Rijksauditdienst
Ministerie van Financiën

> Retouradres Postbus 20201 2500 EE Den Haag

Ministerie van Binnenlandse Zaken en Konikrijksrelaties
DRI

Rijksauditdienst

Kalvermarkt 52
2511 CB Den Haag
Postbus 20201
2500 EE Den Haag
www.rijksoverheid.nl

Ons kenmerk
RAD/2011/356

Uw brief (kenmerk)

Bijlagen

Datum 9 mei 2011
Betreft Aanbieding rapportage 'Uitkomsten audit beheervoorziening BSN'

Hierbij ontvangt u de rapportage 'Uitkomsten audit beheervoorziening BSN'. Deze rapportage is inhoudelijk afgestemd met vertegenwoordigers van de directie DRI en de baten- en lastendienst BPR. Op 17 mei zal de Rijksauditdienst de rapportage toelichten in het directeurenoverleg OBD/DRI/BPR.

Hoogachtend,

P.H.E. Bartholomeus RA
Directeur Rijksauditdienst

Uitkomsten audit beheervoorziening BSN

Een beoordeling op basis van de Wet algemene bepalingen burgerservicenummer

RAD/2011/356

Datum	9 mei 2011
Status	Definitief

Colofon

Titel	RAD/2011/356 Uitkomsten audit beheervoorziening BSN
Auteur(s)	dhr. ir. T.W. Schaap RE CISA dhr. drs. H. Akcay
Bijlage(n)	
Inlichtingen	**Rijksauditdienst** dhr. T.W. Schaap

Inhoud

1 Inleiding

1.1 Algemeen

Het burgerservicenummer (BSN) is een uniek persoonsnummer voor iedereen die een relatie heeft met de Nederlandse overheid. Het BSN is ingevoerd in 2007. Bij invoering zijn in de meeste gevallen de voorheen uitgegeven sofinummers in formele zin omgezet in BSN's. Formaat en inhoud zijn niet daadwerkelijk gewijzigd. De beheervoorziening BSN is het geheel van voorzieningen dat zorgt voor het genereren, distribueren, beheren en raadplegen van het BSN. Deze voorziening draagt er onder meer aan bij dat per persoon maximaal 1 nummer wordt uitgegeven. Gebruikers van het BSN-stelsel kunnen middels de beheervoorziening ook achterliggende registraties van persoonsgegevens raadplegen voor zover zij hiervoor zijn geautoriseerd.

De directie DRI van BZK is vanuit het beleid verantwoordelijk voor de beheervoorziening BSN. Zij treedt op als opdrachtgever voor de baten-/lastendienst BPR die ondermeer het tactisch beheer uitvoert voor de beheervoorziening. BPR is eerst verantwoordelijke voor de uitvoering van alle bepalingen uit wet- en regelgeving verbandhoudend met de beheervoorziening BSN zoals deze is gedefinieerd in artikel 3, lid 1 van de Wet algemene bepalingen burgerservicenummer.

De basis voor het burgerservicenummer is de Wet algemene bepalingen burgerservicenummer. In artikel 21, lid 1 van deze wet is bepaald dat de minister van BZK eens per drie jaar een onderzoek naar de inrichting, de werking en de beveiliging van de beheervoorziening laat uitvoeren. Door de Bestuursraad van BZK is besloten dat de Rijksauditdienst dit onderzoek uitvoert als onderdeel van haar vraaggestuurde werkzaamheden.

1.2 Doelstelling

De doelstelling van de audit is geweest:
Een onderzoek uit te voeren naar de beheervoorziening BSN conform artikel 21, lid 1 van de Wet algemene bepalingen burgerservicenummer (Wabb) waarbij de beoordelingscriteria worden gehanteerd zoals bedoeld in Artikel 21 lid 4 van de Wabb en uitgewerkt in het Besluit burgerservicenummer Artikel 17. Het onderzoek resulteert in een oordeel over de beheervoorziening conform Artikel 17 van het Besluit BSN.

De audit is gericht op het bereiken van een redelijke mate van zekerheid. Dit betreft de hoogst mogelijke zekerheid voor een oordeel conform de handreiking 'Oordelen van gekwalificeerde IT-auditors' van de Nederlandse Orde van Register EDP-Auditors (NOREA).

1.3 Auditobject

De audit heeft zich gericht op de beheervoorziening BSN met inbegrip van de informatiebeveiligingsaspecten zoals bedoeld in artikel 3 van de Wabb inclusief het onderliggende nummerregister (artikel 4 Wabb). De beheervoorziening is beschreven in een systeembeschrijving die bij ministeriële regeling wordt vastgesteld (artikel 2 besluit servicenummer). In artikel 3 besluit BSN wordt is in het kort aangegeven wat de beschrijving dient in te houden. Artikel 3 van de Regeling BSN geeft aan dat de bedoelde systeembeschrijving bestaat uit een aantal

paragrafen van het Logisch ontwerp BSN. Het concrete auditobject is tweeledig. In eerste instantie is het object de beschrijving van de beheervoorziening zoals bepaald in artikel 17 van het Besluit BSN. In tweede instantie richt de audit zich op het functioneren van de beheervoorziening conform de beschrijving.

