PRICEWATERHOUSECOOPERS

UNIVERSITEIT VAN TILBURG

Radboud Universiteit Nijmegen

Beveiligingeisen ten aanzien van identificatie en authenticatie voor toegang zorgconsument tot het Elektronisch Patiëntendossier (EPD)

Definitief

2008-3027/OV/rvdk/mp

Opstellers:
prof. dr. Bart Jacobs, Institute for Computing and Information Sciences (Radboud Universiteit Nijmegen)
dr. mr. Sjaak Nouwt, Tilburg Institute for Law, Technology and Society (Universiteit van Tilburg)
Adri de Bruijn RE RA, PricewaterhouseCoopers Advisory
ir. Otto Vermeulen RE CISSP, PricewaterhouseCoopers Advisory
drs. Roland van der Knaap RE, PricewaterhouseCoopers Advisory
Cas de Bie MSc., PricewaterhouseCoopers Advisory

2 december 2008

PRICEWATERHOUSECOOPERS

UNIVERSITEIT VAN TILBURG

Radboud Universiteit Nijmegen

Inhoud

Management samenvatting

Achtergrond en aanleiding

In Nederland bestaan vergevorderde plannen voor de inrichting van het landelijke Elektronisch Patiëntendossier (EPD). Zorgaanbieders krijgen hiermee de mogelijkheid om een selectie van gegevens uit de eigen informatiesystemen waarin patiëntgegevens worden geregistreerd te koppelen aan het Landelijk Schakelpunt (LSP). Via het LSP zullen zorgaanbieders vervolgens patiëntgegevens van zorgconsumenten onderling kunnen uitwisselen als dat noodzakelijk is voor een goede behandeling of verzorging van die zorgconsument.

In Nederland hebben zorgconsumenten volgens de Wet geneeskundige behandelingsovereenkomst (Wgbo) het recht op inzage in de eigen medische gegevens. De inzage door de zorgconsument in de eigen medische gegevens vindt nu alleen decentraal plaats bij de individuele zorgaanbieders (al dan niet elektronisch). Met de komst van het landelijk EPD ontstaat nu langs elektronische weg ook voor de zorgconsument de mogelijkheid tot (centrale) inzage in (het EPD-deel van) de eigen medische gegevens.

Deze toegang tot het EPD voor zorgconsumenten kan ook belangrijk zijn om het juiste gebruik ervan door zorgaanbieders te bevorderen. Door middel van de toegang tot de centrale gebruiksregistratie kunnen zorgconsumenten immers zelf inzien welke zorgaanbieder wanneer toegang heeft gehad tot hun EPD. Zorgconsumenten kunnen vervolgens actie ondernemen wanneer er in hun ogen sprake is van mogelijk onterechte nieuwsgierigheid of zelfs misbruik in plaats van professionele betrokkenheid op basis van een behandelrelatie.

Het uitwisselen van medische gegevens is zeer privacy gevoelig. Het is dan ook zaak om uiterst zorgvuldig om te gaan met inrichting van de toegang tot het EPD voor de zorgconsument. Het ministerie van Volksgezondheid, Welzijn en Sport (hierna: VWS) heeft daarom onafhankelijk advies gevraagd over de minimale beveiligingseisen voor de identificatie en authenticatie van de zorgconsument in het kader van verlenen van toegang tot het EPD voor de zorgconsument:

- Identificatie betekent in deze context het identificeren van een zorgconsument aan de hand van een uniek kenmerk, zoals een identificerend uniek nummer. Ten aanzien van de identificatie van de zorgconsument wordt in deze analyse uitgegaan van het gebruik van het Burger Service Nummer (BSN). Daarbij is de aanname gebruikt dat het BSN op een juiste en betrouwbare wijze wordt toegekend aan zorgconsumenten. Een toetsing van deze aanname ligt buiten de reikwijdte van het uitgevoerde onderzoek.
- Authenticatie behelst de controle of de zorgconsument daadwerkelijk de persoon is die deze beweert te zijn. Dit kan door middel van iets wat een zorgconsument weet (bijvoorbeeld een wachtwoord), heeft (zoals een reisdocument) of is (zoals vingerafdrukken).

Conclusie en aanbeveling

Gelet op de juridische en technische beveiligingseisen rondom het EPD is – uitgedrukt in DigiD-niveaus - een zekerheidsniveau van meer dan 2 noodzakelijk. Hiervan uitgaande lijkt op de langere termijn eNIK (of een vergelijkbaar elektronisch rijbewijs), gemeten naar de huidige kennis en inzichten rondom eNIK, het meest geschikte authenticatiemiddel om DigiD zekerheidsniveau 3 te bereiken. Omdat eNIK danwel het elektronisch rijbewijs hoogstwaarschijnlijk de komende jaren niet beschikbaar zullen zijn, zijn alternatieve opties met een lager zekerheidsniveau dan 3 maar hoger dan 2 in kaart gebracht.

Op grond van de geïnventariseerde technische en juridische eisen, komen voor EPD-authenticatie twee authenticatiemiddelen in aanmerking, te weten SMS+ (variant 1) en RTDA:

- SMS+ (variant 1) is gebaseerd op DigiD. In verband met de noodzakelijke face-to-face verificatie zal de zorgconsument zich persoonlijk moeten melden bij een controle-instantie[1] alwaar een baliemedewerker diens identiteit wordt vastgesteld. Voor face-to-face verificatie van het bij SMS+ gebruikte mobiele telefoonnummer worden verschillende mogelijkheden onderscheiden. SMS+ (variant 1) maakt hiervoor gebruik van een applicatie die in contact staat met de DigiD server. De DigiD server stuurt vervolgens een SMS naar het (eerder) opgegeven mobiele telefoonnummer (dat bij DigiD gekoppeld is aan het BSN van de betreffende persoon). Deze SMS bevat een specifieke (eenmalige) code, die ook verschijnt in de applicatie. De baliemedewerker controleert op het scherm van de mobiele telefoon dat de juiste code binnengekomen is, en geeft via de applicatie aan dat dit mobiele telefoonnummer gevalideerd is. De uitvoering van het identificatie- en verificatieproces door de betreffende baliemedewerker wordt geregistreerd in de applicatie. Vervolgens krijgt de zorgconsument na gebruikelijke SMS authenticatie een hoger zekerheidsniveau, bijvoorbeeld voor EPD-toegang.
- RTDA (Remote Travel Document Authentication) is eveneens gebaseerd op DigiD, aangevuld met authenticatie door middel van een reisdocument wat na 26 augustus 2006 is uitgegeven en een chip bevat. Omdat de geldigheidsduur van reisdocumenten 5 jaar bedraagt, zal het nog tot 2011 duren voordat alle huidige reisdocumenten zijn vervangen door een reisdocument met een chip. Een persoon meldt zich op een daartoe bestemde webpagina om toegang te krijgen tot zijn EPD. Zoals gebruikelijk bij DigiD wordt (de browser van) deze persoon automatisch doorgestuurd naar de DigiD-server, met het verzoek om een ticket met zekerheidsniveau minstens 2½. De betreffende persoon logt hier eerst in tot zekerheidsniveau 2 via gebruikersnaam en SMS-authenticatie. Vervolgens wordt op de DigiD webpagina gevraagd om het eigen paspoort (of de identiteitskaart) op een contactloze kaartlezer te leggen, en om het nummer en de geldigheidsdatum van het document op de webpagina in te vullen. De DigiD-server communiceert dan met de chip in het reisdocument, controleert de echtheid ervan en ook of de houder ervan dezelfde is, met hetzelfde BSN, als degene die reeds tot zekerheidsniveau 2 ingelogd is. Wanneer alles klopt wordt de betreffende persoon door de DigiD-server met een valide ticket (met BSN) terug naar de oorspronkelijke website verwezen

[1] Het identificatie- en verificatieproces voor SMS+ kan worden uitgevoerd door verschillende controle-instanties. In hoofdstuk 5 van dit rapport wordt ter illustratie de uitvoering van het identificatie- en verificatieproces door zowel het gemeentehuis als de apotheek verder uitgewerkt.

waar de EPD-toegang tenslotte gerealiseerd kan worden.

Beide authenticatiemiddelen werken op basis van het BSN als uniek identificatiemiddel en de bestaande DigiD niveaus 1 en 2. Daarom kunnen zorgconsumenten die niet de beschikking hebben over een BSN[2] of niet geregistreerd zijn in het GBA geen gebruik maken van deze authenticatiemiddelen.

Beide oplossingen zijn niet direct te realiseren omdat zij bouw van programmatuur, inrichting van procedures en controle-instanties et cetera vereisen. Bij de keuze tussen deze twee alternatieven speelt op de achtergrond ook ander overheidsbeleid betreffende authenticatie een rol (de invoering van eNIK, elektronisch rijbewijs, en de eventuele inpassing hiervan binnen DigiD) dat de context van dit rapport overstijgt.

Bij eerste beschouwing lijkt de SMS+ (variant 1) een bredere verspreiding te hebben dan de reisdocumenten voorzien van RTDA en daarmee op dit moment breder implementeerbaar. Bij SMS+ (variant 1) is een controle-instantie noodzakelijk, waarbij in dit advies als mogelijke opties zijn uitgewerkt het gemeentehuis en de apotheek. Het gemeentehuis lijkt meer ervaring te hebben met identiteitscontrole maar dit is niet doorslaggevend. De uiteindelijke keuze voor hetzij SMS+ (variant 1) hetzij RTDA, danwel de controle-instantie, is een veelzijdig vraagstuk waarbij naast het uitgifteproces ook kosten, gebruikersvriendelijkheid, snelle beschikbaarheid, externe afhankelijkheden en technische aspecten meespelen. Een verantwoorde keuze tussen de opties vergt daarom de afweging van middelen en van bijbehorende processen. Een dergelijke afweging valt gezien het doel van het onderzoek (een onafhankelijk advies inzake de minimale beveiligingseisen voor de identificatie en authenticatie van de zorgconsument in het kader van Toegang patiënt tot het EPD) buiten de reikwijdte van dit onderzoek (gericht op de juridische en technische eisen).

Zodra keuzes zijn gemaakt voor het authenticatiemiddel en het uitgifteproces (met daarbij inbegrepen de controle-instantie), wordt nadrukkelijk geadviseerd een praktijkproef te organiseren, voorafgaande aan een grootschalige invoering[3]. Na evaluatie van deze praktijkproef kan dan een definitieve keuze worden gemaakt en een tijdspad worden bepaald voor de invoering.

Deze adviesopdracht is in de periode van september 2008 tot en met november 2008 uitgevoerd door een voor deze opdracht tijdelijk samenwerkingsverband dat bestaat uit het Tilburg Institute for Law, Technology and Society (TILT), van de Universiteit van Tilburg, het Institute for Computing and Information Sciences (ICIS) van de Radboud Universiteit Nijmegen en PricewaterhouseCoopers Advisory NV (PwC).

[2] Het betreft hier thans niet-ingezetenen.
[3] Mogelijk kan zelfs overwogen worden voor beide opties een praktijkproef te houden, en mede op basis van de uitkomsten daarvan een besluit te nemen.

1 Inleiding

1.1 Achtergrond en aanleiding

1.01 In Nederland bestaan vergevorderde plannen voor de inrichting van het landelijke Elektronisch Patiëntendossier (EPD). Zorgaanbieders krijgen hiermee de mogelijkheid om een selectie van gegevens uit de eigen informatiesystemen waarin patiëntgegevens worden geregistreerd te koppelen aan het Landelijk Schakelpunt (LSP). Via het LSP zullen zorgaanbieders vervolgens patiëntgegevens van zorgconsumenten onderling kunnen uitwisselen als dat noodzakelijk is voor een goede behandeling of verzorging van die zorgconsument.

1.02 In Nederland hebben zorgconsumenten volgens de Wet geneeskundige behandelingsovereenkomst (Wgbo) het recht op inzage in de eigen medische gegevens. De inzage door de zorgconsument in de eigen medische gegevens vindt veelal decentraal bij de individuele zorgaanbieders plaats. Met de komst van het EPD ontstaat ook voor de zorgconsument in principe de mogelijkheid op centrale inzage in (het EPD-deel van) de eigen medische gegevens.

1.03 Deze toegang tot het EPD voor zorgconsumenten kan ook belangrijk zijn om het juiste gebruik ervan door zorgaanbieders te bevorderen. Door middel van de toegang tot de centrale gebruiksregistratie kunnen zorgconsumenten immers zelf inzien welke zorgaanbieder wanneer toegang heeft gehad tot hun EPD. Zorgconsumenten kunnen vervolgens actie ondernemen wanneer er in hun ogen sprake is van mogelijk onterechte nieuwsgierigheid of zelfs misbruik in plaats van professionele betrokkenheid op basis van een behandelrelatie.

1.04 Bij de ontwikkeling van het landelijk EPD is men voornemens om zorgconsumenten de volgende functionaliteiten aan te bieden, waarvoor verschillende eisen kunnen gelden:

1. Totaal bezwaar: de zorgconsument kan totaal bezwaar maken tegen het EPD. Dit houdt in dat er geen indexopbouw en gegevens uitwisseling plaatsvindt.
2. Uitsluiten op naam en beroepsgroep: de zorgconsument kan besluiten bepaalde beroepsgroepen of specifieke zorgverleners geen toegang te verlenen tot zijn/haar EPD.
3. Inzage in verwijsindex: de zorgconsument kan via de verwijsindex inzien welke medische gegevens bij welke zorgaanbieders aanwezig zijn.
4. Inzage in logginggegevens: de zorgconsument heeft hiermee inzage in de zorgaanbieders / zorgverleners die toegang hebben gehad tot de medische gegevens.
5. Inzage in medische gegevens: zorgconsumenten krijgen hiermee inzage in (het EPD-deel van) de eigen medische gegevens.

1.05 Bij zowel de uitwisseling van medische gegevens als bij de inzage door de zorgconsument van de eigen medische gegevens gaat het om zeer privacygevoelige (en dus vertrouwelijke) gegevens. Omdat de toegang tot de eigen medische gegevens door zorgconsumenten zal geschieden via het internet (wat een publiek netwerk is), is het noodzakelijk dat bij de ontwikkeling van de bovengenoemde functionaliteiten, strikte beveiligingsmaatregelen worden getroffen. Het ministerie van VWS heeft daarom onafhankelijk advies gevraagd over de minimale beveiligingseisen voor de identificatie en authenticatie van de zorgconsument in het kader van verlenen van toegang tot het EPD voor de zorgconsument:

- ***Identificatie*** ('zeggen wie je bent') betekent in deze context het identificeren van een zorgconsument aan de hand van een uniek kenmerk, zoals een identificerend uniek nummer. Ten aanzien van de identificatie van de zorgconsument wordt in deze analyse uitgegaan van het gebruik van het Burger Service Nummer (BSN). Daarbij is de aanname gebruikt dat het BSN op een juiste en betrouwbare wijze wordt toegekend aan zorgconsumenten. Een toetsing van deze aanname lag buiten de reikwijdte van het uitgevoerde onderzoek.
- ***Authenticatie*** ('bewijzen wie je bent') behelst de controle of de zorgconsument daadwerkelijk de persoon is die deze beweert te zijn. Dit kan door middel van iets wat een zorgconsument weet (bijvoorbeeld een wachtwoord), heeft (zoals een reisdocument) of is (zoals vingerafdrukken).

1.06 Bovengenoemde functionaliteiten 1 en 2 hebben in eerste instantie alleen invloed op de toegang tot het EPD door zorgverleners en geven geen directe toegang tot medische gegevens. Functionaliteiten 3, 4 en 5 geven wel directe inzage in medische gegevens. Ongeautoriseerd gebruik van de functionaliteit 1 of 2 heeft echter wel gevolgen voor wie met behulp van de functionaliteiten 3, 4 of 5 medische gegevens kunnen inzien. Vanuit het perspectief van beveiliging, beschouwt het onderzoeksteam de risico's verbonden aan de 5 functionaliteiten als zijnde vergelijkbaar, en wordt geen aanleiding gezien om het vereiste niveau van identificatie / authenticatie te laten variëren voor de verschillende functionaliteiten.[4]

1.07 Bij de uitvoering van het onderzoek is gebruik gemaakt van informatie die is verkregen uit de in bijlage A genoemde documentatie en uit gesprekken die zijn gevoerd met de in bijlage B genoemde personen.

