudy moet het proces-verbaal naar het hoofdstembureau brengen.

Regelnr	Verzender	Bericht (proces-verbaal)	Ontvanger
1	Trudy	• Voorblad proces-verbaal stembureau nr. 20 te Arnhem 9-6-2010 • VVD: 28 zetels • PVDA: 29 zetels • CDA: 22 zetels • ….. • Pagina met handtekeningen medewerkers lokaal stembureau	Hoofdstembureau
2	Trudy	• Voorblad proces-verbaal stembureau nr. 20 te Arnhem 9-6-2010 • VVD: 32 zetels • PVDA: 15 zetels • CDA: 14 zetels • ….. • Pagina met handtekeningen medewerkers lokaal stembureau	Bob

Diagram 4: Trudy manipuleert een proces-verbaal

In het bovenstaande protocol (diagram 4) brengt Trudy het proces-verbaal met daarin de verkiezingsuitslagen naar het hoofdstembureau. Onderweg manipuleert ze de verkiezingsuitslagen en Bob, die medewerker is van het hoofdstembureau, ontvangt gemanipuleerde uitslagen zonder er iets van te merken: de handtekeningen op de laatste pagina zijn origineel. Doordat er alleen handtekeningen op de laatste pagina staan, is het voor Trudy eenvoudig om tussenliggende pagina's te manipuleren.

3.3 Bevindingen bij het centraal stembureau

Op 24 maart 2011 is er een bezoek gebracht aan de Kiesraad. Tijdens een gesprek met een medewerker van de Kiesraad zijn er een aantal vragen beantwoord over het gebruik van processen-verbaal en digitale bestanden van OSV. De vragen die gesteld zijn waren gericht omtrent het gebruik van processen-verbaal en XML-bestanden die binnen OSV-systemen verstuurd worden.

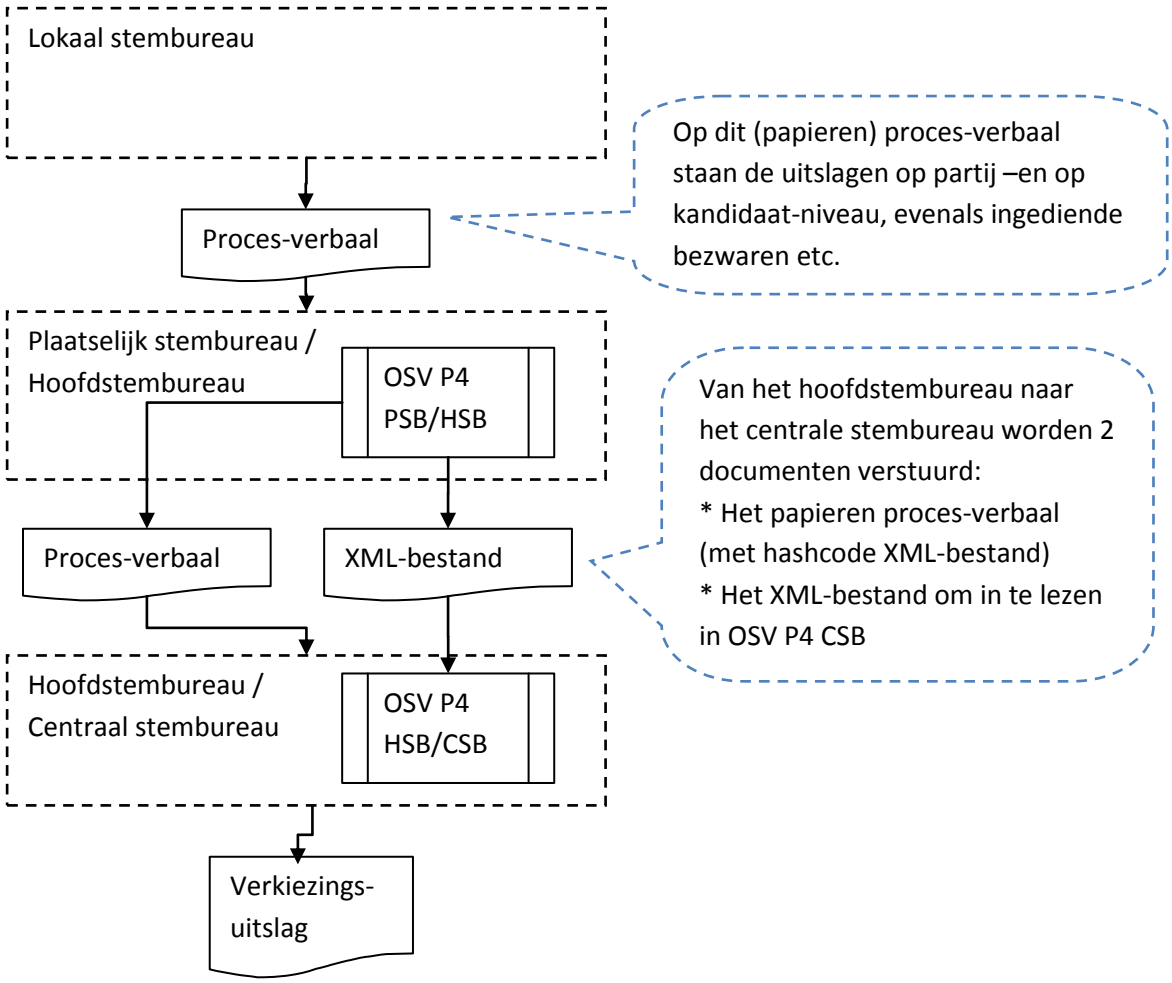


Diagram 5: een globaal overzicht van de bestanden die tussen OSV-systemen en organiserende organen verstuurd worden.

De onderstaande bevindingen hebben betrekking op diagram 5. De Kiesraad beweert omtrent het gebruik van processen-verbaal en XML-bestanden het volgende:

1. Binnen OSV worden, als de verkiezingsuitslagen vastgelegd zijn, 2 bestanden aangemaakt met daarin verkiezingsuitslagen: het proces-verbaal (PDF-bestand) en het XML-bestand. De gegevens op het proces-verbaal zijn leidend. Dat wil zeggen dat het XML-bestand alleen dient om verkiezingsuitslagen in te voeren in OSV. Het proces-verbaal wordt gebruikt om alle verkiezingsuitslagen van op centaal stembureauniveau bij elkaar op te tellen. OSV staat namelijk voor 'Ondersteunende' Software Verkiezingen.
2. De hashcode zorgt ervoor dat de gegevens in het XML-bestand overeenkomen met wat er op papier (het afgedrukte PDF-bestand) staat.
3. Het XML-bestand en het proces-verbaal met daarin de verkiezingsuitslagen worden door een door de burgemeester aangewezen medewerker van het hoofdstembureau doorgestuurd naar het centrale stembureau.
4. Alle gebruikersacties binnen OSV worden vastgelegd in logbestanden. Eventuele manipulaties van XML-bestanden buiten OSV worden niet gelogd. Momenteel is de hashcode (met behulp de hashfunctie sha-1) de enige methode om de authenticiteit van XML-bestanden vast te leggen. Het versturen van het XML-bestand naar het centrale stembureau wordt in de meeste gevallen

door een medewerker van een hoofdstembureau uitgevoerd. Het vervoeren van het XML-bestand gebeurt in een uitzonderlijk geval door een andere organisatie. Doordat het XML-bestand in de meeste gevallen door een eigen medewerker vervoerd wordt, is volgens het centrale stembureau het risico op gegevensmanipulatie beperkt. Het bestand wordt direct naar het centrale stembureau gebracht, waardoor er weinig tijd is voor eventuele manipulatie.

5. De gegevensdrager waarop het XML-bestand staat, is niet beveiligd.
6. Er zijn eisen gesteld aan de omgeving waar OSV draait: deze computers mogen enkel voorzien zijn van software die nodig is om OSV te laten functioneren.
7. Als er een nieuwe hashcode berekend wordt nadat de verkiezingsuitslagen binnen OSV vastgesteld zijn, komt dit niet op het papieren proces-verbaal te staan.

3.4 Bevindingen binnen OSV

In dit hoofdstuk worden de bevindingen die opgedaan zijn tijdens literatuurstudie en de praktijkstudie van OSV beschreven. Vooraf aan de praktijkstudie is er een literatuurstudie gedaan naar aanleiding van verschillende rapporten die de eigenschappen en specificaties van OSV beschreven.

Voorafgaand aan de praktijkstudie is een kopie van OSV gebruikt die op een thuis-pc is geïnstalleerd. Bij het testen van de software hebben de fictieve personen Alice, Trudy en Bob en rol toegewezen gekregen. Alice verstuurt het XML-bestand en het proces-verbaal met daarin de verkiezingsuitslagen naar Bob. Trudy zal proberen om de inhoud van het XML-bestand en het proces-verbaal te manipuleren zonder dat Bob dit zal opmerken.

Er is bewust gekozen om deze scenario's in een thuissituatie te simuleren waarbij tevens fictieve verkiezingsuitslagen gebruikt zijn. Het is onwenselijk om met echte verkiezingsuitslagen te gaan experimenteren om na te gaan of gegevens gemanipuleerd konden worden. Gedurende dit onderzoek is alle informatie die relevant is voor dit onderzoek op een rechtmatige manier verkregen.

3.4.1 Hiërarchische structuur OSV

Het programma-onderdeel P4 van OSV is opgebouwd uit meerdere modules. Hierdoor kan OSV voor alle soorten verkiezingen worden gebruikt. Bij sommige soorten verkiezingen worden meerdere onderdelen van OSV P4 door dezelfde personen gebruikt en vind er geen 'extern' transport plaats van XML-bestanden en processen-verbaal. Dit heeft te maken met de wijze waarop verschillende onderdelen van de verkiezingen georganiseerd zijn. Bij gemeenteraadsverkiezingen worden de definitieve uitslagen op gemeentelijk niveau vastgelegd en bij Tweede Kamerverkiezingen worden de definitieve uitslagen op landelijk niveau vastgelegd. Het onderdeel P4 van OSV is als volgt ingedeeld:

1. OSV P4 PSB: Plaatselijk StemBureau. Nadat alle lokale stembureaus de stemmen geteld hebben en zodra de getelde stemmen vastgelegd zijn op een proces-verbaal, wordt het proces-verbaal van het lokale stembureau naar het plaatselijk stembureau binnen de gemeente gebracht. Er is precies één plaatselijk stembureau per gemeente. Bij het plaatselijk stembureau worden alle verkiezingsuitslagen die op de processen-verbaal staan ingevoerd in het programma OSV P4 PSB. Het programma P4 PSB genereert na het vaststellen van de uitslag een XML-bestand en een PDF-bestand. Het PDF-bestand wordt afgedrukt en vormt het proces-verbaal wat ondertekend wordt. Beide documenten (het XML-bestand op een USB stick en het (afgedrukte) papieren proces-verbaal) worden naar het hoofdstembureau gebracht.

2. OSV P4 HSB: HoofdStemBureau. Met het programma P4 HSB worden alle verkiezingsuitslagen op kieskringniveau worden ingevoerd. De gegevens worden aangeleverd door middel van het XML-bestand, dat afkomstig is van het plaatselijk stembureau.
3. OSV P4 CSB: Centraal StemBureau. Het programma P4 CSB wordt gebruikt om alle gegevens van alle hoofdstembureaus in te lezen en samen te voegen.

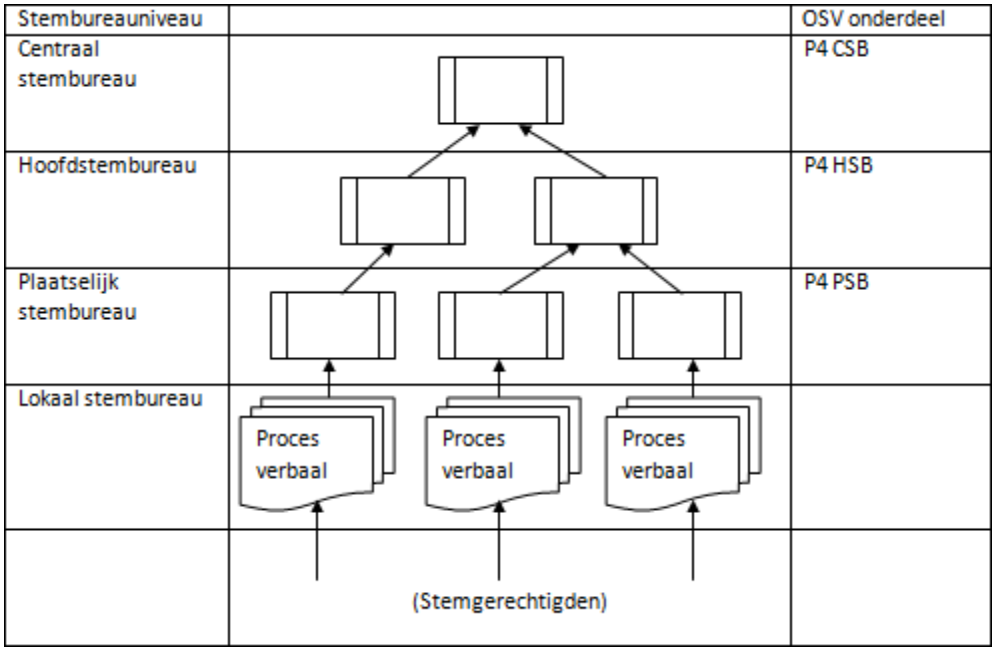


Diagram 6: de hiërarchie van de onderdelen van OSV P4

Het bovenstaande diagram geeft aan dat alle gegevens die aangeleverd zijn via P4 HSB worden samengevoegd in P4 CSB.

In 'Diagram 7: de hiërarchie van OSV' staat beschreven op welke wijze de informatiestroom binnen OSV geordend is tussen de stembureaus. De wijze waarop communicatie tussen OSV-systemen plaatsvindt verschilt per soort verkiezing; zo worden bij gemeenteraadsverkiezingen de uitslagen per gemeente gepubliceerd en uitslagen voor de Tweede Kamer worden op landelijk niveau gepubliceerd. Bij gemeenteraadsverkiezingen worden gegevens tussen P4 PSB, P4 HSB en P4 CSB uitgewisseld binnen hetzelfde (fysieke) gebouw, bijvoorbeeld het gemeentehuis. Vastgelegde verkiezingsuitslagen (in het XML-bestand en op het papieren proces-verbaal) hoeven in dat geval niet buiten het gemeentehuis om vervoerd worden. De gekleurde balk tussen het plaatselijke stembureau en het centrale stembureau is in diagram 4 niet onderbroken. Bij elke verkiezingssoort wordt er een apart proces-verbaal verstuurd van het lokale stembureau naar het plaatselijk stembureau.
Voor de Provinciale Statenverkiezingen en de Tweede Kamerverkiezingen zijn er in diagram 4 op een paar plekken dubbele balken te zien. Deze dubbele balken zijn van toepassing als er één of meerdere provincies onderverdeeld zijn in meerdere kieskringen.

Hieronder staat een tabel met de indeling van centrale stembureaus en hoofdstembureaus die van toepassing zijn op de Provinciale Statenverkiezingen van 2 maart 2011.[10]

Provincie	Gemeente met centraal stembureau	Gemeente met hoofdstembureau
Groningen	Groningen	Groningen
Friesland	Leeuwarden	Leeuwarden
Drenthe	Assen	Assen
Overijssel	Zwolle	Zwolle
Flevoland	Lelystad	Lelystad
Gelderland		Nijmegen Arnhem
Utrecht	Utrecht	Utrecht
Noord Holland	Haarlem	Amsterdam Haarlem Den Helder
Zuid Holland	Den Haag	Den Haag Rotterdam Dordrecht Leiden
Zeeland	Middelburg	Middelburg
Noord Brabant	Den Bosch	Tilburg Den Bosch
Limburg	Maastricht	Maastricht

Tabel 5: centrale stembureaus en hoofdstembureaus tijdens de provinciale statenverkiezingen van 2 maart 2011.

In provincies als Groningen en Overijssel vindt het verzenden van verkiezingsuitslagen plaats binnen dezelfde gemeente. Dit geldt niet voor provincies als Gelderland en Zuid Holland: bestanden en documenten met verkiezingsuitslagen moeten bijvoorbeeld van Dordrecht naar Den Haag verstuurd worden.

10

http://www.kiesraad.nl/nl/Overige_Content/Bestanden/pdf_thema/Provinciale_statenverkiezingen_2011/Kieskringen_verkiezingen_provinciale_staten.pdf

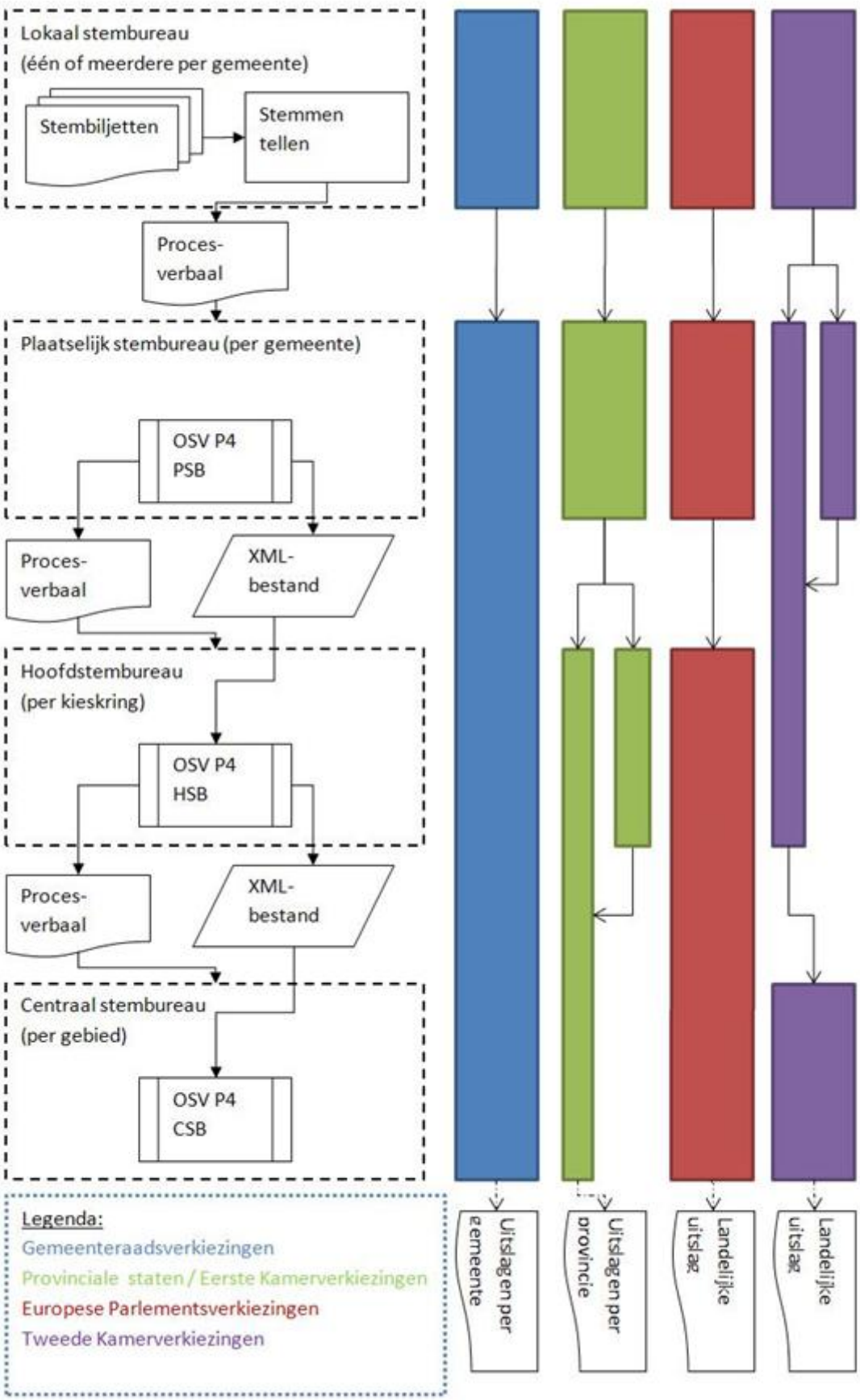


Diagram 7: de hiërarchie van OSV

3.4.1.1 Voorbeeld: locatiegegevens stembureaus

In deze paragraaf wordt een voorbeeld gegeven om meer duidelijkheid te verschaffen over de locaties van stembureaus. Bij de Provinciale Statenverkiezingen is in de onderstaande tabel te zien dat zowel het plaatselijk stembureau, het hoofdstembureau en het centrale stembureau zich in sommige gevallen binnen hetzelfde pand bevinden.