1.4 Kwaliteitscriteria

De kwaliteitscriteria voor de audit naar de beheervoorziening worden genoemd in artikel 17 van het Besluit BSN:

- volledigheid;
- begrijpelijkheid;
- juistheid.

Deze criteria hebben betrekking op de beschrijving van de beheervoorziening. De interpretatie van deze criteria is niet zonder meer eenduidig. Voor het onderzoek hanteren wij de volgende betekenissen. Volledigheid betekent dat alle aspecten van de beheervoorziening worden beschreven voor zover relevant vanuit het oogpunt van wet- en regelgeving en/of vanuit automatiseringsperspectief. Juistheid betekent dat in de beschrijving een redelijke invulling aan alle eisen vanuit wet- en regelgeving wordt gegeven. Het begrip begrijpelijkheid van de beschrijving van de beheervoorziening is lastig te operationaliseren. Wij hanteren hiervoor 'professional judgement' waarbij rekening wordt gehouden met de doelgroep van het betreffende document (burger, overheidsorganisatie, ICT-ontwikkelaar etc.).

De inhoudelijke beoordeling van de informatiebeveiliging van de beheervoorziening (onderdeel van juistheid) heeft plaatsgevonden aan de hand van de kwaliteitscriteria uit het Voorschrift Informatiebeveiliging Rijksdienst:

- integriteit
- exclusiviteit
- beschikbaarheid
- controleerbaarheid (aanvullend om voorgaande criteria te kunnen vaststellen).

In bijlage I is de definitie van deze criteria opgenomen.

1.5 Norm

Op basis van de voor BSN geldende regelgeving, een vooronderzoek en beschikbare documentatie is een uitgewerkt normenkader opgesteld dat op 13 september 2010 is vastgesteld door de directeur DRI en de directeur BPR. Dit normenkader is opgenomen in bijlage II en richt zich op de volledigheid en juistheid van de beheervoorziening. Voor het begrip begrijpelijkheid is geen apart normenkader ontwikkeld.

Het normenkader in bijlage II is grotendeels gestructureerd op basis van de processen die ten grondslag liggen aan de beheervoorziening. De onderwerpen zijn:

- algemeen: de governance rondom de beheervoorziening;
- genereren nummers;
- distribueren en vastleggen uitgifte burgerservicenummers;
- beheren (functioneel en technisch) beheervoorziening inclusief algemene informatiebeveiligingsaspecten;
- raadplegen beheervoorziening.

1.6 Structuur rapport

In dit rapport is als onderdeel van de managementsamenvatting (hoofdstuk 2) het assurance rapport opgenomen dat ons oordeel bevat. In hoofdstuk 3 is een overzicht opgenomen van de belangrijkste bevindingen geordend naar de te onderscheiden deelprocessen voor de Beheervoorziening BSN

2 Managementsamenvatting

2.1 Assurance rapport

2.1.1 *Geadresseerde*

Dit assurance-rapport is bestemd voor de minister van Binnenlandse Zaken en Koninkrijksrelaties (voor deze de directeur van de directie Dienstverlening, Regeldruk en Informatiebeleid (DRI)) en dient mede ter invulling van het onderzoeksvereiste van artikel 21, lid 1 van de Wet algemene bepalingen burgerservicenummer (Wabb). In dit artikel is bepaald dat de minister een keer per drie jaar een onderzoek naar de inrichting, de werking en de beveiliging van de beheervoorziening BSN laat uitvoeren. De beoordelingscriteria voor dit onderzoek zijn ontleend aan Artikel 21 lid 4 van de Wabb en het Besluit burgerservicenummer Artikel 17. Het onderzoek resulteert in een oordeel over de beheervoorziening conform Artikel 17 van het Besluit BSN.

2.1.2 *Object van onderzoek*

Ingevolge onze opdrachtbevestiging van 27 april 2010 met kenmerk RAD/2010/483M hebben wij de opzet en het bestaan van het stelsel van maatregelen in en rondom de beheervoorziening BSN gericht op de kwaliteitscriteria volledigheid, begrijpelijkheid en juistheid beoordeeld naar de stand van 31 oktober 2010.

2.1.3 *Criteria*

Voor de beschrijving van de gehanteerde kwaliteitsaspecten verwijzen wij naar paragraaf 2.3. Uitgaande van de Wet algemene bepalingen burgerservicenummer en bijbehorende regeling en besluit en het onderzoeksobject zijn in overleg met DRI de normen geformuleerd, die bij het onderzoek zijn gehanteerd. Deze normen zijn opgenomen in bijlage 2 .

De opzet omvat de formele inrichting van het onderzoeksobject op een bepaald moment. Het bestaan betreft de geïmplementeerde beheersingsmaatregelen in het onderzoeksobject op een bepaald moment.

2.1.4 *Verantwoordelijkheden en werkzaamheden*

De beschrijving, inrichting en naleving van maatregelen en procedures zijn de verantwoordelijkheid van de leiding van de verwerkingsorganisatie Basisadministratie Persoonsgegevens en Reisdocumenten (BPR, eerstverantwoordelijke partij). Het is onze verantwoordelijkheid om door middel van een onderzoek op onafhankelijke wijze een oordeel over de maatregelen en procedures te geven. Daartoe hebben wij werkzaamheden uitgevoerd die in overeenstemming zijn met de richtlijnen voor assurance-opdrachten en die gericht zijn op het signaleren van materiële afwijkingen en het verkrijgen van een redelijke mate van zekerheid.