1.2 Doelstelling en reikwijdte

1.08 Het doel van deze opdracht is een advies te verstrekken aan het ministerie van VWS inzake de minimale beveiligingeisen aan het identificatie- en authenticatieproces voor de zorgconsument in het kader van het verlenen van toegang tot het landelijk EPD. Hierbij zal er advies worden gegeven op de volgende 3 gebieden:

1. De minimale (beveiligings)eisen voor identificatie- en authenticatiemiddelen voor

[4] Gedurende de onderzoeksperiode heeft de minister van VWS besloten voor functionaliteit 1 (Totaal bezwaar) gebruik te maken van DigiD met zekerheidsniveau 2.

zorgconsumenten binnen het landelijk EPD. Hierbij is vooral gebruik gemaakt van juridische en technische eisen die voortvloeien uit de relevante wet- en regelgeving.

2. De mogelijk geschikte identificatie- en authenticatiemiddelen, waaronder ten minste DigiD, smartcards/tokens en bancaire middelen (zoals een beveiligingscalculator). Op basis van de in het vorige punt opgestelde (beveiligings-)eisen is eerst een inventarisatie uitgevoerd en heeft vervolgens een inschatting plaatsgevonden van de mate van geschiktheid.
3. De inrichting en minimale eisen die worden gesteld aan het verificatie- en uitgifteproces van de identificatie- en authenticatiemiddelen, bijvoorbeeld via de post of face-to-face. Hierbij wordt tevens rekening gehouden met de mate van complexiteit en de kosten van de technische implementatie.

1.09 De uitvoering van deze opdracht had alleen betrekking op de in alinea 1.04 genoemde functionaliteiten voor een zorgconsument.

1.10 Voor de selectie van een EPD-authenticatiemiddel is uitgegaan van de technische en juridische eisen. Andere facetten waaronder kosten, gebruikersvriendelijkheid, snelle beschikbaarheid, externe afhankelijkheden en technische aspecten zijn in de keuze voor het middel niet meegewogen. Wel zijn enkele van deze facetten in het kader van de inrichting van het identificatie- en verificatieproces uitgewerkt in hoofdstuk 5.

1.11 Daarnaast is in het advies verder alleen ingegaan op de beveiligingsaspecten van de voorgestelde identificatie- en authenticatiemiddelen en het in te richten verificatie- en uitgifteproces. Zaken als zorgvuldige omgang door zorgconsumenten met de verkregen authenticatiemiddelen en de beveiliging van de PC van een individuele zorgconsument blijven daarom buiten beschouwing.

1.12 De inrichting van autorisaties voor het verkrijgen van toegang tot het EPD ligt eveneens buiten de reikwijdte van deze opdracht.

1.3 Randvoorwaarden en uitgangspunten

1.13 EPD-authenticatie moet voorkomen dat:

- Medische gegevens door niet-gerechtigden kunnen worden ingezien (ter bescherming van vertrouwelijkheid).
- Toegang tot deze medische gegevens niet wordt ingesteld (noch door gerechtigden, noch door niet-gerechtigden) op een wijze die niet overeenstemt met de wensen van de zorgconsument (ter bescherming van integriteit van toegang, en ook van beschikbaarheid van gegevens voor zorgverleners).

1.14 Technische middelen zullen een belangrijke rol spelen bij het reguleren van toegang tot het EPD. Belangrijk daarbij is dat deze middelen door zorgconsumenten veilig beheerd en goed gebruikt worden. Zorgconsumenten zijn niet geneigd om op straat aan een wildvreemde zomaar hun huissleutel af te staan. Door relatieve onbekendheid en onervarenheid in de digitale wereld komt dergelijk gedrag daar echter vaker voor, bijvoorbeeld in reacties op phishing aanvallen. Dit "zorgvuldig gebruik en beheer" van authenticatiemiddelen is belangrijk en verdient aandacht, maar een advies hieromtrent valt buiten de reikwijdte van dit onderzoek.

1.15 In dezelfde lijn dient opgemerkt te worden dat de PC van individuele gebruikers besmet kan zijn met kwaadaardige software. In dat geval heeft de gebruiker niet langer controle over het apparaat, en kunnen authenticatiemiddelen die voor een specifiek doel aangeboden worden door de kwaadaardige software voor een ander doel gebruikt worden. Concreet zou dergelijke software van een gebruiker die op bijvoorbeeld mijnoverheid.nl via DigiD inlogt de gegevens kunnen misbruiken voor heimelijke EPD-toegang, met alle mogelijke kwade gevolgen van dien. Bescherming van PC's heeft velerlei aspecten (zoals adequaat beheer, fouten in software, agressiviteit van aanvallers) die buiten de reikwijdte van dit rapport vallen.

1.3.1 Gebruik BSN

1.16 Dit onderzoek richt zich op toegang voor zorgconsumenten tot het EPD. De doelgroep voor deze toegang bestaat in principe uit alle zorgconsumenten die de beschikking hebben over een Burger Service Nummer (BSN)[5], omdat EPD's hiermee geïdentificeerd worden. Personen die geen BSN hebben zijn dus uitgesloten van online EPD toegang.

1.17 In beginsel zijn alle sofinummers (uitgereikt aan alle geregistreerde personen bij de belastingdienst) in november 2007 omgezet in een BSN. Voorts krijgt iemand die zich voor het eerst bij een gemeente (GBA) inschrijft een BSN (bijvoorbeeld bij geboorteaangifte).

1.18 De volgende groepen personen hebben (initieel) niet de beschikking over een BSN:

- Personen die niet staan ingeschreven bij een Nederlandse gemeente omdat ze niet in Nederland wonen, maar die wel een relatie hebben met de Nederlandse overheid. Bijvoorbeeld: Duitse toerist met een huis in Zeeland, Poolse schilder die twee maanden in Nederland werkt, Nederlandse AOW-er die in Spanje woont (meer algemeen: personen die in het buitenland wonen en een Nederlandse uitkering ontvangen, bijvoorbeeld via de Sociale Verzekerings Bank), grensarbeiders en buitenlandse studenten. Deze personen worden in de toekomst ingeschreven in de Registratie Niet Ingezetenen (RNI) en krijgen mits zij goed identificeerbaar zijn ook een BSN. Dit RNI (waarvoor momenteel wetgeving in voorbereiding is) zal samen met de GBA (de wel ingezetenen dus) de "Basisregistratie Personen" vormen.

[5] of equivalent, voor Nederlanders in het buitenland

- Personen die niet zijn ingeschreven bij een Nederlandse gemeente, niet de beschikking over een BSN hebben, maar wel belasting moeten betalen in Nederland. Deze personen blijven het sofinummer gebruiken en krijgen geen BSN.
- Kinderen van illegaal in Nederland verblijvende personen (die bijvoorbeeld wel naar school gaan) krijgen geen BSN.
- Vreemdelingen (niet-Nederlanders) krijgen een "vreemdelingennummer" of "V-nummer" zodra de toelatingsprocedure start. Daarmee is de vreemdeling bij de Immigratie en Neutralisatie Dienst (IND) en de ketenpartners (bijvoorbeeld de vreemdelingenpolitie) te identificeren.

1.19 Samenvattend beschikken dus alle personen die zijn geregistreerd in de huidige GBA (en in de toekomstige RNI) over een BSN en kunnen daarmee toegang verkrijgen tot het EPD. Echter, zoals uit de bovenstaande beschrijving blijkt zal er altijd een groep mensen zijn die geen beschikking heeft over een BSN en dus geen toegang zal hebben tot het EPD.

1.20 Het advies voor het authenticatiemiddel en uitgifteproces gaat uit van toegang door zorgconsumenten die zijn geregistreerd in de GBA en beschikken over een BSN. In het advies is geen rekening gehouden met de hiervoor (in alinea 1.18) gespecificeerde mogelijke doelgroepen die nu geen beschikking hebben over een BSN of niet zijn geregistreerd in het GBA.

1.4 Aanpak

1.21 Deze opdracht is uitgevoerd door een tijdelijk samenwerkingsverband voor deze opdracht dat bestaat uit het Tilburg Institute for Law, Technology and Society (TILT), van de Universiteit van Tilburg, het Institute for Computing and Information Sciences (ICIS) van de Radboud Universiteit Nijmegen en PricewaterhouseCoopers Advisory NV (PwC).

1.22 Voor het opstellen van dit rapport zijn de volgende fasen doorlopen:

1. Het opstellen van minimale (beveiligings)eisen aan identificatie- en authenticatiemiddelen.
2. Het inventariseren en beoordelen van identificatie- en authenticatiemiddelen.
3. Het beschrijven van minimale eisen aan de inrichting van het verificatie- en uitgifteproces.

1.23 De taakverdeling van de hierboven beschreven stappen was als volgt:

- De heer dr. mr. Sjaak Nouwt van TILT heeft de minimale (beveiligings)eisen ten aanzien van identificatie- en authenticatiemiddelen beschreven aan de hand van de relevante wetgeving en standaarden (zoals NEN7512).
- De heer prof. dr. Bart Jacobs van ICIS heeft aan de hand van het door de heer Nouwt opgestelde juridische kader de verschillende alternatieve

authenticatiemiddelen beschreven en beoordeeld.

- De heren drs. Roland van der Knaap RE en Cas de Bie MSc. hebben de minimale eisen en inrichtingsaspecten voor het verificatie- en uitgifteproces geïnventariseerd en deze vervolgens beschreven voor de in hoofdstuk 4 aanbevolen authenticatiemiddelen. De overall coördinatie lag bij Adri de Bruijn RE RA (kwaliteitsbewaking), ir. Otto Vermeulen RE CISSP (coördinerend projectleider).
- Dit rapport is vervolgens door alle betrokken uitvoerende partijen gezamenlijk opgesteld.

1.5 Leeswijzer

1.24 Dit rapport bestaat naast de managementsamenvatting en dit inleidende hoofdstuk 1 uit vier hoofdstukken en drie bijlagen.

1.25 In hoofdstuk 2 is een samenvatting opgenomen van het onderzoek, gerangschikt naar fase.

1.26 In hoofdstuk 3 zijn de juridische en technische eisen ten aanzien van de voorhanden identificatie- en authenticatiemiddelen uiteengezet.

1.27 In hoofdstuk 4 zijn de verschillende alternatieve authenticatiemiddelen beschreven waarbij gelet is op de eisen die binnen hoofdstuk 3 beschreven zijn. Het resultaat van hoofdstuk 4 is een advies ten aanzien van de voor het ministerie van VWS meest voor de hand liggende authenticatiemiddelen op basis van de in hoofdstuk 3 beschreven eisen.

1.28 In hoofdstuk 5 worden de eisen en inrichtingsaspecten beschreven voor het verificatie- en uitgifteproces. Vervolgens worden deze eisen en inrichtingsaspecten voor de in hoofdstuk 4 geadviseerde authenticatiemiddelen ingevuld en met elkaar vergeleken. Tenslotte bevat dit hoofdstuk een voorbeeldbeschrijving van de wijze waarop het verificatie- en uitgifteproces voor de geadviseerde authenticatiemiddelen ingericht zou kunnen worden.

1.29 In de bijlagen treft u naast overzichten van geraadpleegde documentatie en geïnterviewde personen een uitgebreide uiteenzetting van toepasselijke wet- en regelgeving aangaande de toegang tot het EPD voor zorgconsumenten.

1.30 Zoveel mogelijk is gebruik gemaakt van de term zorgconsument in plaats van patiënt. In juridische teksten is veelal de term cliënt aangehouden. Het woord patiënt wordt uitsluitend gebruikt indien dat onvermijdbaar is.

2 Samenvatting onderzoek

2.01 In het navolgende worden per onderscheiden fase kort de resultaten van het uitgevoerde onderzoek beschreven. Een nadere uiteenzetting kan worden gevonden in de hoofdstukken 3 tot en met 5 van het voorliggende rapport.

2.1 Fase 1: Het opstellen van minimale (beveiligings)eisen aan identificatie- en authenticatiemiddelen

2.02 In de eerste fase van het onderzoek is een inventarisatie uitgevoerd van de toepasselijke wetgeving en technische kaders voor identificatie- en authenticatiemiddelen.

2.03 De bovengenoemde inventarisatie leidt tot de volgende eisen[6] waaraan identificatie en authenticatie middelen dienen te voldoen:

- De identificatie van zorgconsumenten vindt plaats door middel van het **BSN**.
- Het authenticatieniveau moet **Sterk** zijn.
- Identificatoren[7] met **Registratieniveau 3** moeten worden toegepast.
- Raadpleging van dossiers door cliënten moet voldoen aan **Versleutelingsniveau 2**.

2.04 In hoofdstuk 3 worden de juridische en technische eisen nader toegelicht.

2.2 Fase 2: Het inventariseren en beoordelen van identificatie- en authenticatiemiddelen

2.05 In de tweede fase van het onderzoek zijn de mogelijke identificatie- en authenticatiemiddelen onderzocht.

DigiD als mogelijk identificatie- en authenticatiemiddel

2.06 DigiD is de nationale authenticatie serviceprovider die in het leven is geroepen om burgers online authenticatiemogelijkheden te geven voor contact met overheden. Het ligt voor de hand ook voor EPD-authenticatie aan te sluiten bij DigiD. In het uitgevoerde onderzoek is bekeken of DigiD geschikt is voor EPD-authenticatie. Uit het onderzoek blijkt dat met name de beperkte controle van de identiteit bij aanvraag van een DigiD, in combinatie met een zekere mate van achteloosheid waarmee DigiD door burgers behandeld wordt, DigiD met zekerheidsniveau 1 of 2 ongeschikt maken voor EPD-authenticatie. Het gaat bij het EPD

[6] Terminologie ontleend aan NEN 7512. Voor een nadere toelichting op de betekenis van bovenstaande eisen en begrippen, zie paragraaf 2.2.
[7] Paragraaf 7.1.1 (NEN 7512) stelt daarin dat “identificatoren voor personen kunnen worden gebaseerd op een bestaande registratie van die personen binnen het desbetreffende domein, zoals (…) of patiëntnummer”. Volgens dezelfde norm worden bij elektronische interactie entiteiten (personen, organisaties en informatiesystemen) weergegeven door identificatoren. (NEN 7512, p. 10). De norm vervolgt: “Binnen domeinen waarin het gebruik van de bevolkingsadministratie is toegestaan is het aan te bevelen de identificatoren voor personen daaraan te relateren.”

immers om gegevens waarvan de vertrouwelijkheid, integriteit en beschikbaarheid belangrijker zijn dan bij belastingaangifte of aanvraag van een kapvergunning.

2.07 Gelet op de juridische en technische beveiligingseisen rondom het EPD is – uitgedrukt in DigiD-niveaus - een zekerheidsniveau van meer dan 2 noodzakelijk.

Acht alternatieven

2.08 Uitgaande van een zekerheidsniveau van meer dan 2, lijkt op de langere termijn eNIK (of een vergelijkbaar elektronisch rijbewijs), gemeten naar de huidige kennis en inzichten rondom eNIK, in eerste instantie het meest geschikte authenticatiemiddel om DigiD zekerheidsniveau 3 te bereiken. Omdat eNIK danwel het elektronisch rijbewijs hoogstwaarschijnlijk de komende jaren niet beschikbaar zullen zijn, zijn naast eNIK ook alternatieve opties met een zekerheidsniveau lager dan 3 en hoger dan 2 in kaart gebracht.

2.09 Vanuit dit perspectief zijn acht alternatieve authenticatiemiddelen (c.q. varianten daarbinnen) geëvalueerd op de technische geschiktheid voor het gebruik in de EPD-authenticatie. Navolgende middelen zijn bekeken in DigiD context, als mogelijke (alternatieve) realisatie van een hoger zekerheidsniveau dan het huidige maximum:

- Authenticatie door middel van extra code/wachtwoord, aangetekend verstuurd.
- Face-to-face authenticatie van mobiel nummer, in 2 varianten hierna te noemen SMS+ (variant 1) en SMS+ (variant 2).
- Authenticatiemiddelen van internetbankieren.
- Authenticatie door middel van eNIK.
- Authenticatie door middel van een elektronisch rijbewijs.
- Authenticatie door middel van UZI pas.
- Authenticatie door middel van een reisdocument (RTDA).

2.10 Specifiek ten aanzien van SMS+ zijn twee varianten onderzocht: variant 1 (verificatie van het mobiele telefoonnummer door de controle-instantie aan de hand van een verificatieapplicatie) en variant 2 (verificatie van het mobiele telefoonnummer door middel van een verklaring door de zorgconsument en registratie van deze verklaring door DigiD). Voor wat betreft informatiebeveiliging gaat de voorkeur uit naar variant 1. Bij variant 2 kunnen zich immers problemen ten aanzien van schrijf- en kopieerfouten (bij het inscannen van de verklaringen door DigiD) voordoen. Daarnaast lijkt een dergelijke verklaring meer fraudegevoelig omdat het uitgevoerde verificatieproces niet wordt geregistreerd door een geauthenticeerde baliemedewerker en controles ten aanzien van het op de verklaring aangegeven mobiele telefoonnummer pas worden uitgevoerd nadat de DigiD-organisatie deze verklaring ontvangt en verwerkt. Zie paragraaf 4.2.2 voor een nadere toelichting over de fraudemogelijkheden voor SMS+ variant 2.