Soort verkiezing	**Lokaal stembureau**	**Plaatselijk stembureau**	**Hoofdstembureau**	**Centraal stembureau**
Provinciale staten	Stembureau nr. 5 Nieuwstadweg 40, Arnhem Gevestigd in: kerkgebouw	Koningsstraat 30, Arnhem Gevestigd in: stadhuis	Koningsstraat 30, Arnhem Gevestigd in: stadhuis	Koningsstraat 30, Arnhem Gevestigd in: stadhuis
Provinciale staten	Stembureau nr. 3 Laan van Zevenhuizen 88, Apeldoorn Gevestigd in: basisschool	Marktplein 1, Apeldoorn Gevestigd in: stadhuis	Koningsstraat 30, Arnhem Gevestigd in: stadhuis	Koningsstraat 30, Arnhem Gevestigd in: stadhuis
Gemeenteraad	Stembureau nr. 5 Nieuwstadweg 40, Arnhem Gevestigd in: kerkgebouw	Koningsstraat 30, Arnhem Gevestigd in: stadhuis	Koningsstraat 30, Arnhem Gevestigd in: stadhuis	Koningsstraat 30, Arnhem Gevestigd in: stadhuis
Tweede Kamer	Stembureau nr. 8 Stationsstrat 7, Wijchen Gevestigd in: stationshal	Korte Nieuwstraat 6, Nijmegen Gevestigd in: stadhuis	Koningsstraat 30, Arnhem Gevestigd in: stadhuis	Herengracht 21, Den Haag Gevestigd in: gebouw van de Kiesraad
Europese staten	Stembureau nr. 21 Parkweg 34, Nijmegen Gevestigd in: basisschool	Korte Nieuwstraat 6, Nijmegen Gevestigd in: stadhuis	Herengracht 21, Den Haag Gevestigd in: gebouw van de Kiesraad	Herengracht 21, Den Haag Gevestigd in: gebouw van de Kiesraad

Tabel 6: een voorbeeld van locatiegegevens van lokale, plaatselijke, hoofd –en centrale stembureaus.

3.4.2 Literatuurstudie

De literatuurstudie betreffende OSV is gebaseerd op een toetsingsrapport van o.a. de Software Improvement Group [SIG11] uit Amsterdam en op het document ‘Gedetailleerde specificatie Ondersteunende Software Verkiezingsproces’ van IVU Traffic Technologies, de ontwikkelaar van OSV [IVU09].
Het toetsingsrapport van de Software Improvement Group evalueert de onderdelen P4 en P5 van OSV die gebruikt worden voor alle verkiezingen. Het toetsingsrapport zoals gepubliceerd in [KSR10d] bevat een evaluatie. In deze evaluatie is beschreven of OSV voldeed aan de eisen die de Staatssecretaris van Binnenlandse Zaken heeft gesteld aan OSV.

3.4.2.1 De eisen van de Staatssecretaris aan OSV

Om het aanbestedingstraject van OSV in goede banen te leiden, zijn er een aantal eisen gesteld waaraan OSV moet voldoen. De eisen die de Staatssecretaris van Binnenlandse zaken aan OSV gesteld zijn volgens [KSR10d] als volgt beschreven:

1. De programmatuur bevat de functionaliteiten die (conform de wet- en regelgeving) nodig zijn voor de berekening van de uitslag (inclusief tussenstappen en tussenresultaten) door het centrale stembureau en de uitvoer daarvan.
2. De functionaliteit van de programmatuur is beschreven en vastgelegd in documenten (functioneel ontwerp, technisch ontwerp etc.). Deze documenten zijn openbaar.
3. Het ontwerp van de programmatuur voldoet aan de geaccepteerde kwaliteitseisen c.q. best practices voor de ontwikkeling van programmatuur. Daartoe:
   a. Is de programmatuur gestructureerd opgebouwd, zodanig dat modulaire aanpassingen mogelijk zijn.
   b. Zijn kritische functies in de programmatuur gescheiden.
   c. Zijn gegevens die aan verandering onderhevig zijn (configuratieparameters) zonder aanpassingen van programmatuur te wijzigen.
   d. Wordt toevallig of opzettelijk foutief gebruik van de programmatuur, voor zover als redelijkerwijs technisch mogelijk is, door het ontwerp voorkomen.
4. Conform het actieplan Nederland open in verbinding van het kabinet geldt voor de programmatuur:
   a. Dat gebruik wordt gemaakt van open standaarden. Voor verkiezingsgegevens (waaronder kandidatenlijsten en zetelverdeling) wordt de open standaard EML gebruikt.
   b. Dat deze is geschreven in een gangbare programmeertaal, waarvoor een door een actieve gemeenschap onderhouden open source compiler en/of interpreter beschikbaar is.
   c. Dat deze als open source ontwikkeld is. De broncode van de programmatuur is openbaar. Indien de programmatuur voor de centrale stembureaus wordt ontwikkeld dan dient het intellectueel eigendom van de broncode van de programmatuur te berusten bij een van de centrale stembureaus.
5. De programmatuur is beschikbaar op verschillende systeemarchitecturen en verschillende besturingssystemen, waaronder in ieder geval gangbare open source besturingssystemen.
6. Voor naamgeving dient de programmatuur de diakritische tekens van de GBA tekenset te ondersteunen.
7. Het is mogelijk om de authenticiteit van de programmatuur vast te stellen.
8. Alle elektronische communicatie van of naar andere programmatuur, hetzij via een netwerk, via opslagmedia of anderszins, is voorzien van een mogelijkheid om de authenticiteit van de gegevens vast te tellen, bij voorkeur door middel van een gekwalificeerde elektronische handtekening.
9. Met behulp van formele methoden is wiskundig aangetoond dat berekeningen in de programmatuur precies datgene doen wat door de wet- en regelgeving is voorgeschreven.
10. De programmatuur wordt in opdracht van de centrale stembureaus door een of meer onafhankelijke instanties getoetst voordat de centrale stembureaus de programmatuur accepteren en gebruiken. De uitkomst(en) van de toets(en) zijn openbaar.
11. Voor zover nog verder van toepassing dient de programmatuur te voldoen aan de aanbevelingen van de Raad van Europa voor elektronisch stemmen.

Eis nr. 8 heeft betrekking op de authenticiteit van vastgelegde verkiezingsuitslagen. De Staatssecretaris beschrijft dat de authenticiteit van deze gegevens 'bij voorkeur door middel van een gekwalificeerde elektronische handtekening' kan worden vastgesteld. De Staatssecretaris beschrijft deze methode als een voorkeur, maar niet als een absoluut vereiste. Vanuit het perspectief van informatiebeveiliging kan gesteld worden dat een elektronische handtekening een vereiste is als ervoor wordt gekozen de hashcode niet op een beveiligde locatie op te slaan. Hierop wordt verder ingegaan in hoofdstuk 3.4.2.8: Veronderstelling.

3.4.2.2 Het rapport van de Software Improvement Group

Eén van de door de Staatssecretaris gestelde eis was dat OSV door een onafhankelijke organisatie getoetst zou worden. De Kiesraad heeft de toetsing van OSV P4 en P5 toegewezen aan de Software Improvement Group (SIG) uit Amsterdam. De resultaten van deze toetsing zijn beschreven in het document 'Toetsing eisen OSV 4 en 5 voor alle soorten verkiezingen, rapport t.b.v. Kiesraad' [SIG11]. Het rapport is uitgebracht op 10 februari 2011.

3.4.2.2.1 Authenticiteit vastgelegde verkiezingsuitslagen

Over de integriteit van de vastgelegde verkiezingsuitslagen in OSV wordt er in [SIG11] (pagina 17, eis 8: authenticiteit gegevens) de eis van de Staatssecretaris geciteerd:

> *"Alle elektronische communicatie van of naar andere programmatuur, hetzij via een netwerk, via opslagmedia of anderszins, is voorzien van een mogelijkheid om de authenticiteit van de gegevens vast te tellen, bij voorkeur door middel van een gekwalificeerde elektronische handtekening."*

De Software Improvement Group in [SIG11] stelt dat er aan deze eis is voldaan. De motivatie van de SIG luidt als volgt:

1. Bij elke uitvoer van gegevens wordt een 'hashcode' berekend en weergegeven in een afdrukbaar document. Door dit afgedrukte document kan de authenticiteit bij inladen van gegevens worden gecontroleerd.
2. Er wordt gebruik gemaakt van een cryptografisch sterk hash algoritme (SHA-1) dat voor 2011 voldoende veiligheid biedt. Als het in de toekomst nodig mocht blijken om dit algoritme te wijzigen kan dit door wijziging van één regel in de broncode.
3. In de huidige versie zijn wijzigingen doorgevoerd die foutief gebruik mogelijk kunnen maken. Deze zijn reeds behandeld bij Eis 3d in hoofdstuk 3.3.4 in [SIG11].

De motivatie in hoofdstuk 3.3.4 (motivatie 3d) in [SIG11] omtrent OSV P4 luidt als volgt:

1. In eerdere versies van OSV was vereist dat een gebruiker bij het inlezen van verkiezingsgegevens gedwongen was om de correctheid van het digitale bestand te controleren met de papieren versie. De methode is beschreven onder eis 8. De controle kon niet worden overgeslagen omdat de gebruiker een code vanaf de papieren versie moest invoeren. In de nieuwe versie is het wel mogelijk om in bepaalde gevallen controles over te slaan. Deze gevallen hebben betrekking op situaties waarin het in te lezen bestand is aangemaakt door één en dezelfde gebruiker, of waarin een zeer korte tijd is verstreken tussen het aanmaken en het lezen. Appendix A.3.4 geeft een overzicht van de verschillende stappen en bijbehorende controles. Hierdoor wordt niet meer voldaan aan eis 3d (het ontwerp van de programmatuur voldoen aan geaccepteerde kwaliteitseisen c.q. best practices voor de ontwikkeling van programmatuur. Daartoe: (d) wordt toevallig of opzettelijk foutief gebruik van de programmatuur, voor zover als redelijkerwijs of technisch mogelijk is, door het ontwerp voorkomen).

2. De programmatuur zal gebruikt worden op een afgezonderde netwerkomgeving die geen verbinding met de buitenwereld heeft. Hiermee wordt misbruik van buitenaf uitgesloten.
3. Programma P4 bevat toetsen die onopzettelijke foutieve invoer tegengaan. Deze toetsen zijn weergegeven in Appendix A.3.4 in [SIG11]. Opzettelijke foutieve invoer door een stembureaumedewerker is ook zonder programmatuur mogelijk en kan redelijkerwijs technisch niet voorkomen worden.

De wijze waarop hashcodes binnen OSV P4 gebruikt worden, verschilt per soort verkiezing. In Appendix A.3.4 beschrijft [SIG11] het gebruik van hashcodes volgens die verschillende veiligheidsniveaus:

a. Geen hashcode-controles
b. De gebruiker wordt gevraagd of de getoonde hashcode correct is
c. De gebruiker wordt gevraagd om (een deel van) de hashcode.

De veiligheidsniveaus worden als volgt toegepast:

Bestand	Veiligheidsniveau in OSV P4	Scope onderzoek?
Verkiezingsdefinitie	a	Nee
Kandidatenlijst	b/c	Nee
Verkiezingsuitslag van lokaal stembureau naar hoofdstembureau	a	Ja
Verkiezingsuitslag van hoofdstembureau naar centraal stembureau	a/c	Ja

Tabel 7: de wijze van gebruik van hashcodes in OSV P4.

In tabel 7 staat een overzicht van de wijze waarop hashcodes gebruikt worden. Uit [SIG11] blijkt dat verkiezingsuitslagen op plaatselijk/hoofdstembureauniveau niet altijd worden voorzien van een hashcode. Dit is het geval als het plaatselijk/hoofdstembureau tevens de rol van het centrale stembureau vervult, zoals bij gemeenteraadsverkiezingen.

3.4.2.2.2 Authenticiteit programmatuur

De Staatssecretaris stelde in eis 7 het volgende:

> *"Het is mogelijk de authenticiteit van de programmatuur vast te stellen."*

De Software Improvement Group concludeert dat er aan deze eis voldaan is:

1. Er is een op 'hashcodes' (digitale vingerafdruk) gebaseerde methode om de authenticiteit van de installatiebestanden vast te stellen. Hiermee wordt aan deze eis voldaan.

2. Voor hetzelfde doeleinde heeft de leverancier het gebruik van 'jar-signing' getoond Deze methode is geschikt wanneer alle programmatuur hiermee wordt gecontroleerd. Het is een vooruitgang dat deze alternatieve methode is toegevoegd, doordat gebruikers nu op meer manieren kunnen controleren.

3. Bij he gebruik van de 'jar-signing' methode moet men er wel op letten dat de installatiemedia alleen 'jar'-bestanden bevatten. Men moet geen andere bestanden toevoegen die niet controleerbaar zijn, anders is niet aan deze eis voldaan.

3.4.2.3 De eisen van de staatssecretaris versus het rapport van de Software Improvement Group

De Software Improvement Group concludeert dat er aan eis 8 voldaan is door middel van het gebruik van een hashcode. De SIG gaat ervan uit dat het gebruik van enkel een hashcode voldoende is om de authenticiteit van gegevens te waarborgen. De SIG geeft verder geen details vrij over de wijze waarop hashcodes beschermd worden.
De Staatssecretaris geeft aan dat de voorkeur om de authenticiteit van gegevens te waarborgen ligt bij het gebruik ven een 'gekwalificeerde elektronische handtekening'. Het gaat hier slechts om een voorkeur. Geconcludeerd kan worden dat de Staatssecretaris het gebruik van een elektronische handtekening niet als een absolute eis stelt. Door deze formulering is er voor de SIG nog een andere optie om hashcodes te beveiligen: het opslaan van een hashcode op een beveiligde locatie. Bevindingen bij het hoofdstembureau en het centrale stembureau hebben aangetoond dat hashcodes op het papieren proces-verbaal worden vastgelegd. Processen-verbaal zijn in de huidige vorm te manipuleren, waardoor een proces-verbaal geen veilige locatie is om een hashcode op te slaan. Daarnaast worden hashcodes vastgelegd in logbestanden, die enkel in uitzonderlijke gevallen worden aangesproken om de authenticiteit van vastgelegde verkiezingsuitslagen te controleren. Meer details staan in hoofdstuk 3.4.3: Eigen praktijkstudie OSV. Een elektronische handtekening die is toegevoegd aan een document zegt iets over auteur en de inhoud van het document.[11] Een hashcode is enkel een wiskundige functie die iets zegt over de inhoud, maar niet over de auteur. Gegeven deze informatie kan geconcludeerd worden dat aan eis nr. 8 zoals opgesteld door de staatssecretaris niet voldaan is.
Binnen OSV wordt wel gebruik gemaakt van elektronische handtekeningen op het gebied van de authenticiteit van de software door middel van JAR-signing. Deze methode wordt alleen gebruikt voor de programmatuur zelf, waardoor aan eis nr. 8 niet voldaan wordt. Meer informatie over JAR-signing staat in hoofdstuk 3.4.2.5: Authenticiteit software OSV door middel van Jar-signing.

[11] http://en.wikipedia.org/wiki/Electronic_signature

3.4.2.4 Het versturen van verkiezingsuitslagen door OSV-systemen van het hoofdstembureau naar het centrale stembureau

In het onderstaande schema wordt beschreven welke documenten worden vervoerd van het hoofdstembureau naar het centrale stembureau. Het schema is afgeleid van [SIG11]. Dit schema heeft ook betrekking op documenten die vervoerd worden van het plaatselijke stembureau naar het hoofdstembureau.