Onze belangrijkste werkzaamheden waren:

- het verkrijgen van inzicht in relevante kenmerken van de betrokken organisaties zoals BPR en betrokken marktpartijen;
- het houden van interviews met verantwoordelijke functionarissen, vooral gericht op het onderkennen van risico's in de externe omgeving en de

betrokken organisaties zelf, en onderzoek in hoeverre deze risico's worden afgedekt door maatregelen en procedures;
- het beoordelen van de opzet en het vaststellen van het bestaan van de relevante maatregelen en procedures. Dit door middel van het kennis nemen van documentatie, het kennis nemen van de resultaten van de uitgevoerde interne controles, eigen waarnemingen en het beoordelen van logging. De opzet en het bestaan van de maatregelen en procedures in en rondom de beheervoorziening BSN per 31 oktober 2010 hebben wij beoordeeld.

De opdracht is uitgevoerd volgens de standaard voor assurance opdrachten.

2.1.5 *Conclusie*

Op grond van ons onderzoek zijn wij van oordeel dat aan de normen die invulling geven aan de kwaliteitscriteria volledigheid en juistheid zoals bedoeld in artikel 17 van het Besluit BSN in opzet en bestaan niet in alle opzichten toereikend invulling is gegeven per 31 oktober 2010. Voor het kwaliteitscriterium begrijpelijkheid is de conclusie dat in opzet en bestaan wel toereikend invulling is gegeven.

2.1.6 *Toelichting*

Voorgaande conclusie voor wat betreft de criteria volledigheid en juistheid is gebaseerd op de volgende afwijkingen van de normen:
- de ernstige tekortkomingen op het gebied van de beveiliging van de beheervoorziening BSN die in het eerste kwartaal van 2010 zijn vastgesteld in combinatie met de tekortkomingen in het informatiebeveiligingsplan en -functie; uit ons onderzoek komt overigens het beeld naar voren dat de tekortkomingen niet hebben geleid tot het optreden van incidenten;
- het niet melden van de ernstige tekortkomingen op informatie-beveiligingsgebied door de baten-/lastendienst BPR aan de beleidsverantwoordelijk directie Dienstverlening, Regeldruk en Informatiebeleid;
- het niet volledig informatieloos zijn van het burgerservicenummer; ter nuancering constateren wij dat directe informatie zoals geslacht of geboortedatum niet in het BSN aanwezig is; het betreft een beperkte mate van indirecte informatie, bijvoorbeeld of een BSN voor of na 26 november 2007 is uitgegeven; uit de gesprekken die wij over (de uitgifte van) het BSN hebben gevoerd, zijn verder ook geen belangrijke scenario's voor misbruik in beeld gekomen.

De tekortkomingen op beveiligingsgebied zijn/worden in de loop van 2010 naar is meegedeeld stapsgewijs weggenomen. Het is de bedoeling in het eerste kwartaal van 2011 het bijbehorende verbetertraject af te sluiten.

2.1.7 *Beperkingen*

Ons onderzoek was gericht op de opzet en het bestaan per 31 oktober 2010. Wij hebben ons dus geen oordeel gevormd over toekomstige perioden.

Den Haag, 9 mei 2011
Rijksauditdienst

ir. T.W. Schaap RE CISA
Auditmanager

3 Bevindingen

3.1 Algemeen

In dit hoofdstuk wordt ingaan op de belangrijkste bevindingen uit de audit naar de beheervoorziening BSN. Met name wordt ingegaan op de afwijkingen van de norm die zijn vastgesteld aan de hand van het kader dat in bijlage II is opgenomen. De paragraafindeling van dit hoofdstuk volgt de structuur van dit normenkader. Gestart wordt met een korte beschrijving van de beheervoorziening BSN.

3.2 Beschrijving beheervoorziening BSN

Het burgerservicenummer (BSN) is een uniek persoonsnummer voor iedereen die een relatie heeft met de Nederlandse overheid. Het nummer is ingevoerd in 2007 en vervangt in de meeste gevallen het sofinummer. Grondslag voor het BSN is de Wet algemene bepalingen burgerservicenummer waarin ook is voorzien in de beheervoorziening BSN. De beheervoorziening BSN is het geheel van voorzieningen dat zorgt voor het genereren, distribueren en vastleggen van uitgifte van BSN's en het beheren en raadplegen van de beheervoorziening BSN. Gebruikers van het BSN-stelsel kunnen de beheervoorziening raadplegen voor de benadering van achterliggende registraties van persoonsgegevens voor zover zij hiervoor zijn geautoriseerd. In technische zin is de beheervoorziening BSN een verzameling webservices die opereren op het nummerregister. Ook onderdeel van de voorziening zijn de bijbehorende processen en procedures inclusief de organisatie hiervan. Op deze onderwerpen wordt in de volgende paragrafen onder 'algemeen' ingegaan.