2.11 Op grond van de evaluatie komen aldus de volgende twee opties in aanmerking voor EPD-authenticatie, te weten:

- Face-to-face authenticatie (volgens variant 1) van het binnen het huidige DigiD niveau 2 gebruikte mobiele telefoonnummer, hierna te noemen SMS+ (variant 1).
- Authenticatie door middel van een reisdocument, hierna te noemen RTDA (Remote Travel Document Authentication).

Zie paragraaf 4.2 van dit rapport voor nadere toelichting op deze opties.

2.12 SMS+ (variant 1) is van deze twee opties het minst ingrijpend en het minst omslachtig voor de gebruikers. Daar staat tegenover dat er wel extra werk gestoken zal moeten worden in de authenticatie van het mobiele telefoonnummer bij een controle-instantie. In de huidige DigiD context zou men bij SMS+ (variant 1) kunnen spreken van authenticatie op zekerheidsniveau 2+. RTDA is ingrijpender omdat zorgconsumenten (thuis) een kaartlezer nodig zullen hebben (met bijbehorende distributie en installatieproblemen). Deze optie is echter meer in lijn met geplande ontwikkelingen rond eNIK en rijbewijs: er kan betoogd worden dat een dergelijke infrastructuur op termijn nodig is. Bij RTDA zou men kunnen spreken van zekerheidsniveau 2½, omdat het reisdocument een zorgvuldig proces kent bij uitgifte en verlies en omdat het reisdocument een goed beveiligde chip bevat.

2.13 Beide oplossingen zijn niet direct te realiseren omdat ze bouw van programmatuur, inrichting van procedures, controle-instanties et cetera vereisen. Bij de keuze tussen deze twee alternatieven speelt op de achtergrond ook ander overheidsbeleid betreffende authenticatie een rol (de invoering van eNIK, elektronisch rijbewijs, en de eventuele inpassing hiervan binnen DigiD) dat de context van dit rapport overstijgt.

2.14 Bij eerste beschouwing lijkt SMS+ (variant 1) een bredere verspreiding te hebben dan de reisdocumenten voorzien van RTDA en daarmee op dit moment breder implementeerbaar. Bij SMS+ (variant 1) is een controle-instantie noodzakelijk, waarbij als mogelijke opties zijn uitgewerkt het gemeentehuis en de apotheek. Het gemeentehuis lijkt meer ervaring te hebben met identiteitscontrole maar dit is niet doorslaggevend.

2.15 De uiteindelijke keuze voor hetzij SMS+ (variant 1) hetzij RTDA, danwel de controle-instantie, is een veelzijdig vraagstuk waarbij naast het uitgifteproces ook kosten, gebruikersvriendelijkheid, snelle beschikbaarheid, externe afhankelijkheden en technische aspecten meespelen. Een verantwoorde keuze tussen de opties vergt daarom de afweging van middelen en van bijbehorende processen. Een dergelijke afweging valt gezien het doel van het onderzoek (een onafhankelijk advies inzake de minimale beveiligingseisen voor de identificatie en authenticatie van de zorgconsument in het kader van Toegang patiënt tot het EPD) buiten de reikwijdte van dit onderzoek (gericht op de juridische en technische eisen).

2.16 In dit rapport is nadrukkelijk het advies opgenomen om voor de te kiezen optie een praktijkproef te organiseren, voorafgaande aan een grootschalige invoering. Mogelijk kan zelfs overwogen worden voor beide opties een praktijkproef te houden, en mede op basis van de uitkomsten daarvan een besluit te nemen.

2.17 Het advies gaat uit van toegang door zorgconsumenten die zijn geregistreerd in de GBA of beschikken over een BSN. In het advies is geen rekening gehouden met doelgroepen die nu geen beschikking hebben over een BSN.

2.18 Wanneer SMS+ (variant 1) of RTDA ingevoerd wordt en te zijner tijd ook eNIK beschikbaar is, kan op dat moment het beste bepaald worden of SMS+ (variant 1) of RTDA nog verder ondersteund wordt. Ook kan dan gekeken worden in hoeverre de verschillende alternatieven in de op dat moment actuele Europese context inpasbaar zijn.

2.19 In hoofdstuk 4 wordt bovenstaand advies verder onderbouwd en toegelicht.

2.3 Fase 3: Verificatie- en uitgifteproces

2.20 Een technische oplossing voor authenticatie is alleen betrouwbaar wanneer voldoende zekerheid bestaat dat alleen diegene voor wie het middel bedoeld is in staat is om het te gebruiken. Om deze zekerheid te verkrijgen dient ook procesmatig aan nader te benoemen eisen worden voldaan. Voor de inrichting van het verificatie- en uitgifteproces is in dit rapport daarom een referentiekader opgesteld met daarin eisen en wensen. Deze eisen en wensen zijn gebaseerd op best practices, brondocumentatie (zie bijlage A) en de eisen uit het offerteverzoek van VWS. Dit referentiekader is vervolgens ingevuld voor SMS+ (variant 1) en voor RTDA, om zo de consequenties zichtbaar te maken voor het verificatie- en uitgifteproces van een keuze voor hetzij SMS+ (variant 1) hetzij RTDA. Daarnaast zijn de kostenaspecten voor de verschillende alternatieven voor de invulling van het verificatie- en uitgifteproces kwalitatief beschreven.

2.21 Voor SMS+ zijn hierbij enerzijds de twee uitvoeringsvarianten voor SMS+ beschreven en is anderzijds rekening gehouden met een mogelijke uitvoering van beide scenario's door een gemeentehuis of een apotheek.

2.22 Bij de invulling van dit referentiekader is per eis/wens onderscheid gemaakt naar vier inspanningsniveaus:

1. Geen extra inspanning (G).
2. Lage benodigde inspanning (L).
3. Hoge benodigde inspanning (H).
4. Niet mogelijk (N).

2.23 Aan de hand van bovengenoemd referentiekader zijn de voor SMS+ (variant 1) en voor RTDA geschatte inspanningsniveaus voor het verificatie- en uitgifteproces met elkaar vergeleken. Uit analyse van het aldus ingevulde referentiekader komen de volgende aandachtspunten naar voren voor de inrichting van het verificatie- en uitgifteproces voor respectievelijk SMS+ (variant 1) en RTDA:

- Voor het gebruik van RTDA als authenticatiemiddel is een reisdocument noodzakelijk dat na 26 augustus 2006 is uitgegeven en een chip bevat. Het zal daarom nog tot 2011 duren (vanwege een geldigheidsduur van 5 jaar) voordat alle huidige reisdocumenten zijn vervangen door nieuwe reisdocumenten met een chip. (Indien wordt geopteerd voor een combinatie van RTDA met snelle beschikbaarheid voor alle burgers, dan zou in overleg met BZK moeten worden nagegaan of een versnelde uitgifte van nieuwe reisdocumenten mogelijk is.)
- Wanneer gekozen wordt voor SMS+ (variant 1) dient VWS in samenspraak met het ministerie van Binnenlandse Zaken (BZK) te waarborgen dat het mobiele telefoonnummer 1-op-1 gekoppeld is met een DigiD account. Hierdoor is het meervoudig gebruik van hetzelfde mobiele telefoonnummer voor verschillende DigiD accounts niet meer mogelijk, waardoor de vertrouwelijkheid van SMS+ (variant 1) als authenticatiemiddel initieel vergroot wordt.
- Ten aanzien van de inrichting van het verificatie- en uitgifteproces voor RTDA geldt dat dit hetzelfde is als het al bestaande verificatie- en uitgifteproces voor de uitgifte van reisdocumenten door gemeenten.
- Voor SMS+ (variant 1) geldt dat het verificatie- en uitgifteproces (voor zowel scenario 1 als 2) speciaal voor het gebruik van DigiD niveau 2 voor het EPD vormgegeven moet worden. Dit vergt vanzelfsprekend additionele inspanningen en middelen ten opzichte van het gebruik van RTDA.
- Voor zowel scenario 1 en 2 voor SMS+ (variant 1) als RTDA dient nieuwe functionaliteit te worden ontwikkeld. Voor SMS+ (variant 1) dient een verificatieapplicatie voor de controle-instantie te worden ontwikkeld. Voor SMS+ (variant 2) dient een scanapplicatie te worden ontwikkeld voor het verwerken van de verklaringen van zorgconsumenten. Tenslotte dient voor RTDA functionaliteit ontwikkeld te worden voor de communicatie tussen de chip op het reisdocument en de wireless cardreader ten behoeve van de authenticatie van de zorgconsument. Deze functionaliteit kan wellicht worden toegevoegd aan de reeds bestaande webservices binnen de DigiD-omgeving.

2.24 Aan de hand van een kwalitatieve beschrijving van een zestal kostenaspecten is gebleken dat geen van de onderscheiden alternatieven kan worden ingevoerd zonder additionele kosten. Een nadere analyse van deze kostenaspecten, bijvoorbeeld in de vorm van een door het ministerie van VWS op te stellen business case én een eventueel uit te voeren praktijkproef, zal uitsluitsel moeten geven over de vraag of de kosten voor een nieuw in te

richten verificatie- en uitgifteproces opwegen tegen de kosten voor het vroegtijdig breed beschikbaar maken van RTDA als authenticatiemiddel.

2.25 In hoofdstuk 5 wordt het voorgaande nader toegelicht. Tevens zijn in dit hoofdstuk 5 high-level procesbeschrijvingen opgenomen voor het verificatie- en uitgifteproces voor zowel SMS+ (variant 1) als RTDA.

3 Fase 1: Minimale (beveiligings)eisen identificatie- en authenticatiemiddelen

3.01 In dit hoofdstuk zijn de eisen beschreven waaraan authenticatiemiddelen voor toegang tot het EPD voor zorgconsumenten moeten voldoen. Deze eisen zijn gebaseerd op de bestaande wet- en regelgeving. Hierbij wordt onderscheid gemaakt tussen de juridische en technisch/organisatorische eisen die in de twee navolgende paragrafen zijn beschreven. Vervolgens wordt een samenvattend totaalpakket van eisen beschreven.

3.1 Juridische eisen

3.02 Op grond van art. 13a, tweede lid van het wetsvoorstel tot "Wijziging van de Wet gebruik burgerservicenummer in de zorg in verband met de elektronische informatie-uitwisseling in de zorg"[8] (hierna te noemen: Wet EPD) kan bij Algemene Maatregel van Bestuur (AMvB) worden bepaald dat het Landelijk Schakel Punt (LSP) voorzieningen moet aanbieden waarmee een zorgconsument zelf:

a. Zijn elektronisch patiëntendossier elektronisch kan opvragen en raadplegen.
b. De hem betreffende centrale gebruiksregistratie kan opvragen en raadplegen.
c. Zijn indexgegevens volledig kan afschermen voor het opvragen en raadplegen door een zorgaanbieder of een categorie van zorgaanbieders.

3.03 In art. 13e Wet EPD zijn rechten voor de cliënt geformuleerd ten opzichte van het LSP. Los van het feit of elektronische toegang mogelijk is, heeft de cliënt het recht de beheerder van het LSP inzage te vragen in de indexgegevens en in de centrale gebruiksregistratie met betrekking tot die cliënt. Het vijfde lid van dit artikel bepaalt dat, indien de voorzieningen als bedoeld in art. 13a, tweede lid, zijn gerealiseerd, de cliënt ook het recht heeft daarvan gebruik te maken om:

a. Zijn elektronisch patiëntendossier en de hem betreffende centrale gebruiksregistratie op te vragen en te raadplegen.
b. Zijn indexgegevens volledig af te schermen voor het opvragen en raadplegen door een zorgaanbieder of een categorie van zorgaanbieders.

3.04 Het derde lid van art. 13a Wet EPD bepaalt vervolgens dat eveneens bij AMvB nadere regels zullen worden gesteld met betrekking tot de inrichting en het beheer van het landelijk schakelpunt. Deze regels zullen in ieder geval betrekking hebben op de beveiliging. Zorgaanbieders zullen moeten voldoen aan de eisen die vallen onder het Goed Beheerd Zorgsysteem (GBZ). Aan de beheerder van het LSP worden soortgelijke eisen opgelegd[9].

3.05 Zoals ook wordt gesteld in de memorie van toelichting bij de Wet EPD, vloeien deze

[8] *Kamerstukken II*, 2007/08, 31 466, nr. 2 (voorstel van wet).
[9] *Kamerstukken II*, 2007/08, 31 466, nr. 3 (memorie van toelichting), p. 12.

eisen voort uit de algemene norm die geldt voor de beveiliging van persoonsgegevens (art. 13 Wbp).

3.06 De algemene beveiligingsplicht van artikel 13 Wbp luidt als volgt:
"De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen."

3.2 Technische eisen

3.07 Minister Hoogervorst heeft in 2004 aangegeven dat door de naleving van NEN 7510 tegelijkertijd invulling wordt gegeven aan het vereiste van 'passende technische en organisatorische beveiligingsmaatregelen', zoals bedoeld in art. 13 Wbp:
"Een passend beveiligingsniveau is een vereiste om gegevens uit te wisselen. Als uitgangspunt daarvoor zal de recent vastgestelde norm voor informatiebeveiliging in de zorg gaan gelden, de NEN 7510."[10]

3.08 De norm NEN 7510 is aangevuld met de NEN 7511 (1 t/m 3) en NEN 7512. De norm NEN 7512 bevat een aanvulling voor een vertrouwensbasis voor gegevensuitwisseling in de zorg. In NEN 7512 wordt de voor de gegevensuitwisseling vereiste zekerheid gekoppeld aan de risicoklasse. In Bijlage A van NEN 7512 worden enkele communicatiescenario's uiteengezet ter voorbeeld van toepassing van de norm. Een voorbeeld van een communicatiescenario is "*Scenario 4: Cliënt raadpleegt eigen dossier*". Volgens NEN 7512 moet de norm in een dergelijk geval als volgt worden toegepast:

Vertrouwende partij:	Dossierbeheerder (=Nictiz/beheerder van het Informatiepunt BSN in de zorg en landelijk EPD)
Te vertrouwen partij:	Cliënt
Bedreiging:	Inzage/misbruik door derden
Impact:	Zeer ernstig
Kans:	Middelmatig, maar Groot bijvoorbeeld in geval van Bekende Nederlanders Groot[11]
Risico:	Hoog
Registratieniveau:	3
Authenticatieniveau:	Sterk
Versleuteling:	2

[10] *Kamerstukken II* 2004/05, 29 800 hoofdstuk XVI, nr. 2, p. 135, Vaststelling van de begrotingsstaten van het Ministerie van Volksgezondheid, Welzijn en Sport (XVI) voor het jaar 2005; Memorie van Toelichting.
[11] NEN 7512 noemt de kans in dit scenario "Middelmatig?" (inclusief vraagteken). Wij voegen daaraan toe dat die kans "Groot" is als het bijvoorbeeld gaat om Bekende Nederlanders, inclusief leden van het Koninklijk Huis, ministers, e.d.