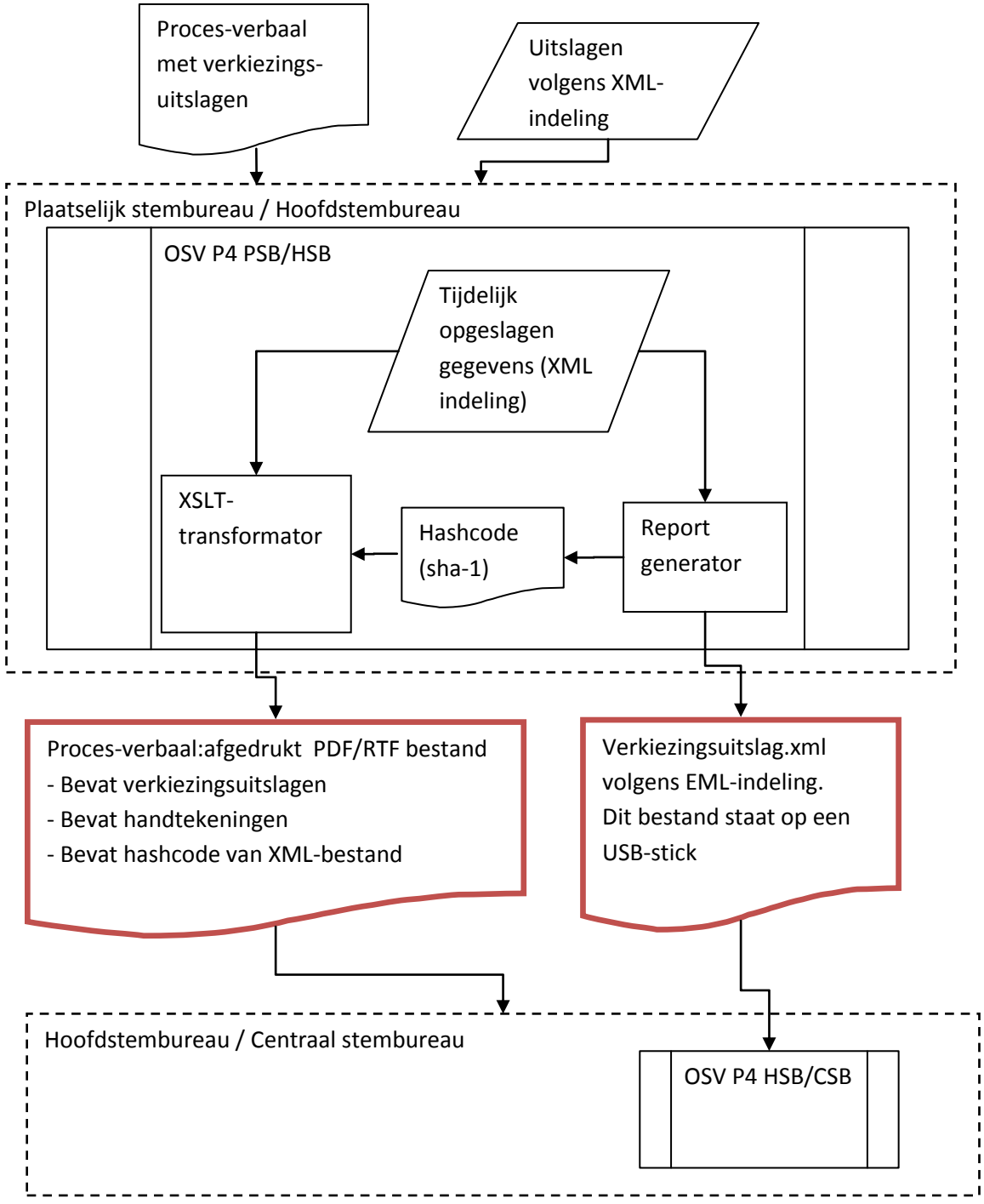
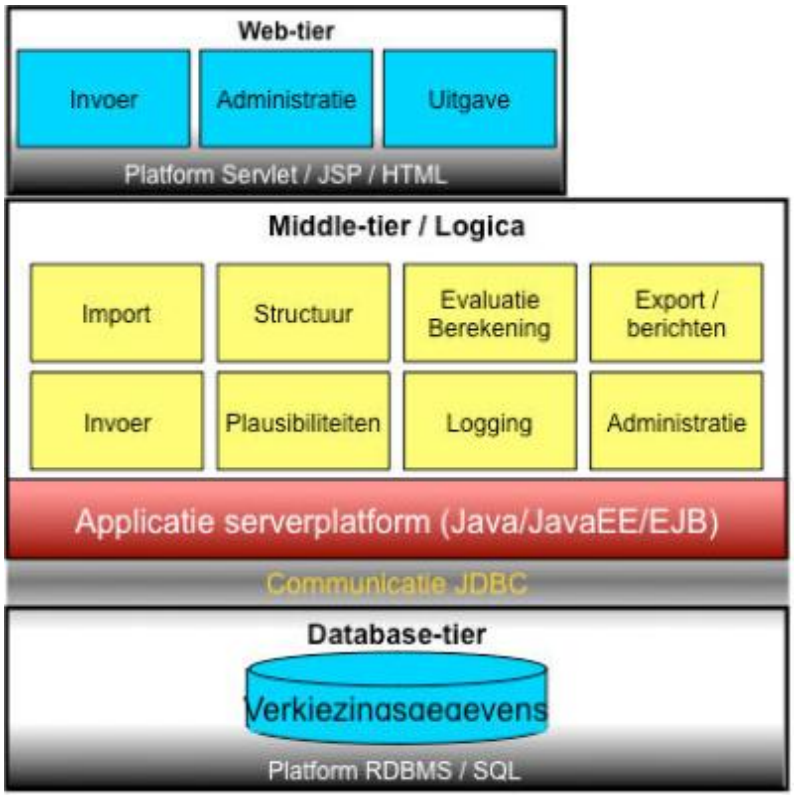


Diagram 8: de invoer, verwerking en uitvoer van data in OSV P4. De rood-gemarkeerde symbolen zijn het proces-verbaal en het XML-bestand. Deze documenten worden door een persoon naar het centrale stembureau gebracht.

3.4.2.5 Authenticiteit software OSV door middel van Jar-signing

Eén van de eisen van de Staatssecretaris was dat het mogelijk moet zijn om de authenticiteit van OSV vast te stellen. Naast het gebruik van hashcodes die op de website van de Kiesraad gepubliceerd zijn, is er nog een andere mogelijkheid om de authenticiteit van OSV vast te stellen. Hiervoor wordt jar-signing[12] gebruikt. Alle installatiebestanden die nodig zijn voor OSV worden in één jar-bestand geplaatst. Het jar-bestand lijkt enigszins op een zip-bestand dat uitgepakt kan worden. Van elk los bestand in het jar-bestand wordt een checksum (bijvoorbeeld een hashcode) berekend en deze checksum wordt door de ontwikkelaar ondertekend. Het jar-bestand wordt zelf niet ondertekend. Bij het inlezen van het jar-bestand (als OSV wordt geïnstalleerd), controleert Java Runtime (het programma dat het jar-bestand inleest), of alle bestanden in het jar-bestand correct zijn ondertekend. Alle niet –of verkeerd ondertekende bestanden in het jar-bestand worden overgeslagen.
Jar-signing bied ook een mogelijkheid voor 'sealed packages'. In een dergelijk geval wordt het gehele jar-bestand alleen ingelezen als alle bestanden in het jar-bestand zijn ondertekend met dezelfde handtekening. Hierdoor kan voorkomen worden dat het jar-bestand van kwaadaardige (niet-ondertekende) bestanden wordt voorzien.

3.4.2.6 Programmaopbouw OSV



De programma onderdelen P4 en P5 zijn opgebouwd als een client-server architectuur, waarbij gebruikt wordt gemaakt van een lokaal netwerk. Op de server worden alle EML-bestanden opgeslagen. Als er maar één computer aanwezig is, kan die computer zowel dienen als server en client.

De opbouw van OSV volgens [IVU09].

[12] http://en.wikipedia.org/wiki/JAR_file

3.4.2.7 Eisen aan de software met betrekking tot gegevensbeveiliging

De Kiesraad stelt eisen[13] aan de omgeving waar OSV gebruikt wordt:

> *"Wordt OSV gebruikt op een laptop of pc met een draadloze netwerk aansluiting (WiFi of Bluetooth), dan dient deze uitgezet te worden om te voorkomen dat de computer (draadloos) van buitenaf benaderd kan worden."*

Er is voor meer details contact opgenomen met de Kiesraad, waarna er een document is verstrekt met wat meer informatie. Deze informatie had betrekking op het gebruik van OSV tijdens de verkiezingen van senatoren voor de Eerste Kamer. In dit document wordt het volgende vermeld:

> *"Het programma OSV P4 kan op een stand-alone computer of laptop worden geïnstalleerd. In verband met de integriteit van de verkiezingsgegevens dient de computer of laptop waarop OSV is geïnstalleerd niet van buitenaf, via het internet of een draadloos netwerk (WiFi of Bluetooth), te kunnen worden benaderd. Eventuele (draadloze) netwerk aansluitingen dienen daarom uitgezet te worden voordat OSV wordt gebruikt."*

Uit deze informatie kan geconcludeerd worden dat het moeilijk is om opgeslagen verkiezingsuitslagen van buitenaf te benaderen. Er wordt echter niets beschreven over het gebruik van de computer zelf: er zijn geen voorschriften bekend of computers vergrendeld moeten worden als ze tijdelijk niet in gebruik zijn. Het is eenvoudig om opgeslagen verkiezingsuitslagen in XML-bestanden op te zoeken door naar de mappen te bladeren waarin OSV opgeslagen is. Voordat vastgestelde processen-verbaal afgedrukt worden, kan een kwaadwillende het PDF-bestand vervangen voor een ander exemplaar, evenals het XML-bestand. Deze bestanden staan bijvoorbeeld in de mappenstructuur C:\OSV\PS2011\export\P4_HSB.

3.4.2.8 Veronderstelling

Verkiezingsuitslagen die binnen OSV formeel nog niet vastgesteld zijn, worden binnen OSV P4 PSB/HSB in XML-bestanden opgeslagen. Na het vaststellen van de verkiezingsuitslagen wordt de hashcode van het XML-bestand berekend. Deze hashcode wordt afgedrukt op het proces-verbaal.
Het XML-bestand met daarin de verkiezingsuitslagen wordt via een USB-stick of een andere gegevensdrager van het hoofdstembureau naar het bovenliggende stembureau gestuurd (bijvoorbeeld het centrale stembureau), gezamenlijk met de afgedrukte hashcode op het proces-verbaal. In hoofdstuk 2.4.2.1 (De beveiliging van hashcodes binnen OSV) zijn 2 opties beschreven waaraan voldaan moest worden om de integriteit van vastgelegde verkiezingsuitslagen te garanderen:

- Het bestand met de uitslagen moet digitaal ondertekend zijn, of
- de hashcode moet opgeslagen zijn op een beveiligde locatie.

[13] http://www.kiesraad.nl/nl/Overige_Content/Bestanden/pdf_thema/pdfs_OSV/Systeemeisen_OSV_2011.pdf

3.4.2.9 Protocol: van proces-verbaal tot uitslag

Het onderstaande protocol beschrijft de informatiestroom vanaf het moment dat Alice (medewerkster lokaal stembureau) het proces-verbaal met daarin de verkiezingsuitslagen naar Bob (medewerker hoofdstembureau) brengt tot het moment dat het programma OSV de uitslag publiceert. In werkelijkheid ontvangt Bob ook nog processen-verbaal van andere lokale stembureaus.

Regelnr	Verzender	Bericht / document	Ontvanger
1	Alice	Proces-verbaal verkiezingsuitslagen stembureau nr. 2 Arnhem	Bob
2	Bob	Verkiezingsuitslagen kieskring nr. 3	Client (C)
3	Client (C)	Verkiezingsuitslagen kieskring nr. 3	Server (OSV P4 HSB)
4	Server (S)	• Verkiezingsuitslagen_kieskring_Arnhem.xml • Uitslagen op papieren proces-verbaal (afgedrukt vanuit PDF-bestand) sha1(Verkiezingsuitslagen_kieskring_3_Arnhem.xml)	Centraal stembureau

Protocol 2: Bob voert de resultaten in die hij ontvangen heeft van Alice.

3.4.2.10 Conclusie

Naar aanleiding van het rapport 'Toetsing eisen OSV 4 en 5 voor alle verkiezingen' in [SIG11] is gebleken dat de hashcodes van de vastgelegde verkiezingsuitslagen niet worden ondertekend. De hashcodes worden wel op een proces-verbaal opgeslagen. Daarnaast wordt het proces-verbaal met de hashcode afgedrukt en gezamenlijk met het XML-bestand naar de ontvanger gestuurd. Deze situatie lijkt op het versturen van het proces-verbaal: het kan in dit geval eenvoudig zijn om vastgelegde verkiezingsuitslagen op de gegevensdrager aan te passen en een nieuwe hashcode van deze aangepaste verkiezingsuitslagen af te drukken. De ontvanger zal de inhoud als valide beschouwen omdat de hashcode ook na aanpassing van de verkiezingsuitslag correspondeert.
Het document van de Software Improvement Group roept vragen op als men kijkt hoe de hashcode wordt gebruikt voor de authenticatie van het XML-bestand. Eis nr. 8 luidde:

> "Alle elektronische communicatie van of naar andere programmatuur, hetzij via een netwerk, via opslagmedia of anderszins, is voorzien van een mogelijkheid om de authenticiteit van de gegevens vast te tellen, bij voorkeur door middel van een gekwalificeerde elektronische handtekening."

Het is opmerkelijk dat de Software Improvement Group geen aandacht heeft besteed aan de wijze van omgang met de hashcode. De hashcode wordt niet beveiligd, waardoor het risico op misbruik niet uitgesloten kan worden. De Staatssecretaris beschrijft dat er een 'gekwalificeerde elektronische handtekening' gebruikt moet worden. Een hashcode is geen gekwalificeerde elektronische handtekening. Een misbruikscenario wordt beschreven in hoofdstuk 3.4.3: Eigen praktijkstudie OSV.

3.4.3 Eigen praktijkstudie OSV

3.4.3.1 Introductie

De Kiesraad heeft het programma OSV ter beschikking gesteld voor de praktijkstudie. Op websites van verschillende gemeenten in Nederland werd beweerd dat OSV te downloaden zou zijn van de site van de Kiesraad, maar op de site van de Kiesraad was OSV als downloadbaar programma moeilijk te vinden. Daarom is er een mail naar de Kiesraad verstuurd met het verzoek of het programma opgestuurd kon worden. Na één dag belde de Kiesraad terug met het bericht dat ik het programma OSV zou ontvangen en de volgende dag lag er een pakje met 3 cd-roms in de brievenbus. Het

programma bevatte de OSV-onderdelen P0 t/m P5 voor de Provinciale Statenverkiezingen van 2 maart 2011. Op twee cd staan alle onderdelen van OSV en de andere cd bevat handleidingen en documentatie.
Voor deze praktijkstudie zijn alleen de onderdelen P4 en P5 geïnstalleerd. Het installeren van het serverprogramma verloopt eenvoudig via een Wizard. OSV is geïnstalleerd op een computer met de volgende specificaties:

CPU	Intel I5 750
Geheugen	4 GB PC10500
Besturingssysteem	Microsoft Windows 7 professional
Gebruikte internet-browser	Microsoft Internet Explorer 8
Hash generator	Slavasoft Hashcalc (freeware), http://www.slavasoft.com/hashcalc/index.htm
Tekst editor	Notepad++ (om XML-bestanden te manipuleren)

Na de installatie van OSV is de gebruikersinterface op te starten via het startmenu (Windows). De gebruikersinterface draait binnen de internet-browser. Voorafgaand aan het gebruik van OSV moet eerst de service van OSV gestart worden door middel van het programma 'starten OSV server'. De eerste keer moet er ingelogd worden met een standaard gebruikersnaam en wachtwoord die in de gebruikershandleiding genoemd worden. De gebruikersnaam is 'OSV' en het wachtwoord is 'wachtwoord'. Na het inloggen met deze gegevens wordt de gebruiker direct gedwongen het wachtwoord te wijzigen.

3.4.3.2 Doel praktijkstudie

Het doel van deze praktijkstudie is om na te gaan in hoeverre het haalbaar is om te manipuleren met vastgelegde verkiezingsuitslagen zonder dat de ontvanger dit opmerkt. In alle onderdelen van OSV P4 worden verkiezingsuitslagen vastgelegd. In deze praktijkstudie worden de XML-bestanden waarin de uitslagen verwerkt zijn met een eenvoudige tekstverwerker doelbewust aangepast. Alle handelingen die door Trudy uitgevoerd zijn worden stap voor stap beschreven.

3.4.3.3 Openen verkiezingsdefinitie en kandidatenlijst

Het vekiezingsdefinitiebestand en de kandidatenlijsten voor de Provinciale Statenverkiezingen zijn meegeleverd op de cd-rom van OSV. In deze bestanden staan een aantal reglementen en de gegevens van de kandidaten waarop de kiezers kunnen stemmen. Na het inloggen in OSV P4 HSB zijn deze bestanden met de volgende gegevens ingevoerd:

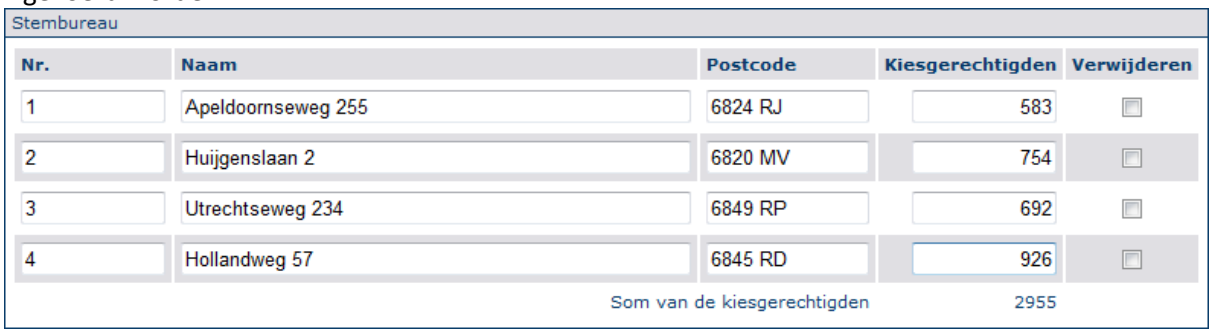
Verkiezingsdefinitie gegevens	
Verkiezings-ID:	PS2011_Gelderland
Naam van de verkiezing:	Provinciale Staten Gelderland 2011
Type verkiezing:	PS2
In provincie:	Gelderland
Dag van de stemming:	2011-03-02
Dag van de kandidaatstelling:	2011-01-18
Aantal zetels:	55
Wettelijke voorkeurdrempel:	25
Aanmaakdatum:	2011-01-25 08:40:35

Tabel 8: ingeladen vekiezingsdefinitiebestand in OSV P4 PSB

Vervolgens moeten de eerste 4 tekens van de hashcode van het bestand met de kandidatenlijst worden ingevoerd om de integriteit vast te stellen. Deze hashcode is te vinden in een PDF-bestand op de cd-rom waarmee OSV geïnstalleerd kan worden. Na het invoeren van de eerste 4 tekens van de hashcode moet er een gemeente worden gekozen waarvan resultaten kunnen worden ingevoerd. In deze praktijkstudie is gekozen voor de gemeente Arnhem.

3.4.3.4 Invoeren stembureaus

Er moet worden aangegeven waar de stembureaus zijn gevestigd. Hiervoor kan een bestand met daarin de informatie van stembureaus worden opgehaald, maar stembureaus kunnen ook handmatig ingevoerd worden.


Stembureau

Nr.	Naam	Postcode	Kiesgerechtigden	Verwijderen
1	Apeldoornseweg 255	6824 RJ	583	☐
2	Huijgenslaan 2	6820 MV	754	☐
3	Utrechtseweg 234	6849 RP	692	☐
4	Hollandweg 57	6845 RD	926	☐
		Som van de kiesgerechtigden	2955	

Figuur 1: een overzicht van de aangemaakte lokale stembureaus in OSV P4 PSB

Er is gekozen om 4 fictieve stembureaus aan te maken. Per stembureau wordt ook het aantal kiesgerechtigden vastgelegd.

3.4.3.5 Invoeren en transport stemresultaten

Het programma-onderdeel P4 van OSV is opgebouwd uit meerdere onderdelen. Hieronder staat een overzicht van deze onderdelen.