3.3 Afspraken en verantwoording beheervoorziening BSN

3.3.1 Algemeen

De basis voor de instandhouding van de beheervoorziening BSN wordt gevormd door een verzameling afspraken tussen betrokken partijen. De belangrijkste afspraken zijn:

- het convenant tussen het programma Dienstverlening, Regeldruk en Informatiebeleid (DRI) als ambtelijk opdrachtgever en het Agentschap BPR als opdrachtnemer voor het onderhoud en het beheer van de beheervoorziening BSN;
- het contract tussen het Agentschap BPR en een marktpartij voor de levering van beheer- en rekencentrumdiensten;
- het contract tussen het Agentschap BPR en een marktpartij voor de levering van ontwikkeldiensten waarop de beheervoorziening is gebaseerd.

In het convenant en in de contracten zijn ondermeer afspraken opgenomen over periodieke rapportage en verantwoording. Hierin wordt onder meer bepaald dat de leverancier van beheer- en rekencentrumdiensten jaarlijks door een externe auditor een rapportage laat opstellen over (met name) de toepassing van het informatiebeveiligingsplan voor de beheervoorziening BSN.

3.3.2 Convenant DRI - agentschap BPR

In het convenant tussen DRI en het agentschap BPR zijn geen expliciete afspraken opgenomen voor de rapportage over de naleving van de Wabb voor de beheervoorziening BSN in zijn totaliteit. Hierdoor krijgt DRI alleen bij de driejaarlijkse audit een integraal beeld van de naleving van de WABB voor de

beheervoorziening BSN. Het risico bestaat dat afwijkingen hierdoor niet tijdig in beeld komen.
Aanbeveling: Neem in het convenant tussen DRI en het agentschap BPR een afspraak op dat jaarlijks expliciet wordt gerapporteerd over de naleving van de WABB waarbij ook rekening dient te worden gehouden met actuele juridische ontwikkelingen.

In februari 2010 is het agentschap BPR door de leverancier van de beheer- / rekencentrumdiensten op de hoogte gesteld van een aantal ernstige tekortkomingen op beveiligingsgebied in de beheervoorziening BSN. Deze tekortkomingen zijn waarschijnlijk langere tijd aanwezig geweest en zijn/worden in de loop van 2010 naar is meegedeeld stapsgewijs weggenomen (zie ook paragraaf 3.7). Het is de bedoeling dit verbetertraject in het eerste kwartaal van 2011 af te sluiten. Het agentschap BPR heeft in februari direct actie ondernomen richting de leverancier maar heeft niet in lijn met paragraaf 3.1 van het convenant gehandeld door DRI niet te informeren over de geconstateerde tekortkomingen. Ons is medegedeeld dat de inschatting van BPR hierbij is geweest dat de vastgestelde tekortkomingen relatief snel konden worden opgelost.
Aanbeveling: Draag binnen BPR zorg voor de adequate uitvoering van de afspraken in het convenant tussen DRI en BPR rondom rapportage. Uitbreiding van het convenant op basis van de voorgaande aanbeveling kan hieraan bijdragen. Ons inziens dient hierbij ook aandacht te worden besteed aan organisatieculturele aspecten als openheid en transparantie.

3.3.3 *Conclusie*

Met name het niet melden van de ernstige tekortkomingen op beveiligingsgebied die zijn vastgesteld in februari 2010 in de beheervoorziening BSN is een significante afwijking van de norm. De conclusie is dat de opzet van de afspraken en de verantwoording an sich wel toereikend is waarbij verbetering op onderdelen mogelijk is (zie bijlage II). De uitvoering (het bestaan) van de afspraken over rapportage tussen BPR en DRI is daarentegen ontoereikend geweest aangezien BPR DRI onvoldoende heeft geïnformeerd over een aantal ernstige tekortkomingen op beveiligingsgebied in de beheervoorziening BSN die in februari 2010 zijn vastgesteld.

3.4 Genereren BSN's

3.4.1 *Algemeen*

Het proces genereren BSN's richt zich op het aanmaken van nieuwe burgerservicenummers. Ter toelichting op dit proces en de vastgestelde tekortkomingen wordt in deze paragraaf kort ingegaan op enkele aspecten van het BSN.

De nummerruimte van het burgerservicenummer bestaat uit 9 cijfers. Ieder nummer moet verder voldoen aan de '11-proef'. Dit is een test waarmee eenvoudig veel voorkomende invoerfouten kunnen worden gedetecteerd. Numeriek is het burgerservicenummer gelijk aan het vroegere sociaal-fiscaal nummer. De nummerruimte bestaat uit een drietal intervallen:

1. Uit het eerste interval zijn door de Belastingdienst op volgorde nummers uitgegeven als sociaal-fiscaal nummer in de periode van de start van het gebruik van het sociaal-fiscaalnummer tot 26 november 2007, de invoeringsdatum van het BSN stelsel. Met de komst van het BSN zijn deze sociaal-fiscaalnummers BSN's geworden.

2. Uit het tweede interval worden door de Belastingdienst na 26 november 2007 op volgorde nummers uitgegeven als sociaal-fiscaalnummer aan personen die geen BSN kunnen krijgen maar wel een relatie hebben met de Belastingdienst. In sommige gevallen worden deze sociaal-fiscaalnummers naderhand omgezet in een BSN.
3. Uit het derde interval worden BSN's na 26 november 2007 uitgegeven door de beheervoorziening BSN. Deze nummers worden (binnen het interval) in beginsel in willekeurige volgorde uitgegeven.