Toelichting:

3.09 Voor de impact (de mogelijke gevolgen van een incident voor het beoogde doel) hanteert NEN 7512 de volgende klassenindeling waarbij het boven beschreven scenario de waarde “zeer ernstig” krijgt:

hinderlijk (eenvoudig herstelbaar)	ernstig (moeilijk herstelbaar)	**zeer ernstig (niet herstelbaar)**	fataal (voor een patiënt)	catastrofaal (fataal voor meer patiënten)

3.10 De kans op een incident wordt in NEN 7512 als volgt ingedeeld waarbij het hierboven beschreven scenario de waarde “middelmatig” krijgt:

zeer klein (verwaarloosbare mogelijkheid van optreden)	klein (zou kunnen optreden, maar zal in vrijwel alle gevallen niet optreden)	**middelmatig (mogelijk; optreden niet onwaarschijnlijk)**	groot (zeer goed mogelijk; zal in een groot deel van de gevallen optreden)	zeer groot (zal zeker of vrijwel zeker optreden)

3.11 De risico’s worden in NEN 7512 onderscheiden in de volgende categorieën waarbij het hierboven beschreven scenario de waarde “hoog risico” krijgt:

laag risico	matig risico	**hoog risico (bijvoorbeeld: zeer ernstige impact + middelmatige kans)**	zeer hoog risico

3.12 Registratieniveau 3 wil zeggen dat een **identificator**[12] met **registratieniveau 3** moet worden toegepast. Volgens NEN 7512 vereist dat directe controle (“face-to-face”) aan de hand van een document volgens artikel 3 van de Wet Identificatie bij Dienstverlening (WID) [13]. De uitgevende instantie **moet** vóór het toekennen van een identificator voor het desbetreffende domein de identiteit van de aanvrager vaststellen op basis van (indirecte) fysieke verschijning[14] en controle aan de hand van een document als bedoeld in artikel 3 van de WID. Eventuele kwalificaties **moeten** daarbij aan de hand van een voor het domein erkend register worden gecontroleerd. Deze eis lijkt te zijn geschreven voor de toekenning van een identificator aan een zorgverlener ten behoeve van de toegang tot patiëntgegevens. In het onderhavige geval gaat

[12] NEN 7512 gebruikt de term “identificator” voor de “unieke representatie van een entiteit in een bepaald domein”.
[13] In art. 3 WID wordt verwezen naar de documenten waarmee in bij de wet aangewezen gevallen de identiteit van personen kan worden vastgesteld: een geldig reisdocument, identiteitsdocumenten voor vreemdelingen, diplomatiek of dienstpaspoort, geldig rijbewijs en door de minister aangewezen documenten (art. 1 Wet op de identificatieplicht).
[14] Het gaat hier om de koppeling van een identificator aan een fysieke identiteit. Bij indirecte fysieke verschijning kan men denken aan een situatie waarin een cliënt op een eerder moment fysiek is verschenen, zoals een bank de identiteit van een nieuwe cliënt alleen de eerste keer vaststelt en daarna niet meer, of aan een situatie waarin mag worden vertrouwd op de controle door een andere instantie.

het echter om het toekennen van een identificator aan de cliënt. Hierbij wordt wel de aanname gedaan dat het BSN correct wordt toegewezen door de “Beheervoorziening BSN” en dat de controle plaatsvindt (of heeft plaatsgevonden) door de Sectorale Berichten Voorziening in de Zorg (SBV-Z).

3.13 Authenticatieniveaus worden in NEN 7512 onderverdeeld in Zwak, Matig en **Sterk**. Voorbeelden van sterke authenticatieniveaus zijn:

- Het gebruik van biometrie in combinatie met een ander authenticatiemiddel. De huidige stand der techniek is echter zodanig dat deze combinatie in de thuissituatie van een zorgconsument niet realistisch is.
- Een fysiek authenticatiemiddel (bijvoorbeeld “tokens” die telkens een eenmalig wachtwoord genereren, bankpassen, SIM-kaarten in een mobiele telefoon en dragers van een digitaal certificaat). Bij toepassing van een fysiek authenticatiemiddel wordt de sterkte bepaald door het geheel van de processen waarin het wordt gebruikt. Alleen wanneer het authenticatiemiddel wordt gebruikt in combinatie met een wachtwoord of een PIN-code en ook bij het initialiseren van het authenticatiemiddel en de uitreiking aan de houder wordt gewaarborgd dat het eenduidig aan de houder wordt gebonden. kan men spreken van een **Sterk** authenticatieniveau. Is aan deze voorwaarden niet voldaan, dan is het authenticatieniveau hooguit **Matig**.

3.14 De NEN norm 7512 onderscheidt 3 versleutelingsniveaus: 0 = geen versleuteling, 1 = versleutelde verbinding en 2 = versleuteld bericht.

3.15 Volgens het communicatiescenario beschreven in bijlage A van de NEN7512 norm moet bij de raadpleging van dossiers door cliënten worden voldaan aan **versleutelingsniveau 2**. Door de versleuteling van een bericht wordt het volledige kanaal tussen zender en ontvanger afgedekt. De verzender gebruikt een publieke sleutel van de geadresseerde om het bericht te versleutelen. De geadresseerde maakt het leesbaar met de bijbehorende privé-sleutel.

3.16 Voor het vertrouwd uitwisselen van de encryptiesleutel kan gebruik worden gemaakt van een Public Key-certificaat. In overeenstemming met NPR-ISO/TS 17090 **moet** daartoe voor elke identificator een derde Public Key-certificaat worden uitgegeven. De voorwaarden voor uitgifte kunnen gelijk zijn aan die voor de uitgifte van de andere twee certificaten. Van de bijbehorende privé-sleutel **moet** in dit geval echter, anders dan bij authenticatie en elektronische handtekening, een kopie beschikbaar blijven om in bijzondere gevallen ontsleuteling mogelijk te maken. Hierbij dient opgemerkt te worden dat bij de huidige inrichting van DigiD slechts aan één kant (de aanbieder = DigiD-server) gebruik gemaakt wordt van één certificaat. Het betreft hier PKIoverheid SSL-certificaten, die zijn uitgegeven onder het stamcertificaat van de Staat der Nederlanden.

3.17 Tot slot wordt benadrukt dat de beveiliging van de toegang voor cliënten tot hun elektronische patiëntendossiers niet alleen betrekking heeft op de authenticatie van de zorgconsument. Informatiebeveiliging dient te allen tijde te worden beschouwd als een continu managementproces waarbij risico's worden geïnventariseerd, beleid en plannen worden opgesteld, maatregelen worden geïmplementeerd en de effectiviteit van de genomen maatregelen wordt geëvalueerd waar vanaf het proces weer opnieuw begint.

3.18 Volgens de Normcommissie die NEN 7510 c.s. heeft opgesteld moet informatiebeveiliging worden gezien als een samenhangend stelsel van maatregelen die nodig zijn om verstoringen in de zorgvuldige en doelmatige informatievoorziening te voorkomen en eventuele schade die onverhoopt uit dergelijke verstoringen voortvloeien te beperken. Dit proces van informatiebeveiliging is er op gericht de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens te waarborgen. De zekerheidsbegrippen die daarbij vervolgens een rol spelen zijn: onweerlegbaarheid (waarborgen dat vastleggen van gegevens of verzenden van een bericht niet kan worden ontkend), verantwoordelijkheid (waarborgen dat steeds vaststaat wie welke verantwoordelijkheid draagt voor gegevens), authenticiteit (waarborgen dat gegevens, informatiediensten, organisaties en gebruikers de juiste identiteit hebben) en betrouwbaarheid (waarborgen van overige kwaliteitseisen aan de informatie, de bron ervan, de berichtenroute en verwerkingen).

3.19 Evenals NEN 7510, volgt uit het de publicatie Achtergrondstudies & Verkenningen 23 betreft de Beveiliging van persoonsgegevens (Registratiekamer, 2001) en uit het Raamwerk Privacy Audit dat de beveiliging van persoonsgegevens de volgende onderdelen omvat:

1. Vaststellen van beveiligingsbeleid, beveiligingsplan en implementatie van het stelsel van maatregelen en procedures.
2. Administratieve organisatie (beschrijving) van de beveiliging.
3. Bevorderen van beveiligingsbewustzijn.
4. Eisen stellen bij werving en selectie van personeel.
5. Juiste inrichting van de werkplek.
6. Beheer en classificatie van de ICT infrastructuur.
7. Toegangsbeheer en –controle.
8. Beveiliging van netwerken en externe verbindingen.
9. Voorwaarden aan het gebruik van software van derden.
10. Beveiliging bij bulkverwerking van persoonsgegevens.
11. Eisen aan het bewaren van persoonsgegevens.
12. Eisen aan de vernietiging van persoonsgegevens.
13. Opstellen van een calamiteitenplan.
14. Aandacht voor beveiliging bij uitbesteden van en overeenkomsten voor de verwerking van persoonsgegevens.

3.20 Het antwoord op de vraag welke maatregelen genomen moeten worden hangt af van een aantal factoren, zoals de afweging van de risico's, de kosten en praktische mogelijkheden zoals de stand van de techniek. Zoals de Normcommissie in NEN 7510 ook opmerkt: "Informatiebeveiliging verlangt een besturingsproces."[15]

3.3 Eisenpakket

3.21 In dit rapport wordt de aanname gehanteerd dat het BSN op een juiste en betrouwbare wijze wordt toegekend.

3.22 De NEN7512 eisen aan de identificatie en authenticatie van een zorgconsument voor het verlenen van toegang tot het EPD zijn:

- Identificatie van cliënten vindt plaats door middel van het **BSN**.
- Het authenticatieniveau moet **Sterk** zijn.
- Identificatoren met **registratieniveau 3** moeten worden toegepast.
- Raadpleging van dossiers door cliënten moet voldoen aan **Versleutelingsniveau 2**.

Hierbij zijn alleen de eerste drie eisen van toepassing voor het authenticatiemiddel.

[15] NEN - Nederlands Normalisatie-Instituut, *Nederlandse norm NEN 7510 (nl). Medische Informatica – Informatiebeveiliging in de zorg – Algemeen*. Delft: Nederlands Normalisatie-Instituut, april 2004, p. 6.

4 Fase 2: Inventarisatie en beoordeling van identificatie- en authenticatiemiddelen

4.1 Geschiktheid van DigiD voor identificatie

4.01 DigiD is de nationale authenticatie serviceprovider die in het leven is geroepen om burgers online authenticatiemogelijkheden te geven voor contact met overheden. DigiD is bijvoorbeeld verplicht bij elektronische belastingaangifte en nodig voor het inloggen op de persoonlijke website voor overheidszaken www.mijnoverheid.nl. Het ligt voor de hand om voor EPD-authenticatie aan te sluiten bij DigiD, zeker gezien het gebruik van het BSN als identiteit binnen DigiD. Daarom zal hier DigiD worden besproken en worden beoordeeld op de geschiktheid voor gebruik in EPD-authenticatie.

4.02 Vervolgens zal de technische geschiktheid van verschillende authenticatiemiddelen voor het gebruik voor de EPD-authenticatie worden geëvalueerd. Hieruit volgt een advies over welk authenticatiemiddel gebruikt kan worden voor EPD-authenticatie.

4.03 DigiD staat voor Digitale Identiteit wat de naam is van een nationale authenticatie serviceprovider via het internet. In principe dient een aanvrager van DigiD ingeschreven te staan in de GBA (Basisregistratie Personen) en te beschikken over een Burger Service Nummer (BSN).

4.04 DigiD werkt als een centrale authenticatiedienst via "tickets" (in grote lijnen zoals Kerberos[16]). Indien een gebruiker een overheidswebsite bezoekt die authenticatie vereist zal (de browser van) die gebruiker automatisch worden doorverwezen naar de DigiD website. Daar vindt authenticatie plaats, over een met SSL beveiligde verbinding. Vervolgens wordt de gebruiker met een "ticket" terugverwezen naar de oorspronkelijke overheidswebsite, waar het ticket gelezen wordt. Het ticket zegt in essentie: "met zekerheidsniveau N is vastgesteld dat deze gebruiker BSN X heeft".

4.05 Bij het ontwerp van DigiD is uitgegaan van drie zekerheidsniveaus voor authenticatie, namelijk "basis" (ook wel: "niveau 1"), "midden" ("niveau 2"), en "hoog" ("niveau 3"). Het eerste niveau vereist simpelweg het inloggen door de gebruiker door middel van een gebruikersnaam en een wachtwoord. Het tweede niveau vereist authenticatie via een one-time-password (OTP), dat bij DigiD verstuurd wordt via SMS. Het derde niveau is op dit moment niet beschikbaar, maar vereist een geavanceerde digitale handtekening. De elektronische Nederlandse identiteitskaart (eNIK) was voorzien voor dit hoogste niveau. De invoering hiervan heeft echter vertraging opgelopen.

[16] http://en.wikipedia.org/wiki/Kerberos_(protocol)

4.06 Het is aan de applicatie (op de overheidswebsite waar een gebruiker in wil loggen) om te bepalen welk zekerheidsniveau vereist is voor toegang tot die applicatie. Ook worden alle gebruikgegevens aan de applicatiekant opgeslagen. Bij DigiD staan alleen die gegevens centraal die voor authenticatie vereist zijn.

4.07 Benadrukt wordt dat DigiD een serviceprovider is voor authenticatie, en niet voor autorisatie of onloochenbaarheid (non-repudiation). DigiD verschaft enkel een bepaalde mate van zekerheid over de identiteit van de gebruiker. Het bepaalt niet wat die gebruiker vervolgens mag doen. En het levert ook geen bewijs dat een gebruiker een bepaalde handeling verricht heeft (zoals een elektronische handtekening doet). Door het ontbreken van een gekwalificeerde handtekening en de huidige gecentraliseerde opzet van DigiD is het mogelijk dat een "insider" die controle heeft over de DigiD infrastructuur zich in principe als iedere gebruiker zou kunnen voordoen (door zelf het gewenste ticket te genereren). Bij het beoogde zekerheidsniveau “hoog” wordt een dergelijke “insider” aanval uitgesloten doordat een extra authenticatiestap vereist is met een middel (zoals de eNIK) waarmee alleen de gebruiker een handtekening kan zetten (na het invoeren van de eigen PIN).

4.08 De volgende punten van kritiek zijn in deze context relevant:

1. Aanvraag van DigiD niveau 1 verloopt in eerste instantie via het web, waarbij loginnaam en wachtwoord gekozen worden. Vervolgens wordt een geheime activeringscode gestuurd naar het huisadres (zoals geregistreerd in de GBA). Er bestaat daarbij geen zekerheid dat de codes (en daarmee de DigiD) bij de juiste persoon terechtkomen, zeker wanneer meerdere personen op eenzelfde adres wonen (bijvoorbeeld in studentenhuizen).
2. Verder is authenticatie met wachtwoorden over het algemeen zwak, bijvoorbeeld omdat:
   - Mensen vaak zwakke wachtwoorden kiezen, en die ook op andere locaties gebruiken.
   - Wachtwoorden afgekeken kunnen worden tijdens het intypen, of gelezen wanneer ze opgeschreven zijn.
   - Verloren of vergeten wachtwoorden leiden tot extra belasting van de helpdesk; mogelijke automatische re-authenticatiemechanismen, zoals controlevragen, zijn vaak zwak en makkelijk te misbruiken.
   - Wachtwoorden door kwaadaardige software (zoals keyloggers) systematisch gestolen kunnen worden.

   Voor niveau 2 dient een mobiel nummer opgegeven te worden bij DigiD, na authenticatie op niveau 1. De activeringscode wordt vervolgens naar het huisadres gestuurd. Dit biedt dus geen extra zekerheid. Wel worden via de one-time-passwords enkele van de bovengenoemde zwakheden van wachtwoorden verzacht. In ieder geval omvat aanvraag van niveaus 1 en 2 geen enkel face-to-

face contact met de gebruiker.

3. De overheid heeft bij de introductie van DigiD altijd het gemak ervan benadrukt. Het is de burger nooit lastig gemaakt om een DigiD te krijgen. Enerzijds is dat begrijpelijk. Anderzijds kan dan ook verwacht worden dat de burger met een zekere achteloosheid met DigiD omgaat. Daartegenover presenteert de overheid het reisdocument aan de burger als iets dat "goud" waard is, waarbij gemak voor de burger niet het hoogste doel is: het uitgifteproces is relatief omslachtig (persoonlijk aanvragen en ophalen), het reisdocument kost geld, en bij verlies moet aangifte gedaan worden. Mensen gaan in het algemeen dan ook zorgvuldig met hun reisdocument om.

4.09 De beperkte controle van de identiteit bij de aanvraag van een DigiD, in combinatie met de zekere mate van achteloosheid waarmee DigiD behandeld wordt, maken DigiD met zekerheidsniveau 1 of 2 ongeschikt voor EPD-authenticatie. Het gaat bij het EPD immers om gegevens waarvan de vertrouwelijkheid, integriteit en beschikbaarheid belangrijker zijn dan bij belastingaangifte of aanvraag van een kapvergunning.

4.10 Gelet op de juridische en technische beveiligingseisen rondom het EPD is – uitgedrukt in DigiD-niveaus - een zekerheidsniveau van meer dan 2 noodzakelijk.

4.2 Beschikbare authenticatiemiddelen

4.11 Hieronder zullen de belangrijkste authenticatiemiddelen besproken worden die in aanmerking zouden kunnen komen voor EPD-authenticatie.

4.12 Al deze middelen zullen bekeken worden in DigiD context, als mogelijke (alternatieve) realisatie van een hoger niveau dan het huidige maximum, namelijk 2. Informeel zou gesproken kunnen worden van DigiD zekerheidsniveau 2+, 2½ , of mogelijk niveau 3.

