



## Architectuur BV BSN

Programma BSN

<b>Project</b>	Programma BSN	<b>Document ID</b>	
<b>Auteur(s)</b>	Joost Koedijk Liesbeth Westenberg	<b>Status</b>	Definitief
		<b>Datum</b>	15 mei 2006
		<b>Versie</b>	1.0 (publicatie)
<b>Bestandsnaam</b>	Architectuur BV BSN v10.doc		

Den Haag, 15 mei 2006

Versiehistorie

<b>Versie</b>	<b>Datum</b>	<b>Auteur</b>	<b>Beschrijving</b>
1.0	15-05-2006	L.H. Westenberg J.M.A. Koedijk	Publicatie versie

## INHOUDSOPGAVE

Voorwoord	5
1. Inleiding	7
1.1.Aanleiding	7
1.2.Bronnen	8
1.3.Leeswijzer	9
2. Overzicht architectuur BV BSN	11
2.1.Overzicht architectuur BV BSN	11
2.2.BV BSN binnen NORA	13
3. Eisen BV BSN	17
3.1.Inleiding	17
3.2.Uitgangspunten	17
3.3.Functionele eisen	18
3.3.1. Hoofdeisen	18
3.3.2. Eisen met betrekking tot het genereren van nummers	18
3.3.3. Eisen met betrekking tot het distribueren van nummers	19
3.3.4. Eisen met betrekking tot het registreren en toekennen van nummers	19
3.3.5. Eisen met betrekking tot matching	20
3.3.6. Eisen met betrekking tot functies voor gebruikers	20
3.3.7. Eisen met betrekking tot nummerfouten	21
3.3.8. Eisen met betrekking tot protocollering	21
3.3.9. Eisen met betrekking tot logging, schoning en detectie van misbruik	21
3.3.10. Eisen met betrekking tot authenticatie en autorisatie	22
3.3.11. Eisen met betrekking tot beheerfunctionaliteit	22
3.4.Prestatie-eisen	22
3.5.Overige technische eisen	23
3.6.Kwaliteitseisen	24
3.7.Beveiligingseisen	25
4. Verdieping Architectuur BV BSN	27
4.1.Inleiding	27
4.2.Functionele architectuur	27
4.2.1. Indeling in functionele eenheden	27
4.2.2. Schets functionele architectuur	29
4.2.3. Functionele architectuur en use cases	30
4.3.Applicatiearchitectuur	33
4.4.Technische architectuur	35
4.5.Infrastructuurarchitectuur	36
5. Realisatie van eisen	39
5.1.Inleiding	39
5.2.Realisatie van functionele eisen	39
5.2.1. Genereren van nummers	39
5.2.2. Distribueren van nummers	40

5.2.3. Registreren en toekennen van nummers	40
5.2.4. Matching	42
5.2.5. Functies voor gebruikers	44
5.2.6. Nummerfouten	45
5.2.7. Protocollering	45
5.2.8. Logging en detectie van misbruik	46
5.2.9. Authenticatie en autorisatie	47
5.2.10. Beheerfunctionaliteit	49
5.3. Realisatie van prestatie-eisen	51
5.4. Realisatie overige technische eisen	54
5.5. Realisatie van kwaliteitseisen	55
5.6. Realisatie beveiligingseisen	55

## Voorwoord

In de aanloop richting de oplevering van de beheervoorziening burgerservicenummer (BV BSN) constateerden we dat een verklarend document gericht op de architectuur van en rond de BV BSN ontbrak. De architectuurbeschrijving van het BSN stelsel was anderhalf jaar oud. Verder was er een groot aantal documenten die ieder voor zich delen van het systeem beschreven. Een overkoepelend document helpt de lezers van de individuele stukken de dynamiek en de samenhang beter te begrijpen.

Als je dan op je neemt om de hoofdlijnen van het systeem in een document te verzamelen lijkt het al snel dat je alleen verantwoordelijk bent voor de inhoud. Niets is minder waar. De BV BSN is de afgelopen anderhalf jaar gerealiseerd door een team van enthousiaste en kundige specialisten onder de bezielende leiding van projectleider Bart-Jan Hindriks.

Dit document is mogelijk gemaakt door de inzet van:

Mike Bandhoesingh	Aniel Biharie	Jan Heim van Blankenstein
Coen Bongers	Aldo Braam	Jan Willem Bunt
Louk Conrads	Joke Dasselaar	Mike Dell
Wiel Erens	Martin Folkerts	Rogier Goede
Dries de Groot	Matthijs den Haan	Ben Kalkhoven
Jonne Kats	Hedde van der Lugt	Koos de Meij
Rob van der Meijden	Rudy van der Pijl	Erwin Reinhoud
Viola Smaal	Andries Stam	Dennis Stam
Marianne Zijderveld	Perica Zivkovic	

Het project floreerde in de zeer prettige omgeving van het programmabureau burgerservicenummer dat onder de zeer deskundige leiding stond van Ineke Ruiter en José Loogman. Voor de goede omgeving waren ook Angelika Hoffmann en Linda Pols van het programmasecretariaat verantwoordelijk.

Wij hebben met genoegen voor dit interessante project mogen werken. Met veel plezier hebben we de hoofdlijnen bijeengebracht en opgeschreven.

We wensen u veel leesplezier!

Den Haag, mei 2006

Liesbeth Westenberg, functioneel architect  
Joost Koedijk, technisch architect  
Beheervoorziening Burgerservicenummer



## 1. Inleiding

### 1.1. Aanleiding

In juni 2002 publiceerde de zogenoemde Tafel van Thijn hun rapportage "Persoonsnummerbeleid in het kader van identiteitsmanagement". In dit advies wordt de basis gelegd voor het burgerservicenummer (BSN) en het bijbehorende stelsel van voorzieningen. Eind 2003 heeft minister De Graaf het Programma Andere Overheid aan de Tweede Kamer aangeboden waarin wordt gesteld dat het invoeren van een BSN één van de belangrijkste instrumenten is voor de overheid om effectief en efficiënt gebruik te maken van ICT. In mei 2004 besluit het kabinet tot invoering van het BSN. Het programmabureau burgerservicenummer, ondergebracht bij de stichting ICTU, krijgt de opdracht om de invoering ter hand te nemen.

Het systeem dat het BSN stelsel mogelijk moet maken wordt de Beheervoorziening burgerservicenummer (BV BSN), destijds de Overkoepelende Beheervoorziening (OBV) genoemd. De BV BSN is het geheel van voorzieningen dat zorgt voor het genereren, distribueren, beheren en raadplegen van het BSN. De Beheervoorziening regelt ook de toegang tot de identificerende gegevens in de achterliggende authentieke registraties (GBA en de toekomstige Registratie Niet-ingezetenen (RNI)) en de verificatieregisters voor de identiteitsbewijzen ter verificatie van de documenten aan het loket. Voor de realisatie en inrichting van de BV BSN richt het programmabureau BSN een project in onder leiding van projectleider Bart-Jan Hindriks. Dit project, de aanpak, organisatie en planning wordt beschreven in het "Project Initiatie Document" [7].

Vanaf najaar 2004 is er intensief gewerkt aan de definitie en uitwerking van de functionaliteit van de BV BSN. Nog voor het einde van het jaar verscheen er een eerste versie van het functioneel ontwerp. In januari 2005 stemde de Stuurgroep in met het in eigen beheer en onder regie van het programmabureau BSN realiseren van het systeem. In maart 2005 werd een eerste werkende "Proof of Concept" van de BV BSN gepresenteerd. Ook daarna is veel inspanning geleverd om de doelstelling, invoering van het BSN per 1 januari 2006, mogelijk te maken.

Gedurende een dergelijk project worden de specificaties en eisen op steeds groter detailniveau uitgewerkt. Het werkveld is zeer divers. Vanuit de regering is de minister voor Bestuurlijke Vernieuwing en Koninkrijksrelaties (BVK) aangesteld als verantwoordelijk minister. De Stuurgroep BSN, onder leiding van het ministerie van Binnenlandse Zaken, bestaat uit een afvaardiging van de ministeries van VWS, FIN, SZW, JUS, OCW, de Vereniging Nederlandse Gemeenten (VNG), de Manifestgroep, het College Bescherming Persoonsgegevens (CBP) en het agentschap Basisadministratie Persoonsgegevens en Reisdocumenten (BPR). Afstemming met de ambtelijk opdrachtgever van het programmabureau BSN het ministerie van BZK, directie IIOS en de Stuurgroep BSN, heeft daarbij met name op basis van notities plaatsgevonden. In dergelijke notities worden de verschillende aspecten van een deelprobleem belicht en een voorstel gedaan op welke wijze het deelprobleem wordt aangepakt.

De gekozen wijze van afstemming is uitermate goed geschikt in het verkeer tussen opdrachtgever en opdrachtnemer. Het resulteert echter in een aanzienlijk verzameling documenten waarin (de motivatie voor) ontwerpbeslissingen zijn opgenomen. Veelal is daarbij het verslag van de stuurgroep BSN bijeenkomsten nodig om zeker te weten dat een besluit ook is overgenomen. Voor een buitenstaander die zich een beeld van de BV BSN wil vormen, inclusief de motivatie van de genomen beslissingen, is deze wijze van documentatie weinig toegankelijk.

Met dit document wordt op hoofdlijnen inzicht gegeven in de eisen die een rol speelden bij het ontwerpen en realiseren van de Beheervoorziening BSN. Naast de eisen wordt ook aangegeven op welke wijze de BV BSN is ingericht zodat aan de eisen wordt voldaan. Ook is de architectuur van het systeem van verschillen kanten belicht. Doelgroep is die buitenstaander die niet is geïnteresseerd in de historie van het project maar die graag wil weten hoe, en waarom zo, de BV BSN werkt.

## 1.2. Bronnen

De onderstaande lijst met bronnen<sup>1</sup> bevatten stukken die zijn vastgesteld door de Stuurgroep Burgerservicenummer dan wel afgeleid van door deze Stuurgroep vastgestelde stukken in de periode juli 2004 tot en met april 2006. Enkele documenten zijn nog in concept, aangezien het parlementaire traject nog niet is afgerond. Een voorbeeld hiervan is het Logisch Ontwerp BSN dat een directe relatie kent met het nog in ontwikkeling zijnde Besluit Burgerservicenummer.

- [1] Software Architecture Document (versie 15 maart 2006)
- [2] Uitkomst onderzoek requirements relatieve relevantie, Mike Dell, 7 april 2005
- [3] Technische Test BV BSN, Plan van Aanpak voor het testen van niet-functionele eisen van de infrastructuur Beheervoorziening Burgerservicenummer, Quick van Rijt/Ben Kalkhoven, versie 1.0, 7 december 2005
- [4] Informatiebeveiligingsplan Beheervoorziening BSN, versie 2.0, 18 april 2006
- [5] Aanvullende Specificatie, Mike Dell, 9 december 2004 (Opgeleverd bij het Functioneel Ontwerp december 2004).
- [6] Logisch Ontwerp BSN, versie 1.01
- [7] Project Initiatie Document, Overkoepelende beheervoorziening, Bart-Jan Hindriks, 20 januari 2005.
- [8] Nederlandse OverheidsReferentieArchitectuur, ICTU Programma Elektronische Overheid, versie 0.8, 31 maart 2006.
- [9] Architectuur infrastructuur Beheervoorziening BSN, Hedde van der Lugt, Versie 1.0, 15 mei 2006.
- [10] Advies van de Tafel van Thijn "Persoonsnummerbeleid in het kader van identiteitsmanagement", juni 2002
- [11] Wetsvoorstel Algemene Bepalingen Burgerservicenummer, Tweede Kamer, vergaderjaar 2005–2006, 30 312, nr. 2
- [12] Notitie "Omgeving BV BSN", Joost Koedijk, versie 11 augustus 2005
- [13] Implementatieplan Burger Service Nummer, 18 december 2005

---

<sup>1</sup> Met uitzondering van [8]

- [14] Notitie nummerreeks BSN, André van Brussel, versie 1.1, 17 augustus 2005
- [15] Plan van aanpak OBV in het kader van het BSN, versie 1.4, 12 augustus 2003, bijlage bij [13]
- [16] Notitie verificatievraag toetsen geldigheid BSN, Liesbeth Westenberg, 05 juni 2005 (afgesteld in werkgroep registerhouders d.d. 17 juni 2005)
- [17] Functioneel Ontwerp BV BSN, versie 1.4.1
- [18] Architectuur burgerservicenummerstelsel, Udo Pijpker, versie 3.3, 15 november 2004 (vastgesteld in stuurgroep 24 november 2004)
- [19] Dienstverleningsafspraken tussen BPR en DIIOS, versie 0.9
- [20] Voorschrift Informatiebeveiliging Rijksdienst 1994, Besluit van 22 juli 1994
- [21] Functioneel Ontwerp BC GBA, versie 1.4.1
- [22] Functioneel Ontwerp BC BVR, versie 1.4.1
- [23] Functioneel Ontwerp Beheer, versie 1.4.1
- [24] Functioneel Ontwerp EVA- Elementaire Verificatie Applicatie, versie 1.4.1
- [25] Logisch Ontwerp GBA, versie 3.4
- [26] Notitie GBA-berichten, Liesbeth Westenberg, 27 februari 2006
- [27] Notitie intelligent zoeken, Liesbeth Westenberg, versie 1.1, 23 september 2005
- [28] Notitie Intelligent zoeken geslachtsnaam, Liesbeth Westenberg, 06 oktober 2005
- [29] Notitie Logging en protocollering, Joost Koedijk, 11 mei 2005
- [30] Notitie Detectie misbruik, Mike Dell, 6 december 2005
- [31] Autorisaties binnen de Beheervoorziening BSN, Joost Koedijk, 1 juni 2005
- [32] Authenticatie binnen de Beheervoorziening BSN, Joost Koedijk, 1 juni 2005
- [33] Rapportage Kwetsbaarheidanalyse Beheervoorziening BSN, Programmabureau BSN, versie 2.0, 20 april 2006
- [34] Rapportage Afhankelijkheidsanalyse BV BSN, Programmabureau BSN, versie 2.0, 19 april 2006

### **1.3. Leeswijzer**

Het document start in hoofdstuk 2 met een korte uitleg van de werking van de BSN voorziening. Daarbij wordt kort een plaatsbepaling gegeven ten opzichte van de "Nederlandse OverheidReferentieArchitectuur" (NORA) [8] zoals die momenteel onder leiding van het ICTU programma "Architectuur" wordt vormgegeven.

In het derde hoofdstuk zijn de zeer gevarieerde eisen opgenomen die aan de BV BSN worden gesteld. Niet alleen worden de belangrijkste functionele eisen genoemd ook prestatie-eisen vinden hun plaats.

In het vierde hoofdstuk wordt de architectuur van de BV BSN verder uitgediept. Naast de applicatie-architectuur wordt daarbij ingegaan op de functionele, technische en infrastructurele architectuur.

In het vijfde en laatste hoofdstuk komt de wijze waarop de gestelde eisen zijn gerealiseerd aan de orde. Juist door keuzen in de architecturen blijken veel van deze eisen te realiseren. Maar ook het gestructureerd werken in een moderne ontwikkelomgeving komt de kwaliteit van het systeem ten goede. In dit hoofdstuk passeren de belangrijkste maatregelen voor een goed functionerende Beheervoorziening burgerservicenummer.



## 2. Overzicht architectuur BV BSN

### 2.1. Overzicht architectuur BV BSN

In deze paragraaf wordt een overzicht gegeven van de architectuur van de BV BSN. Het doel van dit overzicht is om de lezer op een globaal niveau inzicht te geven in de diverse aspecten van de BV BSN. Voor een meer gedetailleerd inzicht wordt verwezen naar hoofdstuk 4.