3.4.2 *Volgordelijkheid en informatieloosheid*

Voor burgerservicenummers gelden onder andere de volgende normen:

- ieder gegenereerd nummer moet informatieloos zijn;
- er mag geen volgordelijkheid uit de nummers blijken.

De norm betreffende informatieloosheid is gebaseerd op artikel 2 van de WABB in combinatie met paragraaf 4.2 van de memorie van toelichting bij de WABB. Kern van deze bepaling is dat het burgerservicenummer geen informatie bevat over de persoon aan wie het nummer is toegekend. Het gaat er hierbij om dat zowel direct als indirect en met of zonder aanvullende informatie uit het BSN geen informatie is af te leiden over de persoon in kwestie. Denk hierbij aan informatie over de periode waarin het BSN is uitgegeven aan een persoon of de instantie die het nummer heeft verstrekt. De norm van volgordelijkheid volgt uit de norm over informatieloosheid. Als nummers in een bepaalde volgorde worden uitgegeven dan is hieraan informatie te ontlenen over het moment van uitgifte en zijn de nummers dus niet informatieloos.

Uit de beschrijving in de voorgaande paragraaf blijkt dat op drie punten strikt genomen niet in alle opzichten voldoende invulling wordt gegeven aan deze normen. Het eerste punt betreft het gebruik van drie intervallen in de beschikbare nummerruimte. Hierdoor is niet voldaan aan de eis van informatieloosheid. Het is bijvoorbeeld zichtbaar of een BSN voor 26 november 2007 (interval 1) of hierna (interval 3) is uitgegeven aan een burger. Ook is zichtbaar of een BSN na 26 november 2007 eerst door de Belastingdienst is uitgegeven als een sociaal-fiscaalnummer (interval 2). Het tweede punt betreft de volgordelijkheid van uitgifte van nummers binnen interval 1 en 2, waardoor informatie over de periode waarin een persoon het BSN heeft ontvangen is af te leiden. Het derde punt betreft de wijze waarop de willekeurige volgorde van de uitgifte van nummers in het derde interval wordt gerealiseerd. De willekeurige uitgifte is gebaseerd op een pseudo randomgenerator. Dit is een generator van schijnbaar willekeurige getallen die bij een zelfde startwaarde altijd dezelfde reeks getallen produceert. Gegeven het beperkte aantal mogelijke startwaarden is het mogelijk om met enige inspanning op basis van twee BSN's die vlak na elkaar zijn uitgeven, ook de BSN's die rond deze twee bekende BSN's zijn uitgegeven, te bepalen.

Uiteraard is de vraag relevant of geconstateerde punten leiden tot concrete (privacy-)risico's rondom het BSN. Geconstateerd wordt dat directe informatie zoals geslacht of geboortedatum niet in het BSN aanwezig is. Het betreft een beperkte mate van indirecte informatie. Uit de gesprekken die wij over (de uitgifte van) het BSN hebben gevoerd, zijn geen belangrijke scenario's voor misbruik in beeld gekomen. Wel is het mogelijk om in combinatie met aanvullende informatie bijvoorbeeld de leeftijd van een persoon te schatten op basis van een BSN dat voor 26 november 2007 is uitgegeven. De verdere beantwoording van deze vraag met betrekking tot privacy-risico's valt niet binnen onze onderzoeksopdracht.

Het oplossen van de geconstateerde afwijkingen van de norm is voor het eerste en tweede punt niet eenvoudig. Aan de ene kant zal de wetgever bewust vanuit bijvoorbeeld privacyoverwegingen de normen op het gebied van informatieloosheid in de Wabb hebben opgenomen. Wel is ons door DRI medegedeeld dat het eerste en tweede aandachtspunt is besproken en geaccepteerd in de Stuurgroep BSN die betrokken was bij de invoering van het BSN in de periode tot en met 2007. Aan de andere kant zijn wijzigingen in het BSN stelsel ondermeer vanwege de omvang en administratieve en bestuurlijke lasten complex en duur. Het is aan de verantwoordelijke beleidsafdeling in een aanvaardbare oplossing te voorzien. Het derde punt kan relatief eenvoudig worden opgelost.

Aanbeveling: Onderzoek de wijze waarop rondom het punt van informatieloosheid en volgordelijkheid van het BSN de wet- en regelgeving en beheervoorziening BSN met elkaar in overeenstemming kunnen worden gebracht. Betrek hier ook de Belastingdienst bij voor wat betreft de uitgave van sociaal-fiscaalnummers.

Aanbeveling: Verbeter de wijze waarop de toevalsgetallen worden gegenereerd die de basis vormen voor de huidige uitgifte van BSN's. Het advies is hierbij gebruik te maken van de expertise van het Nationaal Bureau voor Verbindingsbeveiliging (onderdeel Ministerie van BZK).