4.2.1 Authenticatie door middel van extra code/wachtwoord, aangetekend verstuurd.

4.13 Bij deze opzet wordt ten opzichte van DigiD niveau 2 een extra inlogcode (of wachtwoord) aangetekend verstuurd. De (juiste) ontvanger zal zich (face-to-face) moeten authenticeren tegenover de bezorger. Daarmee kan dus hogere zekerheid verkregen worden (dan bij niet-aangetekende bezorging van activeringscodes).

4.14 Er is echter een aantal problemen:

- De eerder genoemde zwakheden voor wachtwoorden gelden ook voor dit nieuwe wachtwoord.
- Dit extra wachtwoord zal naar verwachting "sterk"/"moeilijk" zijn omdat het bedoeld is voor hogere niveaus. De vraagt dient zich dan aan of de gebruiker het kan veranderen? Zo ja, dan zullen eisen gesteld moeten worden zodat opnieuw een

sterk wachtwoord gekozen wordt. Zulke sterke wachtwoorden zijn lastig om te onthouden en worden dus vaak opgeschreven. Daarmee verliezen ze een deel van hun kracht.

- Hoe verhoudt zo een extra sterk wachtwoord zich tot het originele wachtwoord voor niveau 1 authenticatie?

4.2.2 Face-to-face authenticatie van mobiel nummer (SMS+)

4.15 De zwakheid van het huidige zekerheidsniveau 2 ("midden") in DigiD is dat de gebruiker zelf het gewenste mobiele nummer op mag geven (na authenticatie op niveau 1, "laag"). Er bestaat daarmee geen extra zekerheid dat het opgegeven nummer daadwerkelijk hoort bij de betreffende persoon.

4.16 Men zou kunnen proberen deze zwakheid te ondervangen door hier alsnog een "face-to-face" stap in te voeren, om een betrouwbare koppeling tussen het mobiele telefoonnummer en de persoon te bewerkstelligen.

4.17 Het grote voordeel van een dergelijke aanpak is dat er geen extra infrastructuur (zoals kaartlezers) vereist is bij zorgconsumenten (thuis). Wel is enige extra infrastructuur nodig (zie hierna) voor validatie van het mobiele nummer. Voor het gemak wordt dit authenticatiemiddel SMS+ genoemd.

4.18 De face-to-face verificatie van het bij SMS+ gebruikte mobiele telefoonnummer kan op meerdere manieren worden ingevuld. Onderstaand zijn twee verschillende varianten voor de face-to-face verificatie uitgewerkt.

4.19 Opgemerkt wordt dat het face-to-face verificatieproces in beide varianten door verschillende controle-instanties zou kunnen worden uitgevoerd. In hoofdstuk 5 wordt het identificatie- en verificatieproces voor deze varianten uitgewerkt voor een tweetal voorbeelden van controle-instanties (te weten het gemeentehuis en de apotheek).

SMS+ (variant 1): Verificatie van mobiele telefoonnummer door middel van een applicatie

4.20 De zorgconsument meldt zich eenmalig met zijn mobiele telefoon voor validatie van het eerder bij DigiD opgegeven mobiele telefoonnummer, bij de controle-instantie waar de identiteit van de betreffende persoon door een baliemedewerker wordt vastgesteld (door middel van controle aan de hand van een reisdocument / rijbewijs). Deze baliemedewerker gebruikt een speciale applicatie en voert daar het BSN van de zorgconsument in, verkregen uit het reisdocument. Deze applicatie staat in contact met de DigiD server, die vervolgens een SMS naar het (eerder) opgegeven mobiele telefoonnummer stuurt (dat bij DigiD gekoppeld is aan het BSN van de betreffende persoon). Deze SMS bevat een specifieke (eenmalige) code, die ook verschijnt in de applicatie. De baliemedewerker controleert op het scherm van de mobiele

telefoon dat de juiste code binnengekomen is, en geeft via de applicatie aan dat dit mobiele telefoonnummer gevalideerd is (registratie van uitgevoerde identificatie- en verificatiestappen). Vervolgens krijgt de zorgconsument na gebruikelijke SMS authenticatie een hoger zekerheidsniveau, bijvoorbeeld voor EPD-toegang.

4.21 Voorwaarde bij deze aanpak is dat binnen DigiD mobiele telefoonnummers niet gedeeld worden door meerdere personen: ieder nummer mag bij hooguit één persoon voorkomen. Dat is nu niet het geval. Een belastingconsulent maakt soms gebruik van het DigiD van meerdere klanten om de belastingformulieren in te dienen. Daarbij gebruiken ze dan het eigen mobiele telefoonnummer voor al die klanten.

4.22 Hoewel de DigiD organisatie een actie is gestart om het bovengenoemde probleem te voorkomen, wordt hier benadrukt dat VWS dient te waarborgen dat één mobiel telefoonnummer slechts voor één DigiD account gebruikt mag worden alvorens SMS+ in gebruik te nemen. Alleen op deze wijze kan worden gewaarborgd dat SMS+ als authenticatiemiddel initieel alleen gebruikt kan worden door één zorgconsument.

4.23 Vanzelfsprekend zal bij verandering van het mobiele nummer, bijvoorbeeld na verlies of diefstal van het apparaat, een face-to-face herauthenticatie moeten plaatsvinden.

4.24 Belangrijk bij dit proces is dat niet alleen de identiteit van de zorgconsument vastgelegd wordt, maar ook de identiteit van de baliemedewerker die dit proces uitvoert. Immers, fraudeleuze handelingen door de baliemedewerker dienen voorkomen te worden. Traceerbaarheid is daarbij van belang vanwege de preventieve werking die een eventuele registratie op naam van de baliemedewerker van een fraudeleus / foutief uitgevoerd identificatie- en verificatieproces heeft. Verder dient de baliemedewerker identiteitsdocumenten te kunnen verifiëren en toegang te hebben tot de database met ongeldige identiteitsdocumenten.

SMS+ (variant 2): Verificatie van mobiele telefoonnummer door middel van ondertekend formulier

4.25 De applicatie beschreven in variant 1 wordt in deze variant vervangen door een simpel ondertekend formulier waarin de zorgconsument verklaart, na legitimatie, wat zijn BSN en mobiele telefoonnummer zijn. Nadat de baliemedewerker de ingevulde gegevens op het formulier gecontroleerd heeft wordt dit doorgestuurd naar de DigiD-organisatie waar de gegevens op het formulier verwerkt worden als basis voor de koppeling tussen het BSN en het mobiele telefoonnummer.

4.26 Deze variant heeft de volgende eigenschappen:

- Er bestaan voor SMS+ variant 2 de mogelijkheid tot het plegen van fraude. Zo is het voor een persoon die woonachtig is op hetzelfde GBA-adres als de

zorgconsument mogelijk om de brieven met activatiecodes voor de huidige DigiD niveaus 1 en 2 te onderscheppen. Vervolgens zou deze persoon naar de controle-instantie kunnen gaan en zich weliswaar kunnen legitimeren als zichzelf maar op het formulier het BSN van de zorgconsument in combinatie met het eigen mobiele telefoonnummer kunnen invullen. Deze wijze van fraude dient onmogelijk gemaakt te worden door middel van een visuele controle door de baliemedewerker dat het ingevulde BSN daadwerkelijk is van de persoon die zich identificeert. Of deze controle daadwerkelijk wordt uitgevoerd door de baliemedewerker wordt niet vastgelegd waardoor foutief handelen (al dan niet met opzet) door de baliemedewerker niet kan worden voorkomen (door preventieve werking) of zelfs ook maar opgemerkt. Tenslotte, is het voor de DigiD-organisatie moeilijk om de authenticiteit van de toegestuurde formulieren te verifiëren (hoe weer de DigiD-organisatie zeker dat het formulier is ingevuld door de betreffende zorgconsument). Hierdoor is het voor de DigiD-organisatie niet mogelijk om gestolen of gekopieerde formulieren die worden ingestuurd te herkennen.

- Er dient rekening gehouden te worden met schrijf- of kopieerfouten bij het invullen van het formulier of het overnemen daarvan door DigiD. Nadat het formulier door de DigiD-organisatie wordt ingescand (voor de registratie van de verificatie van het mobiele telefoonnummer binnen de DigiD-omgeving) kan immers blijken dat de informatie op het door de zorgconsument ingevulde formulier niet leesbaar is. Schrijffouten op het formulier zouden deels kunnen worden opgevangen door een controle van het ingevulde formulier door de baliemedewerker. Wanneer dergelijke fouten pas in een later stadium door de DigiD-organisatie geconstateerd worden dienen additionele inspanningen en kosten te worden gemaakt om deze fouten te herstellen (bijvoorbeeld door middel van her-authenticatie).
- Het is onwaarschijnlijk dat zorgconsumenten bewust een mobiel telefoonnummer opgeven waartoe zij geen toegang hebben voor het verkrijgen van toegang tot de eigen medische gegevens. Hierdoor verliest de zorgconsument immers de mogelijkheid tot toegang tot het landelijk EPD. Deze optie is echter binnen SMS+ variant 2 niet uitgesloten. De zorgconsument zou bij de opgave van het mobiele telefoonnummer voor de activatie van DigiD niveau 2 het mobiele telefoonnummer op kunnen geven van een andere persoon. Vervolgens vult de zorgconsument dit mobiele telefoonnummer consequent in op het formulier. Hierdoor is het mogelijk dat door middel van het bewust foutief invoeren van het mobiele telefoonnummer andere personen dan de zorgconsument via het eigen mobiele telefoonnummer toegang krijgen tot de medische gegevens van de betreffende zorgconsument. Hiervoor hoeft de zorgconsument, in tegenstelling tot SMS+ variant 1, bij het invullen van het formulier niet ter plaatse over het betreffende mobiele telefoonnummer te beschikken.

4.27 Vanwege de hierboven beschreven risico's ten aanzien van schrijf- en kopieerfouten en

een grotere kans op fraude bij het gebruik van in te vullen formulieren dan bij het gebruik van een verificatie-applicatie, wordt deze variant voor SMS+ afgeraden.

4.2.3 Authenticatiemiddelen van internetbankieren

4.28 Internetbankieren heeft in Nederland een hoge vlucht genomen. Naar verluidt maakt meer dan 70%[17] van de Nederlanders er gebruik van. Wereldwijd staat Nederland daarmee aan de top. Banken hebben in Nederland veel ervaring opgebouwd met internetbankieren. De authenticatiemiddelen die ze ervoor gebruiken zijn relatief geavanceerd, via "two-factor" authenticatie. Er wordt gebruik gemaakt van one-time-passwords, die op verschillende manieren in handen van de gebruiker komen, zoals via TAN-lijsten, SMS, een beveiligingscalculator, of via een speciaal apparaatje (zoals een random reader) dat de bankkaart leest. Het beveiligen van internetbankieren vergt constante alertheid en adequate reactie op nieuwe bedreigingen. Het is een kat-en-muis spel. Het afgelopen jaar is gebleken dat de huidige authenticatieinfrastructuur kwetsbaar is voor man-in-the-browser aanvallen via geïnfecteerde PC's van bankklanten. Hiervoor bestaat nog geen fundamentele oplossing.

4.29 Er is in het verleden verschillende malen gesproken over het mogelijke gebruik van authenticatiemiddelen uit de bancaire sector binnen de context van DigiD. Een formeel verzoek daartoe vanuit de overheid is echter nooit geformuleerd. Banken hebben van hun kant nooit principieel "ja" of "nee" gezegd met betrekking tot deze kwestie.

4.30 Hierover valt het volgende te zeggen.

- Volgens de eerder genoemde classificatie van zekerheidsniveaus voor authenticatie zitten de bancaire middelen op niveau 2. Er is immers geen sprake van een geavanceerde digitale handtekening.
- Banken hanteren strikt genomen geen face-to-face controle bij de uitgifte van hun authenticatiemiddelen. Wel is het zo dat er bij de invoering van de Wet op identificatie bij dienstverlening (WID)[18] sprake is geweest van een inhaalslag van een dergelijke face-to-face authenticatie van cliënten en dat voor klanten die een eerste rekening openen ook een face-to-face authenticatie wordt uitgevoerd.
- De beslissing om eventueel eigen authenticatiemiddelen in te passen binnen DigiD is aan individuele banken. Aangenomen dat de drie grote banken in Nederland mee zouden doen, wordt meer dan 90% van het publiek bereikt. Echter, niet alle klanten (naar schatting meer dan 70%) beschikken over deze bancaire authenticatiemiddelen voor internetbankieren.
- Er dient een heldere oplossing te komen voor aansprakelijkheidsproblemen: bij wie ligt de verantwoordelijkheid in geval van identiteitsfraude na geslaagde DigiD-authenticatie met bancaire middelen?
- Deze "bancaire" route vergt een sterke regie, aan zowel de kant van de overheid als van de banken. Een snelle realisatie met grote dekking is niet te verwachten[19].

[17] Percentage is afkomstig van de NVB
[18] Deze wet is vervallen per 1 augustus 2008 en samen met de Wet melding ongebruikelijke transacties (Wet MOT) opgegaan in de Wet ter voorkoming van witwassen en financieren van terrorisme.
[19] http://www.forumstandaardisatie.nl/fileadmin/OVOS/Doc_authenticatie.pdf

4.2.4 eNIK

4.31 Kenmerkend voor de elektronische Nederlandse Identiteitskaart (eNIK) is dat de kaart een certificaat zal hebben waarop een geheime sleutel aanwezig is waarmee de burger (kaarthouder) geavanceerde digitale handtekeningen kan zetten. Die handtekeningen zullen dezelfde juridische status hebben als gewone handtekeningen. Vanwege het belang van deze functionaliteit mag verwacht worden dat uitgifte van de eNIK via een face-to-face proces zal verlopen. Het gebruik van de eNIK vereist een kaartlezer.

4.32 Een digitale handtekening kan gebruikt worden voor authenticatie, in een zogenaamd challenge-response protocol. Het is echter uitermate belangrijk deze authenticatierol van ondertekening niet te vermengen met ondertekening als commitment (omdat bij challenge-response de kaart iedere challenge, los van de semantiek, ondertekent). Het vereist dus een tweede "authenticatie" certificaat met daarop een andere geheime sleutel op de eNIK[20]. Het is niet duidelijk of de huidige opzet voorziet in een dergelijk tweede certificaat. Toch kan authenticatie met zekerheidsniveau 3 via de eNIK plaatsvinden, waarbij de gebruiker gevraagd wordt een expliciete login boodschap te ondertekenen, van de vorm: "ik, gebruiker X, log op het tijdstip Y in bij DigiD, ten behoeve van dienst Z".

4.33 Het grote probleem bij de eNIK is echter de onvoorspelbaarheid van de realisatie. Naar verluidt zal de eNIK niet binnen 2 jaar ingevoerd worden. Zekerheid hierover kan alleen binnen BZK verkregen worden. Grootschalige uitrol zal vervolgens nog een aantal jaren vergen.

4.34 Het uitblijven van de eNIK leidt er nu toe dat er van allerlei kanten druk ontstaat om op een andere manier invulling geven aan DigiD zekerheidsniveau 3. Daaraan bestaat steeds grotere behoefte.

4.2.5 Elektronisch rijbewijs

4.35 Sinds kort heeft het Nederlandse rijbewijs de vorm van een plastic kaart, op creditcard formaat. Het is de bedoeling dat deze kaart op termijn een chip zal bevatten met een certificaat waarop een geheime sleutel aanwezig is waarmee digitale handtekeningen gezet kunnen worden. Hiermee zal het rijbewijs op eNIK lijken. Het is echter evengoed onvoorspelbaar wanneer dit e-rijbewijs breed ingevoerd zal zijn. Omdat een rijbewijs 10 jaar geldig is duurt het lang voordat een substantieel deel van de bevolking over een nieuw rijbewijs met chip zal beschikken. De dekkingsgraad van rijbewijzen zal geringer zijn dan die van eNIKs. Ook voor dit nieuwe, elektronisch rijbewijs is een aparte kaartlezer nodig.

4.2.6 UZI pas

4.36 Authenticatie bij EPD-toegang door zorgverleners vindt plaats via de zogenaamde UZI

[20] zie ook NEN 7512, paragraaf 7.3.3

pas. Deze wordt uitgegeven op basis van het voorkomen van de zorgverlener in het BIG-register. De chip in de UZI pas kan elektronische handtekeningen zetten en zorgen voor een sterke vorm van authenticatie (mits goed beheerd en bijvoorbeeld niet uitgeleend aan anderen).

4.37 De UZI pas is echter niet geschikt voor EPD-toegang door EPD-subjecten, want:

- EPD-toegang is georganiseerd op basis van het BSN, en niet op BIG-registratie.
- Uitgifte van een UZI-achtige pas aan een breder publiek vereist een aparte (nieuwe) face-to-face procedure.