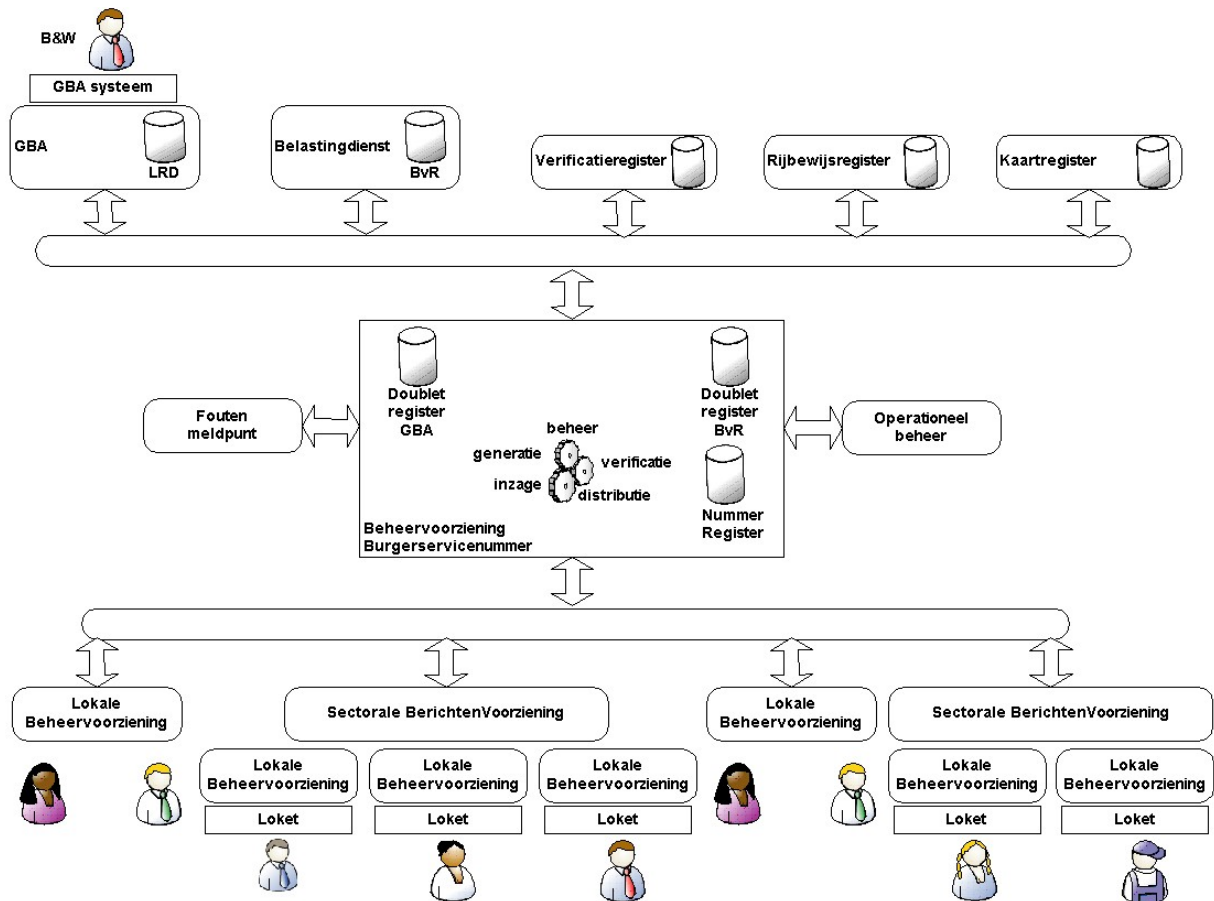
Het BSN is een uniek nummer, dat numeriek gelijk is aan het sofi-nummer. Het gaat binnen de gegevenshuishouding van de overheid een spilfunctie innemen: persoonsgebonden gegevens kunnen doelmatig en – mits wettelijk toegestaan – betrouwbaar worden uitgewisseld tussen overheid en burger en tussen (semi-) overheidsorganisaties onderling. Om dit technisch mogelijk te maken is een systeem, de Beheervoorziening burgerservicenummer (BV BSN), ingericht.

De BV BSN is het geheel van voorzieningen dat het genereren, distribueren, beheren en raadplegen van het BSN verzorgt. De belangrijkste taak is echter gebruikers te ondersteunen bij het betrouwbaar vaststellen van het BSN van een burger. Daartoe wordt met behulp van de beheervoorziening ook (geautoriseerd) toegang verleend tot identificerende persoonsgegevens en kan worden gecontroleerd of identiteitsdocumenten die aan het loket worden gebruikt nog in omloop mogen zijn. Op deze wijze kan een gebruiker voldoen aan de vergewisplicht, die uit de wet algemene bepalingen burgerservicenummer volgt, voordat het nummer in de eigen administratie wordt opgenomen.

De BV BSN functioneert als een berichtenmakelaar; de informatie die vanuit diverse bronnen wordt betrokken wordt aan gebruikerssystemen in de vorm van een elektronisch bericht doorgegeven. Er is binnen de BV BSN geen sprake van een rechtstreekse gebruikersinterface. Het systeem is ingericht op 24 uur gebruik per dag en 7 dagen per week. De Beheervoorziening spreekt de WSI standaard XML/SOAP met haar gebruikers. In onderstaande figuur wordt de architectuur van de BV BSN weergegeven. Centraal staat daarbij de BV BSN zelf.

Aan de bovenkant van de figuur zijn de bronnen voor informatie weergegeven die de BV BSN bij de uitvoering van zijn taken gebruikt. Daaronder vallen drie "identiteitsdocumentregisters" (verificatieregister reisdocumenten, rijbewijsregister en kaartregister) die worden gebruikt om informatie over de status van een Nederlands identiteitsdocument op te vragen. Daarnaast worden (een beperkte set identificerende) persoonsgegevens verkregen uit de registraties GBA (Gemeentelijke Basisadministratie persoonsgegevens) en BvR (Beheer van Relaties van de Belastingdienst. In BvR zijn geen BSN's opgenomen zodat deze verzameling persoonsgegevens uitsluitend rond toekenning wordt geraadpleegd. Heeft een persoon immers geen BSN maar wel een sofi-nummer dan zal dit sofi-nummer tot BSN worden opgewaardeerd.

Toekenning van burgerservicenummers gebeurt door gemeenten. Om dit te kunnen registreren is een koppeling met het GBA-berichtenverkeer gerealiseerd. Een Register Niet-Ingezetenen (RNI) is voorzien. Dit zal in de toekomst alle personen bevatten die niet voor inschrijving in de GBA in aanmerking komen maar die wel een BSN gaan krijgen. Bij de realisatie van RNI zal de BV BSN toegang moeten krijgen tot de opgeslagen persoonsgegevens en zullen berichten rond toekenning moeten worden uitgewisseld.



Op grond van de Wet Algemene Bepalingen Burgerservicenummer [11] zijn overheidsorganen en bepaalde andere organisaties gebruikers. Voorbeelden hiervan zijn gemeenten, pensioenfondsen, ziekenhuizen, politie, justitie, zorgverzekeraars, waterschappen, de Belastingdienst en GGD'en. Voordat gebruikers een BSN in hun processen inzetten vergewissen zij zich ervan dat de betreffende burger en het verkregen BSN bij elkaar horen. Hiervoor kunnen zij gebruik maken van de BV BSN. Ter ondersteuning van de loketfuncties bij gebruikers zullen lokale en sectorale berichtenvoorzieningen worden ingezet.

Gebruikers worden per organisatie of per sector, op basis van sectorale wetgeving, aangesloten. Het is de taak van de sector om de, bij wetgeving vastgelegde, toegang

binnen de sector verder op een verantwoorde wijze door te leveren. Voor de BV BSN wordt nimmer aan personen direct gebruikerstoegang verleend.

Omdat de beheervoorziening uitsluitend in (synchrone) XML-berichten spreekt is de gebruiker zelf verantwoordelijk voor opname in de gebruikersprocessen en het realiseren van een gebruikersinterface.

## **2.2. BV BSN binnen NORA**

Door het inzetten van ICT-oplossingen probeert de overheid doelen te realiseren zoals betere dienstverlening aan burgers en bedrijven, administratieve lastenverlichting en betere samenwerking tussen overheidsorganisaties. Door veel projecten worden componenten gerealiseerd die elk voor een deel invulling geven aan de elektronische overheid.

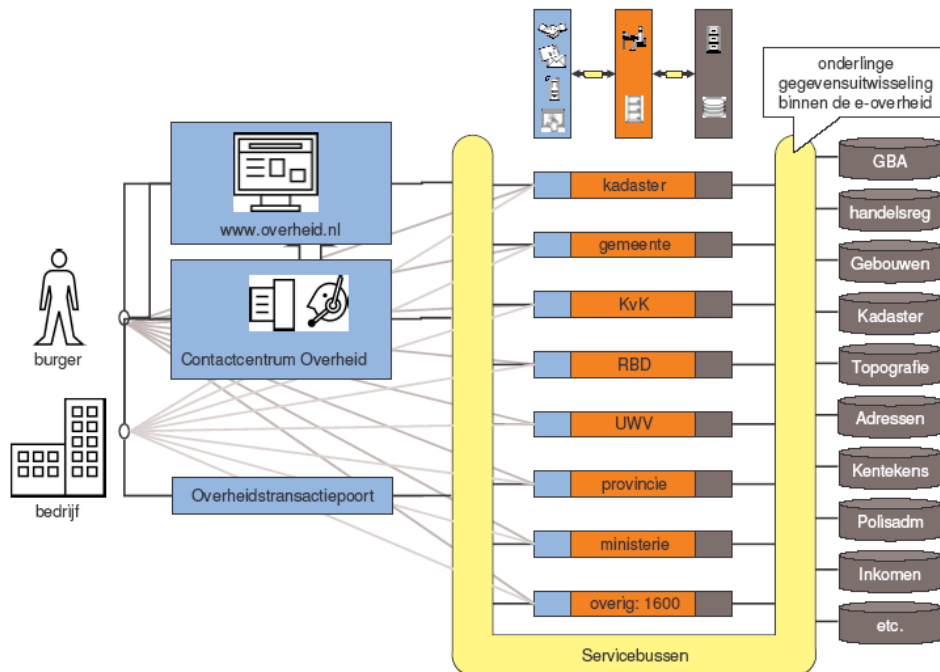
Nu de elektronische overheid meer en meer realiteit begint te worden, neemt de roep om samenhang bij ontwerp, ontwikkeling, implementatie en beheer toe. Zo wordt voorkomen dat gebruikers van deze voorzieningen, zoals gemeenten, een overdaad aan ontwikkelingen bij moet houden. Door het opzetten van een architectuur wordt geborgd dat processen, diensten en producten bij implementatie goed op elkaar zijn afgestemd zodat de doelstellingen behaald worden.

Het programma Architectuur e-overheid heeft in de tweede helft van 2005 een zogenaamde Referentie-architectuur ontwikkeld voor de elektronische overheid. Deze architectuur is het resultaat van intensieve samenwerking van architecten van een aantal grote uitvoeringsorganisaties én die van een aantal ICTU programma's. Het resultaat, de Nederlandse OverheidsReferentieArchitectuur (NORA) [8], sluit naadloos aan bij de "Referentie Architectuur Gemeenten" (Refag). De NORA, die een breed draagvlak heeft, is echter nog niet af: van een aantal kanten zal nog feedback op de huidige versie worden gegeven.

De basisstructuur van de elektronische overheid gaat uit van burgers en bedrijven die een dienst of product vragen van een organisatie in het publieke domein. Een belangrijk stelsel van samenhangende principes is de volgende: het aanbieden van meerdere kanalen, vrije kanaalkeuze voor de aanvrager, één loket, 7 x 24 uur beschikbaar. Een tweede belangrijk uitgangspunt is dat gegevens slechts één maal worden gevraagd aan burgers en bedrijven. De gegevens worden centraal opgeslagen en aan alle overheidsorganisaties ter beschikking gesteld door de basisregistraties. Koppelmechanismen zorgen tenslotte voor een snelle, veilige en betrouwbare uitwisseling van informatie tussen websites, overheidsorganisaties en basisregistraties.

Om de doelstellingen van de elektronische overheid te bereiken wordt in de NORA gekozen voor de Service Gerichte Architectuur (SGA) als ontwerpbenadering. Dit is een fundamentele keuze, gebaseerd op moderne inzichten in de inrichting van bedrijven, ketens en netwerken. In een SGA is de relatie tussen een architectuuronderdeel en zijn omgeving een dienstverleningsrelatie, dat wil zeggen, het

onderdeel levert services aan zijn omgeving en neemt daar services van af. De communicatie tussen de onderdelen binnen de architectuur zijn daarbij gebaseerd op berichten. De architectuuronderdelen worden in de uitvoering van hun dienstverleningsrelatie ondersteund door een servicebus. Servicebussen moeten minimaal berichtenverkeer kunnen afhandelen, maar kunnen ook andere functies bieden waaronder ook het bundelen van services.



Nederlandse overheid als dienstverlener, bron [8]

De beheervoorziening burgerservicenummer is (niet meer dan) een component in het Nederlandse overheids-ICT-landschap. Een systeem dat uitwisseling van persoonsgegevens (uit twee basisregistraties) op basis van een nummer mogelijk maakt. Het spreekt voor zich dat juist voor gegevensuitwisseling de BV BSN moet aansluiten bij toekomstige technische ontwikkelingen. Het is daarom goed op te merken dat de BV BSN, zeker voor wat betreft de communicatie met haar gebruikers, 1-op-1 past binnen een Service Gerichte Architectuur. De diensten van een BV BSN zijn via een servicebus te ontsluiten; de “Sectorale Berichten Voorziening in de Zorg” (SBV-Z) is een voorbeeld van een servicebus die bedoeld is om met de diensten van de BV BSN samen te werken.

De NORA geeft meer richtlijnen die bij de realisatie van nieuwe systemen een rol spelen. Lang niet alle richtlijnen zijn voor de BV BSN relevant of van toepassing. Hier worden echter enkele belangrijkste richtlijnen, en de mate van conformiteit van de BV BSN, gegeven.

Bij het maken geeft de NORA – bij gelijke mate van geschiktheid – de voorkeur aan open standaarden. Hieraan is binnen de BV BSN in ruime mate gehoor gegeven. De interface naar de gebruikers en het softwareontwikkelplatform zijn voorbeelden van het gebruik van open standaarden. Voor het berichtenverkeer geeft de NORA de keuze

tussen de twee open standaarden ebXML en webservices. Bij de realisatie van de BV BSN is voor webservices gekozen. De beveiliging van het berichtenverkeer is gebaseerd op PKIOverheid.

Ook aan andere, meer technische, vereisten aan de NORA wordt bij de BV BSN voldaan. Zo is de BV BSN robuust en heeft hoge beschikbaarheid die gebaseerd is op 7 dagen van 24 uur dienstverlening. De gegevens worden opgeslagen in een relationele database. Voor de gegevensdefinitie van persoonsgegevens wordt nauw aangesloten bij de definitie die binnen de Gemeentelijke Basis Administratie (GBA) wordt gebruikt.

De BV BSN is gebouwd binnen een omgeving die in beweging is. Zo wordt het GBA gemoderniseerd en is een Register Niet Ingezetenen voorzien. Stabiliteit wordt echter nagestreefd, met name op de functies voor gebruikers. Deze functies zullen immers niet wijzigen. Het is goed dat geconcludeerd kan worden dat de BV BSN deze diensten toekomstvast conform de eisen uit de NORA levert.



### **3. Eisen BV BSN**

#### **3.1. Inleiding**

Zoals in de inleiding van dit document reeds is aangegeven, is er vanaf najaar 2004 intensief gewerkt aan de definitie en realisatie van de BV BSN. Er is daarbij gestart met een aantal uitgangspunten en een set eisen op hoofdlijnen, die in de loop van het project steeds verder gedetailleerd zijn. De afstemming op dit detailniveau is in de loop van het project uitgevoerd op basis van notities, die in de verschillende gremia (registerhoudersoverleg, projectleidersoverleg en stuurgroepoverleg) zijn behandeld.

In dit hoofdstuk wordt nader ingegaan op de uitgangspunten en eisen, die hebben geleid tot de huidige realisatie van de BV BSN. De eisen zijn ingedeeld naar:

- Functionele eisen
- Prestatie-eisen
- Overige technische eisen
- Kwaliteitseisen
- Beveiligingseisen

In Hoofdstuk 5 wordt ingegaan op de realisatie van deze eisen en de overwegingen die hierbij een rol hebben gespeeld.

#### **3.2. Uitgangspunten**

Een aantal uitgangspunten heeft ten grondslag gelegen aan de definitie en realisatie van de BV BSN. Deze hebben de keuzes gedurende het project bepaald. In deze paragraaf worden deze behandeld.

Het advies van de Tafel van Thijn [10] heeft gediend als startpunt en uitgangspunt bij met name de beslissingen met betrekking tot de functionele inrichting van de BV BSN. Daarnaast is het wetsvoorstel Algemene Bepalingen Burgerservicenummer (Wabb) [11] een leidraad geweest, waarbij moet worden opgemerkt dat het wetgevingstraject parallel aan het ontwikkelen van de BV BSN heeft plaatsgevonden.

Een belangrijk uitgangspunt is geweest dat voorzien werd dat het BSN-stelsel op 1 januari 2006 van start zou gaan. Dit heeft invloed gehad op de keuzes die tijdens het project zijn gemaakt. Er is bijvoorbeeld niet gekozen voor het aansluiten op een gemoderniseerde GBA, omdat deze per 1 januari 2006 nog niet gerealiseerd was. Bij de keuzes die zijn gemaakt zijn echter nooit de minimale (kwaliteits-)eisen in het geding geweest.

Om de impact van de BV BSN op de gemeente (burgerzaken) en de gemeentelijke systemen te beperken is als uitgangspunt gehanteerd dat er minimale wijzigingen in de GBA-systemen doorgevoerd zouden worden.

Bij de keuzes in de techniek is het gebruik van open standaarden (bij gelijke geschiktheid) één van de uitgangspunten geweest. Daarnaast is aansluiting bij de beoogde beheerorganisatie als uitgangspunt gehanteerd.

Als laatste is speciale aandacht besteed aan het definiëren van de uitgangspunten voor de karakteristieken van het berichtenverkeer.

Uitgangspunt
Er vinden per (werk)dag 2.000 mutaties plaats op het nummerregister (400.000 nieuwe nummers per jaar; 200 werkdagen).
Er worden per (werk)dag 530.000 verificatievragen plaats. Dat zijn 106 miljoen berichten per jaar.
Een enkel bericht (vraag of antwoord) is gemiddeld 5kb groot.
De gemiddelde belasting wordt berekend over kantooruren (66.250 per uur, 18,5 bericht per seconde). De piekbelasting is 10 keer het gemiddelde (185 berichten per seconde).