3.4.3 *Vastlegging informatie genereren BSN's*

De norm is dat een aantal administratieve gegevens wordt vastgelegd in het nummerregister als uitkomst van het proces genereren BSN's. Vastgesteld is dat in afwijking van de norm het gegeven 'datum waarop het nummer is aangemaakt' niet wordt vastgelegd. Dit levert ons inziens een risico op voor bijvoorbeeld het doelmatig analyseren van foutsituaties.

Aanbeveling: Breng de beheervoorziening BSN voor wat betreft het gegeven 'datum waarop het nummer is aangemaakt' in overeenstemming met wet- en regelgeving.

3.4.4 *Conclusie*

Met name de afwijking van de norm op het gebied van volgordelijkheid en informatieloosheid is voor het proces genereren burgerservicenummers zeer relevant. De conclusie is dat voor het proces genereren burgerservicenummers als geheel onvoldoende invulling wordt gegeven aan de norm.

3.5 Distribueren en vastleggen uitgifte BSN's

3.5.1 *Algemeen*

Het proces distribueren en vastleggen uitgifte BSN's richt zich ten eerste op het verstrekken van gegenereerde burgerservicenummers aan gemeenten die vervolgens de nummers kunnen uitgeven aan burgers (bijvoorbeeld bij aangifte van een geboorte). Per aanvraag van een gemeente worden 250 nummers verstrekt. De gemeente doet vervolgens een terugmelding aan de beheervoorziening BSN als een nummer daadwerkelijk wordt uitgegeven. In de beheervoorziening wordt dan vastgelegd dat het nummer in verkeer is genomen.

De Belastingdienst geeft sociaal-fiscaalnummer uit die ook zijn geregistreerd in de beheervoorziening BSN (zie ook paragraaf 3.4.2). Bij de start van de beheer-voorziening BSN zijn ongeveer 1 miljoen nummers gegenereerd en in een keer overgedragen aan de Belastingdienst. Zoals eerder aangegeven in paragraaf 3.4.2. en 3.4.3 worden deze nummers als sociaal-fiscaalnummer op volgorde uitgegeven.

3.5.2 *Conclusie*
Het proces distribueren en vastleggen uitgifte BSN's geeft in redelijke mate invulling aan de norm.

3.6 Functioneel Beheren beheervoorziening BSN

3.6.1 *Algemeen*
Het functioneel beheren van de beheervoorziening BSN richt zich op het aansluiten van gebruikers op de beheervoorziening, het beheren van autorisaties en het controleren en waar nodig het corrigeren van informatie in de beheervoorziening BSN.

3.6.2 *Aandachtspunten functioneel beheren beheervoorziening BSN*
Op een aantal punten wordt onvoldoende invulling gegeven aan de norm. Een eerste punt is de aanwezigheid van een koppeling van de beheervoorziening BSN met Internet. Volgens de norm zou een dergelijke koppeling niet aanwezig mogen zijn. De vraag is hoe realistisch een dergelijke eis in de context van de beheervoorziening BSN is en hoe absoluut deze eis moet worden geïnterpreteerd. Koppeling kan bijvoorbeeld ook indirect plaatsvinden bij een gemeente die zowel een verbinding heeft met de beheervoorziening BSN als met Internet.
Aanbeveling: concretiseer de eis dat de beheervoorziening BSN niet mag worden aangesloten op Internet. Onderzoek vervolgens of de IT-infrastructuur voor de beheervoorziening BSN voldoende invulling geeft aan deze eis en onderneem indien noodzakelijk actie. Zet in ieder geval de voorgenomen opheffing van de Virtual Private Network (VPN) koppeling voor beheerdoeleinden door aangezien deze koppeling in ieder geval strijdig is met de norm.

Een tweede punt betreft het ontbreken van enkele maatregelen rondom authenticatie van beheerders van de beheervoorziening BSN. Zo is voor beheertoegang tot de beheervoorziening alleen kennis (wachtwoord) benodigd en geen bezit (bijvoorbeeld een security token). Ook hoeven sommige beheerders niet periodiek hun wachtwoord te wijzigen. Het ontbreken van afdoende maatregelen wordt enigszins gecompenseerd doordat de fysieke toegang tot de beheerterminals is beperkt.
Aanbeveling: Maak gebruik van kennis en bezit voor authenticatie van beheerders op de beheervoorziening BSN. Stel verder een wachtwoordbeleid vast voor alle beheerders van de beheervoorziening zoals bijvoorbeeld de gedwongen periodieke wijziging van wachtwoorden en implementeer dit beleid. Maak hierbij gebruik van de mogelijkheden die standaard in de gebruikte IT-infrastructuur aanwezig zijn en kies redelijke waarden.

Een derde punt betreft de schoningstermijnen van de logboeken binnen de beheervoorziening BSN. In deze logboeken wordt informatie opgeslagen over het functioneren van het systeem, b.v. over geconstateerde nummerfouten. Schoning vindt wel plaats op het operationele systeem maar de bewaartermijnen worden ruim overschreden doordat de gegevens in backup's aanwezig blijven en dus in principe kunnen worden teruggelezen.
Aanbeveling: Onderzoek de wijze waarop de bewaartermijnen voor logboeken en de langdurige opslag van de gegevens uit de logboeken in backup's met elkaar in overeenstemming kunnen worden gebracht.