4.2.7 Reisdocument (RTDA)

4.38 Sinds 26 augustus 2006 worden Nederlandse reisdocumenten (paspoort of identiteitskaart) uitgegeven met een ingebedde chip, volgens internationale (ICAO) standaarden[21]. Omdat reisdocumenten 5 jaar geldig zijn zullen in 2011 alle documenten een dergelijke chip hebben. Op dit moment heeft naar schatting[22] bijna 50% van de reisdocumenthouders de beschikking over een dergelijk reisdocument. Vanaf 14 jaar dient men te beschikken over een geldig reisdocument, in het kader van de identificatieplicht. Bij het bereiken van de 14-jarige leeftijd wordt eenmalig gratis een identiteitskaart verstrekt. Kinderen tot 16 jaar kunnen worden bijgeschreven in het paspoort van de ouders. Bijschrijving geschiedt door middel van een print in het paspoort (bij bijschrijving wanneer paspoort wordt aangevraagd) of door middel van speciale stickers (wanneer bijschrijving na uitgifte van het paspoort plaatsvindt). De gegevens van de betreffende kinderen worden niet opgeslagen in de chip van het betreffende paspoort van de ouder(s). Kinderen tussen de 12 en 16 jaar hebben weliswaar een zelfstandig recht op inzage in hun medische dossiers “voor zover zij in staat zijn tot een redelijke waardering van hun belangen terzake”[23], maar zouden wanneer zij niet de beschikking hebben over een reisdocument met een chip waarop de benodigde persoonsgegevens aanwezig zijn geen gebruik kunnen maken van EPD-authenticatie.

4.39 De chip in het reisdocument wordt geactiveerd in een "Basic Access Control" (BAC) protocol waarin een geheime cryptografische sleutel nodig is die afgeleid wordt van de Machine Readable Zone (MRZ) op het document. Die MRZ omvat de onderste twee regels op de identiteitskaart of op de harde plastic pagina in het reisdocument. De MRZ kan optisch gescand worden. Het achterliggende idee is dat deze chiptoegang via de MRZ correspondeert met het fysiek overhandigen van het document.

4.40 In de chip van het reisdocument staan in principe dezelfde gegevens als op de plastic kaart[24]. Deze gegevens staan in een lijstje, dat de Logical Data Structure (LDS) heet. De

[21] Dit geldt niet voor zogenaamde nooddocumenten met een geldigheidsduur van 12 maanden; het noodpaspoort en de Laisser-Passer, hebben dus geen chip.
[22] Lineaire extrapolatie op basis van geldigheidsduur en moment van ingebruikname RTDA
[23] Artikel 7:465, lid 2 BW
[24] Zoals te vinden op www.paspoortinformatie.nl bevat de chip de volgende gegevens: Weergave van de foto (in kleur), Document type, Landcode uitgevende staat, Voorvoegsel(s), Naam, voornamen, Documentnummer, Nationaliteit houder, Geboortedatum, Geslacht, Datum einde geldigheid, Persoonsnummer (in casu het BSN).

integriteit van de gegevens in deze LDS wordt gegarandeerd via een digitale handtekening van de Nederlandse overheid[25]. De chip bevat echter ook een eigen geheime sleutel, waarmee de authenticiteit gecontroleerd kan worden in een zogenaamd "Active Authentication" (AA) protocol. De corresponderende publieke sleutel staat in de LDS.

4.41 In dit kader is het relevant op te merken dat de BAC en AA protocollen ook op afstand uitgevoerd kunnen worden. Daarmee is het mogelijk dat een gebruiker zich op afstand authenticeert. Binnen DigiD kan dan op een hoger zekerheidsniveau gecontroleerd worden dat de vermeende gebruiker met BSN X ook een authentiek reisdocument heeft met BSN X en juiste naam. Hiervoor heeft de gebruiker een (contactloze) kaartlezer nodig. Voor deze “Reisdocument Authenticatie Op Afstand” zal de Engelse omschrijving “Remote Travel Document Authentication” afgekort worden als RTDA.

4.42 Zekerheidsniveau 3 wordt niet bereikt met RTDA omdat met het reisdocument geen geavanceerde digitale handtekening gezet kan worden. Men zou wel kunnen spreken van niveau 2½ omdat:

- Er sprake is van face-to-face contact bij uitgifte.
- De chip naam + BSN gegevens bevat, die vertrouwd kunnen worden (omdat er een elektronische handtekening overheen staat).
- De authenticiteit van de chip gecontroleerd kan worden: een eventuele kloon van de chip kan herkend worden.

4.43 Er zijn ook de volgende nadelen:

- Op afstand kan niet gecontroleerd worden of het aangeboden reisdocument ook echt hoort bij de persoon die inlogt. Het reisdocument bevat weliswaar biometrische gegevens die het mogelijk maken te controleren of de opgeslagen biometrie past bij de aanbieder maar deze controle is op afstand niet betrouwbaar. Echter, deze extra controle van het reisdocument maakt identiteitsfraude moeilijker: een fraudeur dient niet alleen over geldige middelen te beschikken voor inloggen op DigiD zekerheidsniveau 2 (gebruikersnaam, wachtwoord en mobiele telefoon) maar ook over het bijbehorende reisdocument.
- Voor controle van de integriteit van de gegevens in de chip en voor de authenticiteit van de chip moeten specifieke "datagroepen" uit de LDS door de DigiD server opgehaald worden, om precies te zijn de datagroepen 1 en 15 (officieel aangeduid als DG1, met daarin de MRZ gegevens, en DG15, met daarin de publieke sleutel voor AA)[26]. Na het ophalen van deze twee data groepen moet hun hash berekend worden en vergeleken worden met die in het Security Document; daarin staat ook de handtekening over alle hashes. Indien er echter eenmaal toegang tot de chip verkregen is, is er geen enkele beperking om ook de andere datagroepen uit te lezen, met daarin onder andere ook de pasfoto. Voor RTDA zijn deze andere datagroepen niet nodig. Je zou het uitlezen daarvan dus

[25] Deze handtekening staat in het zogenaamde "Security Document" SOd, dat daarnaast ook de hashes bevat van de gegevens in de LDS; de handtekening beslaat deze hashes.

[26] Dit soort technische informatie is beschikbaar op: www.icao.int

willen blokkeren. Technisch kan dat echter niet. Het zal dus in regulering en implementatie duidelijk vastgelegd moeten zijn dat bij authenticatie op afstand via het reisdocument door DigiD geen andere (onnodige) datagroepen uitgelezen worden.

4.44 Het is belangrijk op te merken dat het elektronische reisdocument nooit expliciet bedoeld is voor authenticatie op afstand. De primaire rol van het document is versterking van de authenticatie in face-to-face contact, typisch bij grenspassages of in situaties waarin een legitimatieplicht bestaat, waarbij door elektronische handtekeningen en biometrische controle identiteitsfraude (in het bijzonder: look-alike fraude) beter bestreden kan worden. Technisch gezien is RTDA wel degelijk mogelijk. Ook lijkt het bestaande juridische kader hiertegen geen beperking op te werpen. Bij het ontwerp van het elektronische reisdocument is RTDA als mogelijkheid erkend. Er zijn destijds geen (technische) maatregelen tegen ingebouwd.

4.45 Het is zeer wel mogelijk dat allerlei andere (niet-overheid) partijen geïnteresseerd zijn in RTDA. Zo zou een e-commerce bedrijf de klant kunnen vragen het eigen reisdocument thuis even op een kaartlezer te leggen en de MRZ gegevens in te typen. Op dat moment kan het reisdocument in principe "leeggezogen" worden, waarbij het bedrijf de beschikking krijgt over velerlei persoonsgegevens van de klant (naam, geboortedatum, BSN, digitale foto, enz.) en de authenticiteit van de gegevens en het reisdocument kan controleren. Dit private gebruik van het e-reisdocument is mogelijk niet gewenst maar technisch wel degelijk mogelijk. Bedrijven kunnen RTDA niet verplicht stellen, maar kunnen klanten natuurlijk wel vragen er aan mee te werken (en daarbij aantrekkelijke korting bieden). Het Telematica Instituut werkt op dit moment aan een prototype implementatie die RTDA inpast binnen Microsoft's Card Space architectuur voor identiteitsmanagement. Uitbreiding van DigiD met RTDA is minder bezwaarlijk dan privaat gebruik, omdat de persoonsgegevens van de gebruiker nadrukkelijk binnen overheidscontext blijven. De bij DigiD aangesloten organisaties ontvangen nog steeds hetzelfde ticket, zoals hierboven beschreven (met BSN en zekerheidsniveau).

4.46 Bij realisatie van dit authenticatiemiddel verdient het aanbeveling om een automatische notificatie in te richten vanuit de centrale reisdocumentadministratie naar DigiD, bijvoorbeeld bij vernieuwing of verlies/diefstal van het reisdocument, om authenticatie met niet-geldige documenten te voorkomen.

4.47 Een van de aanstaande veranderingen binnen DigiD betreft het gebruik van sectorale nummers. Dit maakt het mogelijk dat ook bedrijven gebruik maken van DigiD als authenticatie service provider (zonder BSN, maar met voor iedere burger per bedrijf verschillende nummers). Deze ontwikkelingen rondom het gebruik van sectorale nummers zijn ook in de context van RTDA van belang. Het gebruik van sectorale nummers voorkomt enerzijds dat bedrijven zelf met RTDA gaan experimenteren en draagt er anderzijds aan bij dat bedrijven wel van DigiD kunnen profiteren en dat dit op gecontroleerde wijze geschiedt. Verder kan, in combinatie met

DigiD zekerheidsniveau 2½ (of 3), op deze wijze adequate invulling gegeven worden aan de Wbp-verplichting van bedrijven om klanten inzage te geven in de gegevens die over hen zijn opgeslagen.

4.48 Praktisch gebruik van RTDA voor EPD-toegang kan als volgt voorgesteld worden. Een persoon meldt zich op een daartoe bestemde webpagina om toegang te krijgen tot zijn EPD. Zoals gebruikelijk bij DigiD wordt (de browser van) deze persoon automatisch doorgestuurd naar de DigiD-server, met het verzoek om een ticket met zekerheidsniveau minstens 2½. De betreffende persoon logt hier eerst in tot zekerheidsniveau 2 via gebruikersnaam en SMS-authenticatie. Vervolgens wordt op de DigiD webpagina gevraagd om het eigen paspoort (of de identiteitskaart) op een contactloze kaartlezer te leggen, en om het nummer en de geldigheidsdatum van het document op de webpagina in te vullen[27]. De DigiD-server communiceert dan met de chip in het reisdocument, controleert de echtheid ervan en ook of de houder ervan dezelfde is, met hetzelfde BSN, als degene die reeds tot zekerheidsniveau 2 ingelogd is. Wanneer alles klopt wordt de betreffende persoon door de DigiD-server met een valide ticket (met BSN) terug naar de oorspronkelijke website verwezen waar de EPD-toegang tenslotte gerealiseerd kan worden.

4.49 Realisatie van RTDA behelst beperkte aanpassing van de DigiD infrastructuur. Software om met het reisdocument "te praten" is als open source gratis beschikbaar[28] RTDA sluit aan bij interne ontwikkelingen binnen de DigiD-organisatie.

4.3 Gebruik van een chipkaart

4.50 Een aantal van bovenstaand besproken authenticatiemiddelen maakt gebruik van een chipkaart (namelijk de eNIK, rijbewijs, UZI pas en RTDA). Het gebruik van een chipkaart vereist echter een chipkaartlezer[29]. Slechts weinigen zullen op dit moment thuis beschikken over een dergelijke chipkaartlezer (met bijbehorende software). Onderdeel van de invoering van het gebruik van chipkaarten voor EPD-authenticatie zal een aanbeveling moeten zijn aan EPD-subjecten aangaande de soorten chipkaartlezers die geschikt zijn (en met welke software). Bij aankoop van grote aantallen zullen kosten van naar schatting 10 tot 20 Euro per kaartlezer mogelijk zijn. Deze kosten zijn sterk afhankelijk van de functionaliteit van de kaartlezer (alleen contact, alleen contactloos of beide, met of zonder eigen (numerieke) toetsen en display et cetera).

4.51 Bij het huidige gebrek aan brede beschikbaarheid van dergelijke kaartlezers bij mensen (thuis) kan overwogen worden om bij aanbieders van medische zorg speciale PC's neer te zetten waar EPD-subjecten, met de juiste authenticatiemiddelen, toegang kunnen krijgen tot hun eigen EPD.

[27] Desgewenst kan de DigiD-server deze documentgegevens ook bewaren.

[28] De Java software staat op http://jmrtd.org/

[29] In dit verband verdienen "intelligente" kaartlezers die end-to-end (versleuteld) kan communiceren met de DigiD-server de voorkeur.

4.4 Advies ten aanzien van het te implementeren authenticatiemiddel

4.52 Gelet op de juridische en technische beveiligingseisen rondom het EPD is – uitgedrukt in DigiD-niveaus - een zekerheidsniveau van meer dan 2 noodzakelijk. Hiervan uitgaande lijkt op de langere termijn eNIK (of een vergelijkbaar elektronisch rijbewijs), gemeten naar de huidige kennis en inzichten rondom eNIK, het meest geschikte authenticatiemiddel om DigiD zekerheidsniveau 3 te bereiken. Omdat eNIK danwel het elektronisch rijbewijs hoogstwaarschijnlijk de komende jaren niet beschikbaar zullen zijn, zijn ook alternatieve opties met een lager zekerheidsniveau dan 3 maar hoger dan 2 in kaart gebracht.

4.53 Op grond van de geïnventariseerde technische en juridische eisen, komen voor EPD-authenticatie twee authenticatiemiddelen in aanmerking, te weten SMS+ SMS+ (face-to-face authenticatie van mobiel nummer) en RTDA (gebruik van Reisdocument).

4.54 Van de twee onderzochte varianten ten aanzien van SMS+ heeft - voor wat betreft informatiebeveiliging - variant 1 de voorkeur (verificatie van het mobiele telefoonnummer door de controle-instantie aan de hand van een verificatieapplicatie) boven variant 2 (verificatie van mobiele telefoonnummer door middel van een verklaring door de zorgconsument en registratie van deze verklaring door DigiD). Bij variant 2 kunnen zich immers problemen ten aanzien van schrijf- en kopieerfouten (bij het inscannen van de verklaringen door DigiD) voordoen. Daarnaast lijkt een dergelijke verklaring meer fraudegevoelig omdat het uitgevoerde verificatieproces niet wordt geregistreerd door een geauthenticeerde baliemedewerker en controles ten aanzien van het op de verklaring aangegeven mobiele telefoonnummer pas worden uitgevoerd nadat de DigiD-organisatie deze verklaring ontvangt en verwerkt.

4.55 SMS+ is ten opzichte van RTDA het minst ingrijpend en omslachtig voor de gebruikers. Daar staat tegenover dat er wel extra werk gestoken zal moeten worden in de authenticatie van het mobiele telefoonnummer, met inzet van de baliemedewerkers van de controle-instantie. In de huidige DigiD context zou men bij SMS+ kunnen spreken van authenticatie op zekerheidsniveau 2+.

4.56 RTDA is ingrijpender dan SMS+ omdat EPD-subjecten (thuis) een kaartlezer nodig zullen hebben (met bijbehorende distributie en installatieproblemen). Dit authenticatiemiddel is echter meer in lijn met geplande ontwikkelingen rond de eNIK en rijbewijs: er kan betoogd worden dat een dergelijke infrastructuur op termijn nodig is. Bij RTDA zou men kunnen spreken van zekerheidsniveau 2½. RTDA is sterken dan SMS+ omdat het reisdocument een zorgvuldig proces kent bij uitgifte en verlies en omdat het reisdocument een goed beveiligde chip bevat.

4.57 Beide oplossingen zijn niet direct te realiseren omdat zij bouw van programmatuur, inrichting van procedures en controle-instanties et cetera vereisen. Bij de keuze tussen deze

twee alternatieven speelt op de achtergrond ook ander overheidsbeleid betreffende authenticatie een rol (de invoering van eNIK, elektronisch rijbewijs, en de eventuele inpassing hiervan binnen DigiD) dat de context van dit rapport overstijgt.