Bron: Notitie "Omgeving BV BSN 050811" [12]

De hierna geformuleerde prestatie-eisen kunnen tezamen met de karakteristieken van het berichtenverkeer en de eisen voor logging nader worden uitgewerkt in technische eisen van het systeem. De belasting van het systeem wordt daarbij vrijwel uitsluitend bepaald door de verificatievragen. Op basis van genoemde kengetallen, kunnen (bij een responsetijd van 1 seconde) een aantal technische eisen worden bepaald.

### 3.3. Functionele eisen

#### 3.3.1. Hoofdeisen

- 1.0 De BV BSN moet BSN's genereren
- 2.0 De BV BSN moet BSN's distribueren
- 3.0 De BV BSN moet registreren welk nummer wanneer is toegekend
- 4.0 De BV BSN moet voorkomen dat één persoon meerdere nummers krijgt
- 5.0 De BV BSN moet gebruikers transparant toegang geven tot het BSN-domein
- 6.0 De BV BSN moet fouten met betrekking tot de uniciteit van het nummer registreren

bron: Implementatieplan Burger Service Nummer [13]

#### 3.3.2. Eisen met betrekking tot het genereren van nummers

Nr	Eis	Herkomst eis
1.10	leder gegenereerd nummer moet uniek zijn.	Impliciet
1.20	Er mag geen volgorde van nummers blijken.	Advies tafel van Thijn [10] (Het nummer moet informateloos zijn)
1.30	leder gegenereerd nummer moet 9-cijferig zijn en aan de 11-proef	Advies tafel van Thijn [10] (Het BSN moet (inhoudelijk) gelijk aan het Sofi-

	voldoen.	nummer zijn)
1.40	Er moet een instelbaar interval zijn waarbinnen BSN's worden gegenereerd.	Advies tafel van Thijn [10] (Wie een sofi-nummer heeft, behoudt dit nummer) Notitie nummerreeks BSN [14] (Beperking nummerrange tbv UWV)
1.50	Nummers moeten in batches gegenereerd worden	Plan van aanpak OBV [15]

### 3.3.3. Eisen met betrekking tot het distribueren van nummers

Nr	Eis	Herkomst eis
2.10	Een toekennende instantie moet een voorraad nummers kunnen aanvragen	Plan van aanpak OBV [15]
2.20	Ieder gegenereerd nummer mag slechts eenmaal aan een gemeente worden uitgegeven	Impliciet
2.30	Er moet worden geregistreerd aan welke partij het nummer is gedistribueerd	Implementatieplan Burger Service Nummer [13]
2.40	Het distribueren van nummers aan de gemeente moet per set nummers plaatsvinden.	Plan van aanpak OBV [15]

### 3.3.4. Eisen met betrekking tot het registreren en toekennen van nummers

Nr	Eis	Herkomst eis
3.10	Het moet duidelijk zijn in welke fase van de 'levenscyclus' het nummer verkeert. Hierbij worden de volgende statussen onderscheiden: - Aangemaakt - Gedistribueerd - In verkeer - Uit verkeer	Notitie verificatievraag toetsen geldigheid BSN [16]
3.20	Er moet worden geregistreerd door welke instantie een nummer is toegekend	Implementatieplan Burger Service Nummer [13]
3.30	Er moet worden geregistreerd op welke datum een nummer is toegekend	Implementatieplan Burger Service Nummer [13]
3.40	Het moet mogelijk zijn een sofi-nummer op te waarden tot BSN	Implementatieplan Burger Service Nummer [13]

3.50	(mogelijke) Sofinnummers moeten in het nummerregister geregistreerd zijn	Impliciet (volgt uit vorige eis)
3.60	Er moet historie met betrekking tot de mutaties in het nummerregister worden bijgehouden	Implementatieplan Burger Service Nummer [13]
3.70	Er mogen geen persoonsgegevens opgeslagen worden in het nummerregister	Implementatieplan Burger Service Nummer [13]

### 3.3.5. Eisen met betrekking tot matching

Nr	Eis	Herkomst eis
4.10	Er moet onderzocht kunnen worden of een persoon niet reeds een BSN of sofi-nummer heeft.	Implementatieplan Burger Service Nummer [13]

### 3.3.6. Eisen met betrekking tot functies voor gebruikers

Nr	Eis	Herkomst eis
5.10	Gebruikers krijgen een faciliteit waarmee zij aan het loket kunnen controleren of het nummer en de naam die zij opgeven bij elkaar horen. <ul style="list-style-type: none"> <li>- Toetsen geldigheid BSN</li> <li>- Opvragen identificerende gegevens op basis van een BSN</li> <li>- Toetsen van de combinatie BSN en identificerende gegevens</li> </ul>	Implementatieplan Burger Service Nummer [13] Functioneel Ontwerp BV BSN [17] (en voorgaande versies) Architectuur burgerservicenummerstelsel [18]
5.20	Gebruikers dienen een faciliteit te krijgen waarmee zij op basis van enkele persoonsgegevens het nummer kunnen zoeken <ul style="list-style-type: none"> <li>- Opvragen BSN op basis van identificerende gegevens</li> </ul>	Implementatieplan Burger Service Nummer [13] Functioneel Ontwerp BV BSN [17] (en voorgaande versies) Architectuur burgerservicenummerstelsel [18]
5.30	Gebruikers dienen een faciliteit te krijgen waarmee zij de geldigheid van identiteitsdocumenten (rijbewijs, paspoort,	Architectuur burgerservicenummerstelsel [18]

	vreemdelingenkaart) kunnen controleren	
--	--	--

### 3.3.7. Eisen met betrekking tot nummerfouten

Nr	Eis	Herkomst eis
6.10	Nummerfouten moeten door gebruikers en gemeenten gemeld kunnen worden	Implementatieplan Burger Service Nummer [13]

### 3.3.8. Eisen met betrekking tot protocollering

Nr	Eis	Herkomst eis
7.10	Burgers moeten binnen 4 weken geïnformeerd kunnen worden over welke gegevens door welke gebruikers zijn geraadpleegd in het afgelopen jaar	Wet GBA

### 3.3.9. Eisen met betrekking tot logging, schoning en detectie van misbruik

Nr	Eis	Herkomst eis
8.10	Berichten moeten worden vastgelegd en gedurende een bepaalde periode worden bewaard	Functioneel Ontwerp BV BSN [17] (en voorgaande versies)
8.20	Elke processtap dient te worden vastgelegd ten behoeve van traceerbaarheid. Als een proces goed is afgerond, hoeft alleen de laatste stap te worden vastgelegd	Functioneel Ontwerp BV BSN [17] (en voorgaande versies)
8.30	Systeemfouten moeten vastgelegd worden	Functioneel Ontwerp BV BSN [17] (en voorgaande versies)
8.40	Geconstateerde nummerfouten dienen vastgelegd te worden	Functioneel Ontwerp BV BSN [17] (en voorgaande versies)
8.50	Er dient detectie van misbruik door gebruikers te vinden	Functioneel Ontwerp BV BSN [17] (en voorgaande versies)
8.60	Alle logboeken dienen periodiek geschoond te worden	Functioneel Ontwerp BV BSN [17] (en voorgaande versies)

### 3.3.10. Eisen met betrekking tot authenticatie en autorisatie

Nr	Eis	Herkomst eis
9.10	Voordat een dienst kan worden afgenomen, moet zowel authenticatie als autorisatie plaatsvinden	Functioneel Ontwerp BV BSN [17] (en voorgaande versies)

### 3.3.11. Eisen met betrekking tot beheerfunctionaliteit

Nr	Eis	Herkomst eis
10.10	De beheerder moet functies ter beschikking krijgen waarmee de volgende functies uitgevoerd kunnen worden: <ul style="list-style-type: none"> <li>- Opvragen gegevens uit logboeken</li> <li>- Functies voor het corrigeren van foutieve situaties</li> <li>- Inloggen, uitloggen en het loggen hiervan</li> <li>- Gebruikersbeheer</li> <li>- Beheer beheeraccounts</li> </ul>	Functioneel Ontwerp BV BSN [17] (en voorgaande versies)

## 3.4. Prestatie-eisen

Er zijn in deze categorie met name eisen gesteld ten aanzien van de prestaties van de beheervoorziening Burgerservicenummer. Deze worden in de volgende paragraaf weergegeven. Bij de invulling van deze eisen is kennis van (met name de omvang van) het berichtenverkeer wenselijk. Omdat deze kennis (logischerwijs) ontbreekt is de voorspelling voor de karakteristieken van het berichtenverkeer opgenomen. Deze karakteristieken waren uitgangspunt om te verifiëren hoe aan de eisen kon worden voldaan.

Nr	Eis	Herkomst eis
	De beheervoorziening burgerservicenummer kan omgaan met een groeiend aantal bevragingen.	Schaalbaar
	De beheervoorziening burgerservicenummer wordt zodanig uit componenten opgebouwd dat uitval van één	Fouttolerant

	component niet kan leiden tot uitval van het gehele systeem.	
	De beheervoorziening burgerservicenummer verleent 365*24 uur dienstverlening per jaar. De beschikbaarheid in deze periode is groter dan 99,8%.	Dienstverleningsafspraken tussen BPR en DIIOS [19]
	Het uitvoeren van onderhoudswerkzaamheden heeft geen invloed op de beschikbaarheid van de BV BSN.	Dienstverleningsafspraken tussen BPR en DIIOS [19]
	De maximaal verloren tijd per storing van de beheervoorziening burgerservicenummer is 120 minuten. Maximaal is er 17,5uur uitval (door storingen én wijzigingen) per jaar.	Dienstverleningsafspraken tussen BPR en DIIOS [19]
	Er zijn maximaal 2 storingen van de beheervoorziening burgerservicenummer per maand.	Dienstverleningsafspraken tussen BPR en DIIOS [19]
	De beheervoorziening burgerservicenummer is na een calamiteit binnen 24 uur weer beschikbaar.	Dienstverleningsafspraken tussen BPR en DIIOS [19]
	De responsetijd van de beheervoorziening burgerservicenummer bij gemiddelde belasting is maximaal 1 seconde. Bij piekbelasting is de responsetijd maximaal 3 seconden.	Dienstverleningsafspraken tussen BPR en DIIOS [19] (Deze responsetijden zijn met name van toepassing voor alle diensten waarvoor geen externe bron, zoals een register voor identiteitsdocumenten, hoeft te worden geraadpleegd.)

### 3.5. Overige technische eisen

Naast de eerder genoemde prestatie en functionele eisen zijn aanvullende technische eisen geformuleerd. Hieronder is een overzicht, met bronvermelding, opgenomen.

- De maatwerksoftware van de BV BSN dient goed onderhoudbaar te zijn zodat realisatie van nieuwe wensen, aanpassingen ten gevolge van veranderingen in de omgeving of het herstel van fouten kostenefficiënt en eenvoudig uitvoerbaar zijn. Dit brengt met zich mee dat het systeem transparant van opzet moet zijn waardoor de diverse mogelijke aanpassingen goed zijn uit te voeren. De technische architectuur van het systeem moet voorzien in een stabiele basis die na een aanpassing passend in de architectuur stabiel blijft. Evenzo moet het systeem goed testbaar blijven.[5]
- De interfaces van de BS BSN moeten in detail gespecificeerd zijn. [5]

- Op alle maatwerk software componenten mogen geen beperkingen rusten die publieke publicatie van broncode zouden kunnen verhinderen. [5]

### 3.6. Kwaliteitseisen

In de voorgaande paragrafen is beschreven aan welke (niet-)functionele eisen het systeem, het geheel van software en ondersteunende processen, moet gaan voldoen. In voorjaar 2005 heeft het team dat verantwoordelijk is voor de realisatie van de Beheervoorziening burgerservicenummer besproken aan welke kwaliteitseisen de (toen nog) te realiseren software dient te voldoen [2].

Deze kwaliteitsaspecten hangen natuurlijk nauw samen met de geformuleerde (niet-) functionele eisen. Ze bieden echter in sommige opzichten wel een ander perspectief: het gaat hier om kwaliteitscriteria waaraan tijdens de realisatie expliciet aandacht wordt gegeven.

Bij deze bespreking is uitgegaan van (een vertaling naar het Nederlands van) de ISO9126 kwaliteitscriteria. In deze normering wordt uitgegaan van een aantal kwaliteitsaspecten die worden onderverdeeld in 6 categorieën. Door het scoren van de kwaliteitsaspecten is bepaald op welke categorieën de nadruk dient te liggen. Dit leidde tot het volgende resultaat (met een score tussen nul en tien):

Categorie	Score	Classificatie
Betrouwbaarheid	8,3	Zeër belangrijk
Functionaliteit	6,7	Zeër belangrijk
Efficiëntie	6,4	Zeër belangrijk
Onderhoudbaarheid	5,3	Belangrijk
Portabiliteit	2,0	Neutraal
Bruikbaarheid	1,6	Neutraal

Uit deze resultaten kan worden geconcludeerd dat het systeem vooral betrouwbaar moet zijn. Vervolgens dient het systeem, op een efficiënte wijze, te voorzien in de gevraagde functionaliteit.

De belangrijkste drie categorieën laten zich als volgt omschrijven:

- **Betrouwbaarheid:**  
Het vermogen om gedurende een vastgestelde periode onder vastgestelde omstandigheden het prestatieniveau te handhaven. Beperkingen aan de betrouwbaarheid worden opgelegd door fouten in de requirements, het ontwerp en de implementatie.
- **Functionaliteit:**  
Aanwezigheid van bepaalde functies die (uitgesproken en onuitgesproken) behoeften vervullen en de eigenschappen van die functies.
- **Efficiëntie:**  
De relatie tussen het prestatieniveau en het middelenbeslag, onder vastgestelde

omstandigheden. Middelen zijn onder meer software producten, hardware faciliteiten, materialen en diensten van personeel.

Uit de scores van de onderliggende kwaliteitsaspecten is de volgende top 10, in volgorde van belangrijkheid, op te maken:

Categorie	Kwaliteitsaspect	Classificatie
Betrouwbaarheid	Herstelbaarheid	Zeer Belangrijk
Efficiëntie	Transactiesnelheid	Zeer Belangrijk
Functionaliteit	Beveiligbaarheid	Zeer Belangrijk
Functionaliteit	Juistheid en volledigheid	Zeer Belangrijk
Betrouwbaarheid	Bedrijfszekerheid	Zeer Belangrijk
Betrouwbaarheid	Foutbestendigheid	Belangrijk
Functionaliteit	Koppelbaarheid	Belangrijk
Onderhoudbaarheid	Analyseerbaarheid	Belangrijk
Onderhoudbaarheid	Stabiliteit	Belangrijk
Onderhoudbaarheid	Wijzigbaarheid	Belangrijk

### 3.7. Beveiligingseisen

De beheervoorziening dient zodanig te zijn ingericht, dat zij uitsluitend toegankelijk is voor gebruikers en anderen die daartoe op grond van de BSN-regelgeving bevoegd zijn. De beveiliging van de systemen dient daarbij conform het Voorschrift Informatiebeveiliging Rijksdiensten (VIR) [20] te worden ingericht.



## 4. Verdieping Architectuur BV BSN

### 4.1. Inleiding

In Hoofdstuk 2 is een globaal overzicht van de architectuur van de Beheervoorziening gegeven. In dit hoofdstuk wordt een verdieping van de architectuur gegeven. Hierbij wordt onderscheid gemaakt naar verschillende niveaus:

- Functionele architectuur
- Applicatie-architectuur
- Technische architectuur
- Infrastructuurarchitectuur

Op elk van deze niveaus wordt dieper ingegaan. Indien meer gedetailleerde informatie gewenst is verwijzen wij graag naar de bij de BV BSN opgeleverde documentatie:

- In de functioneel ontwerpen van de BV BSN [17], BC GBA [21], BC BVR [22], Beheer (EBA) [23] en EVA [24] is gedetailleerde informatie te vinden met betrekking tot de functionele werking van de verschillende onderdelen.
- In het SAD [1] wordt de applicatie-architectuur en de technische architectuur in detail beschreven.
- Meer informatie over de infrastructuur kan worden gevonden in het document Infrastructuur architectuur Beheervoorziening BSN [9].