P4-onderdeel	Functies
P4_PSB (Plaatselijk StemBureau)	Het programma-onderdeel P4 PSB kan door het plaatselijk stembureau gebruikt worden om verkiezingsresultaten samen te voegen op gemeenteniveau.
P4_HSB (HoofdStemBureau)	P4 HSB wordt gebruikt door het hoofdstembureau om de verkiezingsuitslagen die ontvangen zijn van plaatselijke stembureaus samen te voegen.
P4_CSB (Centraal StemBureau)	P4 CSB wordt gebruikt door het centrale stembureau om de verkiezingsuitslagen die ontvangen zijn van hoofdstembureaus samen te voegen.

Tabel 9: een overzicht van de verschillende onderdelen van OSV P4

Het programma dat gebruikt wordt om stemuitslagen in te voeren op hoofdstembureauniveau kan worden gestart via het 'Startmenu, Programma's OSV, HSB – Invoeren en samenvoegen stemtotalen (P4 HSB).' Het programma-onderdeel HSB biedt een mogelijkheid om verkiezingsuitslagen (XML-bestanden) die aangemaakt zijn in P4 PSB in te voeren. Als deze gegevens niet beschikbaar zijn, kunnen uitslagen ook in P4 HSB handmatig ingevoerd worden. Het invoeren van de stemresultaten is

een secuur werk. Als eerste kan opgegeven worden hoeveel stemmen er uitgebracht zijn en hoeveel ongeldige/blanco stembiljetten er geteld zijn. Daarna kunnen per kandidaat de totaalaantallen ingevuld worden. De som van de hoeveelheden stemmen van alle kandidaten bij elkaar moet overeenkomen met het eerder ingevoerde aantal geldige stemmen die zijn uitgebracht. OSV telt tussentijdse totaalaantallen per kandidaat niet bij elkaar op om op deze manier het totaal aantal stemmen per partij te verkrijgen. Hiermee is de bewering dat 'het tellen van stemmen een secuur werk is' van een medewerker van het hoofdstembureau in Maarssen bevestigd (zie hoofdstuk 3.1: Bevindingen bij het lokale stembureau).

Het invoeren van uitslagen is als volgt geordend:

Invoeren gebiedseenheid 1: Apeldoornseweg 255		
	Kiesgerechtigden (aantal opgeroepenen)	583
	6.1 Ongeldige stembiljetten in de stembus	2
	6.2 Blanco stembiljetten in de stembus	2
	6.3 Totaal op de kandidaten uitgebrachte stemmen (Verzamelstaat)	100
	6.4 Totaal uitgebrachte stemmen	104
	Christen Democratisch Appèl (CDA)	
	1.1 van Dijk, J.J.	10
	1.2 Hutten, G.J.	10
	1.3 …	

Tabel 10: een voorbeeld van ingevoerde stemuitslagen binnen OSV P4 PSB

De resultaten van de verkiezing zijn voor deze praktijkstudie fictief ingevuld. Voor het rekengemak wordt er gebruik gemaakt van ronde getallen. De gebruiker van OSV moet alle resultaten per stembureau 2 keer invullen, evenals de aantallen per partij en per kandidaat. Beide invoeren moeten met elkaar overeenkomen. Helaas rekent het programma OSV de aantallen per partij niet uit op basis van het aantal stemmen per kandidaat voor een partij. Hierdoor moeten de totaalaantallen door de persoon die de resultaten invoert handmatig bij elkaar opgeteld worden, wat een tijdrovende klus is. Ditzelfde geldt ook voor het aantal uitgebrachte stemmen per stembureau. Als de gegevens ingevuld zijn kan OSV deze gegevens tussentijds opslaan in een XML-bestand. Voordat de gegevens daadwerkelijk opgeslagen worden, controleert OSV eerst of de totaalaantallen wel corresponderen met de aantallen die in de uitslagenlijst ingevoerd zijn.
Als alle uitslagen correct ingevoerd zijn, kan de verkiezingsuitslag definitief gemaakt worden. Het stappenplan (een PDF-bestand met daarin een beschrijving van OSV P4 HSB) beschrijft na het definitief maken van de uitslag het volgende:

1. *Selecteer 'Definitief maken verkiezing' en daarna in deze pagina de knop 'Definitief maken. (dit is noodzakelijk om de volgende stap te laten slagen)*
2. *selecteer Model O3 en voer de gevraagde gegevens in. Dit levert (in de map ..\OSV\export\P4_HSB):*
    a. *proces verbaal volgens model O 3 (Vaststelling aantallen stemmen…)*
    b. *bestand Telling … .eml.xml (met de uitslag van de kieskring)*
3. *print de O3 op papier (met hashcode) zodat het ondertekend[14] kan worden*
4. *zet bestand Telling … .eml.xml op USB-stick en breng het naar het centraal stembureau zodat zij in programma 4 de tellingen van de kieskringen binnen de provincie samen kan voegen*
5. *u kunt nu ook een .csv bestand aanmaken van het resultaat om in te lezen in Excel*

[14] Met 'ondertekenen' worden hier handgeschreven handtekeningen bedoeld.

Na afsluiten van de OSV-server dient u nog enkele zaken te doen: Het kopiëren van alle OSV-bestanden naar een CD of DVD. Daarbij horen in ieder geval:

- *de verkiezingsdefinitie*
- *de Ingediende lijsten...eml.xml en Geldige lijsten...eml.xm uit P2*
- *de Kandidatenlijsten..eml.xml en de Totaallijsten...eml.xml uit P3*
- *de map osv..\export die door P4 is gevuld*
- *de map osv..\jboss-4.2.3.GA\server\osv\log met daarin de log-bestanden*

Er zijn nu 2 bestanden aangemaakt:

1. F:\OSV\PS2011\export\P4_PSB\ Telling_PS2011_Gelderland_gemeente_Arnhem.eml.xml
    a. In dit bestand staat volgens de EML/XML indeling hetzelfde wat er in het PDF-bestand staat.
    b. De hashcode staat in het bijbehorende PDF-bestand.
    c. Dit XML-bestand wordt opgeslagen op een USB stick en naar het hoofdstembureau gebracht, gezamenlijk met het afgedrukte PDF-bestand.
2. F:\OSV\PS2011\export\P4_PSB\N11_Vaststelling aantallen stemmen in gemeente_PS2011_Gelderland_gemeente_Arnhem.pdf
    a. In dit PDF-bestand staat een overzicht per hoofdstembureau van het aantal uitgebrachte stemmen, het aantal geldige, ongeldige en blanco stemmen, per partij het totaal aantal stemmen en ook per kandidaat het totaalaantal stemmen.
    b. Onderaan elke pagina staat de hashcode van het bijbehorende XML-bestand, afgeleid uit(1).
    c. Dit PDF-bestand moet afgedrukt worden.
    d. Dit PDF-bestand is tevens het proces-verbaal: de laatste pagina moet door alle aanwezige leden van het hoofdstembureau ondertekend worden.

3.4.3.6 Manipulatie XML-bestand en de herberekening van de hashcode

Er zijn 2 documenten met verkiezingsuitslagen beschikbaar die van het hoofdstembureau naar het centrale stembureau verstuurd worden: het afgedrukte proces-verbaal (het PDF-bestand dat is aangemaakt in OSV P4 HSB) en het XML-bestand. In het XML-bestand staan de verkiezingsuitslagen volgens de EML-indeling:

```
- <Selection>
- <AffiliationIdentifier Id="1">
  <RegisteredName>Christen Democratisch Appèl (CDA)</RegisteredName>
  </AffiliationIdentifier>
  <ValidVotes>290</ValidVotes>
  </Selection>
- <Selection>
- <Candidate>
  <CandidateIdentifier Id="1" />
  </Candidate>
  <ValidVotes>50</ValidVotes>
  </Selection>
```

De waarden die bij de attributen staan kunnen zonder moeite in een teksteditor zoals Notepad++ bewerkt worden. In dit XML-bestand, dat onderschept is door Trudy, worden een aantal gegevens aangepast. Trudy wil een aantal zetels van het CDA aan de PVV geven, en verandert een aantal waarden in het XML-bestand.

```
kiesraad-eml-extensions.xsd"><!--Created by: Ondersteunende Software Verkiezingen by IVU Traffic Technologies AG
<TransactionId>1</TransactionId><ManagingAuthority><AuthorityIdentifier Id="0202">Arnhem
</AuthorityIdentifier><AuthorityAddress></AuthorityAddress></ManagingAuthority><kr:CreationDateTime>
2011-02-19T14:47:20.695</kr:CreationDateTime><ds:CanonicalizationMethod Algorithm=
"http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"
></ds:CanonicalizationMethod><Count><EventIdentifier></EventIdentifier><Election><ElectionIdentifier Id=
"PS2011_Gelderland"><ElectionName>Provinciale Staten Gelderland 2011</ElectionName><ElectionCategory>PS
</ElectionCategory><kr:ElectionSubcategory>PS2</kr:ElectionSubcategory><kr:ElectionDomain>Gelderland
</kr:ElectionDomain><kr:ElectionDate>2011-03-02
</kr:ElectionDate></ElectionIdentifier><Contests><Contest><ContestIdentifier Id="1"><ContestName>Arnhem
</ContestName></ContestIdentifier><TotalVotes><Selection><AffiliationIdentifier Id="1"><RegisteredName>Christen
Democratisch Appèl (CDA)</RegisteredName></AffiliationIdentifier><ValidVotes>290
</ValidVotes></Selection><Selection><Candidate><CandidateIdentifier Id="1"
></CandidateIdentifier></Candidate><ValidVotes>50
</ValidVotes></Selection><Selection><Candidate><CandidateIdentifier Id="2"
></CandidateIdentifier></Candidate><ValidVotes>50
```

Hierboven staat een gedeelte van het originele XML-bestand. Het CDA heeft hier in totaal 290 stemmen behaald. Trudy wil 10 stemmen aan de PVV geven, dus verandert het totaalaantal stemmen van het CDA in 280 en geeft één CDA-kandidaat 10 stemmen minder.

```
kiesraad-eml-extensions.xsd"><!--Created by: Ondersteunende Software Verkiezingen by IVU Traffic Technologies AG
<TransactionId>1</TransactionId><ManagingAuthority><AuthorityIdentifier Id="0202">Arnhem
</AuthorityIdentifier><AuthorityAddress></AuthorityAddress></ManagingAuthority><kr:CreationDateTime>
2011-02-19T14:47:20.695</kr:CreationDateTime><ds:CanonicalizationMethod Algorithm=
"http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"
></ds:CanonicalizationMethod><Count><EventIdentifier></EventIdentifier><Election><ElectionIdentifier Id=
"PS2011_Gelderland"><ElectionName>Provinciale Staten Gelderland 2011</ElectionName><ElectionCategory>PS
</ElectionCategory><kr:ElectionSubcategory>PS2</kr:ElectionSubcategory><kr:ElectionDomain>Gelderland
</kr:ElectionDomain><kr:ElectionDate>2011-03-02
</kr:ElectionDate></ElectionIdentifier><Contests><Contest><ContestIdentifier Id="1"><ContestName>Arnhem
</ContestName></ContestIdentifier><TotalVotes><Selection><AffiliationIdentifier Id="1"><RegisteredName>Christen
Democratisch Appèl (CDA)</RegisteredName></AffiliationIdentifier><ValidVotes>280
</ValidVotes></Selection><Selection><Candidate><CandidateIdentifier Id="1"
></CandidateIdentifier></Candidate><ValidVotes>50
</ValidVotes></Selection><Selection><Candidate><CandidateIdentifier Id="2"
></CandidateIdentifier></Candidate><ValidVotes>40
```

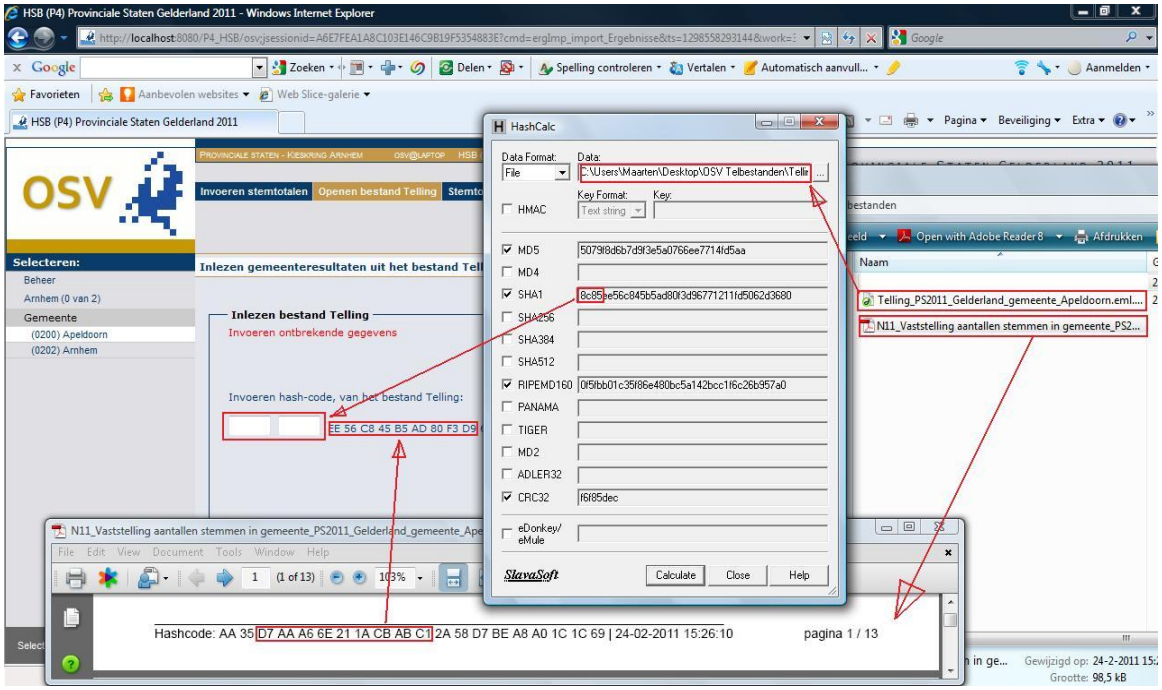
In het XML-bestand worden in totaal 10 stemmen aan de PVV toegevoegd, dus ook in totaal 10 stemmen aan de kandidaten van de PVV.

```
Id="10"><RegisteredName>PVV (Partij voor de Vrijheid)</RegisteredName></AffiliationIdentifier><ValidVotes>25
</ValidVotes></Selection><Selection><Candidate><CandidateIdentifier Id="1"
></CandidateIdentifier></Candidate><ValidVotes>5</ValidVotes></Selection><Selection><Candidate><CandidateIdentifier
 Id="2"></CandidateIdentifier></Candidate><ValidVotes>5
</ValidVotes></Selection><Selection><Candidate><CandidateIdentifier Id="3"
></CandidateIdentifier></Candidate><ValidVotes>5</ValidVotes></Selection><Selection><Candidate><CandidateIdentifier
 Id="4"></CandidateIdentifier></Candidate><ValidVotes>5
</ValidVotes></Selection><Selection><Candidate><CandidateIdentifier Id="5"
></CandidateIdentifier></Candidate><ValidVotes>5</ValidVotes></Selection><Selection><Candidate><CandidateIdentifier
 Id="6"></CandidateIdentifier></Candidate><ValidVotes>0
</ValidVotes></Selection><Selection><Candidate><CandidateIdentifier Id="7"
></CandidateIdentifier></Candidate><ValidVotes>0</ValidVotes></Selection><Selection><Candidate><CandidateIdentifier
 Id="8"></CandidateIdentifier></Candidate><ValidVotes>0
</ValidVotes></Selection><Selection><Candidate><CandidateIdentifier Id="9"
></CandidateIdentifier></Candidate><ValidVotes>0</ValidVotes></Selection><Selection><Candidate><CandidateIdentifier
 Id="10"></CandidateIdentifier></Candidate><ValidVotes>0
```

Hierboven staat de oorspronkelijke situatie: de PVV krijgt in Arnhem 25 stemmen. Na de actie van Trudy krijgt de PVV 10 stemmen erbij ten koste van het CDA:

```
Id="10"><RegisteredName>PVV (Partij voor de Vrijheid)</RegisteredName></AffiliationIdentifier><ValidVotes>35
</ValidVotes></Selection><Selection><Candidate><CandidateIdentifier Id="1"
></CandidateIdentifier></Candidate><ValidVotes>10
</ValidVotes></Selection><Selection><Candidate><CandidateIdentifier Id="2"
></CandidateIdentifier></Candidate><ValidVotes>10
</ValidVotes></Selection><Selection><Candidate><CandidateIdentifier Id="3"
></CandidateIdentifier></Candidate><ValidVotes>5</ValidVotes></Selection><Selection><Candidate><CandidateIdentifier
 Id="4"></CandidateIdentifier></Candidate><ValidVotes>5
</ValidVotes></Selection><Selection><Candidate><CandidateIdentifier Id="5"
></CandidateIdentifier></Candidate><ValidVotes>5</ValidVotes></Selection><Selection><Candidate><CandidateIdentifier
 Id="6"></CandidateIdentifier></Candidate><ValidVotes>0
</ValidVotes></Selection><Selection><Candidate><CandidateIdentifier Id="7"
></CandidateIdentifier></Candidate><ValidVotes>0</ValidVotes></Selection><Selection><Candidate><CandidateIdentifier
```

De door Trudy aangebrachte wijzigingen in het XML-bestand worden opgeslagen. Voor het aangepaste XML-bestand berekent ze met het programma ‘Hashcalc’ een nieuwe hashcode en legt deze hashcode vast in het proces-verbaal, gezamenlijk met de ‘nieuwe’ uitslagen voor het CDA en de PVV. De laatste pagina van het originele proces-verbaal bevat de handtekeningen van de aanwezige leden van het hoofdstembureau. Trudy heeft een vast handschrift en kan daarom de handtekeningen nabootsen en op de laatste pagina schrijven. In een ander geval had Trudy de originele handtekeningen kunnen inscannen en kunnen afdrukken op het gemanipuleerde proces-verbaal.



Figuur 2: Het herberekenen van hashcodes na het vaststellen van de verkiezingsuitslag

3.4.3.7 Resultaat aanvalsprotocol

Bob is medewerker van het centrale stembureau en ontvangt van Trudy het gemanipuleerde XML-bestand dat op de USB stick staat en het vervalste proces-verbaal. Bob opent het programma P4 CSB van OSV en voert het telbestand in wat hij van Trudy ontvangen heeft.

Figuur 3: het inlezen van een gemanipuleerd EML/XML-bestand.

Er wordt gevraagd om een hashcode. Bob voert de hashcode in die hij van Trudy op het proces-verbaal heeft ontvangen en het bestand wordt zonder enige problemen ingelezen. Mocht de hashcode niet overeenkomen, dan zou OSV de melding ‘inlezen mislukt’ moeten afgeven, maar ook dit is nu niet het geval. Op het eerste oog lijkt het manipuleren van de gegevens geslaagd.