4.58 Bij eerste beschouwing lijkt de SMS+ (variant 1) een bredere verspreiding te hebben dan de reisdocumenten voorzien van RTDA en daarmee op dit moment breder implementeerbaar. Bij SMS+ (variant 1) is een controle-instantie noodzakelijk, waarbij in dit advies als mogelijke opties zijn uitgewerkt het gemeentehuis en de apotheek. Het gemeentehuis lijkt meer ervaring te hebben met identiteitscontrole maar dit is niet doorslaggevend. De uiteindelijke keuze voor hetzij SMS+ (variant 1) hetzij RTDA, danwel de controle-instantie, is een veelzijdig vraagstuk waarbij naast het uitgifteproces ook kosten, gebruikersvriendelijkheid, snelle beschikbaarheid, externe afhankelijkheden en technische aspecten meespelen. Een verantwoorde keuze tussen de opties vergt daarom de afweging van middelen en van bijbehorende processen. Een dergelijke afweging valt gezien het doel van het onderzoek (een onafhankelijk advies inzake de minimale beveiligingseisen voor de identificatie en authenticatie van de zorgconsument in het kader van Toegang patiënt tot het EPD) buiten de reikwijdte van dit onderzoek (gericht op de juridische en technische eisen).

4.59 In dit rapport is nadrukkelijk het advies opgenomen om voor de te kiezen optie een praktijkproef te organiseren, voorafgaande aan een grootschalige invoering. Mogelijk kan zelfs overwogen worden voor beide opties een praktijkproef te houden, en mede op basis van de uitkomsten daarvan een besluit te nemen.

4.60 In het algemeen is het zo dat een hoger zekerheidsniveau over de identiteit van klanten aanbieders in staat stelt om meer diensten online toegankelijk te maken. Dit geldt in principe voor alle huidige en toekomstige afnemers van DigiD, waaronder te zijner tijd commerciële partijen (via sectorale nummers). Alleen met zekerheidsniveau 3 (digitale handtekeningen) kan onloochenbaarheid van klanttransacties bewerkstelligd worden. De hier voorgestelde (tussen)oplossingen (SMS+ en RTDA) bieden niet dat zekerheidsniveau 3. Ze kunnen dienstafnemers echter wel doen besluiten meer online aan te bieden. VWS vervult hierin met EPD-toegang op dit moment een voortrekkersrol.

4.61 Wanneer SMS+ en/of RTDA ingevoerd wordt en te zijner tijd ook de eNIK beschikbaar is kan op dat moment het beste bepaald worden of SMS+/RTDA dan nog verder ondersteund dient te worden. Ook kan dan gekeken worden in hoeverre de verschillende alternatieven in een op dat moment geldende Europese context inpasbaar zijn, zie bijvoorbeeld het Stork project http://www.eid-stork.eu/.

5 Fase 3: Inrichting en minimale eisen aan het verificatie- en uitgifteproces

5.01 Informatiebeveiliging is meer dan techniek alleen. Een technische oplossing voor authenticatie is alleen betrouwbaar wanneer er een bepaalde mate van zekerheid bestaat dat alleen diegene voor wie het middel bedoeld is in staat is om het te gebruiken. Om deze zekerheid te verkrijgen dient ook procesmatig aan nader te benoemen eisen te worden voldaan.

5.02 In dit hoofdstuk zijn de eisen ten aanzien van het face-to-face verificatie- en uitgifteproces beschreven. In paragraaf 5.1 zullen deze eisen uiteengezet worden in het referentiekader voor het verificatie- en uitgifteproces. Vervolgens is in paragraaf 5.2 het referentiekader ingevuld voor de twee voorgeselecteerde alternatieven uit hoofdstuk 4, respectievelijk SMS+ en RTDA. Voor een zo volledig mogelijk beeld zijn voor SMS+ beide varianten in dit hoofdstuk behandeld. In paragraaf 5.3 is het verificatie- en uitgifteproces voor SMS+ varianten 1 en 2 en RTDA grafisch uiteengezet. Tenslotte, is in paragraaf 5.4 een analyse van de inrichting van het verificatie- en uitgifteproces opgenomen.

5.1 Referentiekader voor het verificatie- en uitgifteproces

5.03 In het onderstaande referentiekader voor de inrichting van het verificatie- en uitgifteproces zijn enerzijds eisen ten aanzien van de inrichting en anderzijds zogenaamde inrichtingsaspecten beschreven.

5.04 De eisen en wensen in het referentiekader zijn gebaseerd op best practices, brondocumentatie (zie bijlage A) en de eisen uit het offerteverzoek van VWS.

5.1.1 Eisen en wensen voor het verificatie- en uitgifteproces

Ref	Eis / wens	Toelichting eis / wens
1. Eisen aan het verificatie- en uitgifteproces zelf		
E.1.1	Face-to-Face identificatie	Om een bepaalde mate van zekerheid te verkrijgen over de uitgifte van het authenticatiemiddel aan de juiste persoon, is het noodzakelijk dat het authenticatiemiddel pas fysiek wordt overgedragen aan de persoon danwel geactiveerd wordt nadat de identiteit van de betreffende persoon visueel is vastgesteld. Hiermee dient bijvoorbeeld voorkomen te worden dat op elkaar lijkende familieleden zich identificeren met elkaars identiteitsbewijzen.
E.1.2	Verificatie echtheid authenticatiemiddel	De controle-instantie moet in staat zijn een vervalst of gestolen authenticatiemiddel te herkennen.
E.1.3	Verificatie van bezit van authenticatiemiddel	Wanneer een authenticatiemiddel wordt gebruikt dat reeds in het bezit is van de gebruiker dan dient het bezit van dit middel bij het verificatieproces geverifieerd te worden door de controle-instantie.

Ref	Eis / wens	Toelichting eis / wens
E.1.4	Registratie van verificatie en uitgifte	Door middel van een door de controle-instantie te voeren registratie dient te achterhalen te zijn dat de identiteit van een gebruiker door middel van een face-to-face is geverifieerd en welk authenticatiemiddel vervolgens aan deze persoon is verstrekt. Op deze wijze is altijd traceerbaar welke gebruikers over welke authenticatiemiddelen beschikken. Zodoende wordt ook het aanvragen van meerdere authenticatiemiddelen voor één persoon/BSN voorkomen.
E.1.5	Natuurlijke controlemomenten hebben de voorkeur	Hierbij moet gedacht worden aan de inschrijving voor behandeling in het ziekenhuis of het ophalen van een nieuw authenticatiemiddel bij het gemeentehuis.
E.1.6	Aansluiting bij toekomstscenario's	Het is wenselijk dat het in te richten verificatie- en uitgifteproces relatief eenvoudig kan aansluiten bij toekomstige initiatieven zoals de invoering van eNIK.
E.1.7	Voorregistratie is wenselijk	Op deze wijze worden de administratieve lasten voor zowel de betrokken persoon als de controle-instantie beperkt.
E.1.8	Terugkoppeling van gebruik of activering van authenticatiemiddel	Gebruik of activering van het middel kan aan de gebruiker worden teruggekoppeld via een ander kanaal (bijvoorbeeld post, e-mail). Hierdoor wordt het moeilijker om ongemerkt een middel voor een andere persoon aan te vragen en te gebruiken. Mogelijke invulling kan zijn een melding van gebruik via mail/sms aan gebruiker, inzage in gebruik via EPD/LSP portal.
2. Eisen aan het authenticatiemiddel in het kader van het verificatie- en uitgifteproces		
E.2.1	Authenticatiemiddel dient uniek identificeerbaar te zijn.	Het authenticatiemiddel dient uniek identificeerbaar te zijn door middel van één registratienummer.
E.2.2	1-op-1 koppeling tussen gebruikersaccount en authenticatiemiddel	Met 1 authenticatiemiddel kan alleen toegang verkregen worden tot 1 specifiek gebruikersaccount. Dit betekent dat toegang tot meerdere accounts met 1 authenticatiemiddel en toegang tot 1 account met meerdere authenticatiemiddelen voorkomen dient te worden.
E.2.3	Authenticatiemiddel dient niet kopieerbaar te zijn	Een middel mag technisch niet (eenvoudig) te kopiëren zijn, zodat als de persoon het middel in bezit heeft met een grote mate van zekerheid kan worden vastgesteld dat het middel alleen in het bezit van de betreffende gebruiker is.
E.2.4	Initiële beschikbaarheid van authenticatiemiddel voor gehele bevolking gewenst.	Om de adoptiegraad van het authenticatiemiddel en het gebruik van de geboden functionaliteit door de zorgconsument zo hoog mogelijk te maken dienen zoveel mogelijk Nederlanders het middel vanaf introductie te kunnen gebruiken.

5.1.2 Kostenaspecten voor het verificatie en uitgifteproces

Ref	Aspect	Toelichting aspect
K.1	Kosten voor gebruiker	Voor een hogere adoptiegraad van het authenticatiemiddel en de functionaliteit van het EPD voor zorgconsumenten dient ernaar gestreefd te worden om de kosten voor de gebruiker zo laag mogelijk te houden. Hierbij kan een onderscheid gemaakt worden tussen de kosten voor de aanschaf van het authenticatiemiddel en de kosten voor de noodzakelijke uitleesapparatuur zoals cardreaders.

Ref	Aspect	Toelichting aspect
K.2	Implementatiekosten voor controle-instantie	Hiermee worden de (eenmalige) kosten voor de inrichting van het verificatie- en uitgifteproces bij de controle-instantie bedoeld. Hierbij zal ook rekening gehouden worden met het feit of het hier kosten voor een tijdelijke inrichting betreffen of dat de kosten ook kunnen worden gezien als investeringen in toekomstscenario's (zoals invoering van een eNIK).
K.3	Uitvoeringskosten voor controle-instantie	Hiermee worden de structurele kosten voor de uitvoering van het verificatie- en uitgifteproces door de controle-instantie bedoeld.
K.4	Implementatiekosten voor DigiD organisatie	Hiermee worden de (eenmalige) kosten bedoeld voor noodzakelijke wijzigingen binnen DigiD.
K.5	Uitvoeringskosten voor DigiD organisatie	Hiermee worden de structurele kosten voor de ondersteuning van het betreffende authenticatiemiddel door de DigiD organisatie bedoeld.
K.6	Kosten voor VWS	Hiermee worden onder andere kosten bedoeld voor de aansluiting tussen het te gebruiken authenticatiemiddel en het EPD, project- en programmamanagement, communicatie en voorlichting.

5.2 Referentiekader ingevuld voor SMS+ en RTDA

5.05 In onderstaande tabel is het bovenstaande referentiekader ingevuld voor zowel SMS+ varianten 1 en 2 als het RTDA.

5.06 Het identificatie- en verificatieproces voor SMS+ kan door meerdere controle-instanties uitgevoerd worden. Ter illustratie is bij de invulling van het referentiekader voor varianten 1 en 2 van SMS+ onderscheid gemaakt tussen de invulling van het identificatie- en verificatieproces door respectievelijk het gemeentehuis en de apotheek als controle-instanties.

5.07 Aan de eisen en wensen kan het verificatie- en uitgifteproces op verschillende niveaus voldoen. Onderscheid wordt gemaakt naar de volgende niveaus van inspanning die voor het betreffende authenticatiemiddel benodigd is om aan de eisen en wensen te voldoen:

1. Geen extra inspanning (G)
2. Lage benodigde inspanning (L)
3. Hoge benodigde inspanning (H)
4. Niet mogelijk (N)

5.08 Voor de kostenaspecten geldt dat deze per authenticatiemiddel uitsluitend kwalitatief zijn beschreven.

5.2.1 Eisen en wensen voor het verificatie en uitgifteproces ingevuld voor SMS+ en RTDA

Ref	Eis / wens	SMS+ (variant 1)	SMS+ (variant 2)	RTDA
1. Eisen aan het verificatie en uitgifteproces zelf				
E.1.1	Face-to-face identificatie	**Gemeentehuis:** (G), het gemeentehuis is immers vanuit andere uitgifteprocessen voor bijvoorbeeld reisdocumenten gewend om face-to-face verificatie van de identiteit van een burger uit te voeren (met behulp van de GBA). **Apotheek:** (L), een apotheek is, in het kader van het gebruik van de BSN in de zorg, per 1 juli 2009 verplicht om een face-to-face verificatie van de identiteit van een zorgconsument uit te voeren. Een onderdeel van deze verificatie is de controle of het aangeboden identificatiemiddel echt is via de SBV-Z.	**Gemeentehuis:** (G), het gemeentehuis is immers vanuit andere uitgifteprocessen voor bijvoorbeeld reisdocumenten gewend om face-to-face verificatie van de identiteit van een burger uit te voeren (met behulp van de GBA). **Apotheek:** (L), een apotheek is, in het kader van het gebruik van de BSN in de zorg, per 1 juli 2009 verplicht om een face-to-face verificatie van de identiteit van een zorgconsument uit te voeren. Een onderdeel van deze verificatie is de controle of het aangeboden identificatiemiddel echt is via de SBV-Z.	(G), heeft reeds plaatsgevonden door balie gemeentehuis bij afhalen reisdocument.

Ref	Eis / wens	SMS+ (variant 1)	SMS+ (variant 2)	RTDA
E.1.2	Verificatie echtheid authenticatiemiddel	Door middel van een applicatie die in contact staat met de DigiD server kan de baliemedewerker van de controle-instantie controleren of het mobiele telefoonnummer wel echt bestaat (immers wanneer de zorgconsument ter plekke kan aantonen over het mobiele telefoonnummer te beschikken, dan bestaat het ook). **Gemeentehuis:** (L), De uitvoering van de verificatie van het mobiele telefoonnummer zal de gemeentehuizen structureel meer inspanningen kosten. Echter dergelijke handelingen zijn voor gemeentehuizen gemeengoed vanuit de publiekrechtelijke taken die zij reeds uitvoeren. **Apotheek:** (H), De uitvoering van de verificatie van het mobiele telefoonnummer zal de apotheken structureel meer inspanningen kosten. Daarnaast zal de uitvoering van het verificatieproces voor zowel zorgconsumenten die niet vaak bij de eigen apotheek komen als voor zorgconsumenten die niet bij de eigen apotheek komen ook additionele inspanningen vergen van de apotheken.	**Gemeentehuis / Apotheek:** (N), de controle-instantie heeft geen mogelijkheid om bij de face-to-face controle van de identiteit van de zorgconsument te controleren of het door de zorgconsument opgegeven mobiele telefoonnummer daadwerkelijk geregistreerd is binnen DigiD. Deze controle wordt immers door de DigiD-organisatie uitgevoerd nadat zij het formulier hebben verkregen en verwerkt. Hierdoor is het mogelijk dat een niet bestaand mobiele telefoonnummer opgegeven wordt door de zorgconsument. (L), De baliemedewerker dient wel te controleren of het op het formulier ingevulde BSN overeenkomst met het BSN op het identiteitsbewijs (om fraude door de zorgconsument te voorkomen) en of er duidelijke schrijffouten zijn gemaakt.	(G), bij bestaand uitgifteproces balie gemeentehuis wordt het reisdocument op primaire en secundaire echtheidskenmerken gecontroleerd. Tevens heeft het gemeentehuis toegang tot de GBA en het register reisdocumenten.

Ref	Eis / wens	SMS+ (variant 1)	SMS+ (variant 2)	RTDA
E.1.3	Verificatie van bezit van authenticatiemiddel	**Gemeentehuis / Apotheek:** (L), bij de face-to-face controle wordt, mits door middel van een applicatie die in contact staat met de DigiD server, gecontroleerd of het opgegeven mobiele telefoonnummer in bezit is van de gebruiker die zich legitimeert. Initieel gaat het hier dan om eenmalige verificatie. Wel dient bij het wijzigen of verliezen van het mobiele telefoonnummer herauthenticatie plaats te vinden.	**Gemeentehuis / Apotheek:** (N), de controle-instantie heeft geen mogelijkheid om het bezit van het mobiele telefoonnummer door de zorgconsument te verifiëren. De zorgconsument verklaart immers slechts door middel van een formulier te beschikken over het betreffende mobiele telefoonnummer. Er vindt alleen een registratie achteraf van de verklaring van de zorgconsument door DigiD plaats.	(G), automatisch, wordt uitgegeven op de persoon. Daarnaast wordt door middel van het challenge-response mechanisme wat wordt gebruikt bij authenticatie aan de hand van de RTDA bij elke succesvolle login geverifieerd dat de persoon die inlogt daadwerkelijk in het bezit is van het reisdocument.
E.1.4	Registratie van verificatie en uitgifte	**Gemeentehuis / Apotheek:** (L), wanneer de baliemedewerker via een applicatie toegang heeft tot DigiD voor de registratie van de uitgevoerde verificatie- en uitgifte. Hierbij dient tevens geregistreerd te worden welke baliemedewerker het identificatie- en verificatieproces heeft uitgevoerd om zodoende fraude door de baliemedewerker (via preventieve werking en detectie) tegen te gaan.	**Gemeentehuis / Apotheek:** (H), de registratie van de verificatie van het mobiele telefoonnummer gebeurd immers achteraf doordat de DigiD organisatie de verklaring van de zorgconsument dient in te scannen en te registeren binnen DigiD systeem. Dit proces is tevens gevoelig voor fouten bij inscannen en invoeren van de verklaring. Daarnaast vindt geen registratie plaats van het door de baliemedewerker uitgevoerde identificatie- en verificatieproces.	(G), uitgifte van identiteitsbewijzen wordt geregistreerd in register reisdocumenten.