### 4.2. Functionele architectuur

#### 4.2.1. Indeling in functionele eenheden

De beheervoorziening BSN is verdeeld in een aantal functionele eenheden. Deze eenheden zijn zo gekozen, dat zij 'deelsystemen' opleveren die, indien nodig vervangen kunnen worden, waarbij het koppelvlak tussen de functionele eenheden, eenduidig beschreven is. Dit geeft vrijheid in de toekomst. Juridisch heeft deze scheiding geen betekenis, omdat de functionele eenheden samen de Beheervoorziening BSN (in brede zin) vormen. De volgende functionele eenheden worden onderscheiden:

- BV BSN- Beheervoorziening BSN  
De BV BSN met daarin het nummerregister, vormt de kern van het systeem en levert diensten aan de actoren met betrekking tot verificatie, het muteren van het nummerregister en diverse beheerfuncties. Naast de diensten is er een aantal batchprocessen te onderscheiden, waarin een deel van de primaire en secundaire processen van de BV BSN worden uitgevoerd (bijvoorbeeld het genereren van nummers, het detecteren van misbruik en schonen van logboeken)
- BC GBA- Beheercomponent GBA  
De beheercomponent GBA bevat diensten voor gemeenten, die aansluiten op diverse GBA-processen (zoals inschrijfprocessen). Op basis van de diensten van de BC GBA worden diensten op de BV BSN aangeroepen. Daarnaast geeft de BC GBA onderdak aan de GBA-gegevensset, die in diverse processen (bijvoorbeeld

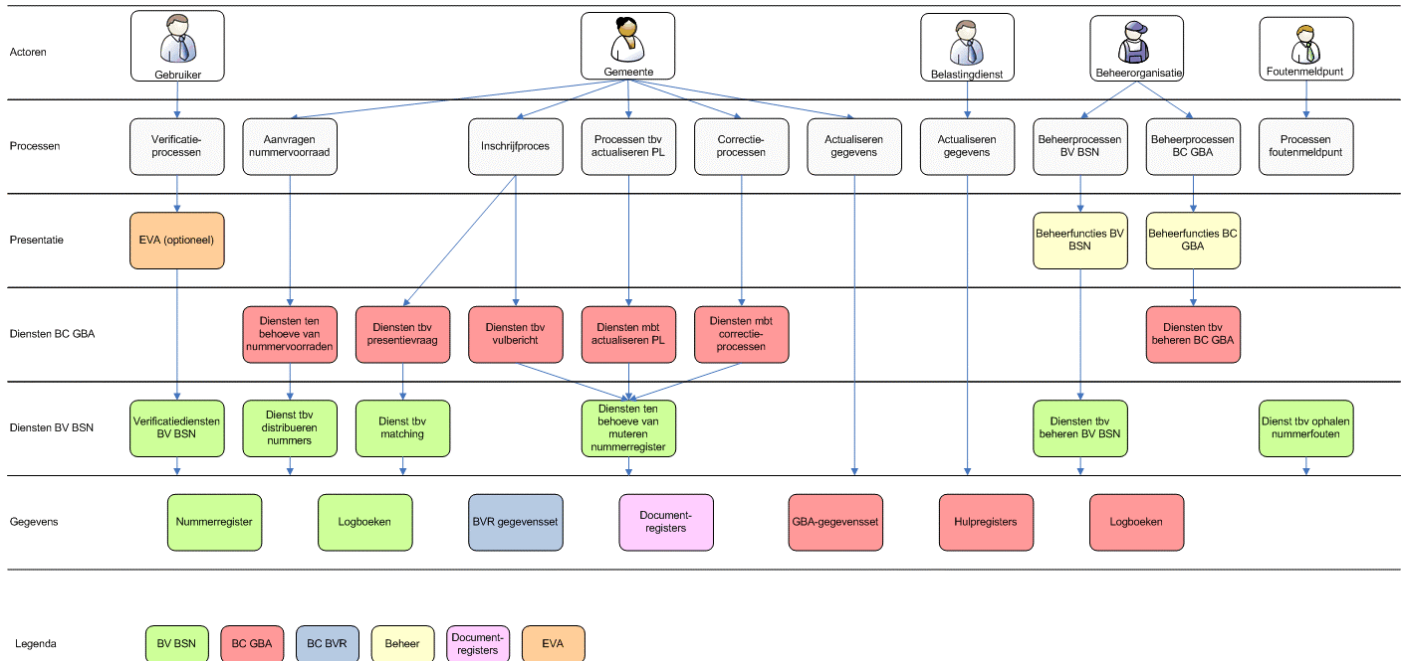
bij verificatie en bij matching) geraadpleegd wordt. Deze gegevensset wordt periodiek (dagelijks) bijgewerkt. Ook binnen de BC GBA wordt een aantal batchprocessen uitgevoerd (bijvoorbeeld het schonen van logboeken)

- BC BVR- Beheercomponent BVR  
De beheercomponent BVR bevat de BVR-gegevensset. Deze wordt dagelijks door de Belastingdienst aangeleverd. De BVR gegevensset wordt bij matching geraadpleegd.
- EBA- Elementaire Beheerapplicatie  
De beheerapplicatie bevat functies (met schermen), die de beheerorganisatie in staat stelt diverse acties in de BV BSN en de BC GBA uit te voeren (bijvoorbeeld het raadplegen van logboeken, maar ook het doorvoeren van correcties). De beheerapplicatie maakt hierbij gebruik van diensten, die de BV BSN en de BC GBA ter beschikking hebben.
- EVA- Elementaire Verificatieapplicatie  
EVA bevat functies (met schermen), die gebruik maken van de verificatiediensten van de BV BSN. EVA is bedoeld voor gebruikersorganisaties, die met EVA over een eenvoudige en naar eigen wensen aan te passen applicatie kunnen beschikken. Het staat gebruikers vrij om een eigen voorziening te realiseren. Het gebruik van EVA is optioneel.
- Foutenmeldpunt  
Het melden en registreren van nummerfouten door gebruikers, gemeenten en de belastingdienst zijn niet gerealiseerd binnen de BV BSN, maar worden op organisatorische wijze gefaciliteerd. Wel biedt de BV BSN een dienst voor het ophalen van binnen de BV BSN geconstateerde nummerfouten. Hier kan een te realiseren applicatie voor het foutenmeldpunt op aansluiten.

Per functionele eenheid (met uitzondering van het foutenmeldpunt) is een uitgebreide functionele beschrijving opgeleverd in de vorm van use cases. Aan de hand van deze use cases heeft de technische realisatie plaatsgevonden.

#### 4.2.2. Schets functionele architectuur

In de bijgaande figuur wordt de functionele architectuur geschetst. Hierbij zijn de volgende lagen onderscheiden:



#### Actoren

Als actoren worden onderscheiden: Gebruikers, Gemeenten, Belastingdienst, Beheerorganisatie en Foutmeldpunt.

#### Processen

De actoren maken gebruik van diverse processen. Als onderdeel van deze processen kunnen/moeten functies en diensten van de BV BSN gebruikt worden. Voor het overzicht zijn diverse (samenhangende) processen samengenomen

#### Presentatie

In de presentatielaag zijn vanuit functioneel perspectief verschillende functies gerealiseerd. Het gaat hier om EVA, die aansluit op de verificatiediensten van de BV BSN en EBA, die aansluit op diverse diensten van de BV BSN en de BC GBA. Voor detailinformatie met betrekking tot EVA en EBA wordt verwezen naar de respectievelijke FO's (FO EVA [24] en FO Beheer [23]).

#### Diensten BV BSN

De BV BSN levert aan de diverse actoren diverse diensten. Deze diensten worden direct benaderd door de actoren of (dit geldt voor de gemeenten) indirect (via de BC

GBA). Ten behoeve van het overzicht zijn de diensten van de BV BSN gegroepeerd. Voor detailinformatie wordt verwezen naar het functioneel ontwerp (FO BV BSN [17]).

### **Diensten BC GBA**

De BC GBA levert diensten aan gemeenten. Hierbij kan het zowel het traditionele sPd-berichtenverkeer betreffen, alsook SOAP-berichtenverkeer. Ten behoeve van het overzicht zijn de diensten van de BC GBA gegroepeerd. Voor detailinformatie wordt verwezen naar het functioneel ontwerp (FO BC GBA [21]) en het LO GBA [25].

### **Gegevens**

In de gegevenslaag worden diverse gegevensverzamelingen onderscheiden. Hierbij is (door kleur) aangegeven binnen welke functionele eenheid de gegevensverzameling valt. Voor gedetailleerde informatie wordt verwezen naar de logisch objectmodellen, die zijn opgenomen in de diverse functioneel ontwerpen.

Binnen de BV BSN worden de volgende gegevensverzamelingen onderscheiden:

- Nummerregister: In het nummerregister zijn de nummers opgenomen. Het betreft hier ofwel (toekomstige) sofi-nummers ofwel (toekomstige) BSN's. Naast een aantal hulpgegevens betreffende het nummers, wordt ook historie bijgehouden.
- Logboeken: Er worden binnen de BV BSN diverse logboeken onderscheiden: Berichtenlogboek, auditlogboek, nummerfoutenlogboek, systeemfoutenlogboek en protocollogboek.

Binnen de BC GBA worden de volgende gegevensverzamelingen onderscheiden:

- GBA-gegevensset: Dit is een afslag van de LRD. Hierin zijn GBA-gegevens van personen, die in een Nederlandse gemeente zijn ingeschreven opgenomen.
- Hulpregisters: Binnen de BC GBA worden een tweetal hulpregisters bijgehouden: In het koppelregister is de relatie tussen het A-nummer en het BSN opgenomen. Op basis hiervan kunnen vragen van de gemeenten, waarin geen BSN (maar wel een A-nummer) is opgenomen worden omgezet naar een vraag voor de BV BSN. In het presentievragenregister wordt enkele gegevens met betrekking tot een presentievraag van een gemeente vastgelegd. Hiermee kan gesignaleerd worden dat een andere gemeente eenzelfde vraag heeft gesteld.
- Logboeken: Er worden binnen de BC GBA de volgende logboeken onderscheiden: Berichtenlogboek, auditlogboek en systeemfoutenlogboek.

In BC BVR is de BVR-gegevensset opgenomen. Een deelverzameling van het bestand Beheer van Relaties van de Belastingdienst.

Daarnaast worden in het overzicht de documentregisters getoond. Dit zijn de volgende registers:

- Verificatieregister: Ten behoeve van het verifiëren van reisdocumenten
- Rijbewijsregister: Ten behoeve van het verifiëren van rijbewijzen
- Kaartregister: Ten behoeve van het verifiëren van vreemdelingendocumenten.

### **4.2.3. Functionele architectuur en use cases**

Per functionele eenheid (met uitzondering van het foutenmeldpunt) is een uitgebreide functionele beschrijving opgeleverd in de vorm van use cases in verschillende

functioneel ontwerpen. De use cases met betrekking tot de presentatielaag en de diensten hebben een bepaalde samenhang. Deze zijn hier per actor (met uitzondering van de actoren Belastingdienst en Foutenmeldpunt) opgenomen. Voor de overige use cases wordt verwezen naar de FO's [17], [21], [22], [23], [24].

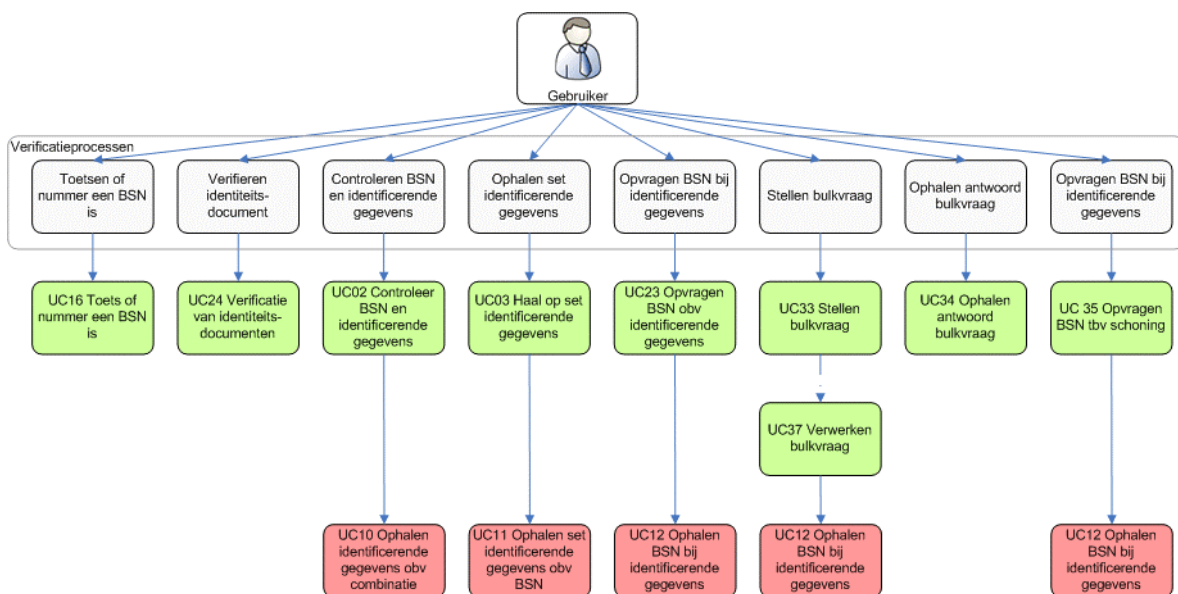
In deze overzichten kan ook het verband gelegd worden tussen de schets van de functionele architectuur (in de vorige paragraaf) en de use cases.

### Gebruiker

De gebruiker kan voor zijn verificatieprocessen gebruik maken van de volgende diensten van de BV BSN:

- Controleer BSN en identificerende gegevens
- Haal op set identificerende gegevens
- Toets of nummer een BSN is
- Opvragen BSN op basis van identificerende gegevens
- Verificatie van identiteitsdocumenten
- Stellen bulkvraag
- Ophalen antwoord bulkvraag
- Opvragen BSN t.b.v. schoning en initiële vulling

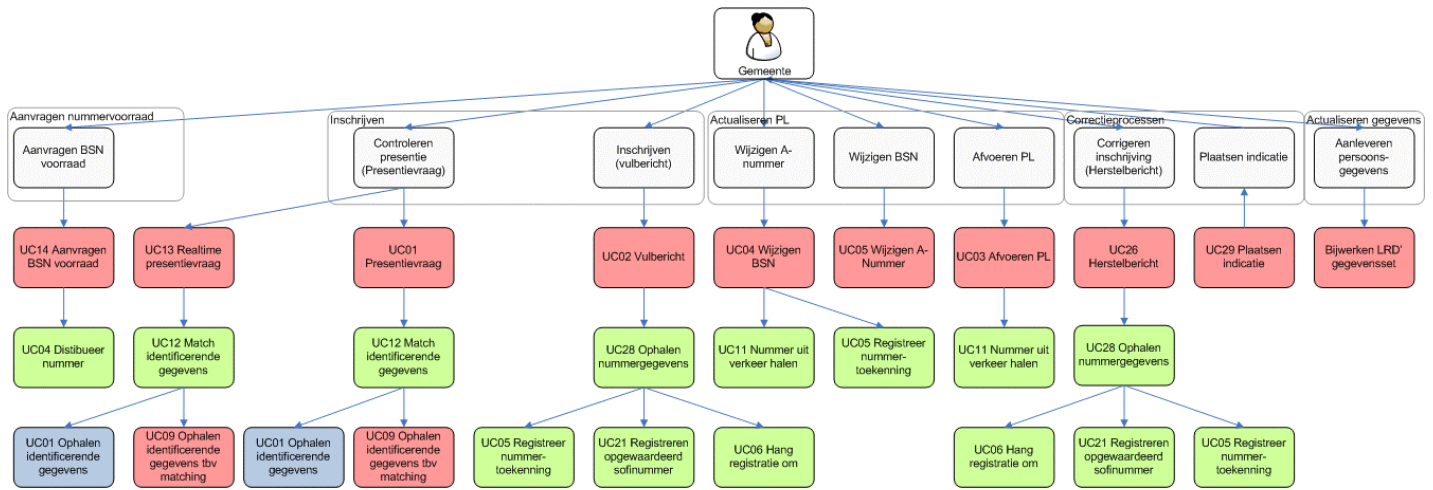
Het betreft hier allemaal SOAP-diensten.



**Gemeente**

De gemeente maakt voor zijn werkzaamheden gebruik van de volgende diensten:

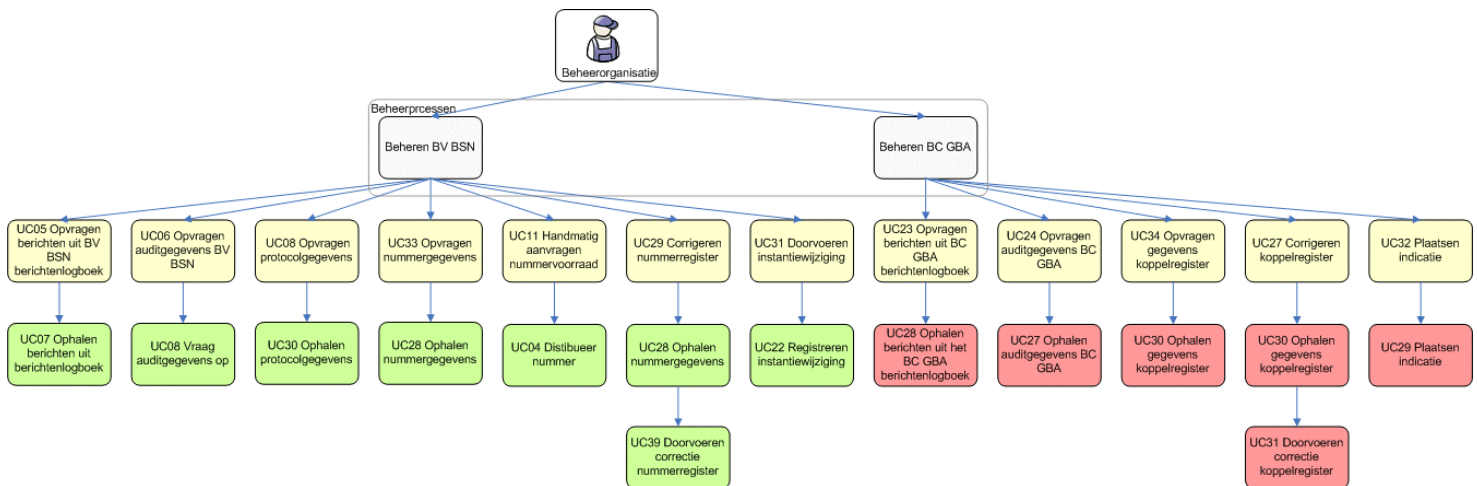
- Aanvragen nummervoorraad (SOAP)
- Vulbericht (sPd)
- Afvoeren PL (sPd)
- Wijzigen BSN (sPd)
- Wijzigen A-nummer (sPd)
- Herstelbericht (sPd)
- Presentievraag (sPd)
- Realtime presentievraag (SOAP)



### Beheerorganisatie

De beheerorganisatie heeft een applicatie tot zijn beschikking, waarbij via verschillende schermen diensten op de BV BSN en BC GBA uitgevoerd kunnen worden.