1	Christen Democratisch Appèl (CDA)		280	38,9
2	Partij van de Arbeid (P.v.d.A.)		190	26,4
3	VVD		90	12,5
4	SP (Socialistische Partij)		30	4,2
5	ChristenUnie		20	2,8
6	GROENLINKS		10	1,4
7	Staatkundig Gereformeerde Partij (SGP)		20	2,8
8	Democraten 66 (D66)		20	2,8
9	Partij voor de Dieren		25	3,5
10	PVV (Partij voor de Vrijheid)		35	4,9
11	DPS/Groep van Bergen/De Groenen		0	0,0
12	Partij voor Mens en Spirit (MenS)		0	0,0
13	50PLUS		0	0,0
14	Gelderse Centrumdemocraten (Gelderse C.D.)		0	0,0

Figuur 4: de resultaten van het inlezen van het gemanipuleerde XML- bestand met daarin de verkiezingsuitslagen

Het CDA had eerst 290 stemmen, nu zijn dat er 280. De PVV heeft er 10 bij gekregen. In dit voorbeeld is er gekozen voor het CDA en de PVV, dit hadden ook andere partijen kunnen zijn.

3.4.3.7.1 Logbestanden binnen OSV

Elke transactie en de eventuele daarbij behorende hashcode wordt in een logbestand vastgelegd. Zodra er een XML-bestand met daarin verkiezingsuitslagen wordt aangemaakt, wordt ook de bijbehorende hashcode in het logbestand vastgelegd:

- 2011-02-19 14:47:23,241 INFO [de.ivu.wahl.wus.reportgen.ReportGenerator] (osv@0:0:0:0:0:0:0:1) SHA1-HashCode: E0 FE 31 F9 7A A0 EC 85 3B A3 B8 68 AD 7F 4C 23 D1 13 E5 CF

Dit logbestand staat op de server op de lokatie ‘F:\OSV\PS2011\jboss-4.2.3.GA\server\osv\log\server.log.’ Bij verzending van het XML-bestand en het bijbehorende PDF bestand worden ook alle logbestanden op een cd-rom weggeschreven.

3.5 Conclusie en samenvatting

Als verkiezingsuitslagen op hoofdstembureauniveau geteld en ingevoerd zijn in OSV, worden verkiezingsuitslagen vastgesteld. De uitslagen worden binnen OSV vastgelegd in een XML-bestand. De hashcode (sha-1) wordt berekend. Naast het XML-bestand wordt het proces-verbaal met daarop de verkiezingsuitslagen afgedrukt, gezamenlijk met de hashcode van het XML-bestand. Het XML-bestand wordt opgeslagen op een USB-stick en gezamenlijk met het proces-verbaal naar het centraal stembureau gebracht.
Door de beperkte echtheidskenmerken van het proces-verbaal is het mogelijk om het proces-verbaal te manipuleren en te voorzien van een hashcode van een XML-bestand waarvan de uitslagen gemanipuleerd zijn. Van beveiliging van de hashcode is geen sprake. De hashcode wordt niet ondertekend en van opslag op een veilige locatie kan niet gesproken worden, aangezien de hashcode op een proces-verbaal staat wat gemanipuleerd kan worden. Door deze tekortkomingen in de beveiliging is het mogelijk om te frauderen met verkiezingsuitslagen.

4 Risico analyse

In dit hoofdstuk worden de risico's beschreven die invloed kunnen hebben op de integriteit en authenticiteit van vastgelegde verkiezingsuitslagen. Voorafgaand is er een inventarisatie opgemaakt van alle gegevens (inventaris) die beschermd moeten worden. De literatuurstudie, de interviews en de praktijkstudie van OSV vormen een basis voor een inventarisatie van alle bedreigingen die invloed kunnen hebben op de integriteit van vastgelegde verkiezingsuitslagen op processen-verbaal en in OSV.

4.1 Inventaris

In deze paragraaf wordt de inventaris behandeld. De inventaris kan binnen het proces van risicoanalyse ook wel worden gezien als de 'assets': de onderdelen die door kwetsbaarheden en bedreigingen in gevaar komen. Het is van belang dat deze onderdelen door middel van hulpmiddelen (controls) beschermd worden tegen bedreigingen van buitenaf.

4.1.1 Asset 1: Integriteit vastgelegde verkiezingsuitslagen op processen-verbaal

De integriteit van vastgelegde verkiezingsuitslagen op een proces-verbaal moet altijd gewaarborgd worden. Deze integriteit moet bewaakt worden vanaf het moment dat het proces-verbaal is aangemaakt totdat het bij de ontvanger aangekomen en verwerkt is. Het betreft hier de volgende onderdelen:

1. Het verzenden van het proces-verbaal van het lokale stembureau naar het plaatselijk stembureau;
2. Het transport van het proces-verbaal van het plaatselijk stembureau naar het hoofdstembureau;
3. Het transport van het proces-verbaal van het hoofdstembureau naar het centraal stembureau.

4.1.2 Asset 2: Integriteit verkiezingsuitslagen in XML-bestanden

De integriteit van vastgelegde verkiezingsuitslagen in XML-bestanden moet gewaarborgd zijn tijdens transport. Het moet voor kwaadwillenden praktisch onmogelijk zijn vastgelegde verkiezingsuitslagen tijdens transport ongemerkt aan te passen.

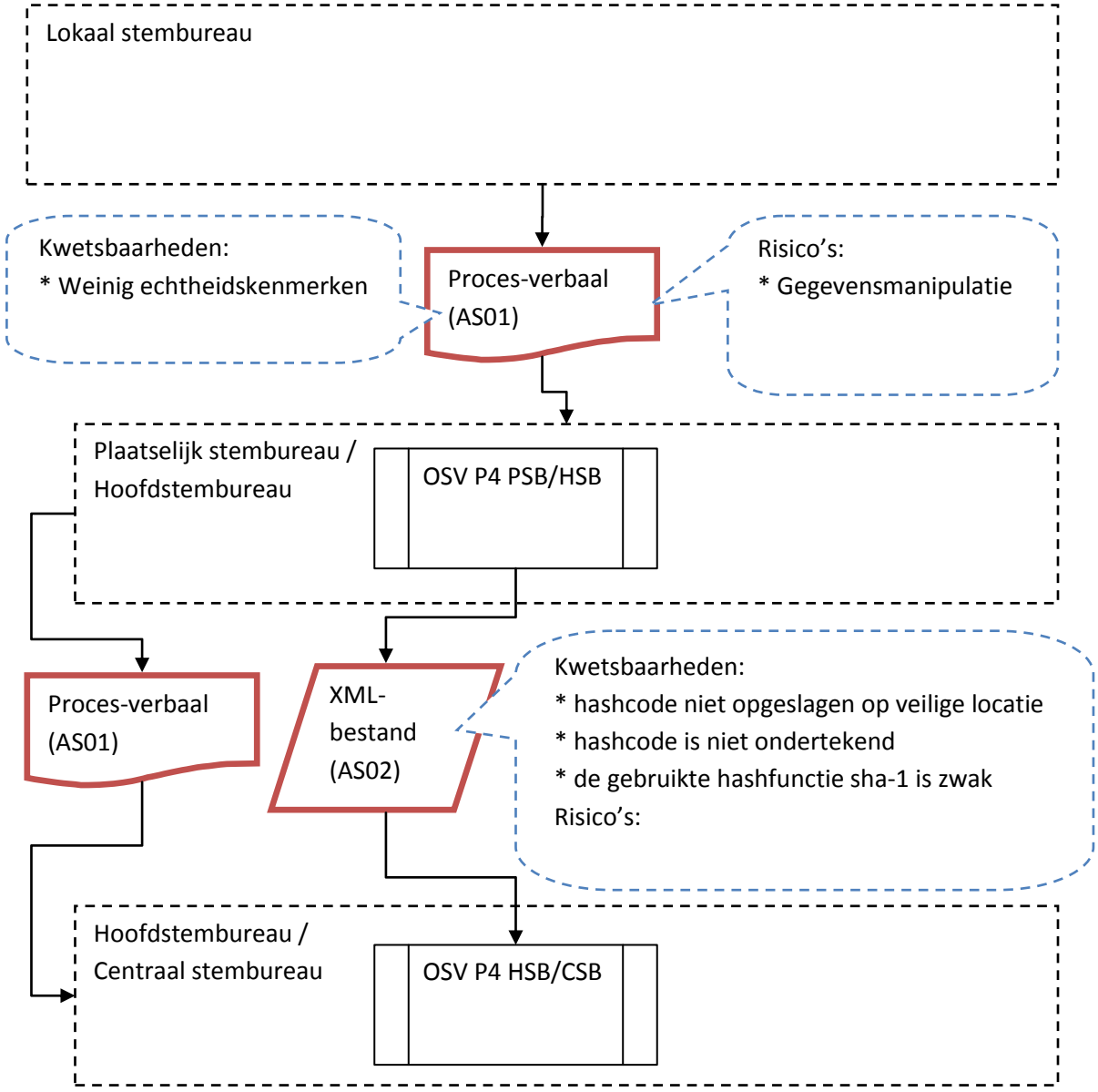


Diagram 9: een schematisch overzicht van een aantal kwetsbaarheden en risico's die zich voordoen bij het gebruik van processen-verbaal en XML-bestanden.

4.2 Gevonden kwetsbaarheden

In dit hoofdstuk worden alle kwetsbaarheden beschreven die een negatieve invloed kunnen hebben op de in hoofdstuk 4.1 'Inventaris' genoemde onderdelen. Alle gevonden kwetsbaarheden zijn vastgelegd naar aanleiding van de waarnemingen, literatuurstudie, interviews en de praktijkstudie van OSV. Elke kwetsbaarheid wordt geïdentificeerd met een nummer. Er wordt per kwetsbaarheid beschreven waar deze kwetsbaarheid betrekking op heeft en op welke mogelijke manier hier misbruik van gemaakt kan worden.

Nummer:	KW01
Titel:	Processen-verbaal bevatten weinig identiteitskenmerken
Omschrijving:	Een proces-verbaal is niet voorzien van een watermerk of andere echtheidskenmerken. De enige aanwezige echtheidskenmerken zijn de handtekeningen van de aanwezige leden van het lokale stembureau. Dit maakt het eenvoudig om het proces-verbaal te kopiëren en te voorzien van valse uitslagen.
Mogelijk misbruik:	Een kwaadwillende kan ook medewerker van het lokale stembureau zijn en tussenliggende pagina's van het proces-verbaal met stemuitslagen vervangen voor pagina's met valse uitslagen.
Heeft betrekking op:	Integriteit verkiezingsuitslagen op proces-verbaal
Geconstateerd bij:	Lokaal stembureau, plaatselijk stembureau, hoofdstembureau en centraal stembureau

Nummer:	KW02
Titel:	Binnen OSV P4 worden hashcodes niet ondertekend en ook niet op een beveiligde locatie opgeslagen.
Omschrijving:	De hashcode van het XML-bestand wordt onderaan op elke pagina van het papieren proces-verbaal geplaatst dat van het hoofdstembureau naar het centrale stembureau wordt gebracht. Deze hashcode kan aangepast worden. Hierdoor is het manipuleren van gegevens eenvoudiger.
Mogelijk misbruik:	Het onderscheppen en doorsturen van hashcodes van gemanipuleerde XML-bestanden door de persoon die deze gegevens transporteert. De verantwoordelijke persoon kan ook omgekocht of bedreigd worden om gegevens af te staan of te manipuleren.
Heeft betrekking op:	Integriteit verkiezingsuitslagen in OSV
Geconstateerd bij:	OSV P4 PSB, OSV P4 HSB, OSV P4 CSB

Nummer:	KW03
Titel:	De (binnen OSV gebruikte) hashfunctie sha-1 is onveilig
Omschrijving:	In [MAR05] worden voorbeelden beschreven waaruit blijkt dat het gebruik van de hashfunctie sha-1 onveilig is: er zijn meerdere 'botsingen' (collisions) gevonden bij het gebruik van sha-1
Mogelijk misbruik:	Het vinden van een 'collisions' is erg ingewikkeld, maar niet onmogelijk. Steeds verder toenemende rekenkracht van processoren kan het vinden van nieuwe 'collisions' wel eenvoudiger maken, wat de hashfunctie sha-1 als authenticatiemethode minder betrouwbaar maakt. Praktijksituatie: Trudy maakt zelf een XML-bestand aan met aangepaste verkiezingsuitslagen dat resulteert in dezelfde hashcode op een authentiek proces-verbaal.
Heeft betrekking op:	Integriteit verkiezingsuitslagen in OSV
Geconstateerd bij:	Alle OSV-onderdelen die gebruik maken van de hashfunctie sha-1.

4.3 Gevonden risico's

In deze paragraaf worden alle risico's beschreven die gedurende het onderzoek zijn geïdentificeerd. De risico's vormen een direct gevaar voor de in hoofdstuk 4.1 (Inventaris) genoemde onderdelen. Per risico wordt vastgesteld hoe groot de impact van een risico is en hoe groot de kans is dat een risico zich voordoet. De schaal bedraagt van 1 tot 5. Als de impact klein is, wordt deze variabele gewaardeerd met een 1. Als de impact hoog is, dan wordt deze variabele gewaardeerd met 5. Ditzelfde geldt voor de kans waarop een risico zich voordoet. Om de ernst van het risico te bepalen worden de waarden van impact en kans met elkaar vermenigvuldigd. Deze waarde wordt vastgelegd in de 'risico-index'. De risico-index wordt onderverdeeld in 3 niveaus: laag, gemiddeld en hoog. De niveaus worden als volgt ingedeeld:

- 1 – 8: laag risico
- 9 – 16: gemiddeld risico
- 17 – 25: hoog risico

Nummer:	RS01
Titel:	Gegevensmanipulatie van een proces-verbaal verzonden door een lokaal stembureau naar het plaatselijk stembureau
Omschrijving:	Mede door de samenstelling van processen-verbaal zijn de gegevens op een proces-verbaal eenvoudig te manipuleren. Dit komt mede doordat de pagina's waar de uitslagen op partijniveau –en op kandidaat-niveau op genoteerd zijn niet voorzien zijn van de handtekeningen van de medewerkers van het stembureau. Dit proces-verbaal is aangemaakt vanuit OSV en geprint op normaal A4-papier. Pagina's waar geen handtekeningen op staan kunnen gekopieerd worden en onderweg naar het hoofdstembureau handmatig worden voorzien van valse uitslagen.

Impact [1..5]	2
Kans [1..5]	2
Risico-index	4 (laag)
Toelichting risico-index	De impact van het manipuleren van een proces-verbaal dat verzonden wordt van een lokaal stembureau naar een hoofdstembureau is relatief klein, omdat er maar met een zeer klein deel van de (landelijke) verkiezingsuitslagen gemanipuleerd wordt. Als er bijvoorbeeld in heel Nederland 500 stemlokalen zijn en er wordt gefraudeerd met één proces-verbaal, is maar met ongeveer 1/500ste deel van de stemmen gefraudeerd.
Bijbehorende kwetsbaarheden:	KW01

Nummer:	**RS02**
Titel:	Gegevensmanipulatie van een proces-verbaal verzonden door een plaatselijk stembureau naar het hoofdstembureau en van het hoofdstembureau naar het centraal stembureau
Omschrijving:	Mede door de samenstelling van processen-verbaal zijn de gegevens op een proces-verbaal eenvoudig te manipuleren. Dit komt mede doordat de pagina's waar de uitslagen op partijniveau –en op kandidaat-niveau op genoteerd zijn niet voorzien zijn van de handtekeningen van de medewerkers van het stembureau. Dit proces-verbaal is aangemaakt vanuit OSV en geprint op normaal A4-papier. Pagina's waar geen handtekeningen op staan kunnen gekopieerd worden en onderweg naar het centraal stembureau handmatig worden voorzien van valse uitslagen en valse hashcodes.
Impact [1..5]	5
Kans [1..5]	2
Risico-index	10 (gemiddeld)
Toelichting risico-index	De impact van het manipuleren van een proces-verbaal dat verzonden wordt van een plaatselijk stembureau of een hoofdstembureau naar een centraal stembureau is aanzienlijk groter omdat er op hoofdstembureauniveau veel meer stemmen bij elkaar opgeteld zijn. Als er bijvoorbeeld in heel Nederland 12 hoofdstembureaus zijn en er wordt gefraudeerd met één proces-verbaal, is met ongeveer 1/12ste deel van de stemmen gefraudeerd. Het is niet geheel uit te sluiten dat het mogelijk is om te manipuleren met een proces-verbaal. De Kiesraad geeft aan dat XML-bestanden en processen-verbaal in de meeste gevallen door een medewerker van een hoofdstembureau verzonden worden, maar dat het daarnaast mogelijk is dat dit transport uitgevoerd wordt door een externe persoon of organisatie.
Bijbehorende kwetsbaarheden:	KW01

Nummer:	RS03
Titel:	Gegevensmanipulatie van het XML-bestand dat door het hoofdstembureau vervoerd is naar het centrale stembureau
Omschrijving:	XML-bestanden kunnen op een eenvoudige manier aangepast worden in een tekstverwerker. De kwaadwillende kan de nieuwe hashcode eenvoudig bereken doordat de hashcode onvoldoende beveiligd is.
Impact [1..5]	3
Kans [1..5]	3
Risico-index	9 (gemiddeld)
Toelichting risico-index	De verkiezingsuitslagen op het papieren proces-verbaal zijn leidend. Daardoor is de impact van een gemanipuleerd XML-bestand lager gewaardeerd dan de manipulatie van het proces-verbaal. De kans is hoger gewaardeerd; dit ligt aan de mate van eenvoud van manipulatie van het XML-bestand.
Bijbehorende kwetsbaarheden:	KW02, KW03

4.4 Conclusie

Er doen zich op dit moment geen grote risico's voor op het gebied van manipulatie van verkiezingsuitslagen op processen-verbaal en in OSV. Tot op heden zijn er geen gevallen van fraude bekend met processen-verbaal en OSV, maar deze informatie zegt niets over wat er in de toekomst kan gebeuren. Verkiezingsfraude is in veel landen helaas een normale zaak. Ook in Nederland is er in het verleden gefraudeerd met het vastleggen van stemmen door een medewerker van een lokaal stembureau die tevens verkozen kon worden. [15] Het is van belang om het voor kwaadwillenden zo moeilijk mogelijk te maken om te frauderen met verkiezingsuitslagen.