3.6.3 *Conclusie*
Het proces functioneel beheren beheervoorziening BSN geeft in redelijke mate invulling aan de norm met uitzondering van:

- internetkoppeling beheervoorziening BSN;
- authenticatie van beheerders;
- schoningstermijnen van logboeken.

3.7 Technisch Beheren beheervoorziening BSN

3.7.1 *Algemeen*

Zoals beschreven in paragraaf 3.3 zijn de beheer- en rekencentrumdiensten voor de beheervoorziening BSN door BPR uitbesteedt aan een externe leverancier. Deze leverancier voert het operationeel / technisch beheer uit op de beheervoorziening BSN die dubbel is uitgevoerd en fysiek is geplaatst in twee gescheiden rekencentra. De marktpartij huurt hiervoor rekencentrumcapaciteit in bij twee andere marktpartijen.

3.7.2 *Informatiebeveiligingsplan*

Een informatiebeveiligingsplan (IBP) dient in samenhang een beschrijving te geven van technische en organisatorische beheersings- en beveiligingsmaatregelen. Het bereik van het IBP is dus veel breder dan technisch beheer en algemene beveiligingsmaatregelen alleen. Het achterliggende doel van een IBP is om aan te tonen dat risico's in voldoende mate zijn afgedekt en dat aan specifieke (wettelijke) eisen voldoende invulling is gegeven. in opdracht van BPR heeft de leverancier van beheer- en rekencentrumdiensten een informatiebeveiligingsplan opgesteld voor de beheervoorziening BSN. Door BPR is een appendix opgesteld op het IBP. Zowel IBP als appendix zijn niet geformaliseerd al wordt het IBP in de praktijk wel gebruikt. Het IBP biedt inzicht in de maatregelen die relevant zijn voor het technisch beheer en de rekencentrumfunctie. Maatregelen die bijvoorbeeld bij BPR zelf (beheer van de gegevens) of in de applicatie zijn getroffen, zijn niet in het plan opgenomen en hier wordt ook niet naar verwezen. Een volledig overzicht van de maatregelen in en rondom beheervoorziening BSN ontbreekt hierdoor, waardoor ook een integrale vaststelling van de toereikendheid van deze maatregelen niet eenvoudig mogelijk is. Tevens wordt voor het informatiebeveiligingsplan de Wabb en de onderliggende regelgeving niet expliciet als uitgangspunt gehanteerd. Een specifiek aandachtspunt is dat de leverancier gebruik maakt van haar vestiging in India voor het monitoren van de beheervoorziening BSN omgeving. Ons is medegedeeld dat deze werknemers hierbij geen toegang hebben tot beheervoorziening BSN dienstverlening of data. Gegeven de privacy rechtelijke aspecten die samenhangen met de inzet van medewerkers van buiten de EU zou hier in het IBP expliciet op moeten worden ingegaan.

Aanbeveling: Stel als BPR een nieuw IBP beheervoorziening BSN op waarin de WABB en andere relevante regelgeving expliciet als uitgangspunt wordt gehanteerd en stel dit IBP formeel vast. In dit IBP dient een integraal overzicht te worden gegeven van het stelsel van maatregelen in en rondom de beheervoorziening BSN. Hiervoor kan worden verwezen naar b.v. het handboek functioneel beheer, ontwerpdocumentatie van de beheervoorziening BSN applicatie, werkinstructies, eventueel het IBP BPR, het huidige IBP beheervoorziening BSN etc. Ook moet expliciet aandacht worden besteed aan maatregelen die worden getroffen om de toegang van medewerkers van de leverancier van buiten de EU tot beheervoorziening BSN te beperken. Vervolgens kan BPR vaststellen of het stelsel van maatregelen in voldoende mate de eisen afdekt.

3.7.3 *Toezicht en verantwoording*

BPR houdt onder meer toezicht op de uitvoering van het huidige IBP door jaarlijks een assurance rapport te vragen van de leverancier van beheer- en rekencentrumdiensten. Dit is afgesproken in het contract tussen BPR en leverancier.

Het assurance rapport wordt in opdracht van de leverancier opgesteld door een externe auditor en vervolgens aangeboden aan BPR. BPR is wel betrokken bij de opdrachtformulering voor het opstellen van dit rapport. Het assurance rapport wordt gekenmerkt door een onderzoeksopdracht die zich beperkt tot toetsing van opzet en bestaan (momentopname) van maatregelen uit het informatiebeveiligingsplan waarbij deels gesteund wordt op ISO 27001 certificering van de leverancier. Gegeven het belang van beheervoorziening BSN is dit onwenselijk. Het risico is dat BPR een onvolledig beeld krijgt van de stand van de informatiebeveiliging van de beheervoorziening BSN.
Aanbeveling: Evalueer en verbeter de wijze waarop het instrument assurance rapport voor beheervoorziening BSN wordt ingezet in samenhang met de uitvoering van de aanbeveling uit paragraaf 3.7.2.Wij maken hierbij de vergelijking met de Berichtendienst GBA waarbij jaarlijks een assurance rapport wordt verkregen dat zekerheid biedt over de aanwezigheid van het stelsel van maatregelen gedurende het volledige jaar en dat een bredere afbakening kent. In dit rapport wordt naast een uitgebreidere beoordeling van de beveiligingsmaatregelen ook een oordeel gegeven over een aantal belangrijke beheerprocessen.