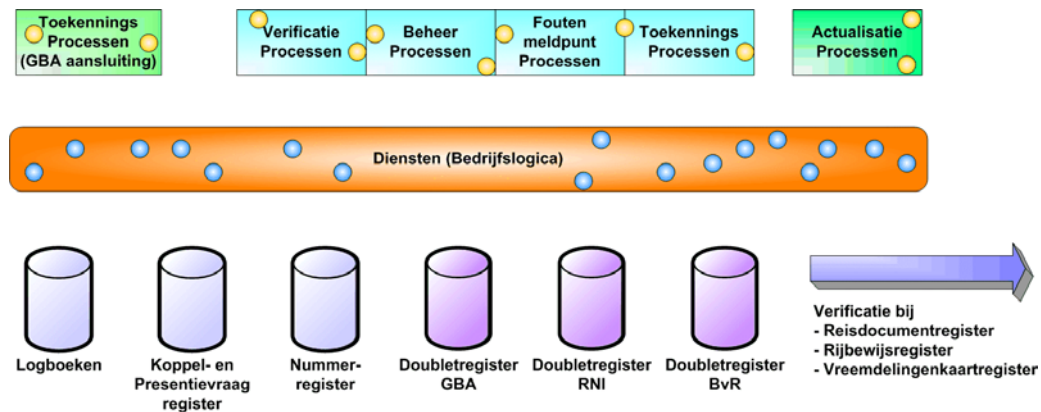
- Opvragen berichten uit berichtenlogboek BV BSN
- Opvragen auditgegevens uit auditlogboek BV BSN
- Opvragen protocolgegevens uit protocollogboek
- Opvragen nummergegevens
- Corrigeren nummerregister
- Handmatig aanvragen nummervoorraad
- Doorvoeren instantiewijziging
- Opvragen berichten uit berichtenlogboek BC GBA
- Opvragen auditgegevens uit auditlogboek BC GBA
- Opvragen gegevens koppelregister
- Corrigeren koppelregister
- Plaatsen indicatie



### 4.3. Applicatiearchitectuur

Bij de ontwikkeling van dit systeem was al bij de start een gegeven dat de communicatie met de gebruikers diende te verlopen binnen een dienstgerichte architectuur (SOA). Alleen op deze wijze kon worden zeker gesteld dat gebruikers eenvoudig konden aansluiten en de functionaliteit in bestaande systemen kon worden opgenomen. Daarnaast past een dienstgerichte architectuur volledig binnen de richting die, onder leiding van Stichting ICTU, voor de gehele overheid wordt ingeslagen. Om het koppelen voor de gebruikers zo eenvoudig mogelijk te maken is daarbij besloten om nauw aan te sluiten bij de WSI standaarden voor webservices. Dit heeft tot gevolg dat de diensten kunnen worden aangesproken met XML-berichten binnen het SOAP-protocol.

Ook intern is het systeem zo veel mogelijk conform de richtlijnen van een SOA gebouwd. Dit heeft onder meer tot gevolg dat in de applicatiearchitectuur, zoals hieronder weergegeven, een aantal lagen zijn te onderkennen. (In [1] is een overigens een verdere detaillering, en opsplitsing, van de hier gepresenteerde lagen opgenomen.)



In het systeem zijn drie lagen te herkennen: de proceslaag, de dienstenlaag en de gegevenslaag. Zij worden hieronder kort besproken:

### Proceslaag

In de proceslaag worden diensten aangesproken die direct de gebruiker ondersteunen. Voor elke individuele dienst die een gebruiker kan afnemen is derhalve in deze laag een component te herkennen. Daarbij worden veel van deze componenten op dezelfde wijze aangesproken. Daarom is veel van de dienstafhandeling, zoals het ontvangen en verzenden van berichten, binnen centrale componenten in deze laag vormgegeven. De in lichtblauw weergegeven verificatieprocessen, beheerprocessen, foutenmeldpunt processen en toekenningsprocessen kunnen via de webservices standaard worden ontsloten. De toekenningsprocessen die via een GBA-aansluiting verlopen worden aangesproken via het binnen het GBA-berichtenverkeer. Reden voor deze afwijking van de webservices standaard was de bij aanvang van het project geformuleerde uitgangspunt dat er aan GBA-systemen (zoals in gebruik bij gemeenten) als gevolg van het BSN-stelsel zo min mogelijk moest veranderen. Tenslotte zijn er nog specifiek actualisatieprocessen onderkend. Deze zijn bedoeld om de doubletregisters te verversen. Hierbij is sprake van een puntkoppeling waarbij grote hoeveelheden data gemoeid zijn. Bij de implementatie van deze processen zijn met name de prestaties (snelheid) van deze koppeling geoptimaliseerd.

### Dienstenlaag

In de diensten of bedrijfslogica laag wordt het specifieke deel van het gebruikersproces afgehandeld. In deze laag bevinden zich componenten die alleen of samen met andere de logica bevatten om deze taken uit te voeren. De componenten in deze laag hebben daarbij toegang tot de in de volgende laag opgeslagen gegevens.

### **Gegevenslaag**

In de gegevenslaag worden de voor het systeem noodzakelijke gegevens bewaard. Allereerst worden daarbij een aantal externe bronnen onderkend voor de vragen omtrent de status van een identiteitsdocument. Deze systemen worden, zoals voor deze systemen gebruikelijk is, vanuit de logica laag door middel van XML- berichten over het http-protocol ontsloten.

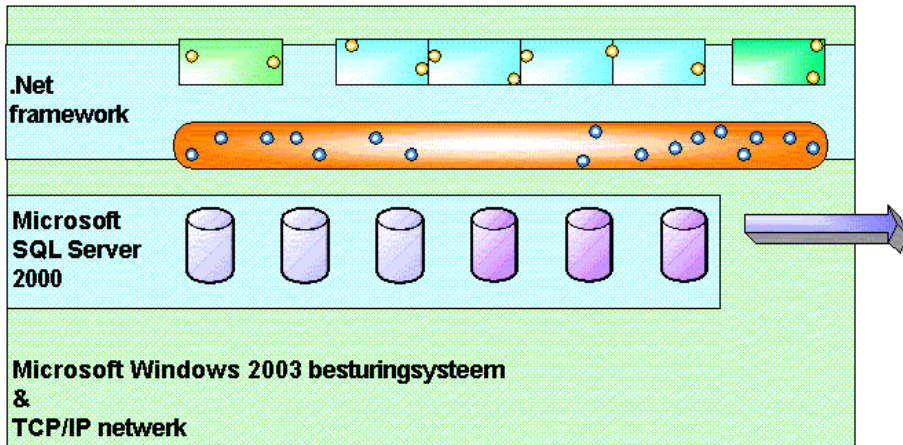
De overige gegevens zijn opgeslagen in databases. Daarin zijn twee groepen gegevensbronnen te onderkennen. Allereerst is dat de groep van de doubletregisters; gegevens uit andere "authentieke" registers die om de prestaties van het systeem te bevorderen zijn gekopieerd. Deze doubletregisters worden uitsluitend gebruikt om persoonsgegevens te raadplegen. De actualiteit van de gegevens is, mede door de beheerprocessen in de registers die deze gegevens onderhouden, niet bijzonder belangrijk. Een dagelijks "actualisatieproces" is voor deze doubletregisters voldoende. Transacties worden er verder op deze registers niet uitgevoerd.

In de tweede groep gegevensbronnen houdt het systeem de gegevens bij die voor de processen noodzakelijk zijn of die ondersteunen. Een centrale rol is weggelegd voor het nummerregister waarin alle burgerservicenummers zijn opgeslagen. Met de logboeken wordt voldaan aan wettelijke verplichtingen en kan de goede werking van het systeem worden gecontroleerd. Het koppel- en presentievragenregister, tenslotte, ondersteunen het proces van het toekennen van burgerservicenummers. In deze groep van gegevensbronnen spelen transacties en updates wel een grote rol.

## **4.4. Technische architectuur**

Voor de realisatie van de Beheervoorziening Burgerservicenummer is gekozen voor maatwerkstelsel binnen een veel gebruikt ontwikkelplatform. De beoogde beheerorganisatie had daarbij aangegeven bij voorkeur een stelsel op het Microsoft platform te willen beheren. Dit heeft geleid tot de keuze voor de door Microsoft geleverde .Net ontwikkelomgeving. De keuze voor deze omgeving is ook zonder de voorkeur van de beheerorganisatie prima te verdedigen. Het .Net platform is modern. De omgeving wordt ondersteund door een grote leverancier en een grote gemeenschap van ontwikkelaars. In het algemeen wordt dit platform (zowel in binnen als buitenland) door IT-deskundigen gezien als één van de twee courante ontwikkelomgevingen voor maatwerkapplicaties.

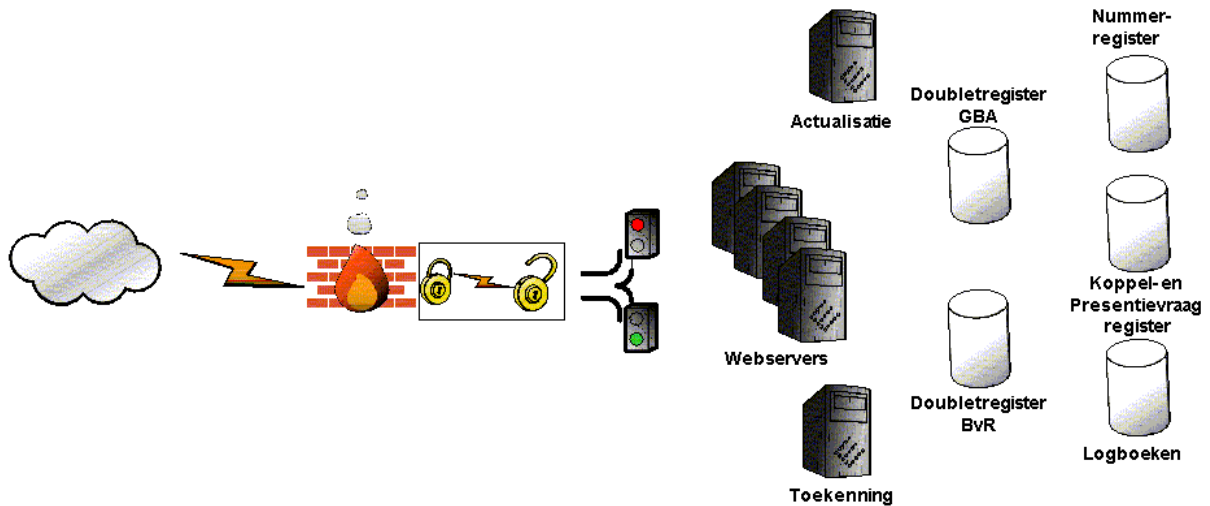
De ontwikkelde maatwerkapplicatie dient binnen het platform ondersteund te worden door de hardware. De belangrijkste verbinding wordt geleverd door het besturingssysteem (OS) Windows 2003. Binnen het OS zijn ook functies voor bijvoorbeeld het registreren en inzien van systeemfouten, het toekennen van autorisaties ("Active Directory") en het afhandelen van Internetverkeer ("Internet Information Server") opgenomen. Voor de opslag van gegevens wordt daarnaast gebruik gemaakt van de SQL Server database software. De maatwerk applicatie maakt verder gebruik van het .Net framework. Dit framework levert een omgeving voor ontwikkeling en gebruik van het stelsel. Voor de communicatie tussen systemen wordt gebruik gemaakt van het TCP/IP netwerk protocol. In onderstaande figuur staat de hier beschreven software architectuur geschetst.





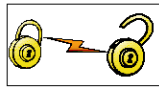


Een dergelijke omgeving, die voornamelijk uit producten van één leverancier bestaat, is uitstekend te beheren. Er kan daarbij met name worden gedacht aan het product “Microsoft Operations Manager”.

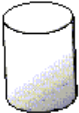






#### 4.5. Infrastructuurarchitectuur

In onderstaande overzicht staat de architectuur van de infrastructuur weergegeven. In dit overzicht hebben de diverse componenten van de applicatie architectuur een plaats gekregen in de infrastructuur. Doordat het “Register Niet Ingezetenen” (RNI) bij de in productie name van de beheervoorziening BSN nog niet is gerealiseerd is hier nog geen voorziening voor getroffen.



In onderstaande tabel worden de onderdelen nader toegelicht:

Component		Omschrijving
	Aansluiting netwerk	Er dient een netwerkaansluiting te zijn tussen de BV BSN en zijn gebruikers. Er is voor gekozen om een redundante verbinding met een netwerkleverancier te realiseren. Veel gebruikte netwerken (in de doelgroep), GEMnet en Haagse Ring, sluiten aan bij de netwerkleverancier.
	Firewall	Met behulp van een firewall wordt al het netwerkverkeer dat niet voor de Beheervoorziening BSN bestemd kan zijn afgevangen. Dit gebeurt op basis van IP-adres van de gebruiker en gewenste "poort" van de Beheervoorziening.
	SSL-Offloader	Al het dataverkeer wordt versleuteld verzonden met behulp van SSL dat ook voor authenticatie wordt gebruikt. Om de ontsleuteling en authenticatie efficiënt te laten verlopen wordt hiervoor hardware ingezet. Dit kan een factor 10 schelen.
	Loadbalancer	Er wordt gekozen voor meerdere webserver die onafhankelijk van elkaar berichten kunnen verwerken (zie hierna). Om de last goed over deze servers te verdelen worden loadbalancers ingezet. Een dergelijk instrument kan detecteren dat een server niet meer functioneert en zorgt, door daarna naar die server geen verkeer meer te sturen, gelijk voor fouttolerantie. Ook kan, op een rustig moment, een update van de software op de helft van de servers plaatsvinden terwijl de andere helft van de servers de cliënten nog bedient.
	Webservers	De webservers verwerken de webservices die door de gebruikers worden gestuurd. Een belangrijk kenmerk van deze berichten is dat ze onafhankelijk van elkaar zijn en dat er dus geen sessie-informatie op de servers hoeft te worden bewaard. In de software zijn twee lagen te onderkennen die de mogelijkheid geeft om de applicatie over verschillende servers in te zetten. Van deze mogelijkheden wordt geen gebruik gemaakt;

		de proces- en dienstenlaag wordt tezamen op de servers geïnstalleerd. Door meerdere servers in te zetten wordt niet alleen (horizontale) schaalbaarheid bereikt maar ook fouttolerantie.
<p><b>Nummerregister</b></p> 	Nummerregister	In deze database worden de nummers opgeslagen. Er vinden updates plaats maar dit register wordt toch voornamelijk geraadpleegd! De BV BSN communiceert direct met het register.
<p><b>Logboeken</b></p> 	Logboeken	In deze database worden met name het berichtenlogboek en auditlog bijgehouden. Snel gegevens wegschrijven is echter de belangrijkste functie. De BV BSN communiceert direct met het register.
<p><b>Koppel- en Presentievraagregister</b></p> 	Koppel- en Presentievraagregister	Deze registers ondersteunen de toekenning van burgerservicenummers. In het koppelregister wordt de relatie bijgehouden tussen A nummers (vanuit GBA) en het burgerservicenummer. Bijwerken vindt plaats op basis van het GBA berichtenverkeer. Het Presentievraagregister wordt gebruikt om instanties te kunnen waarschuwen als mogelijk voor dezelfde persoon een tweede procedure wordt gestart.
<p><b>Toekenning</b></p> 	Toekenning functies	Via het GBA berichtenverkeer komen een aantal berichten binnen die een rol spelen rond het toekennen van burgerservicenummer. Op deze server(s) vindt de afhandeling van deze berichten plaats.
<p><b>Doubletregister GBA</b></p> 	Doubletregister GBA	Deze database wordt voornamelijk geraadpleegd. Updates vinden éénmaal daags plaats vanuit de LRD. De BV BSN communiceert direct met het register.
<p><b>Doubletregister BvR</b></p> 	Doubletregister BvR	Deze database wordt voornamelijk geraadpleegd. Eenmaal daags wordt de hele gegevensverzameling (1,2 miljoen records) opnieuw ingeladen. De BV BSN communiceert direct met het register.
<p><b>Actualisatie</b></p> 	Actualisatie	Dagelijks worden de doubletregisters bijgewerkt. Op deze server(s) worden de nieuwe gegevens opgevangen en op juiste wijze in de doubletregisters geplaatst.

## 5. Realisatie van eisen

### 5.1. Inleiding

In dit hoofdstuk wordt ingegaan op welke wijze de functionele en niet-functionele eisen gerealiseerd zijn. Daarbij zijn gedurende het proces verschillende alternatieven overwogen, afgestemd en is uiteindelijk tot een keuze gekomen. Hierbij is vaak eerst een notitie geschreven, waarin alternatieven genoemd zijn en een voorstel is geformuleerd. Daarna is op basis van deze notitie afstemming geweest in de verschillende overlegstructuren. Afhankelijk van het onderwerp is dit binnen het BV BSN-team behandeld, in de werkgroep registerhouders, tijdens het projectleidersoverleg en/of in de stuurgroep BSN.