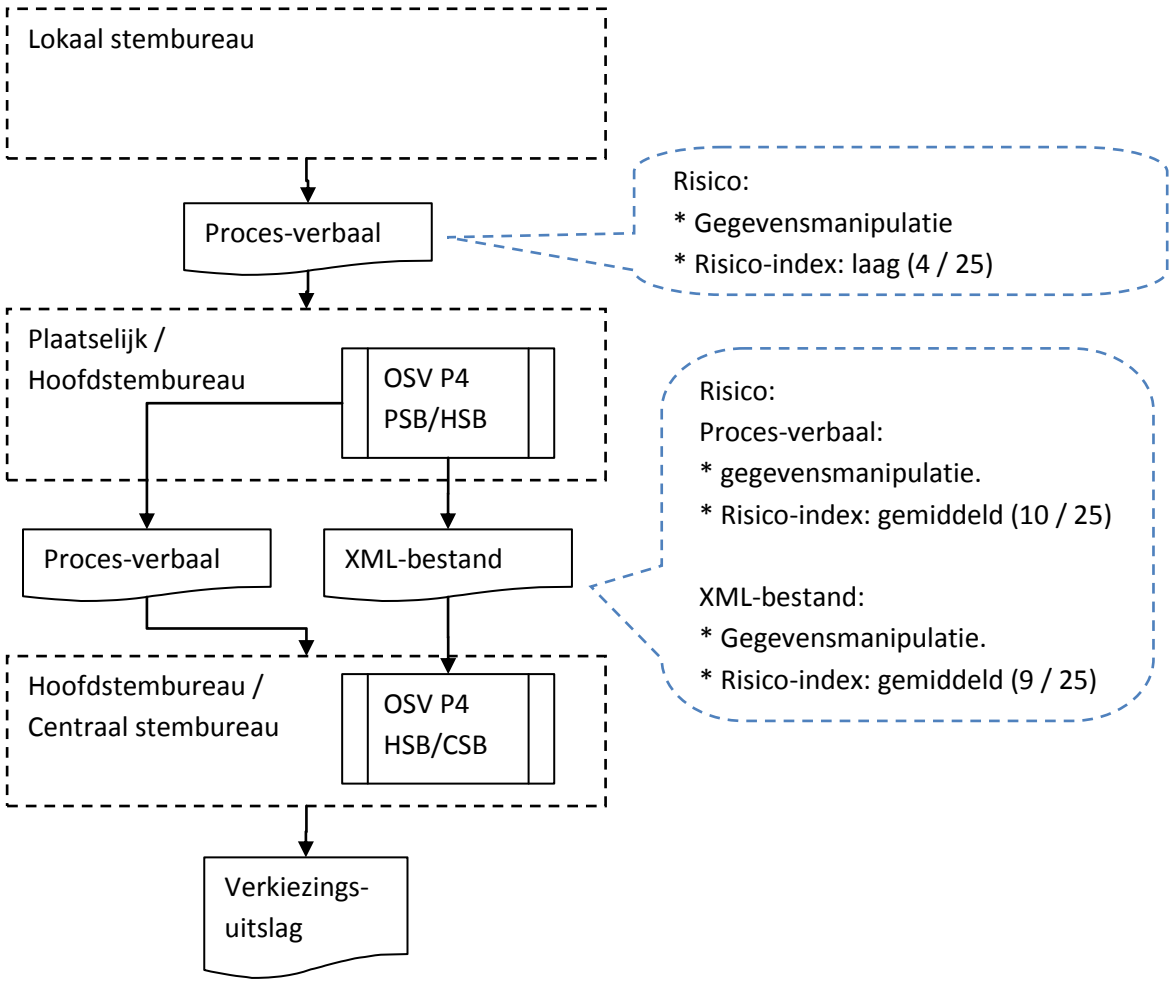
[15] http://www.bof.nl/nieuwsbrief/nieuwsbrief_2006_14.html

5 Methoden voor risicobeheersing

In dit hoofdstuk staat beschreven welke methoden en middelen er beschikbaar zijn om de vastgestelde risico's te beheersen. De focusgebieden van de aanpak van de risico's ligt voor het grootste gedeelte bij de communicatie tussen het plaatselijk stembureau, het hoofdstembureau en het centrale stembureau. De in hoofdstuk 4 (Risico analyse) beschreven risico's hebben wat betreft het gebruik van het proces-verbaal dat wordt verstuurd van het plaatselijk stembureau naar het hoofdstembureau en van het hoofdstembureau naar het centrale stembureau een risico-index van 10 (maximaal 25) gekregen, waardoor dit risico als 'gemiddeld' beschouwd kan worden. Hetzelfde geldt voor het gebruik van XML-bestanden waarbij de hashcode onvoldoende beveiligd is.
Voor de toekomstige implementatie van deze methoden en middelen is rekening gehouden met de kosten, de impact en de uitvoerbaarheid. Per risico worden meerdere mogelijkheden genoemd om het risico beheersbaar te houden. In alle gevallen is rekening gehouden met de volgende uitgangspunten:

- Het transparante karakter van het verkiezingsproces moet gewaarborgd blijven;
- Het vervoeren van verkiezingsuitslagen moet uitvoerbaar blijven;
- Integriteit en authenticiteit van gegevens moet gewaarborgd blijven.

Van confidentialiteit van gegevens is geen sprake: verkiezingsuitslagen zijn openbaar en moeten door iedereen raadpleegbaar zijn.



5.1 Afwegingen

Vastgelegde verkiezingsuitslagen moeten transparant van karakter zijn: uitslagen zijn openbaar en moeten zonder drempels te raadplegen zijn. Vanuit dit oogpunt lijkt het voor kwaadwillenden eenvoudig om gegevens te manipuleren, aangezien van volledige versleuteling van vastgelegde verkiezingsuitslagen geen sprake mag zijn. Daarom wordt er in alle gevallen voor gekozen om de nadruk te leggen op detectie van manipulatie. Daarnaast wordt er voor gekozen om in een aantal situaties voor aanpassingen te kiezen die het manipuleren van verkiezingsuitslagen op processen-verbaal moeilijker maken.
Om de integriteit van vastgelegde verkiezingsuitslagen te waarborgen, worden meerdere mogelijkheden aangeboden om fraude op te merken en fraude praktisch onmogelijk te maken. Het is aan de Kiesraad om een keuze te maken uit de beschreven middelen en methoden om de integriteit van vastgelegde verkiezingsuitslagen te waarborgen.

5.2 Focusgebieden

5.2.1 Verkiezingsuitslagen op processen-verbaal

Uit hoofdstuk 3.1 (Bevindingen bij het lokale stembureau) en hoofdstuk 3.2 (Bevindingen bij het hoofdstembureau) is gebleken dat er weinig veranderingen hebben plaatsgevonden op het gebied van processen-verbaal toen duidelijk was geworden dat stemmachines geen recht deden aan o.a. de transparantie van het verkiezingsproces. Medewerkers van het hoofdstembureau gaan ervan uit dat gegevens op het proces-verbaal op een integere wijze worden behandeld. Tot op heden zijn er geen gevallen van integriteitsfraude met processen-verbaal bekend, maar deze informatie geeft geen garanties voor komende verkiezingen wat betreft gegevensmanipulatie. Doordat een proces-verbaal weinig echtheidskenmerken bevat, kunnen personen of groeperingen mogelijk acties ondernemen om uitslagen op processen-verbaal te manipuleren.
De risico's op het gebied van manipulatie van verkiezingsuitslagen op processen-verbaal zijn klein. Ondanks het relatief kleine risico op gegevensmanipulatie moeten er maatregelen genomen worden om het praktisch onmogelijk te maken om in de toekomst te frauderen met verkiezingsuitslagen. Op het gebied van gegevensbeveiliging zal er gekeken moeten worden naar een juiste balans tussen kosten en baten. Een aantal eenvoudige aanpassingen van het proces-verbaal kunnen een bijdrage leveren om manipulatie van verkiezingsuitslagen moeilijker of zelfs praktisch onmogelijk te maken.

5.2.2 Verkiezingsuitslagen in OSV

De praktijkstudie van OSV zoals beschreven is in hoofdstuk 3.4.3 heeft aangetoond dat het relatief eenvoudig is om XML-bestanden die aangemaakt zijn in OSV te manipuleren. Het is tevens eenvoudig om van het gemanipuleerde XML-bestand een nieuwe hashcode te berekenen. In combinatie met beperkte echtheidskenmerken op het proces-verbaal is het mogelijk om opnieuw het proces-verbaal inclusief de (vooraf ingescande of nageschreven) handtekeningen af te drukken en op deze manier de hashcode van het gemanipuleerde XML-bestand door te sturen naar het centrale stembureau.
De beveiliging van te transporteren verkiezingsuitslagen tussen onderdelen van OSV is anno 2011 gebaseerd op de hashcode. Het gebruik van enkel de hashcode is onvoldoende om de authenticiteit van verkiezingsuitslagen te garanderen. Daarbij geldt ook dat het algoritme sha-1 gekraakt is [MAR05] en dat hashfunctie sha-1 daardoor als onvoldoende betrouwbaar beschouwd kan worden.

5.2.2.1 Beveiliging hashcodes

De hashcodes van vastgelegde verkiezingsuitslagen dienen beter beveiligd te worden. Men kan er ook voor kiezen om alle vastgelegde verkiezingsuitslagen in XML-bestanden voor het verzenden naar het centraal stembureau volledig te versleutelen met een persoonlijke sleutel, maar hierdoor kan de transparantie van het verkiezingsproces in het geding komen. Daarom moet de focus van de

authenticiteit van verkiezingsuitslagen worden gelegd op detectie: het moet voor de ontvanger van de XML-bestanden waarneembaar zijn dat er tussentijds een nieuwe hashcode is berekend.

5.2.2.2 Het gebruik van de hashfunctie sha-1

Onderzoek volgens [MAR]05 heeft aangetoond dat er zwaktes gevonden zijn in de hashfunctie sha-1. Tot op heden zijn er relatief weinig botsingen gevonden binnen sha-1. Men kan spreken van een botsing als voor 'document A' een 'document B' gevonden kan worden die beide resulteren in dezelfde hashcode. Om een volledig veilige hashfunctie binnen OSV te gebruiken, is het aan te raden om een betere hashfunctie als sha-512 te gaan gebruiken, waarbij anno 2011 geen problemen gevonden zijn.

5.3 Van lokaal stembureau naar plaatselijk stembureau: processen-verbaal

De voorstudie heeft aangetoond dat het manipuleren van processen-verbaal door de persoon die deze processen-verbaal verstuurt eenvoudig is. Het proces-verbaal wordt ondertekend door alle aanwezige leden. Deze handtekeningen staan alleen op de eerste en laatste pagina van het proces-verbaal, wat de manipulatie van tussenliggende pagina's eenvoudiger kan maken. In de subparagraaf hieronder staan een aantal maatregelen die ervoor zorgen dat het manipuleren van verkiezingsuitslagen moeilijker maakt.

5.3.1 Stappenplan verbetering echtheidskenmerken proces-verbaal

Hieronder staan een aantal mogelijkheden beschreven die bijdragen aan verbeterde echtheidskenmerken van een proces-verbaal. Deze mogelijkheden kunnen afzonderlijk geïmplementeerd worden, maar een implementatie van meerdere maatregelen tegelijkertijd maakt het voor een kwaadwillende steeds moeilijker om te frauderen met vastgelegde verkiezingsuitslagen.

1. Voorzie elke pagina van het proces-verbaal van echtheidskenmerken zoals een watermerk.
2. Voorzie elke pagina van het proces-verbaal van een paar handtekeningen van medewerkers van het lokale stembureau.
3. Hecht alle pagina's aan elkaar vast met een nietmachine zodat het makkelijker op te merken is pagina's uitgescheurd zijn.

5.4 Van plaatselijk stembureau naar centraal stembureau: processen-verbaal en vastgelegde verkiezingsuitslagen in OSV

Uit de praktijkstudie van OSV is gebleken dat vastgelegde verkiezingsuitslagen binnen de XML-bestanden en binnen de PDF-bestanden (processen-verbaal) te manipuleren zijn. Door de hashcode van het gemanipuleerde bestand opnieuw te berekenen, merkt OSV de wijzigingen niet op en schiet de hashcode zijn doel als authenticatiemethode voorbij. Het moet voor de ontvanger van het XML-bestand mogelijk zijn om manipulatie op te merken. Dit hoofdstuk heeft betrekking op de processen-verbaal en het XML-bestand met verkiezingsuitslagen die verstuurd worden van het plaatselijk stembureau naar het hoofdstembureau en van het hoofdstembureau naar het centraal stembureau.

5.4.1 Ondertekende hashcodes

Het is voor een kwaadwillende eenvoudig om van elk stuk informatie een hashcode te berekenen. Daarom is het noodzakelijk dat er iets gedaan wordt aan de beveiliging van de hashcode: de hashcode moet ondertekend worden of men moet de hashcode apart (via een beveiligd kanaal) verzenden. Het is voor een fraudeur, mits de methode van ondertekende hashcodes op een correcte wijze wordt toegepast, praktisch onmogelijk om een ondertekende hashcode te berekenen. Om hashcodes te onderteken wordt asymmetrische cryptografie gebruikt.
Asymmetrische cryptografie zorgt er onder andere voor dat men ondertekende hashcodes kan controleren op authenticiteit. Een ondertekende hashcode kan iets vertellen over de inhoud van de bijbehorende gegevens en over degene die de hashcode ondertekend heeft. Hiervoor moeten sleutelcombinaties worden aangemaakt: een persoonlijke sleutel en een bijbehorende openbare sleutel.

5.4.1.1 Persoonlijke sleutel

Een persoonlijke sleutel wordt gebruikt om de hashcode te ondertekenen. De persoonlijke sleutel is alleen bekend bij de persoon die een hashcode wil ondertekenen. Verder is er niemand die kennis heeft van deze persoonlijke sleutel. Persoonlijke sleutels kunnen op meerdere manier worden vastgelegd:

1. Op een smartcard: in dit geval is de persoonlijke sleutel opgeslagen op een smartcard die in bezit is van de eigenaar van de persoonlijke sleutel. Om toegang tot de persoonlijke sleutel te krijgen, moet de eigenaar eerst een pincode invoeren om de persoonlijke sleutel op de smartcard te kunnen gebruiken.

2. In de computer. Er kan gekozen worden om de persoonlijke sleutel op een beveiligde locatie in de computer van de eigenaar op te slaan. De persoonlijke sleutel is dan alleen toegankelijk via een additioneel wachtwoord.

Hashcodes die zijn ondertekend met de persoonlijke sleutel kunnen alleen gecontroleerd worden met de bijbehorende openbare sleutel van dezelfde persoon.

5.4.1.2 Openbare sleutel

De openbare sleutel van een persoon is openbaar en voor iedereen toegankelijk. Deze openbare sleutel kan gebruikt worden om berichten voor de betreffende eigenaar van de openbare sleutel te versleutelen en om met de persoonlijke sleutel ondertekende hashcodes te verifiëren. De openbare sleutel is te raadplegen bij een CA, wat staat voor Certificate Authority.

1. Openbare sleutels kunnen gebruikt worden om ondertekende hashcodes te controleren op integriteit en herkomst.

2. De openbare sleutel is door iedereen op te vragen.

5.4.1.3 Maatregelen

Als men er voor kiest om verkiezingsuitslagen te beveiligen met asymmetrische cryptografie, is het binnen OSV noodzakelijk om hashcodes van XML-bestanden met daarin verkiezingsuitslagen te ondertekenen met een persoonlijke sleutel. De sleutelcombinaties moeten aangemaakt worden door de Kiesraad. De Kiesraad treedt hier op als CA. De openbare sleutel blijft voor de Kiesraad beschikbaar, terwijl de persoonlijke sleutel aan een verantwoordelijk persoon wordt meegegeven om hashcodes van verkiezingsuitslagen te ondertekenen. Daarnaast publiceert de Kiesraad de openbare

sleutels op een website zodat deze openbare sleutels publiekelijk toegankelijk zijn. Dit proces gaat als volgt:

1. De Kiesraad maakt voor elke verantwoordelijke medewerker van een plaatselijk en/of hoofdstembureau een sleutelcombinatie aan. Deze sleutelcombinatie bestaat uit een persoonlijke sleutel en een bijbehorende openbare sleutel. De persoonlijke sleutel wordt opgeslagen op een cd-rom.

2. De verantwoordelijke medewerker van het plaatselijk/hoofdstembureau komt de cd-rom met daarop de persoonlijke sleutel onder vertoon van een identiteitsbewijs persoonlijk ophalen bij de Kiesraad.

3. De eigenaar van de persoonlijke sleutel dient ervoor te zorgen dat deze cd-rom met de persoonlijke sleutel in zijn bezit blijft. Niemand anders hoort te weten te komen welke persoonlijke sleutel op deze cd-rom staat.

4. Na het invoeren van verkiezingsuitslagen in OSV en voor het verzenden van de XML-bestanden met daarin de verkiezingsuitslagen naar het bovenliggende stembureau, dient de verantwoordelijke persoon de hashcode van het XML-bestand ondertekenen met de persoonlijke sleutel die op de cd-rom staat.

5. De ondertekende hashcode wordt onderaan elke pagina van het proces-verbaal geplaatst, net zoals eerder het geval was met de niet-ondertekende hashcode.

6. Het proces-verbaal met de ondertekende hashcode van het XML-bestand wordt op papier afgedrukt en op de gebruikelijke manier voorzien van de handtekeningen van de aanwezige leden. Tevens wordt het proces-verbaal (in PDF-formaat) met de ondertekende hashcode van het XML-bestand opgeslagen op de USB-stick.

7. Het XML-bestand met daarin de verkiezingsuitslagen, inclusief het proces-verbaal met de ondertekende hashcode in PDF-formaat op de USB-stick en het papieren proces-verbaal worden op de gebruikelijke wijze verzonden naar het bovenliggende stembureau.

8. Onmiddellijk na het verzenden van het XML-bestand en het proces-verbaal vernietigd de eigenaar van de persoonlijke sleutel de cd-rom door de cd-rom in stukken te breken. Hierdoor wordt de persoonlijke sleutel vernietigd om misbruik in een later stadium te voorkomen.

9. Bij ontvangst van het XML-bestand en het proces-verbaal op de USB-stick en het afgedrukte proces-verbaal wordt er door een medewerker op het centrale stembureau een hashcode van het XML-bestand berekend.

10. De medewerker verifieert de ondertekende hashcode zoals deze op het proces-verbaal staat met de openbare sleutel van de verantwoordelijke persoon. Deze openbare sleutel is in bezit van de Kiesraad zelf en kan daar ook opgevraagd worden in geval van verkiezingen waarbij het centrale stembureau niet in Den Haag gevestigd is. In dat geval kan de Kiesraad de openbare sleutels op de website plaatsen.

11. De ontvanger vergelijkt de verifieerde hashcode met de hashcode die berekend is van het XML-bestand. Als beide hashcodes overeenkomen, dan is de inhoud van het XML-bestand authentiek.