Inhoudelijk geeft het assurance rapport inzake de beheervoorziening BSN dat in mei 2010 is opgeleverd op hoofdlijnen het volgende beeld:

- een van de twee betrokken rekencentra ligt in een gevoelig gebied (Schiphol) waar de kans op een calamiteit een hogere is;
- restore testen (van back-up) worden niet aantoonbaar uitgevoerd en opslag van back-up media op een externe locatie vindt niet plaats;
- het onderliggende operating system is niet 'gehard' (=optimaal beveiligd) en software updates bleken sinds 23 oktober 2008 niet meer uitgevoerd;

De leverancier heeft in februari 2010 zelf een security test uitgevoerd op de IT-infrastructuur van o.a. de beheervoorziening BSN (zie ook paragraaf 3.3.2). De test heeft een aantal ernstige tekortkoming op beveiligingsgebied in de beheervoorziening BSN omgeving zichtbaar gemaakt die deels samenhangen met het niet uitvoeren van eerdergenoemde software updates. BPR heeft hierop actie ondernomen en de leverancier rapporteert over de voortgang van de verbeteracties. Op basis van de rapportage van de leverancier is het beeld dat een aantal verbeteringen is gerealiseerd. Het plan is dat in het eerste kwartaal van 2011 alle verbeteringen zijn afgerond. Uit ons onderzoek komt het beeld naar voren dat de tekortkomingen niet hebben geleid tot het optreden van incidenten.
Aanbeveling: Ga door met het uitvoeren van een verbeter-programma gericht op het wegnemen van de vastgestelde tekortkomingen.

Binnen BPR zijn de taken op het gebied van informatiebeveiliging verbijzonderd. Dit leidt er in de praktijk toe dat een groot aantal functies op het gebied van informatiebeveiliging is belegd bij één persoon van BPR. Mede als gevolg hiervan worden activiteiten binnen BPR op beveiligingsgebied niet geïntegreerd met andere beheeractiviteiten uitgevoerd. Dit is ongebruikelijk en brengt risico's met zich mee voor de aantoonbare implementatie van het informatiebeveiligingsplan.

Aanbeveling: Breng een duidelijke functiescheiding aan tussen de uitvoerende taken op het gebied van informatiebeveiliging (inclusief de aansturing hiervan door BPR bij Logica) en de controlerende taken op dit gebied zoals betrokkenheid van BPR bij de (de opdrachtformulering voor) het assurance rapport bij Logica.

3.7.4 *Conclusie*

Gegeven de tekortkomingen in de opzet van het informatiebeveiligingsplan en de ernstige tekortkomingen op beveiligingsgebied in de beheervoorziening BSN, is het beeld dat de norm op dit gebied niet toereikend is ingevuld.

3.8 Raadpleegfunctie beheervoorziening BSN

3.8.1 *Algemeen*

De raadpleegfunctie biedt gebruikers van de beheervoorziening BSN een aantal mogelijkheden die noodzakelijk zijn vanuit de processen rondom het burgerservicenummer. Het betreft raadpleegfuncties waarmee:

- van een Nederlands identiteitsdocument op basis van nummer en -type kan worden vastgesteld of het betreffende document in verkeer mag zijn;
- van een BSN kan worden vastgesteld of het geldig is;
- op basis van een BSN een aantal identificerende gegevens kunnen worden opgevraagd;
- op basis van een aantal identificerende gegevens het bijbehorende BSN of sociaal-fiscaalnummer kan worden opgevraagd.

3.8.2 *Aandachtspunt raadpleegfunctie beheervoorziening BSN*

De raadpleegfunctie waarmee op basis van een BSN een aantal identificerende gegevens kan worden opgevraagd, geeft meer informatie terug dan op basis van wet- en regelgeving is toegestaan. Het betreft het gegeven 'land vanwaar ingeschreven'.

Aanbeveling: Breng wet- en regelgeving en het gebruik van het gegeven 'Land vanwaar ingeschreven' met elkaar in overeenstemming.

3.8.3 *Conclusie*

De raadpleegfunctie beheervoorziening BSN geeft in redelijke mate invulling aan de norm met uitzondering van de teruggeven van het gegeven 'Land vanwaar ingeschreven' in de functie voor het opvragen van identificerende gegevens op basis van een BSN.

Bijlage I

Beschikbaarheid:
De mate waarin een object continu beschikbaar is en de gegevensverwerking ongestoord voortgang kan hebben.

Integriteit:
De mate waarin de verwerking van de ingevoerde gegevens juist, volledig en tijdig verloopt en de programma's en bestanden ongeschonden blijven.

Exclusiviteit:
De mate waarin uitsluitend geautoriseerde personen of apparatuur via geautoriseerde procedures en beperkte bevoegdheden gebruik maken van IT-processen.

Controleerbaarheid:
De mate waarin het mogelijk is kennis te verkrijgen over de structurering (documentatie) en werking van een object. Tevens omvat dit kwaliteitsaspect de mate waarin het mogelijk is vast te stellen dat de informatieverwerking in overeenstemming met de eisen ten aanzien van de overige kwaliteitsaspecten is uitgevoerd.

Bijlage II