Het is onmogelijk om alle ontwerpbeslissingen en overwegingen te beschrijven. In dit hoofdstuk wordt getracht deze keuzes op hoofdlijnen weer te geven. Indien meer gedetailleerde informatie gewenst is, wordt verwezen naar de archieven van het programma BSN, waarin de betrokken notities en verslagen van overleggen zijn terug te vinden.

### 5.2. Realisatie van functionele eisen

#### 5.2.1. Genereren van nummers

##### **Realisatie**

Het genereren van nummers is gerealiseerd in de volgende use case:  
*BV BSN UC27 Genereren nummers*

##### **Overwegingen en keuzes**

Om te voldoen aan de eis van “informatieloosheid” van het nummer is ervoor gekozen om nummers random te genereren. In verband met het reserveren van reeksen (voor de Belastingdienst en voor testdoeleinden) is ervoor gekozen om nummers te genereren binnen een opgegeven interval. (bron: Notitie nummerreeks BSN [14]). In aansluiting op overwegingen om batches random nummers te distribueren (zie verderop) is ervoor gekozen nummers in batches te genereren. Hierna kunnen de nummers in volgorde van generatie worden gedistribueerd.

Om te voldoen aan de uniciteit is ervoor gekozen om een aantal technische en functionele maatregelen te hanteren: Op de nummerpool en het nummerregister zit een databasebeperking die de garantie geeft dat de nummers uniek zijn. Daarnaast toetst de generator of een nummer voorkomt in de nummerpool of het nummerregister, voordat het nummer wordt toegevoegd aan de nummerpool. Als laatste wordt het plaatsen van het nummer in de database binnen een transactie op de database uitgevoerd.

##### **Beschrijving gerealiseerde oplossing**

Het systeem controleert “continu” hoeveel nummers er nog in voorraad zijn. Als dit aantal onder een bepaald minimum komt, wordt een (ingesteld) aantal nieuwe

nummers gegenereerd. Dit gebeurt op basis van een pseudo randomgenerator, die voldoet aan de chi-kwadraat-test. Een gegenereerd nummer krijgt in het nummerregister de status “aangemaakt”.

### 5.2.2. Distribueren van nummers

#### **Realisatie**

Het distribueren van nummers is gerealiseerd in de volgende use cases:

*BC GBA UC14 Aanvragen nummervoorraad*

*BV BSN UC04 Distribueer nummer*

*Beheer UC11 Handmatig aanvragen nummervoorraad*

#### **Overwegingen en keuzes**

Ten behoeve van het distribueren zijn verschillende alternatieven overwogen:

- Batches random nummers
- Online random nummers
- Reeksen opeenvolgende nummers
- Toekenning volgens bestaand proces van de belastingdienst

Er is gekozen voor het distribueren van batches random nummers omdat dit proces eenvoudig in te passen is in de GBA-processen. Daarnaast is het proces vanwege het aanhouden van een voorraad bij de gemeenten minder gevoelig voor storingen (bron: Plan van aanpak OBV [15]).

#### **Beschrijving gerealiseerde oplossing**

In de gerealiseerde oplossing vraagt de gemeente via een webservice een nieuwe voorraad nummers aan. De gemeente geeft hierbij aan hoeveel nummers ze wensen te ontvangen. (Dit is overigens wel gebonden aan een maximum). De beheervoorziening verzamelt deze nummers in een batch en registreert in het nummerregister aan welke gemeente een nummer is gedistribueerd. Daarnaast is het via de beheerapplicatie mogelijk dat een beheerder een batch nummers voor een gemeente aanvraagt. Deze functie is mogelijk gemaakt voor het uitgeven van nummers aan gemeenten, waarbij het gebruik van de webservice (nog) niet mogelijk is.

Er is een onafhankelijke controle gedefinieerd (in UC25 Periodieke controle nummerregister), waarmee wordt gecontroleerd of een nummer correct (slechts één maal) is gedistribueerd.

De gerealiseerde oplossing maakt het overigens ook mogelijk om in de toekomst per nummer te distribueren. Het aantal gewenste nummers kan dan op één gezet worden.

### 5.2.3. Registreren en toekennen van nummers

#### **Realisatie**

Het registreren en toekennen van nummers is gerealiseerd in de volgende use cases:

*BC GBA UC02 Vulbericht*

*BC GBA UC03 Afvoeren PL*

*BC GBA UC04 Wijzigen BSN*

*BC GBA UC05 Wijzigen A-nummer*

*BC GBA UC26 Herstelbericht*  
*BV BSN UC28 Ophalen nummergegevens*  
*BV BSN UC05 Registreer nummertoekenning*  
*BV BSN UC06 Hang registratie om bij BSN*  
*BV BSN UC11 Nummer uit verkeer halen*  
*BV BSN UC21 Registreren opgewaardeerd Sofi-nummer*

### **Overwegingen en keuzes**

Op basis van het LO GBA is besloten de volgende berichten vanuit de gemeente te verwerken binnen de BV BSN:

Ag11	BC GBA UC02 Vulbericht
Ng01	BC GBA UC03 Afvoeren PL
Gv01	BC GBA UC04 Wijzigen BSN
Wa11	BC GBA UC05 Wijzigen A-nummer
Ag31	BC GBA UC26 Herstelbericht

Deze berichten worden verwerkt omdat ze direct invloed hebben op de registratie van het nummer in het nummerregister (en het koppelregister). Alle andere berichten vanuit de gemeente worden vooralsnog opgeslagen in het berichtenlogboek van de BC GBA (bron: Notitie GBA-berichten [26]).

Omdat van een vulbericht niet afgeleid kan worden of hiermee een toekenning van een nummer, een opwaardering of een omhanging wordt beoogd, wordt dit afgeleid op basis van de vastgelegde gegevens m.b.t. het nummer in het nummerregister. In het koppelregister ligt de relatie tussen het BSN en het A-nummer vast. Het koppelregister is ingesteld om berichten, die geen BSN bevatten (bijvoorbeeld Afvoeren PL) te kunnen verwerken in het nummerregister. Een alternatief dat hierbij is overwogen is om het A-nummer in de LRD'-gegevensset op te nemen. Hier is niet voor gekozen, omdat het proces hiermee (tijds)afhankelijk wordt van het (periodiek) bijwerken van de gegevensset. Het koppelregister wordt bijgewerkt op basis van de door de beheervoorziening ontvangen berichten. Daarnaast is het toekomstvaster om de afhankelijkheid van het A-nummer tot een minimum te beperken, zodat het op termijn uitfaseren van het A-nummer eenvoudiger wordt.

### **Beschrijving gerealiseerde oplossing**

Indien een inschrijving in de GBA wordt uitgevoerd, heeft dit een vulbericht tot gevolg. Als dit bericht binnenkomt wordt op basis van de gegevens in het nummerregister bepaald hoe het bericht in het nummerregister verwerkt moet worden. Het nummer wordt dan in verkeer genomen door het registreren van de nummertoekenning, het opwaarderen van het sofi-nummer of (in de toekomst) het omhangen van het nummer van RNI naar GBA.

Indien in de GBA een persoonslijst wordt afgevoerd, wordt dit in het nummerregister geregistreerd door het nummer uit verkeer te halen.

Indien in de GBA een BSN op een persoonslijst wordt gewijzigd heeft dit in het nummerregister tot gevolg dat het oude nummer uit verkeer en het nieuwe nummer in verkeer wordt genomen.

Indien het A-nummer op de persoonslijst wordt gewijzigd heeft dit alleen gevolgen voor het koppelregister, waar de relatie tussen het BSN en het A-nummer is vastgelegd. Een herstelbericht vanuit de gemeente wordt op dezelfde manier verwerkt als een vulbericht.

Voordat een mutatie in het nummerregister wordt doorgevoerd, wordt eerst de oude situatie vastgelegd in de historie.

#### 5.2.4. Matching

##### **Realisatie**

De realisatie van de eisen met betrekking tot het matchingsmechanisme zijn gerealiseerd in de volgende use cases:

*BC GBA UC01 Presentievraag*

*BC GBA UC09 Ophalen identificerende gegevens tbv matching*

*BC GBA UC13 Realtime presentievraag*

*BV BSN UC12 Match identificerende gegevens*

*BC BVR UC01 Ophalen identificerende gegevens*

##### **Overwegingen en keuzes**

Het matchingsmechanisme heeft tot doel om, indien een persoon reeds een BSN of een sofi-nummer heeft, dit op basis van een zoekvraag aan de registraties van de Belastingdienst en de GBA te kunnen vaststellen.

Het matchingsmechanisme is uitgerust met een zekere mate van intelligentie. Bij het ontwerpen van dit mechanisme is een aantal belangrijke uitgangspunten gehanteerd. Ten eerste is er vanuit gegaan dat de zoekvraag altijd op basis van brondocumenten wordt samengesteld. Een voorwaarde voor het verkrijgen van een BSN (en voor het inschrijven in de gemeente) is dat de persoon zich goed kan identificeren. Ten tweede is uitgegaan van de situatie zoals die nu geldt voor het registreren van gegevens bij de gemeente en de Belastingdienst. Dat wil vooral zeggen dat met de historische situatie, waarbij personen zonder deugdelijke identificatie in de registratie van de Belastingdienst zijn opgenomen, geen rekening is gehouden. Ten derde is een uitgangspunt bij matching dat de uiteindelijke keuze uit de lijst van zoekresultaten bij de ambtenaar ligt.

Bij het inrichten van het intelligent zoeken zijn verschillende alternatieven overwogen:

- Het afpelmechanisme: bij het afpelmechanisme wordt eerst gezocht met alle opgegeven zoekvelden. Als hiermee geen resultaat wordt gevonden, wordt een zoekveld van de zoekvraag afgehaald (afgepeld) en wordt opnieuw getracht een zoekresultaat te verkrijgen.
- Het aankleedmechanisme: bij het aankleedmechanisme wordt eerst gezocht met een minimaal zoekpad. Indien hierbij te veel resultaten worden gevonden, wordt een extra gegeven aan het zoekpad toegevoegd, om zo het eindresultaat te verfijnen.

Er is gekozen om te werken volgens het aankleedregime omdat dit een aantal voordelen biedt: Op deze wijze worden de zoekvelden in volgorde van belangrijkheid toegevoegd (dit volgt een natuurlijke manier van werken) en leidt dit, indien één van de (minder belangrijke) zoekvelden foutief is, niet gelijk tot het niet vinden van een resultaat. Daarnaast worden op deze wijze onnodige vragen aan de database voorkomen.

Het minimale zoekpad is gesteld op: geslachtsnaam, geboortedatum en geslacht. Hier is voor gekozen omdat uit onderzoek is gebleken dat meer dan 90% van de personen

in de registraties (LRD' en BVR') op basis van deze gegevens uniek geïdentificeerd kan worden. Aangezien er voor gekozen is om maximaal 10 resultaten terug te geven (dit aantal is configureerbaar), wordt hiermee bijna 100% van de personen, die zijn opgenomen in de registraties, gevonden op basis van het minimale zoekpad.

Per zoekveld in de zoekvraag is bepaald of hiervoor een intelligente zoekmethode ingezet moet worden. Een intelligente zoekmethode is gedefinieerd als een andere zoekmethode dan een exacte match van gegevens. Deze intelligente zoekmethoden zijn na intensief overleg en onderzoek geformuleerd (bron: Notitie intelligent zoeken [27]). Bij het vaststellen van deze zoekmethoden is altijd een afweging gemaakt tussen het vergroten van de kans op het vinden van de juiste persoon, en het verkleinen van het risico van het niet vinden van de juiste persoon en het risico van te veel zoekresultaten.

Onderdeel van de overwegingen is geweest om een pakket voor intelligent zoeken in te zetten. Hier is niet voor gekozen omdat er volledige transparantie van het zoekmechanisme is vereist en omdat dergelijke pakketten over het algemeen niet gericht zijn op de specifieke taak die de beheervoorziening BSN vraagt.

Als laatste wordt hier ingegaan op de keuze om geen fonetische zoekmethode in te zetten. Hier is niet voor gekozen, omdat dit niet overeenkomt met de uitgangspunten (de zoekvraag wordt samengesteld aan de hand van getoonde brondocumenten) en omdat de bestaande methoden voor fonetisch zoeken een te grote kans op te veel zoekresultaten zouden opleveren. Wel is gekozen voor het toepassen van regels voor transcriptie en transliteratie op de geslachtsnaam. Dit is ingericht op basis van de volgende overwegingen (bron [28]):

- De methode is gericht op het oplossen van verschillen in buitenlandse geslachtsnamen, omdat de verwachting is dat Nederlandse geslachtsnamen goed gedocumenteerd (paspoort, rijbewijs) zijn
- Het doel van de methode is het oplossen van verschillen in het omzetten van niet Romaanse schriften opgelost. (In Russische paspoorten is bijvoorbeeld vaak het cyrillisch omgezet volgens een Franse transliteratie. Deze verschilt van de Nederlandse of Engelse transliteratie).
- Er is met name aandacht besteed aan de omzetting van Cyrillisch (en afgeleide schriften), Chinees, Koreaans en Arabisch.

### **Beschrijving gerealiseerde oplossing**

Ofwel via de sPd-presentievraag of via de realtime presentievraag (in de toekomst) kan de gemeente zijn zoekvraag opgeven. Hierna wordt eerst in het presentievragenregister gecontroleerd of niet een andere gemeente in de afgelopen vier weken dezelfde vraag heeft gesteld (die nog niet tot een inschrijving heeft geleid). Op deze wijze wordt gedeeltelijk voorkomen dat personen zich gelijktijdig melden bij meerdere gemeenten. Daarnaast wordt gezocht op basis van de vastgestelde methode in de gegevens van de GBA en de Belastingdienst. Hierbij is het mogelijk dat er geen resultaten worden gevonden, dat er één tot tien resultaten worden gevonden en dat er te veel resultaten worden gevonden. Het resultaat wordt aan de gemeente teruggemeld. Op basis hiervan kan de ambtenaar een besluit nemen.

### 5.2.5. Functies voor gebruikers

#### Realisatie

De gedefinieerde eisen voor gebruikers zijn gerealiseerd in de volgende use cases:

*BV BSN UC02 Controleer BSN en identificerende gegevens*

*BV BSN UC03 Haal op set identificerende gegevens*

*BV BSN UC16 Toets of nummer een BSN is*

*BV BSN UC23 Opvragen BSN op basis van identificerende gegevens*

*BV BSN UC24 Verificatie van identiteitsdocumenten*

*BV BSN UC33 Stellen bulkvraag*

*BV BSN UC34 Ophalen antwoord bulkvraag*

*BV BSN UC35 Opvragen BSN t.b.v. schoning en initiële vulling*

*BV BSN UC37 Verwerken bulkvraag*

*BC GBA UC10 Ophalen identificerende gegevens obv combinatie BSN en gegevens*

*BC GBA UC11 Ophalen identificerende gegevens obv BSN*

*BC GBA UC12 Ophalen BSN obv identificerende gegevens*

#### Overwegingen en keuzes

De keuze voor het aanbieden van verificatiefuncties voor gebruikers vindt zijn oorsprong in het advies van de Tafel van Thijn [10]. Dit is later uitgewerkt tot de definitie van voorzieningen voor verificaties, waarbij persoonsgegevens mogen worden gebruikt en basisvoorzieningen, waarbij de achterliggende registraties met persoonsgegevens niet worden geraadpleegd. Op verzoek van de zorgsector is de 'combinatievraag' geïntroduceerd. Hierbij moet zowel het BSN als enkele persoonsgegevens worden opgegeven, zodat oneigenlijk gebruik, zoals 'raden' en het ophalen van persoonsgegevens op basis van een opeenvolgende reeks BSN's bemoeilijkt wordt.

Als laatste zijn functies geïntroduceerd voor het schonen en initieel vullen van registraties van gebruikers. Dit zijn tijdelijke diensten. Hierbij wordt de gebruikers twee mogelijkheden geboden: Het in bulk aanbieden van gegevens, waarbij het antwoord later opgehaald kan worden (de 'afhaal-service') en een kopie van de reguliere verificatiemogelijkheid voor het opvragen van een BSN op basis van identificerende gegevens, waarbij het de bedoeling is dat de er afspraken worden gemaakt wanneer deze uitgevoerd wordt. Er is voor gekozen om voor deze laatste mogelijkheid een aparte dienst aan te bieden, zodat er onderscheid gemaakt kan blijven worden tussen de reguliere bevraging en bevraging ten behoeve van schoning en initiële vulling. Hiermee kan de tijdelijkheid van de service praktisch uitgevoerd worden en kan bij analyse van de resultaten (bijvoorbeeld voor intelligent zoeken) onderscheid gemaakt worden op basis waarvan de vraag is gesteld (op basis van een handeling aan het loket, waarbij een burger aanwezig was of op basis van een geautomatiseerde registratie van personen van de gebruiker).

Er zijn ten behoeve van de verificatievraag 'Opvragen BSN' meerdere mogelijke zoekpaden overwogen. Uiteindelijk is besloten om twee verplichte minimale zoekpaden te benoemen: één op basis van geslachtsnaam, geboortedatum en geslachtsaanduiding. Het andere zoekpad bevat geboortedatum, geslachtsaanduiding, huisnummer, postcode. Hiervoor is gekozen omdat verwacht wordt dat deze gegevens snel leiden tot een uniek resultaat in de achterliggende registraties en omdat deze gegevens (relatief) minder foutgevoelig zijn.