5.4.1.4 Praktijkvoorbeeld: aanmaken sleutelcombinaties

Sleutelcombinaties kunnen aangemaakt worden met behulp van RSA [16]. Dit proces gaat als volgt:

Symbool	Beschrijving	Waarde in decimale getallen
P	Kies een willekeurig priemgetal met een minimale lengte van 512 bits. Noem dit getal P. In deze tabel worden kleinere getallen gebruikt om het rekenvoorbeeld overzichtelijk te houden.	P=223
Q	Kies een willekeurig priemgetal met een minimale lengte van 512 bits. Noem dit getal Q. Dit priemgetal mag niet gelijk zijn aan P.	Q=277
N	Bereken de modulus N voor zowel de persoonlijke sleutel als de openbare sleutel. N = P*Q	N=61771
PHI(N)	Bereken Euler's phi (N). [17] Phi(N) = (P-1) * (Q – 1)	Phi(N)= 61272
E	Kies een getal E dat co-priem[18] is aan Phi(n). Dat betekent dat de grootste gemene deler van E en phi(N) 1 is. Dit getal is de openbare sleutel.	E=5
D	Bereken de persoonlijke sleutel D: $D – E^{-1}$ mod phi(N)	D=24509

Tabel 11: het aanmaken van sleutelcombinaties

[16] http://en.wikipedia.org/wiki/RSA

[17] http://en.wikipedia.org/wiki/Euler_phi_function

[18] http://en.wikipedia.org/wiki/Coprime

5.4.1.4.1 Rekenvoorbeeld: een hashcode ondertekenen

Om een hashcode te ondertekenen wordt de persoonlijke sleutel gebruikt. In dit voorbeeld is de tekst van de hashcode vervangen door de tekst 'Kiesraad' om het overzicht te behouden. Voor het ondertekenen van de hashcode wordt de volgende berekening gebruikt:

$Sign^{Alice} = M^{D} \bmod N$

Legenda:

Symbool	**Uitleg**
SignAlice	De hashcode die ondertekend is door Alice
M	De hashcode die ondertekend moet worden
D	De persoonlijke sleutel van Alice
N	Zie Tabel 11: het aanmaken van sleutelcombinaties

Ondertekenen

Omschrijving / actie	**Gegevens**	**Uitleg**
Bericht	Kiesraad	In een normale situatie wordt de hashcode ondertekend. Voor de duidelijkheid is de hashcode veranderd in 'Kiesraad'.
Bericht omzetten naar decimale getallen volgens een ASCII-tabel	75 105 101 115 114 97 97 100	Elk karakter in de hashcode wordt omgezet naar ASCII.[19] De 'A' staat voor '65', de B voor '66', etc
Decimale getallen omzetten naar binaire getallen volgens een ASCII-tabel.	01001011 01101001 01100101 01110011 01110010 01100001 01100001 01100100	
Binaire getallen verdelen in message-blokken. Hiermee worden 16-bits blokken gegenereerd.	0100101101101001 0110010101110011 0111001001100001 0110000101100100	
Omzetten 16-bits binaire blokken in decimale blokken	19305 25971 29281 24932	

[19] http://cisnet.baruch.cuny.edu/holowczak/classes/9444/rsademo/ascii.html

Elk decimaal blok versleutelen d.m.v. blok^{D} mod N.	36116 58398 34597 37151	
Versleutelde tekst omzetten via ASCII naar Ciphertext	$:'";%[20]	Dit is de digitaal ondertekende hashcode. Deze digitaal ondertekende hashcode kan via een onbeveiligd kanaal verzonden worden naar het Centrale stembureau

5.4.1.4.2 Rekenvoorbeeld: een ondertekende hashcode verifiëren

In het onderstaande voorbeeld ontvangt Bob (medewerker van het centrale stembureau) de digitaal ondertekende hashcode van Alice. Het verifiëren van de ondertekende hashcode gaat als volgt:

$Sign^{Alice} = M^{E} \bmod N$

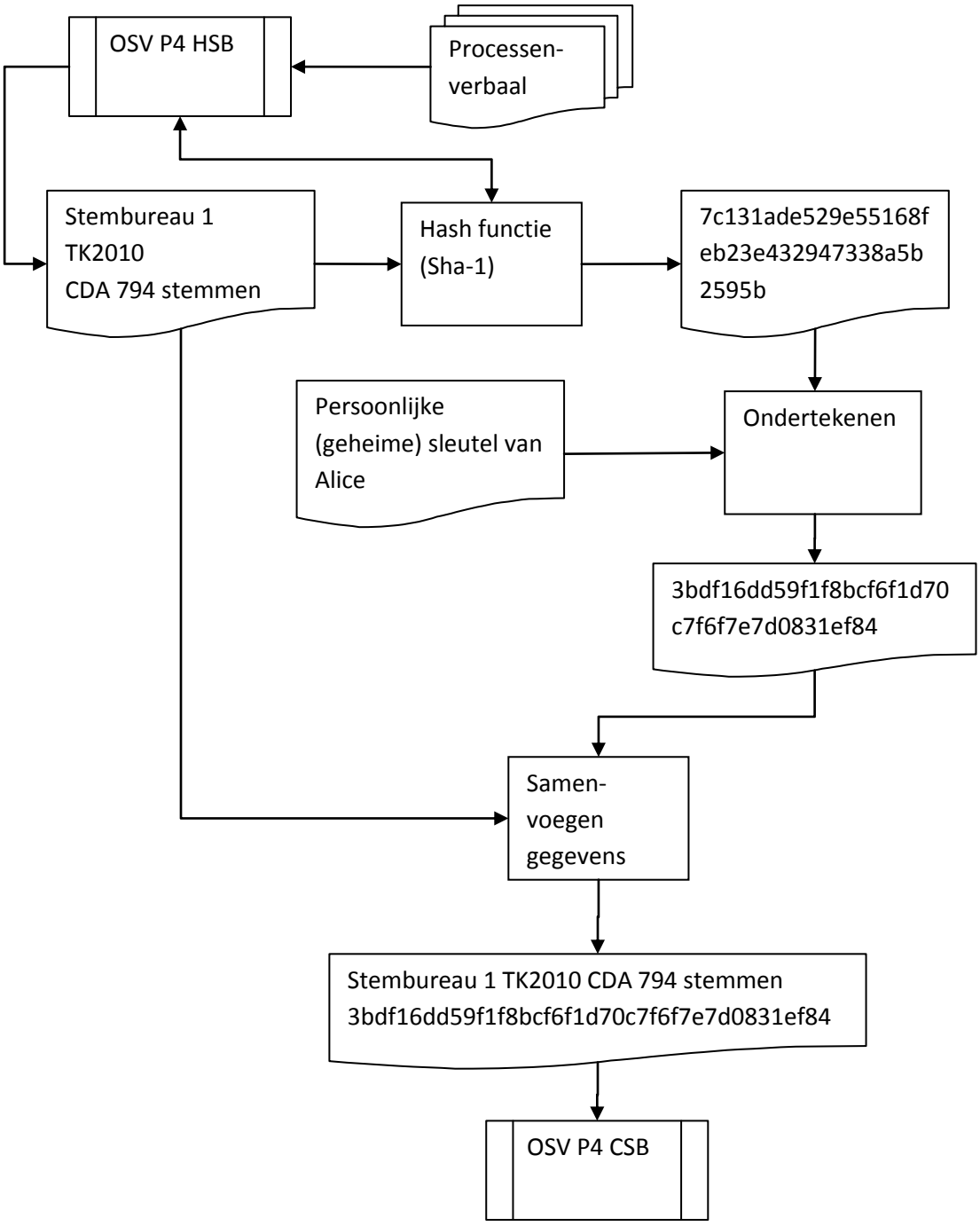
De onderstaande tabel beschrijft in omgekeerde volgorde de werking van het ondertekenen van hashcodes. Voor het verificatieproces wordt de publieke sleutel E gebruikt.

Omschrijving / actie	**Gegevens**	**Uitleg**
Bericht	$:'";%	Dit is de digitaal ondertekende hashcode die Bob, gezamenlijk met het XML-bestand van Alice heeft ontvangen.
Versleutelde cipher omzetten naar decimale blokken	36116 58398 34597 37151	Deze actie is nodig om de ciphertext te kunnen ontsleutelen.
Ontsleutelen: blok^{E} mod N	19305 25971 29281 24932	
Ontsleutelde decimale blokken omzetten in Binaire 16-bits blokken	0100101101101001 0110010101110011 0111001001100001 0110000101100100	
16-bits binaire message-blokken verdelen in 8-bits blokken	01001011 01101001 01100101 01110011 01110010 01100001 01100001 01100100	
8-bits binaire blokken omzetten naar ASCII	75 105 101 115 114 97 97 100	
ASCII-tekst omzetten naar leesbare plaintext	Kiesraad	

[20] Deze symbolen refereren volgens een ASCII-tabel aan de versleutelde 16-bits blokken. Niet alle versleutelde tekens zijn hier weergegeven, omdat veel ASCII-symbolen op elkaar lijken.

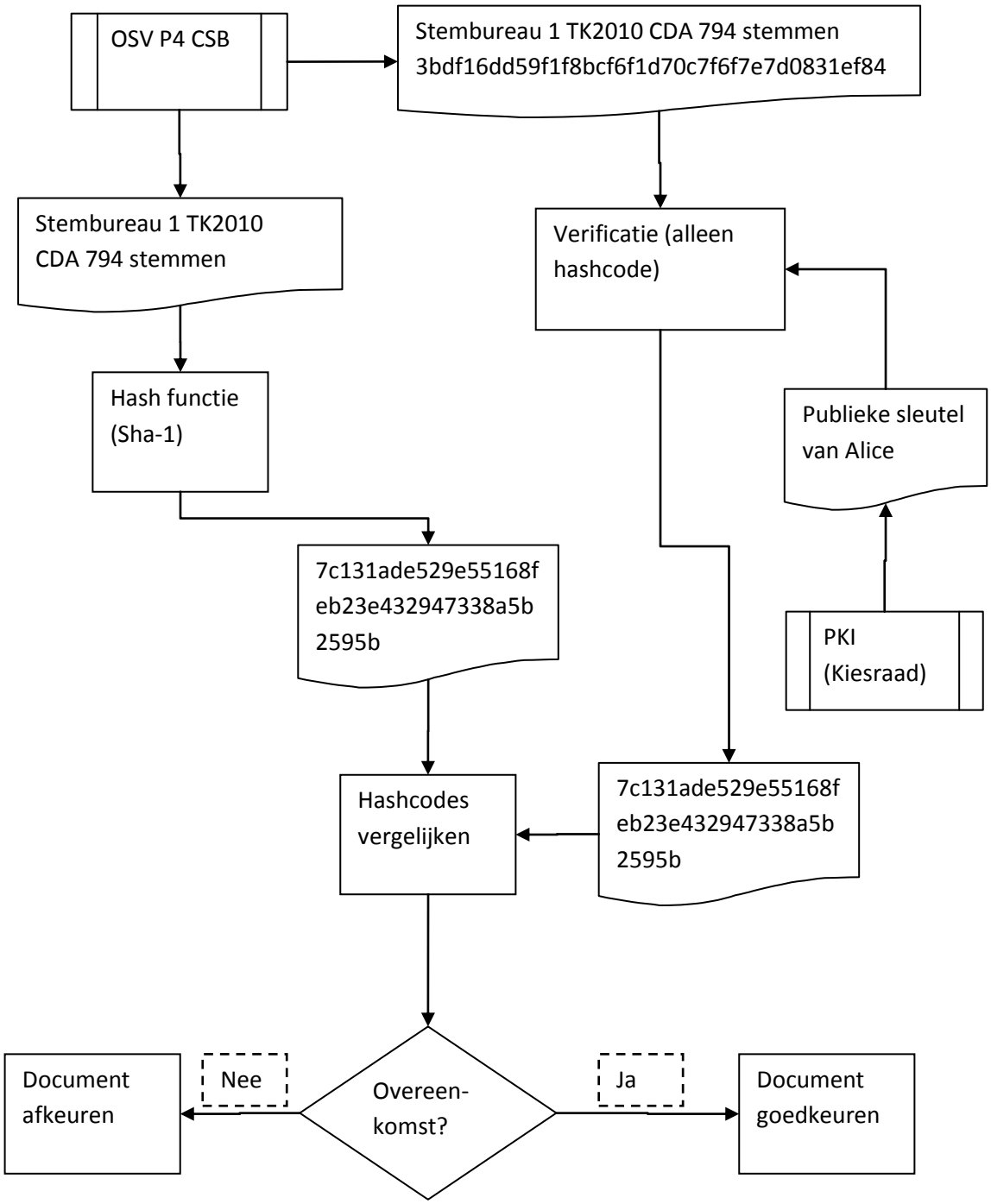
5.4.1.5 Schema: het ondertekenen van hashcodes

Het onderstaande diagram geeft schematisch weer hoe hashcodes ondertekend worden.



5.4.1.6 Schema: het verifiëren van hashcodes

Het onderstaande schema geeft weer hoe ondertekende hashcodes verifieert kunnen worden op authenticiteit.



5.4.1.7 Praktijksituatie

Hieronder staat een protocol waarin Trudy probeert om XML-bestanden met daarin verkiezingsuitslagen te manipuleren. Dit voorbeeld zal aantonen dat de pogingen van Trudy om gegevens te manipuleren niet zullen slagen. De bestanden zijn voorzien van een ondertekende hashcode.

1	Alice	Verkiezingsuitslag.xml Proces-verbaal + $Sign_{Alice}$(sha1(verkiezingsuitslag.xml))	Trudy
2	Trudy	Proces-verbaal + $Sign_{Trudy}$ (sha1(verkiezingsuitslag_vervalst.xml))	Bob

Protocol 3: de poging van Trudy om de frauderen met verkiezingsuitslagen mislukt.

In het bovenstaande protocol is Alice medewerkster van een hoofdstembureau. Bob is medewerker van het centrale stembureau. Alice heeft de verkiezingsuitslag in OSV P4 HSB vastgelegd en een ondertekende hashcode op het proces-verbaal geplaatst. Ze stuurt het afgedrukte proces-verbaal met de ondertekende hashcode, inclusief een digitale versie van het proces-verbaal en het XML-bestand op de USB-stick naar Bob.
In het bovenstaande protocol onderschept de kwaadwillende Trudy het afgedrukte proces-verbaal en de USB-stick. (zie regel 1). Het is voor Trudy nog steeds mogelijk om met een tekstverwerker verkiezingsuitslagen in het XML-bestand aan te passen. Maar nu staat ze voor de uitdaging om een ondertekende hashcode te berekenen. Trudy weet dat de verkiezingsuitslagen afkomstig zijn van Alice en dat Bob de ontvanger van de verkiezingsuitslagen is. Om een ondertekende hashcode te berekenen, heeft Trudy de persoonlijke sleutel van Alice nodig. Trudy kan onmogelijk deze persoonlijke sleutel van Alice achterhalen, aangezien Alice de cd-rom met daarop de persoonlijke sleutel heeft vernietigd. Trudy kan wel een niet-ondertekende hashcode berekenen van een vervalst XML-bestand, maar Bob accepteert alleen ondertekende hashcodes die zijn ondertekend met de persoonlijke sleutel van Alice.
Trudy besluit om de berekende hashcode van het vervalste XML-bestand te ondertekenen met haar eigen persoonlijke sleutel: $Sign_{Trudy}$ (sha1(verkiezingsuitslag.xml)). Zodra Trudy de vervalste verkiezingsuitslag naar Bob wil sturen in regel 2, gaat het fout. Bob weet dat de uitslagen door Alice verzonden zijn. Bob berekent zelf een hashcode van het XML-bestand. Vervolgens gebruikt Bob de openbare sleutel van Alice om de door Trudy ondertekende hashcode te verifiëren. De beide hashcodes komen niet overeen, en Bob besluit om direct contact op te nemen met de politie.

5.4.2 Het faxen van het proces-verbaal met de hashcode

Gedurende het onderzoek is gebleken dat het proces-verbaal wat in de huidige vorm gebruikt wordt om verkiezingsuitslagen te versturen naar een bovenliggend stembureau kwetsbaar is voor fraude. Door de beperkte echtheidskenmerken kunnen gegevens zoals uitslagen en de hashcode tussentijds aangepast worden.
Een alternatieve methode om fraude tegen te gaan is het faxen van het proces-verbaal naar een bovenliggend stembureau. Het faxen van een proces-verbaal heeft met name betrekking op processen-verbaal die verstuurd worden van het plaatselijk stembureau naar het hoofdstembureau en van het hoofdstembureau naar het centrale stembureau. Faxapparaten zijn veel gebruikte communicatiemiddelen om documenten op een veilige wijze te versturen. Het is voor een kwaadwillende moeilijk om een te faxen proces-verbaal te onderscheppen. De kwaadwillende kan ervoor kiezen om de fax voor het verzenden of na het ontvangen van de fax te manipuleren. Beide

faxmachines staan in gemeentelijke, hoofd –en centrale stembureaus. Zodra een proces-verbaal door de aanwezige leden van het hoofdstembureau ondertekend is, kan het proces-verbaal direct gefaxt worden naar bijvoorbeeld het centrale stembureau. Het is voor een kwaadwillende in een dergelijke situatie praktisch onmogelijk om het proces-verbaal tussentijds nog onopgemerkt te manipuleren. Een andere mogelijkheid bij het faxen van het proces-verbaal is dat de verzender per ongeluk een verkeerd faxnummer invoert, waardoor het gefaxte proces-verbaal op een andere plaats terechtkomt. De gegevens op het proces-verbaal zijn niet geheim. Het heeft geen grote impact als een gefaxt proces-verbaal op een verkeerde plaats terechtkomt.

5.4.2.1 Stappenplan

Hieronder staat stap voor stap beschreven wat de procedures zijn om een proces-verbaal op een veilige wijze via een faxapparaat bij een bovenliggend stembureau af te leveren.

1. Het proces-verbaal met de hashcode wordt afgedrukt en door de aanwezige leden van het (hoofd)stembureau op de gebruikelijke wijze ondertekend.
2. Het (ondertekende) papieren proces-verbaal met de hashcode wordt gefaxt naar het bovenliggende stembureau.
3. Zodra de fax binnengekomen is bij het bovenliggende stembureau, geeft een medewerker van het bovenliggende stembureau telefonisch een ontvangstbericht door aan het (hoofd)stembureau. Als de fax niet is aangekomen, kan men ervoor kiezen het proces-verbaal nogmaals te faxen.
4. Het originele ondertekende proces-verbaal met de niet-ondertekende hashcode en het XML-bestand worden op de gebruikelijke manier verzonden naar het bovenliggende stembureau.
5. Bij ontvangst van het proces-verbaal en het XML-bestand worden de gegevens vanuit het XML-bestand ingelezen in OSV.

Als een kwaadwillende besluit om het proces-verbaal dat handmatig naar het hoofdstembureau of het centrale stembureau wordt vervoerd te manipuleren, beschikt de ontvangende partij altijd nog over een gefaxte versie van het proces-verbaal, waarvan men er praktisch zeker van kan zijn dat de gefaxte versie niet gemanipuleerd is.

5.4.2.2 Diagram

Het onderstaande diagram geeft schematisch weer hoe de informatiestromen geordend zijn als het proces-verbaal naar de huidige wijze van verzenden gefaxt wordt. Het is praktisch onmogelijk om een gefaxt proces-verbaal met daarop de hashcode van het XML-bestand te manipuleren. De ontvangende partij kan er voor kiezen om het gefaxte proces-verbaal te vergelijken met het op gebruikelijke wijze ontvangen proces-verbaal.

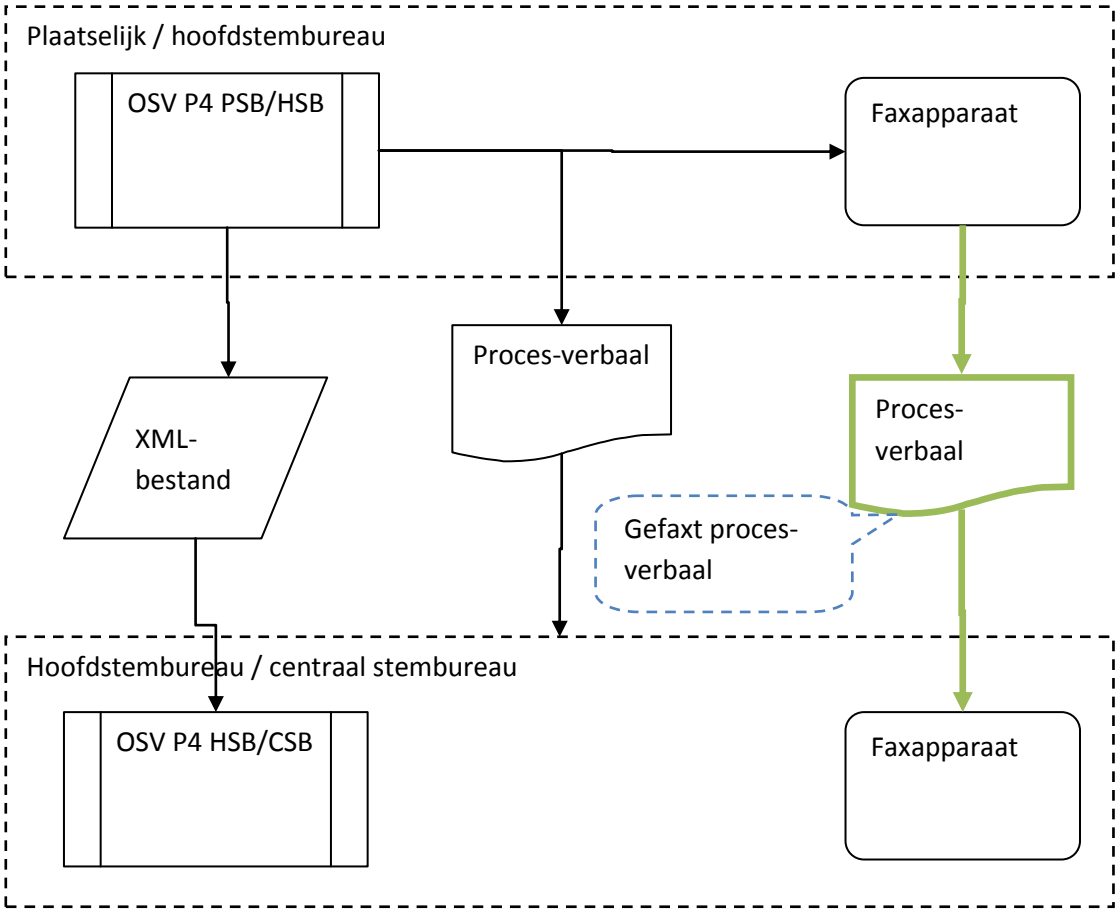


Diagram 10: het faxen van het proces-verbaal

5.4.2.3 Praktijksituatie

In deze paragraaf staat een situatie beschreven waarmee wordt aangetoond dat het voor een kwaadwillende praktisch onmogelijk is verkiezingsuitslagen onopgemerkt te manipuleren. Alice is medewerkster van het hoofdstembureau en wil de vastgestelde verkiezingsuitslag opsturen naar Bob, die medewerker is van het centrale stembureau. Alice voert de volgende werkzaamheden uit:

1. Alice stelt in OSV P4 HSB de verkiezingsuitslag vast.
2. Alice print het proces-verbaal uit op papier, en laat deze onderteken door de aanwezige leden van het hoofdstembureau.
3. Het ondertekende proces-verbaal met de hashcode van het XML-bestand wordt gefaxt naar het centrale stembureau.
4. Het XML-bestand inclusief een PDF-versie van het proces-verbaal wordt op een USB-stick geplaatst.
5. De USB-stick met het XML-bestand en de PDF versie, gezamenlijk met het afgedrukte, ondertekende proces-verbaal met de hashcode van het XML-bestand wordt verstuurd naar het centrale stembureau.

De kwaadwillende Trudy onderschept het afgedrukte proces-verbaal en de USB-stick. Ze verandert een aantal gegevens in het XML-bestand op de USB-stick en creëert een nieuw proces-verbaal met daarop de herberekende hashcode van het gemanipuleerde XML-bestand. Ze zorgt ervoor dat de gemanipuleerde documenten bij het centrale stembureau worden bezorgd.
Bob ontvangt de documenten en leest het XML-bestand in. Bob vergelijkt de hashcode van het afgedrukte proces-verbaal met de hashcode die op het gefaxte proces-verbaal staat. Hij komt erachter dat beide hashcodes niet overeenkomen.
De actie van Trudy kan niet onopgemerkt blijven, aangezien Trudy niet in staat is om een hashcode op een gefaxt proces-verbaal te manipuleren.

5.5 De implementatie van de hashfunctie sha256/512

Het is niet ondenkbaar dat er in de toekomst in de huidige (binnen OSV gebruikte) hashfunctie sha-1 meer collisions gevonden worden. Tot op heden zijn er in andere hashfuncties zoals sha-256 en sha-512 geen collisions aangetroffen. Het is daarom aan te raden om de huidige gebruikte hashfunctie sha-1 binnen OSV te vervangen door sha-256 of sha-512. De hashfunctie kan binnen OSV aangepast worden in de report-generator.

6 Conclusies en aanbevelingen

6.1 OSV in de toekomst

Verkiezingen zijn belangrijk voor de democratie. Verkiezingen moeten correct verlopen om de kernwaarden van democratie te kunnen waarborgen. In veel landen wordt er gefraudeerd met verkiezingsuitslagen. Het is niet geheel ondenkbaar dat dit ook in Nederland kan gaan gebeuren.
Asymmetrische cryptografie biedt voor de toekomst uitstekende mogelijkheden om de authenticiteit van verkiezingsuitslagen vast te garanderen. Als men in de toekomst methoden als asymmetrische cryptografie gaat gebruiken om hashcodes te onderteken, kunnen verkiezingsuitslagen via onbeveiligde kanalen uitgewisseld worden zoals internet en email. Het voordeel hiervan is dat verkiezingsuitslagen veel sneller op de plek van bestemming zijn dan wanneer deze uitslagen door een persoon vervoerd moeten worden. In een voorbeeldsituatie kan een hoofdstembureau een hashcode van een XML-bestand ondertekenen en (vanaf een computer waar geen OSV op staat) per email doorsturen naar het centrale stembureau. Daarnaast kan het hoofdstembureau ervoor kiezen om beide bestanden (het XML-bestand en het proces-verbaal met daarop de ondertekende hashcode) te publiceren op een openbare website, zodat elke bezoeker kan zien wat er in het proces-verbaal staat en of de inhoud van het XML-bestand authentiek is. De Kiesraad moet er dan voor zorgen dat de openbare sleutels van de medewerkers van het hoofdstembureau op bijvoorbeeld de site van de Kiesraad gepubliceerd zijn.

6.2 Evaluatie onderzoek en slotwoord

Dankzij het open-source karakter van OSV en de toegankelijke bijbehorende documentatie was het goed mogelijk om dit onderzoek uit te voeren en om naar aanleidingen van de bevindingen methoden en middelen vast te stellen om de risico's te beheersen.
Gedurende het onderzoek zijn er een aantal opmerkelijke bevindingen gedaan. Het is niet geheel duidelijk waarom organisaties als de Software Improvement Group weinig aandacht hebben gegeven aan de beveiliging van hashcodes. Voor toekomstige ontwikkelingen omtrent OSV en het verkiezingsproces kunnen meerdere organisaties en instituten deelnemen als het gaat om bijvoorbeeld onderzoek naar gegevensbeveiliging. De Kiesraad kan ervoor kiezen om kopieën van toekomstige versies van OSV meer onder de aandacht te brengen en op een website te plaatsen zodat geïnteresseerden hiermee kunnen experimenteren. Universiteiten en andere wetenschappelijke instellingen kunnen een uitstekende bijdrage leveren aan een verdere veilige ontwikkeling van OSV.

7 Bronnen en referenties

[BZK07] Adviescommissie inrichting Verkiezingsproces p/a Ministerie van Buitenlandse Zaken en Koninkrijksrelaties. Stemmen met vertrouwen. Den Haag, september 2007.

[KSR10d] Drs. A.Th.B. (Ank) Bijleveld-Schouten – Eisen voor de programmatuur die door de centrale stembureaus wordt gebruikt ten behoeve van de vaststelling van de uitslag van verkiezingen van leden van de Tweede Kamer, de Leden van het Europees parlement, de leden van de Provinciale Staten en de gemeenteraden. Den Haag, http://www.kiesraad.nl/nl/Overige_Content/Bestanden/pdf_thema/pdfs_OSV/Eisen_staatssecretaris_OSV.pdf

[IVU09] IVU Traffic Technologies AG – Gedetailleerde specificatie Ondersteunende Software Verkiezingen versie 1.3.4. http://www.kiesraad.nl/nl/Overige_Content/Bestanden/Advies-Adviezen/Functionele_en_Technische_Specificatie_OSV.pdf. Berlijn, april 2009.

[KSR10a] Kiesraad.nl – Kiesdeler. http://www.Kiesraad.nl/nl/Onderwerpen/Uitslagen/Kiesdeler.html, 30 september 2010.

[KSR08] Kiesraad.nl – Ondersteunende Software Verkiezingen (OSV), nieuwsbericht. http://www.Kiesraad.nl/nl/Actueel/Nieuwsberichten/2008/Ondersteunende_Software_Verkiezingen_(OSV).html, 22 december 2008.

[KSR10] Kiesraad.nl – Ondersteunende Software Verkiezingen (OSV). http://www.Kiesraad.nl/nl/Verkiezingen/Verkiezingen-Algemene_informatie_OSV.html, 24 september 2010

[KSR10b] Kiesraad.nl – Achtergrond: van stemcomputers naar OSV. http://www.Kiesraad.nl/nl/Verkiezingen/Verkiezingen-Algemene_informatie_OSV/Achtergrond_van_stemcomputers_naar_OSV.html, november 2010.

[MAR05] Martin, Luther – Weaknesses in Sha-1. The ISSA Journal, september 2005. http://www.issa.org/Library/Journals/2005/September/Martin%20-%20Weaknesses%20in%20SHA-1.pdf

[SIG11] Dr. S. van Otterloo, Software Improvement Group. Toetsing eisen OSV 4 en 5 voor alle soorten verkiezingen; rapport t.b.v. de Kiesraad. Amsterdam, 10 februari 2011. http://www.kiesraad.nl/nl/Overige_Content/Bestanden/pdf_thema/pdfs_OSV/SIG_2011_alle_verkiezingen.pdf

[PRC10] Procura.nl – Uitslagverwerking. http://www.procura.nl/pages/verkiezingen/images/uitslagpresentatie/uitslag_presentatie_voorbereiding.pdf, 1 oktober 2010.

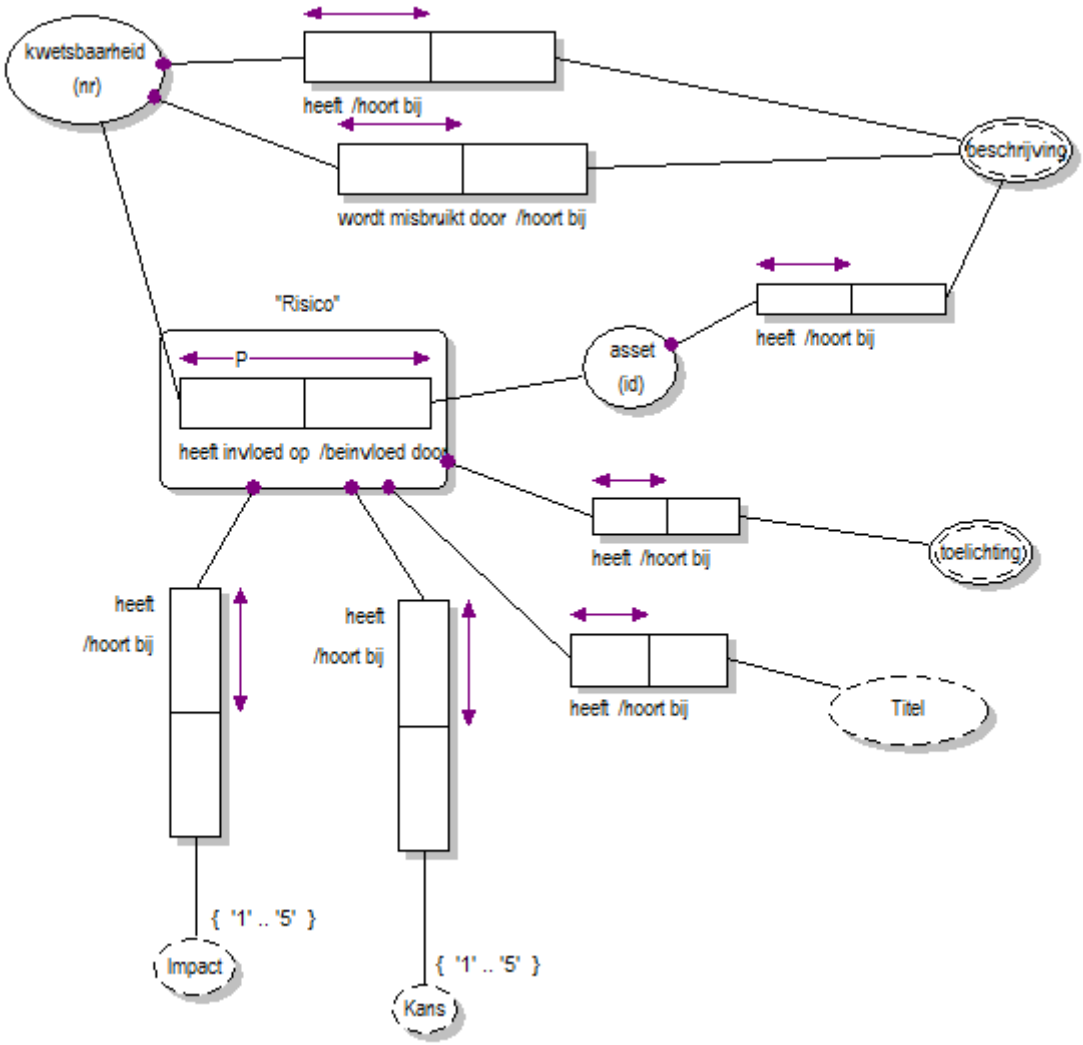
[RNS07] Rechtennieuws.nl - Schorsing Sdu-stemcomputers gehandhaafd. http://rechtennieuws.nl/13094/schorsing-sdu-stemcomputers-gehandhaafd.html, 17 januari 2007.

[OVH10] Wetten.nl – Wetten en regelgeving, Afdeling II, artikelen B1 – P25. http://wetten.overheid.nl/BWBR0004627/AfdelingII/geldigheidsdatum_16-08-2010, 16 augustus 2010

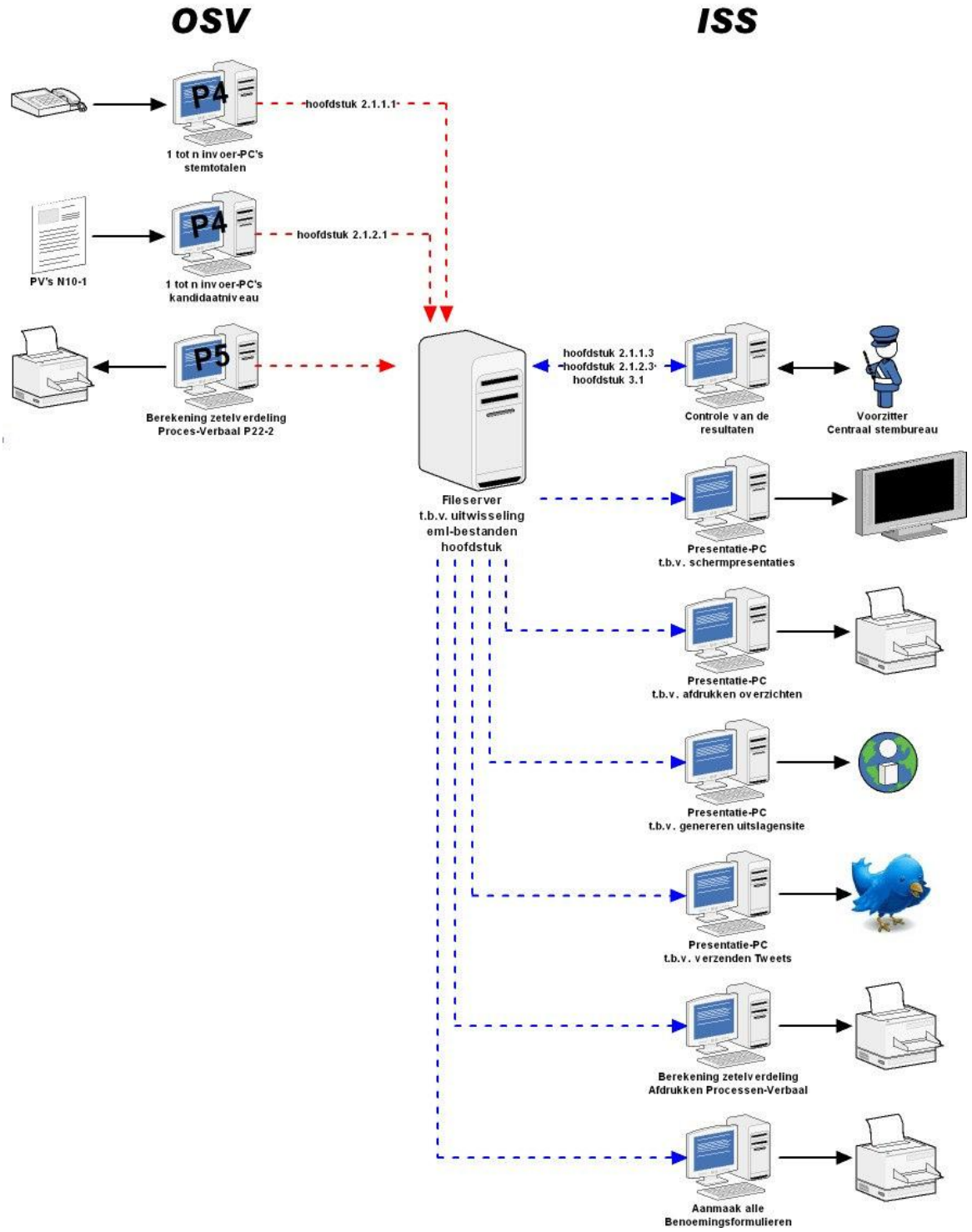
[STN10] Wij vertrouwen stemcomputers niet. Even kort recapituleren. http://wijvertrouwenstemcomputersniet.nl/blog/, 29 juli 2010.

8 Bijlagen

8.1 ORM model



8.2 Schema OSV



De globale werking van OSV volgens [PRC10]. Deze afbeelding is ook in het verwezen document te vinden.