### **Beschrijving gerealiseerde oplossing**

Via de betreffende dienst komt de zoekvraag binnen bij de BV BSN. Afhankelijk van de vraag wordt het antwoord opgehaald uit het nummerregister, de GBA-gegevensset of de documentregisters.

## **5.2.6. Nummerfouten**

### **Realisatie**

De eisen met betrekking tot het melden en registreren van nummerfouten door gebruikers, gemeenten en de belastingdienst zijn niet gerealiseerd met behulp van de BV BSN, maar worden op organisatorische wijze gefaciliteerd. Wel worden fouten en vermoedens van fouten, die binnen de systeemgrenzen van de BV BSN worden geconstateerd vastgelegd in een nummerfoutenlogboek. Hiervoor zijn de volgende use cases beschikbaar:

*BV BSN UC29 Ophalen nummerfouten uit het nummerfoutenlogboek*

*BV BSN UC32 Vastleggen foutvermoeden*

*BC GBA UC22 Melden foutvermoeden*

### **Overwegingen en keuzes**

De keuze om het melden van een foutvermoeden door gemeenten, de belastingdienst en gebruikers vooralsnog op organisatorische wijze te faciliteren (en niet via een dienst van de BV BSN) is tot stand gekomen tijdens verschillende workshops en overleggen met betrokkenen. Hierbij is de voorkeur gegeven aan het melden van fouten en het volgen van de foutafhandeling via een separate website.

Er is voor gekozen om binnen de systeemgrenzen van de BV BSN (in brede zin) geconstateerde nummerfouten in een centraal nummerfoutenlogboek op te nemen. Hierdoor kan de organisatie foutmeldpunt de fouten periodiek uit één logboek ophalen.

### **Beschrijving gerealiseerde oplossing**

Nummerfouten of vermoedens van nummerfouten, die in de BV BSN worden geconstateerd, worden direct in het nummerfoutenlogboek opgenomen.

Nummerfouten, die in de BC GBA worden geconstateerd worden via het melden van het foutvermoeden aan de BV BSN, vastgelegd in het nummerfoutenlogboek.

## **5.2.7. Protocollering**

### **Realisatie**

De gedefinieerde eisen met betrekking tot protocollering zijn gerealiseerd in de volgende use cases:

*BV BSN UC26 Vastleggen protocolgegevens*

*BV BSN UC30 Ophalen protocolgegevens*

*Beheer UC08 Opvragen protocolgegevens uit het protocollageboek*

### **Overwegingen en keuzes**

Er is voor gekozen om de protocolgegevens dagelijks (in een batchproces) samen te stellen op basis van het berichtenlogboek. Hier is om verschillende redenen voor gekozen: Ten eerste wordt op deze wijze de bevraging van het systeem niet belast met de processen voor protocollering. De snelheid van de beschikbaarheid van de protocolgegevens vereist dit ook niet. Een aanvraag voor protocolgegevens moet binnen vier weken beantwoord worden.

Bij het vastleggen van protocolgegevens is ervoor gekozen om alleen de raadplegingen van gebruikers te protocolleren. Het vastleggen van protocolgegevens als gevolg van de matchingsvraag is niet nodig, omdat de gegevens binnen de omgeving van de gemeenten blijven. Daarnaast is het mogelijk dat er op basis van een zoekvraag bij matching meerdere resultaten worden doorgegeven. Het is niet zinvol om alle resultaten te protocolleren, omdat de burger dan informatie zou krijgen dat zijn gegevens zijn gebruikt, omdat ze heel erg op de gegevens van een ander lijken. In het protocollogboek worden geen persoonsgegevens vastgelegd. Er is voor gekozen om alleen aan te geven welke dienst is gebruikt. Op basis daarvan kan worden afgeleid welke gegevens zijn verstrekt.

### **Beschrijving gerealiseerde oplossing**

Periodiek (dagelijks) wordt van de betreffende berichten in het berichtenlogboek, die nog niet zijn verwerkt in het protocollogboek, de protocolgegevens afgeleid en vastgelegd.

Vanuit de beheerapplicatie is het mogelijk om de protocolgegevens, behorende bij een BSN op te vragen.

## **5.2.8. Logging en detectie van misbruik**

### **Realisatie**

Er worden binnen het systeem drie soorten logging onderscheiden:

- Logging van berichten in het berichtenlogboek  
Het eisen met betrekking tot het loggen van berichten zijn gerealiseerd in de volgende use cases:  
*BV BSN UC19 Leg bericht vast*  
*BC GBA UC15 Vastleggen GBA-bericht vast*  
*BC GBA UC16 Vastleggen SOAP-bericht*
- Logging van processtappen in het auditlogboek  
De eisen met betrekking tot vastlegging in het auditlogboek zijn gerealiseerd in iedere use case. In iedere use case is opgenomen dat de processtappen worden vastgelegd in het auditlogboek.
- Logging van systeemfouten in het systeemfoutenlogboek

De eisen met betrekking tot het detecteren van misbruik zijn gerealiseerd in de use case:

*BV BSN UC38 Detecteren misbruik*

### **Overwegingen en keuzes**

Het vastleggen van gegevens in een “logboek” geschiedt om transacties te verantwoorden, foutoorzaken op te sporen en fouten te herstellen. De inrichting van de verschillende logboeken is hierop gericht. (Notitie Logging en protocollering [29]). Bij het vastleggen van berichten is er rekening mee gehouden dat uitgaande berichten voor de ene functionele eenheid (bv BC GBA) inkomende berichten zijn voor de andere functionele eenheid (BV BSN). Deze berichten zijn gelijk en binnen het domein van de BV BSN (in brede zin) en worden daarom slechts op één plaats vastgelegd. In het auditlogboek worden alle processtappen vastgelegd. Indien een proces succesvol is afgerond, worden alle tussenstappen verwijderd en wordt één auditrecord opgenomen. Hier is voor gekozen om de benodigde opslagcapaciteit te beperken. Daarnaast is het niet interessant om details van processen, die goed zijn verlopen vast te leggen.

De eisen met betrekking tot detectie misbruik hebben tot doel het signaleren van niet toegestaan gebruik van de beheervoorziening gebruikersfuncties of foutief gebruik als gevolg van storingen. Hierbij is onderscheid gemaakt naar de sensoren op basis waarvan de detectie plaatsvindt, de verwerking van de gegevens afkomstig van de sensoren en de signalering. Daarnaast is ervoor gekozen om de detectie initieel op basis van vijf patronen uit te voeren. De selectie van deze patronen is gebaseerd op het detecteren van de volgende situaties (bron Notitie Detectie misbruik [30]):

- Fouten in de software
- Niet toegestane bevragingen
- Foutsituaties
- Scannen van nummers

### **Beschrijving gerealiseerde oplossing**

Inkomende en uitgaande berichten worden vastgelegd in een berichtenlogboek. Zowel voor de BV BSN en de BC GBA is een berichtenlogboek ingesteld.

In iedere use case is vastgelegd dat de processtappen worden vastgelegd in het auditlogboek. Indien een proces succesvol is afgerond, worden alle tussenstappen verwijderd en wordt één auditrecord opgenomen.

De eisen met betrekking tot vastlegging in het systeemfoutenlogboek zijn gerealiseerd in de alternatieve scenario's in de use cases. Van hieruit worden de signalen gegeven naar de beheerorganisatie. Voor de technische realisatie is nauw aangesloten bij het gebruikte platform: de fouten worden in het “eventlog” weggeschreven en kunnen van daaruit door de beheerorganisatie worden ingezien.

Bij de gerealiseerde functies voor detectie misbruik wordt op basis van het berichtenlogboek een aantal controles uitgevoerd. Er is gekozen om deze functie te realiseren op basis van instelbare configuratievariabelen. Hierdoor is het mogelijk de detectie aan te passen na een evaluatieperiode en op basis van het aantal aangesloten gebruikers.

## **5.2.9. Authenticatie en autorisatie**

### **Realisatie**

De eisen met betrekking tot authenticatie en autorisatie worden mede gerealiseerd in de volgende use cases:

*BV BSN UC18 Autoriseer verzoek*

*BV BSN UC17 Authenticeren*  
*BC GBA UC18 Authenticeren SOAP-bericht*  
*BC GBA UC19 Autoriseer verzoek*

### **Overwegingen en keuzes**

In twee notities ([31], [32]) is de basis gelegd voor de implementatie van authenticatie en autorisatie. Hierbij is met name de focus gelegd op de authenticatie en autorisatie van afnemersystemen.

In eerste instantie is onderzocht of een autorisatiemechanisme diende te worden ingezet dat nauw aansloot bij de autorisatietabelregels die binnen het GBA gebruikelijk zijn. Dat bleek niet nodig, met name omdat voor gebruikers feitelijk maar twee autorisatieniveaus worden onderscheiden. Dit terwijl de GBA autorisatietabelregels autorisatie op attribuuat niveau mogelijk maken.

Vanuit de memorie van toelichting bij het wetsvoorstel werd geconcludeerd dat niet personen, maar de organisatie waarin ze werken geautoriseerd moet worden. De controle op de eindgebruikersautorisatie wordt daarmee naar de organisatie, eventueel van een Sectorale Berichtenvoorziening, gedelegeerd.

Voor authenticatie werden eisen, zoals er is sprake van “twee-weg” authenticatie; er wordt gebruik gemaakt van methoden en identiteitsgegevens die voldoen aan open standaarden, voor authenticatie en versleuteling van de gegevens tijdens transport worden dezelfde identiteitsgegevens gebruikt en autorisatie zal plaatsvinden op basis van een kenmerk dat onderdeel is van de identiteitsgegevens, geformuleerd die rechtstreeks naar het gebruik van een Public Key Infrastructure leiden. Er is toen een afweging gemaakt tussen de PKI zoals die bij de GBA en LRD in gebruik is én de PKI voor de Overheid (PKIOverheid). Beide mogelijkheden voldoen aan de open X5.09 standaard. Er is, vanwege een beleidsregel binnen de overheid die zegt dat voor (nieuwe) PKIs PKIOverheid moet worden gebruikt, gekozen voor PKIOverheid. Hierbij is wel geverifieerd dat de gehele (mogelijke) gebruikersgroep een dergelijk certificaat kan verkrijgen. Een onderkend voordeel is dat deze openstaat voor (toekomstige) ontwikkelingen waarbij de relatie tussen afnemer en de BV BSN op basis van certificaten niet (noodzakelijkerwijs) 1 op 1 is. Met het gekozen wordt aangesloten bij toekomstige ontwikkelingen, zoals een dienstenbus. Daarnaast is uitsluitend de certificaat hiërarchie en uitgifte afwijkend van hetgeen binnen GBA systemen wordt gebruikt waardoor goede aansluiting met de bestaande situatie bij de beheerorganisatie mogelijk is.

Voor het verlenen van autorisatie maakt de wijze waarop een certificaat wordt verkregen weinig uit. Omdat er voldoende goede leveranciers zijn van PKIOverheid certificaten is besloten de verwerving van het certificaat buit de beheerprocessen van de BV BSN te houden.

Uit performance overweging is ervoor gekozen om de authenticatie (en verder SSL afhandeling) te laten afhandelen door een hardware onderdeel.

Met deze oplossing was ook aan de beveiligingseisen voldaan.

### **Beschrijving gerealiseerde oplossing**

Afnemersystemen gebruiken voor authenticatie en autorisatie X.509 certificaten. Deze certificaten zijn niet uniek op toepassing binnen het BSN stelsel gericht. De gebruikte certificaten vallen binnen de PKI voor de overheid. Certificaten worden afgenomen van een PKIOverheid CSP

Authenticatie en verdere SSL afhandeling vindt plaats op een "SSL Offloader". Op dit apparaat vindt de controle van het certificaat plaats waarbij ook de Certificate Revocation List (SRL) wordt geraadpleegd. Na de SSL Offloader apparaat worden certificaatgegevens (voor de autorisatie) doorgegeven in de "HTTP headers" bij het bericht. Deze headers worden door de applicatie uitgelezen.

Voor de definitie van rollen is binnen het gebruikte besturingssysteem gebruik gemaakt van standaardvoorzieningen (Active Directory en AzMan). De rollen zijn zodanig ingericht dat de geauthenticeerde gebruiker slechts toegang krijgt tot de diensten die bij de rol(len) past die de gebruiker vervult. Voor autorisatie wordt de "Distinguished Name" (DN) uit het certificaat gebruikt. Deze unieke variabele is ook het element waaraan de autorisatie binnen het systeem wordt opgehangen (als een eigenschap van het user account).

Afnemers worden aangemoedigd ook PKIOverheid en/of DigiD in te zetten om hun gebruikers te authenticeren en autoriseren. Voor aansluiting van een afnemer zal worden getoetst dat de toegangscontrole van de gebruikers afdoende is geregeld. De autorisatie is gebaseerd op rollen en er wordt zowel op netwerkniveau als applicatieniveau autorisatie verleend. Het autorisatiemechanisme in de SSL-component en de applicatie, bepaalt op basis van de "distinguished name" (DN) uit een digitaal certificaat het autorisatieniveau

### **5.2.10. Beheerfunctionaliteit**

#### **Realisatie**

De gedefinieerde eisen met betrekking tot de beheerfunctionaliteit worden gerealiseerd in de beheerapplicatie en de bijbehorende diensten in de BV BSN en BC GBA:

*Beheer UC05 Opvragen berichten uit berichtenlogboek BV BSN*

*Beheer UC06 Opvragen auditgegevens uit auditlogboek BV BSN*

*Beheer UC08 Opvragen protocolgegevens uit protocollogboek*

*Beheer UC11 Handmatig aanvragen nummervoorraad*

*Beheer UC23 Opvragen berichten uit berichtenlogboek BC GBA*

*Beheer UC24 Opvragen auditgegevens uit auditlogboek BC GBA*

*Beheer UC27 Corrigeren koppelregister*

*Beheer UC29 Corrigeren nummerregister*

*Beheer UC31 Doorvoeren instantiewijziging*

*Beheer UC32 Plaatsen indicatie*

*Beheer UC33 Opvragen nummergegevens*

*Beheer UC34 Opvragen gegevens koppelregister*

*BV BSN UC07 Ophalen berichten uit berichtenlogboek*

*BV BSN UC08 Vraag auditgegevens op*  
*BV BSN UC22 Registreren instantiewijziging*  
*BV BSN UC28 Ophalen nummergegevens*  
*BV BSN UC30 Ophalen protocolgegevens*  
*BV BSN UC39 Doorvoeren correctie nummerregister*  
*BC GBA UC27 Ophalen auditgegevens BC GBA*  
*BC GBA UC28 Ophalen berichten uit BC GBA berichtenlogboek*  
*BC GBA UC29 Plaatsen indicatie*  
*BC GBA UC30 Ophalen gegevens koppelregister*  
*BC GBA UC31 Doorvoeren correctie koppelregister*

### **Overwegingen en keuzes**

De beheerapplicatie is een losstaande applicatie, die op basis van berichten communiceert met de BV BSN en de BC GBA. Hier is voor gekozen omdat op deze wijze de beheerapplicatie onafhankelijk van de lokatie van de BV BSN en de BC GBA ingezet kan worden.

Voor de beheerapplicatie (ook wel EBA genoemd) is ervoor gekozen om een aantal elementaire functies aan te bieden, die de beheerorganisatie de mogelijkheid geven om zowel in de BV BSN als in de BC GBA de verschillende logboeken in te zien en die de mogelijkheid geeft om (bij hoge uitzondering) correcties door te voeren in het nummerregister en het koppelregister. Er is geen functie gemaakt voor het corrigeren van het presentievragenregister, omdat dit register niet blokkerend werkt bij de presentievraag en omdat een presentievraag toch na vier weken geschoond wordt. Omdat de logboeken een aanzienlijke omvang kunnen krijgen is besloten een maximum te zetten op het aantal op te vragen gegevens.

Bij het opstellen van de functie ten behoeve van het plaatsen van een indicatie op een persoonslijst (zodat de Beheervoorziening BSN op de hoogte wordt gebracht van de relevante spontane mutaties) is ervoor gekozen dit op basis van het BSN te doen en niet op basis van het A-nummer, omdat het gewenst is het gebruik van het A-nummer binnen de BV BSN tot een minimum te beperken, zodat een eventuele uitfasering van het A-nummer niets in de weg staat.

Er is voor gekozen om voor het beheren van accounts voor toegang tot de beheerapplicatie en voor het inloggen gebruik te maken van standaard Windows-functionaliteit.

Met deze beheerapplicatie wordt een aantal basisfuncties aangeboden, waarbij het voor de hand ligt dat bij het inrichten van de beheerorganisatie en het inpassen van de beheerfuncties in de processen de functies in de beheerapplicatie worden uitgebreid, aangepast of worden overgenomen door een andere applicatie.

### **Beschrijving gerealiseerde oplossing**

De beheerapplicatie (EBA) is een eenvoudige webapplicatie, die functies biedt voor het raadplegen van gegevens uit de logboeken van de BV BSN en de BC GBA. Hierbij is het voor de beheerder mogelijk om op basis van een aantal zoekcriteria de gewenste loggegevens op te vragen.

Daarnaast kan de beheerder gegevens met betrekking tot een nummer uit het nummerregister opvragen en, indien nodig, muteren. Dit geldt ook voor het koppelregister.

In de beheerapplicatie is een functie gerealiseerd, die het mogelijk maakt om handmatig een nummervoorraad voor een gemeente aan te vragen. Deze kan als xml- of tekstbestand worden opgeslagen.

Als laatste kan de beheerder een indicatie plaatsen op een persoonslijst.

### **5.3. Realisatie van prestatie-eisen**

Voor een belangrijk deel worden de prestatie-eisen gerealiseerd door het op de juiste manier inzetten van hardware.

Overwegingen en keuzes bij de infrastructuurinrichting

#### **Algemeen**

Om aan de beschikbaarheidseis van 99,8% te voldoen wordt het systeem redundant uitgevoerd. Er wordt altijd voor een 'n+1' configuratie gekozen, waarbij 'n' voldoende moet zijn om de verwachte systeemplas te dragen. Dit betekent dat de uitval van een enkel hardware element nimmer tot verstoring van de dienstverlening leidt.

#### **Firewall**

Er is gekozen voor een hardwarematige firewall. Dergelijke componenten kunnen in de Gbps netwerkverkeer afhandelen met honderdduizenden "concurrent sessions". Veel meer dan de 15Mbps die in piekbelasting via het externe netwerk wordt aangeleverd. Vanwege de "n+1" wens zijn er voor de productieomgeving dus twee firewalls te worden aangeschaft.

#### **SSL Offloader en Loadbalancer**

Een hardware matige SSL Offloader kan veel sneller het SSL protocol afhandelen in vergelijking tot een software matige oplossing. Een Loadbalancer zorgt ervoor dat het systeem schaalbaar en fouttolerant wordt.

Er is een apparaat gekozen die deze twee functies combineert; de "Alteon 2424-SSL application switch" van de leverancier Nortel. Een dergelijk systeem bezit 24 100Mb poorten en kan 51.000 SSL-sessies per seconde afhandelen.

Karakteristiek dat voor dit systeem relevant is betreft het extern netwerkverkeer. In piekbelasting is dat 15Mbps hetgeen voor een enkel exemplaar van dit systeem geen enkel probleem is. Zolang het aantal webserver (zie hieronder) beneden de 22 blijft voldoet 1 exemplaar van de voorgestelde "SSL Offloader en Loadbalancer". Vanwege de "n+1" eis zijn er voor de productieomgeving dus twee componenten aangeschaft.

#### **Webservers**

Omdat er vrij veel servers nodig zijn is er gekozen voor blade servers; die zijn bij grotere aantallen (meer dan 10) gemakkelijker te onderhouden en nemen minder ruimte in. Gekozen is voor HP hardware waarin 4x 1Gb netwerkkaarten zijn opgenomen. De webserver zijn derhalve niet "network bound"; één netwerk kaart zou (inclusief allerlei overhead die veelal op een netwerk wordt gevonden) het hele gevraagde netwerkverkeer van de BV BSN bij piekbelasting (15 + 44Mb) kunnen afhandelen.

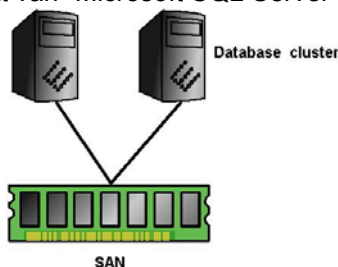
Het is moeilijk theoretisch te bepalen hoeveel berichten een webserver per seconde kan verwerken, zeker ook omdat sprake is van vrij specifieke maatwerksoftware. Dit kan het beste worden bepaald met behulp van experimentele meetresultaten. Deze experimenten zijn, met hulp van een Microsoft consultant, uitgevoerd. Hieruit volgde dat er per webserver zeker 50 berichten (vraag én antwoord met een responsetijd kleiner dan 1 seconde) per seconde kunnen worden afgehandeld. Dit zou betekenen dat er om de piekbelasting van 185 berichten aan te kunnen er 5 (4+1) servers noodzakelijk zijn.

Voor bladeservers moet een “enclosure” worden aangeschaft.

### **Nummerregister, logboeken en koppel- en presentievraagregister**

Omdat ook gegevens moeten worden opgeslagen / gewijzigd is voor het nummerregister (en ook voor de logboeken en het presentievraagregister) gekozen voor een “Storage Area Network” (SAN). Een dergelijke component is feitelijk een doos redundante harde schijven. Ook hier is voor HP hardware gekozen, de “HP StorageWorks Modular Smart Array 1000”; waarin tot 2TB aan gegevens met een “throughput” tot 200Mbps past.

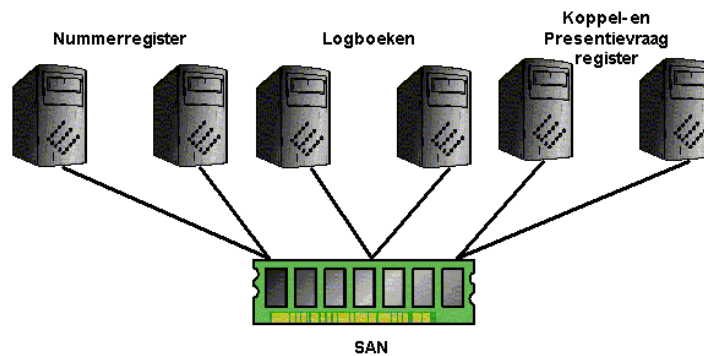
Dit schijvenkabinet wordt aangestuurd door een cluster van databaseservers waarvoor wederom (de ook voor webserver voorgestelde) bladeservers worden ingezet. In dit cluster van twee servers vervuld één server een actieve rol terwijl de ander passief pas in actie komt als de andere server onverhoopt uitvalt (“Active/passive” configuratie). Er wordt hierbij gebruik gemaakt van “Microsoft SQL Server” software.



Veruit het grootste deel van het gebruik van het nummerregister zal bestaan uit bevestigingen. Er moeten ongeveer 25miljoen nummers in het nummerregister kunnen waarbij elke record in de orde van 10kB zal zijn. Totaal gevraagde opslag is derhalve ongeveer 250GB.

Voor de Logboeken is een vergelijkbare configuratie ingericht. Verschil is wel dat hier de opslagfunctionaliteit centraal staat en dat er weinig (tot geen) bevestigingen zullen zijn. Bij de gemiddelde belasting van 530.000 berichten per werkdag groeit het logboek met 8GB per werkdag of 180GB per maand.

Ook bij het koppel- en presentievragenregister is voor het SAN gekozen. Het netwerkverkeer naar deze registers is te verwaarlozen. In het koppelregister zitten 25miljoen relaties van ongeveer 1kB. Er worden maximaal 40.000 presentievragen, van circa 10kB, bewaard (de bewaartermijn is 1 maand). De totaal gevraagde opslagcapaciteit is derhalve ongeveer 250 GB.

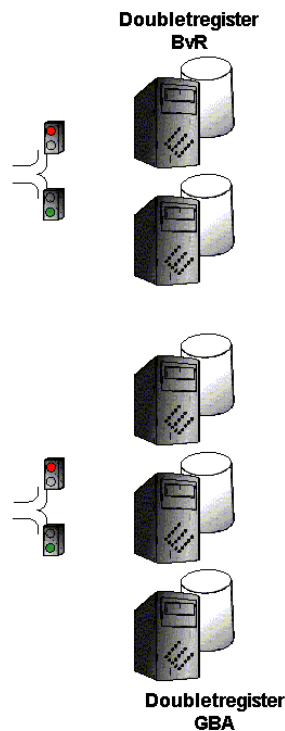


Eén SAN van het voorgestelde type heeft derhalve meer dan voldoende opslagcapaciteit. Ook de netwerk bandbreedte van een dergelijk SAN is voldoende; ook dat is door middel van experimenten geverifieerd.

### Doubletregisters GBA en BvR

Om de beschikbaarheid van deze “read only” database te optimaliseren worden afzonderlijke databases (met identieke gegevenssets) ingezet waarbij de belasting via een loadbalancer wordt verdeeld (Als er een uitvalt neemt de ander het over; tijdens het update mechanisme is ook slechts een deel niet beschikbaar).

Gezien het feit dat vrijwel elke verificatie vraag met persoonsgegevens gebruik maakt van het Doubletregisters GBA is er voor dit systeem gekozen voor drie afzonderlijke databasesystemen (gebaseerd op eerder genoemde bladeservers en Microsoft SQL Server software). Het doubletregister BvR wordt alleen in presentievragen gebruikt. Hiervoor volstaat derhalve het minimum van 2 servers.



Voor loadbalancing tussen de database wordt hetzelfde apparaat gebruikt dat de SSL Offloading en loadbalancing tussen de webserver verzorgt.

#### **Toekenning en actualisatie**

Deze noodzakelijke functionaliteit levert, in vergelijking met de webservices voor gebruikers, nauwelijks een belasting van de systemen op. Deze services kunnen daarom zonder probleem op een cluster worden bijgeplaatst. Omdat het cluster van het koppel- en presentievraagregister het minst belast wordt is op dit cluster deze functionaliteit bijgeplaatst.

#### **Ondersteunende systemen en netwerk**

Naast de hierboven genoemde primaire systemen zijn ook aanvullende server aangeschaft om noodzakelijk windows services, zoals Activer Directory en (Dynamic) DNS, mogelijk te maken. Ook is er rekening gehouden met twee servers die beheerssoftware draaien en één server voor het uitvoeren van back-ups.

### **5.4. Realisatie overige technische eisen**

De onderhoudbaarheid van de maatwerksoftware is geborgd door een veelheid aan maatregelen, waaronder het opzetten van een ontwikkelomgeving waarin dagelijks de applicatie bijeen wordt gebracht waarna unittesten (over de gehele breedte) worden uitgevoerd. In deze ontwikkelomgeving worden metriecken bijgehouden die dagelijks de complexiteit van de broncode in beeld brengen. Er is een “penalty” systeem dat er voor zorgt dat de kwaliteitsstandaarden door de bouwers wordt nageleefd.

Er wordt gebruik gemaakt van één codeerstandaard en naamgevingstandaard die duidelijk gedocumenteerd is en tot doel heeft de begrijpelijkheid te bevorderen. Omdat het de onderhoudbaarheid ten goede komt is er voor een stijl van coderen gekozen waarbij stukken gedrag van het systeem (functies, processen, use cases of services) zijn hierdoor op één plaats uitgecodeerd). Hierdoor wordt het inzicht in de werking van de code vereenvoudigd. In de praktijk is ook gebleken dat deze stijl inderdaad de onderhoudbaarheid ten goede komt: nieuwe programmeurs bleken zeer snel productief zijn.

Er is binnen de broncode veelal de voorkeur gegeven aan primitieve datatypen (zoals een long voor een BSN). Hierdoor wordt een lager geheugengebruik en een betere performance (ook doordat niet steeds geconverteerd hoeft te worden) bereikt.

In het Logisch Ontwerp BSN [6] wordt in detail de interface ten behoeve van externe systemen gespecificeerd. Daarnaast is, met behulp van de Webservice DeScription Language (WSDL), de interface gedefinieerd zodat softwareontwikkelaars snel een aansluiting kunnen realiseren. Voor gebruikers is deze WSDL gepubliceerd via <https://wsdl.burgerservicenummer.nl>.

Er wordt in de broncode van de maatwerksoftware geen gebruik gemaakt van onderdelen van derden. De applicatie heeft om goed te functioneren uitsluitend bestaande functies binnen de gekozen omgeving nodig. Deze omgeving (besturingssysteem, database software, netwerkondersteuning) is gebaseerd op bestaande producten.

Er is veel gebruik gemaakt van Open standaarden waarbij de nadruk ligt op de componenten die de communicatie met de gebruikers verzorgen. De berichten zijn opgemaakt conform de WSI standaard dit is ondermeer getoetst met het product SOAPScope. Bij de uitwisseling van de berichten wordt gebruik gemaakt van Internet standaarden als SOAP, HTTP, en SSL.

Al het netwerkverkeer is gebaseerd op het internet protocol TCP/IP.

Er is uitgegaan van de ISO 10646 UTF-8 tekenset die overeenkomt met de (beperkte) GBA Teletex tekenset. Deze tekenset ondersteunt de noodzakelijke diakrieten.

Tot slot zijn de bouwstenen van de maatwerkapplicatie, het .Net framework en de C# programmeertaal Open (ECMA) standaarden.

## **5.5. Realisatie van kwaliteitseisen**

De kwaliteitsaspecten zijn, mede door de aard van het gebruikte ISO9126 raamwerk, redelijk generiek van aard. Voordat ze getoetst kunnen worden moeten de aspecten verder worden uitgewerkt. Dit is voor de genoemde tien belangrijkste aspecten gebeurt in het plan van aanpak voor de technische testen [3]. Met deze uitwerkingen worden de aspecten testbaar. De resultaten van deze testen worden daarmee meegenomen in het vrijgaveadvies.

Vanuit het bouwteam bestond de wens om al tijdens de realisatie van software aandacht te besteden aan de kwaliteitsaspecten. In samenwerking met een specialist van Microsoft is de software en de resulterende applicatie gereviewed en aan toetsen onderworpen. Daarbij is met name aandacht gegeven aan de categorieën Betrouwbaarheid, Efficiëntie en het aspect Beveiligbaarheid. Vanuit de review- en toetsresultaten zijn verbetervoorstellen gedaan en gerealiseerd. Daarnaast zijn een aantal aandachtspunten en aanvaardbare risico's onderkend die aan de beheerorganisatie kunnen worden doorgegeven.

Het kwaliteitsaspect beveiligbaarheid is bij het opstellen van het Informatie BeveiligingsPlan (IBP) [4]. Voor dit plan zijn, in overeenstemming met het VIR (Voorschrift Informatiebeveiliging Rijksdiensten) [20], een Afhankelijkheids- en Kwetsbaarheidsanalyse ([34], [33]) uitgevoerd voor de centrale voorzieningen van het BSN-stelsel. In het IBP, dat na een audit door een externe partij is vastgesteld in de stuurgroep BSN, zijn maatregelen benoemd voor de informatiebeveiliging.

Aanvullend is door Govcert een penetratietest uitgevoerd op de "Conference Room Pilot" omgeving die op vergelijkbare wijze is ingericht als de productieomgeving. In deze test zijn geen kwetsbaarheden aan het licht gekomen. Voor de in productiename wordt een tweede test uitgevoerd op de productieomgeving.

## **5.6. Realisatie beveiligingseisen**

Conform het Voorschrift Informatiebeveiliging Rijksdiensten (VIR) [20] is een Afhankelijkheids- en Kwetsbaarheidsanalyse (A+K-analyse) ([34], [33]) uitgevoerd voordat het informatiebeveiligingsplan BSN (IBP) is opgesteld. In dit IBP zijn, als resultaat van de A+K-analyse, een groot aantal beveiligingsmaatregelen opgenomen.

Voor de identificatie en communicatie met gebruikers maakt het systeem gebruik van het hoogste veiligheidsniveau van de PKI Overheidsstandaard (Public Key Infrastructure certificaten). Tevens wordt op basis hiervan het beveiligd netwerk gerealiseerd. Daarenboven wordt aan de hand van de identificatie met de certificaten voor elke afzonderlijke dienst van de beheervoorziening vastgesteld of autorisatie verleend mag worden.

Er is fysieke toegangsbeveiliging die garandeert dat alleen geautoriseerd personeel toegang heeft tot de voor het beheer bestemde ruimtes en voorzieningen. Een geïntegreerd bewakingsstelsel waakt voortdurend over fysieke ruimtes en de goede werking van de hard- en software van de beheervoorziening. Ook het klimaat in deze ruimten wordt beheerst zodat deze ideaal is voor het functioneren van de systemen. Op de systemen is controlesoftware geïnstalleerd die elke wijziging en toevoeging in de gebruikte programmatuur, zowel de standaard- als de maatwerksoftware, registreert.

Voor het personeel dat de beheervoorziening gaat beheren zijn er processen en procedures ingericht die zorgen voor screening, onder meer rond het aannemen. Er zijn goede werkinstructies en er is een opleidingsplan dat er voor zorgt dat de kennis van de medewerkers van het goede niveau is. De werkzaamheden zijn zodanig ingericht dat men elkaar kan vervangen zodat, samen met een verloopplanning, is geborgd dat essentiële taken tijdig kunnen worden uitgevoerd.

Met geautomatiseerde controles wordt de integriteit van het nummerregister en de registers met persoonsgegevens dagelijks gecontroleerd. Het systeem is op alle onderdelen tenminste dubbel, en dus redundant, uitgevoerd zodat maximaal wordt voorkomen dat er verstoringen in de dienstverlening zijn of dat de integriteit van het nummerregister in het geding komt. Reservekopieën van de software van de beheervoorziening en de gegevens in het nummerregister dragen zorg voor een minimaal verlies aan gegevens in geval van een storing. In geval van een calamiteit kan conform een vastgesteld calamiteitenplan worden uitgeweken naar een alternatieve, even beveiligde locatie.

Gebruikers die verificatievragen willen stellen aan de beheervoorziening dienen zich aan te melden voor aansluiting op de beheervoorziening bij de beheerder ervan. In de gestandaardiseerde aansluitprocedure wordt onder meer vastgesteld of de organisatie inderdaad gebruiker is in de zin van de Wet algemene bepalingen BSN.

De doelmatigheid van de maatregelen is middels diverse audits door verschillende onafhankelijke specialisten vastgesteld.