Ref	Eis / wens	SMS+ (variant 1)	SMS+ (variant 2)	RTDA
E.1.5	Natuurlijke controlemomenten hebben de voorkeur	**Gemeentehuis:** (H), de gebruiker dient een specifieke verificatieactie bij een controlerende instantie uit te voeren voor het activeren van het mobiele telefoonnummer als authenticatiemiddel. Hiervoor dient de zorgconsument het mobiele telefoon(nummer) bij zich te hebben en het verificatieproces aan de balie bij de controle-instantie te doorlopen. **Apotheek:** (L), reguliere klanten van apotheken kunnen bij het eerstvolgende bezoek aan de apotheek de face-to-face verificatie van de identiteit en het opgegeven mobiele telefoonnummer doorlopen.	**Gemeentehuis:** (L), de gebruiker dient een specifieke verificatieactie bij een controlerende instantie uit te voeren voor het activeren van het mobiele telefoonnummer als authenticatiemiddel. Hiervoor hoeft de zorgconsument echter alleen een formulier in te vullen en te ondertekenen. **Apotheek:** (L), reguliere klanten van apotheken kunnen bij het eerstvolgende bezoek aan de apotheek de face-to-face verificatie van de identiteit en het opgegeven mobiele telefoonnummer doorlopen.	(G), is niet specifiek voor EPD-authenticatie. Het reisdocument moet toch worden opgehaald. Dit is niet het geval indien het reisdocument versneld wordt vervangen.
E.1.6	Aansluiting bij toekomstscenario's	**Gemeentehuis:** (L), mits de verificatie van de identiteit van de zorgconsument uitgevoerd wordt zoals dat ook voor de uitgifte van reisdocumenten het geval is. Hierdoor is een geleidelijke overgang naar de uitgifte van eNIK mogelijk. Bij deze overgang wordt de verificatie van het mobiele telefoonnummer door middel van een applicatie uitgefaseerd. **Apotheek:** (H), het verificatieproces bij apotheken is van tijdelijke aard en zal moeten worden uitgefaseerd wanneer overgegaan wordt op eNIK. Dit betekent dat zowel de verificatie van de identiteit als de verificatie van het mobiele telefoonnummer (door middel van de applicatie) uitgefaseerd worden.	**Gemeentehuis:** (L), mits de verificatie van de identiteit van de zorgconsument wordt zoals dat ook voor de uitgifte van reisdocumenten het geval is. Hierdoor is een geleidelijke overgang naar de uitgifte van eNIK mogelijk. Bij deze overgang wordt de verificatie van het mobiele telefoonnummer door middel van een verklaring van de zorgconsument uitgefaseerd. **Apotheek:** (L), het verificatieproces bij apotheken is van tijdelijke aard en zal moeten worden uitgefaseerd wanneer overgegaan wordt op eNIK. Dit betekent dat zowel de verificatie van de identiteit als de verificatie van het mobiele telefoonnummer (door middel van een verklaring van de zorgconsument) uitgefaseerd worden.	(G), het uitgifteproces van RTDA is gelijk aan dat van het reisdocument en zal naar alle waarschijnlijkheid ook gelijk zijn aan het uitgifteproces voor eNIK.

Ref	Eis / wens	SMS+ (variant 1)	SMS+ (variant 2)	RTDA
E.1.7	Voorregistratie is mogelijk	**Gemeentehuis / Apotheek:** (G), zorgconsumenten hebben voor DigiD midden al een mobiele telefoonnummer geregistreerd bij DigiD. In deze variant heeft de baliemedewerker bij de betreffende controle-instantie via een applicatie inzage in door de zorgconsumenten geregistreerde mobiele telefoonnummers in het kader van de verificatie van dit telefoonnummer.	**Gemeentehuis / Apotheek:** (G), zorgconsumenten hebben voor DigiD midden al een mobiele telefoonnummer geregistreerd bij DigiD. In deze variant heeft de baliemedewerker bij de betreffende controle-instantie echter geen toegang tot deze voorregistratie.	(H) voor 2011, (L) vanaf 2011. Ieder met een geldig reisdocument dat in of na 2006 is uitgegeven heeft automatisch toegang tot zijn EPD/LSP. Echter, niet iedereen beschikt over een reisdocument en daarnaast duurt het nog een tijd (tot 2011) voordat alle reisdocumenten in omloop hiervoor geschikt zijn.
E.1.8	Terugkoppeling van gebruik of activering van authenticatiemiddel	**Gemeentehuis / Apotheek:** **Activering:** (L), mogelijk door middel van post naar een via GBA/DigiD geregistreerd adres. **Gebruik:** (L), wanneer binnen het EPD de datum en tijdstip van laatste login wordt teruggemeld.	**Gemeentehuis / Apotheek:** **Activering:** (L), mogelijk door middel van post naar een via GBA/DigiD geregistreerd adres. **Gebruik:** (L), wanneer binnen het EPD de datum en tijdstip van laatste login wordt teruggemeld.	**Activering:** (L), mogelijk door middel van post naar adres geregistreerd in de GBA/adres geregistreerd in DigiD. **Gebruik:** (L), wanneer binnen het EPD de datum en tijdstip van laatste login wordt teruggemeld.
2. Eisen aan het authenticatiemiddel in het kader van het verificatie- en uitgifteproces				
E.2.1	Authenticatiemiddel dient uniek identificeerbaar te zijn.	(G), via het mobiele telefoonnummer van DigiD niveau 2. Dit is een uniek nummer.	(G), via het mobiele telefoonnummer van DigiD niveau 2. Dit is een uniek nummer.	(G), via reisdocumentnummer. Dit is een uniek nummer.

Ref	Eis / wens	SMS+ (variant 1)	SMS+ (variant 2)	RTDA
E.2.2	1-op-1 koppeling tussen gebruikersaccount en authenticatiemiddel	(L), wanneer een mobiel telefoonnummer niet voor meerdere DigiD niveau 2 accounts te gebruiken is en indien het mogelijk wordt gemaakt dat een baliemedewerker van de controle-instantie door middel van een applicatie kan controleren of het opgegeven mobiele telefoonnummer al eens is gebruikt.	(H), om een 1-op-1 koppeling te kunnen maken tussen gebruikersaccount en SMS+ dienen de door de zorgconsument ingevulde formulieren bij DigiD ingescand en verwerkt te worden, hierdoor kan het veelvoudige gebruik van het hetzelfde mobiele telefoonnummers voor verschillende gebruikersaccounts pas achteraf worden gesignaleerd.	(G), het reisdocument bevat integraal het BSN. Hierdoor is het niet mogelijk dit reisdocument voor een ander DigiD account (met immers een ander BSN) te gebruiken.
E.2.3	Authenticatiemiddel dient niet kopieerbaar te zijn	(G), het is niet eenvoudig een mobiel nummer te klonen, daarvoor is toegang tot het netwerk van de provider nodig. Wel zouden mogelijke problemen kunnen optreden wanneer malware (kwaadaardige programma's) is geïnstalleerd op smartphones (die SMS berichten automatisch doorstuurt).	(G), het is niet eenvoudig een mobiel nummer te klonen, daarvoor is toegang tot het netwerk van de provider nodig. Wel zouden mogelijke problemen kunnen optreden wanneer malware (kwaadaardige programma's) is geïnstalleerd op smartphones (die SMS berichten automatisch doorstuurt).	(G), technisch zeer moeilijk om het fysieke reisdocument en de digitale gegevens die hierop aanwezig zijn te kopiëren, aangezien de bevattende gegevens worden beschermd middels een elektronische handtekening van de Nederlandse Staat.
E.2.4	Initiële beschikbaarheid van authenticatiemiddel voor gehele bevolking gewenst.	(L), voor het gebruik van SMS+ dient de zorgconsument te beschikken over een mobiele telefoon. Bijna alle zorgconsumenten in Nederland beschikken hier momenteel over[30].		(H), voor RTDA heeft de zorgconsument een reisdocument nodig dat na 26 augustus 2006 is uitgegeven. Voor sommige gebruikers zal daarom gelden dat zij tot uiterlijk 2011 (in verband met geldigheidsduur van 5 jaar) moeten wachten om zonder gezonken kosten een nieuw reisdocument aan te schaffen.

[30] Telecompaper schatte naar aanleiding van een uitgevoerd onderzoek over de Nederlandse telecommarkt in 2007 dat er in 2008 20 miljoen mobiele telefoons in gebruikt zouden zijn. Zie ook http://www.telecompaper.com/news/article.aspx?id=195384&yr=2007. Hierbij dient te worden opgemerkt dat door het toenemende aantal Nederlanders die beschikken over meerdere mobiele telefoons (bijv. privé en zakelijk) niet alle Nederlanders per se de beschikking hoeven te hebben over een mobiele telefoon.

5.2.2 Kostenaspecten voor verificatie- en uitgifteproces ingevuld voor SMS+ en RTDA

Ref	Kostenaspect	SMS+ (variant 1)	SMS+ (variant 2)	RTDA
K.1	Kosten voor gebruiker	Wanneer niet beschikbaar aanschaf van een mobiel telefoonnummer (alleen een SIM-kaart met tegoed vanaf ongeveer 15 euro, incl. prepaid telefoon vanaf ongeveer 50 euro).	Wanneer niet beschikbaar aanschaf van een mobiel telefoonnummer (alleen een SIM-kaart met tegoed vanaf ongeveer 15 euro, incl. prepaid telefoon vanaf ongeveer 50 euro).	- Aanschaf van wireless card reader (10 a 20 euro). - Aanschaf van een nieuw reisdocument (tarieven voor 2008[31]: € 48,35 voor het paspoort en € 40,73 voor een identiteitsbewijs) voor zorgconsumenten die niet reeds over een dergelijk paspoort beschikken. Echter het gaat hier dan om een vervroeging van de aanvraag van een nieuw reisdocument, vanaf 2011 zullen immers alle reisdocumenten via de vervaldatum van het oude reisdocument vervangen zijn en beschikken over een ingebouwde chip.
K.2	Implementatiekosten voor controle-instantie	**Gemeentehuis:** - Nieuw in te richten verificatieproces van mobiele telefoonnummer. - Training en opleiding voor het gebruik van de applicatie om het mobiele telefoonnummer te verifiëren. **Apotheek:** - Mogelijk vervroegde implementatie en bijbehorende training en opleiding voor verificatie van identiteit door middel van SBV-Z. - Training en opleiding voor het herkennen van echtheidskenmerken van een reisdocument. - Nieuw in te richten verificatieproces van mobiele telefoonnummer.	**Gemeentehuis:** - Nieuw in te richten verificatieproces van mobiele telefoonnummer. - Training en opleiding voor het laten invullen (en mogelijk controleren van ingevulde formulier) van een verklaring van de zorgconsument ten aanzien van het bezit van het mobiele telefoonnummer. **Apotheek:** - Mogelijk vervroegde implementatie en bijbehorende training en opleiding voor verificatie van identiteit door middel van SBV-Z. - Training en opleiding voor het herkennen van echtheidskenmerken van een reisdocument.	Geen tot zeer weinig additionele implementatiekosten aangezien het verificatie- en uitgifteproces voor reisdocumenten met een chip al bestaat bij gemeentehuizen.

[31] Tarieven overgenomen van www.paspoortinformatie.nl. Dit zijn de voor 2008 door de overheid vastgestelde maximumtarieven. In de praktijk kunnen gemeenten ervoor kiezen om lagere tarieven te hanteren.

Ref	Kostenaspect	SMS+ (variant 1)	SMS+ (variant 2)	RTDA
		- Training en opleiding voor het gebruik van de applicatie om het mobiele telefoonnummer te verifiëren.	- Nieuw in te richten verificatieproces van mobiele telefoonnummer. - Training en opleiding voor het laten invullen (en mogelijk controleren van ingevulde formulier) van een verklaring van de zorgconsument ten aanzien van het bezit van het mobiele telefoonnummer.	
K.3	Uitvoeringskosten voor controle-instantie	**Gemeentehuis / apotheek:** Additioneel uit te voeren handelingen: in het kader van het verkrijgen van toegang tot het EPD door de zorgconsument uitvoeren van een additionele verificatie van de identiteit en het mobiele telefoonnummer aan de hand van een applicatie die in contact staat met de DigiD-server voor een groot deel van alle burgers in Nederland[32].	**Gemeentehuis / apotheek:** Additioneel uit te voeren handelingen: in het kader van het verkrijgen van toegang tot het EPD door de zorgconsument uitvoeren van een additionele verificatie van de identiteit en het laten invullen (en mogelijk controleren) van de verklaring van de zorgconsument dat deze een bepaald mobiele telefoonnummer in bezit heeft.	Gelijk aan de bestaande kosten voor het al bestaande verificatie- en uitgifteproces voor reisdocumenten met een chip.

[32] De inschatting van de DigiD-organisatie is dat 12 miljoen Nederlanders de beschikking hebben over een BSN en dus gebruik kunnen maken van DigiD.

Ref	Kostenaspect	SMS+ (variant 1)	SMS+ (variant 2)	RTDA
K.4	Implementatiekosten voor DigiD-organisatie	- Ontwikkelen van een applicatie waarin de volgende zaken per zorgconsument door de controle-instantie op afstand kunnen worden geregistreerd per zorgconsument: 1. De (gebruikers)naam van de baliemedewerker welke de verificatie van de identiteit van de zorgconsument en diens mobiele telefoonnummer heeft uitgevoerd (in het kader van controleerbaarheid). 2. Registratie van verificatie van identiteit en het mobiele telefoonnummer (voor beide zijn de mogelijke waarden “uitgevoerd / niet uitgevoerd” en dient een datum te worden geregistreerd). Hieruit vloeit een registratie voor het gebruik van DigiD 2+ door de zorgconsument voort. 3. Opnieuw sturen van SMS in geval van vertraging of niet aankomen van de SMS. - Er dient te worden gewaarborgd dat een mobiele telefoonnummer slechts eenmaal gebruikt kan worden voor de koppeling aan een gebruikersaccount (1-op-1 koppeling van het gebruikersaccount aan het authenticatiemiddel). Mogelijk vergt dit opschoonacties binnen de DigiD-omgeving.	- Ontwikkelen van een scanapplicatie waarmee de verklaringen van de zorgconsumenten dat deze beschikken over een bepaald telefoonnummer worden gedigitaliseerd, verwerkt en geregistreerd binnen de DigiD-omgeving. In deze applicatie dienen de volgende aspecten te worden meegenomen: 1. Controle of het door de zorgconsument opgegeven mobiele telefoonnummer zo ook geregistreerd was voor DigiD niveau 2. 2. Registratie van verklaring van de zorgconsument betreffende het bezit van het mobiele telefoonnummer binnen de DigiD-omgeving. - Implementatie van processen voor de afhandeling van fouten in de verwerking van verklaringen gemaakt door de controle-instantie, de zorgconsument of de scanapplicatie. - Er dient te worden gewaarborgd dat een mobiele telefoonnummer slechts eenmaal gebruikt kan worden voor de koppeling aan een gebruikersaccount (1-op-1 koppeling van het gebruikersaccount aan het authenticatiemiddel). Mogelijk vergt dit opschoonacties binnen de DigiD-omgeving.	- Er dient een dient een applicatie te worden ontwikkeld waarmee de zorgconsument door middel van de wireless cardreader het reisdocument kan thuis uitlezen op de eigen PC. Dit kan eventueel door deze functionaliteit in te bouwen in de binnen de DigiD-omgeving bestaande webservices. In deze applicatie dienen de volgende aspecten te worden meegenomen: 1. Bieden van de mogelijkheid aan de zorgconsument om de benodigde gegevens uit de MRZ in te voeren. 2. Door middel van een challenge-response mechanisme het uitlezen van de chip op het reisdocument door de wireless card reader. 3. Registratie van initiële activering van RTDA door een zorgconsument binnen de DigiD-omgeving. 4. Registratie van gebruik van RTDA binnen DigiD - Er dienen supportprocessen te worden geïmplementeerd ten aanzien van fouten of vragen ten aanzien van het gebruik van RTDA. - Er dient een uitgifteproces voor de distributie van kaartlezers geïmplementeerd te worden.

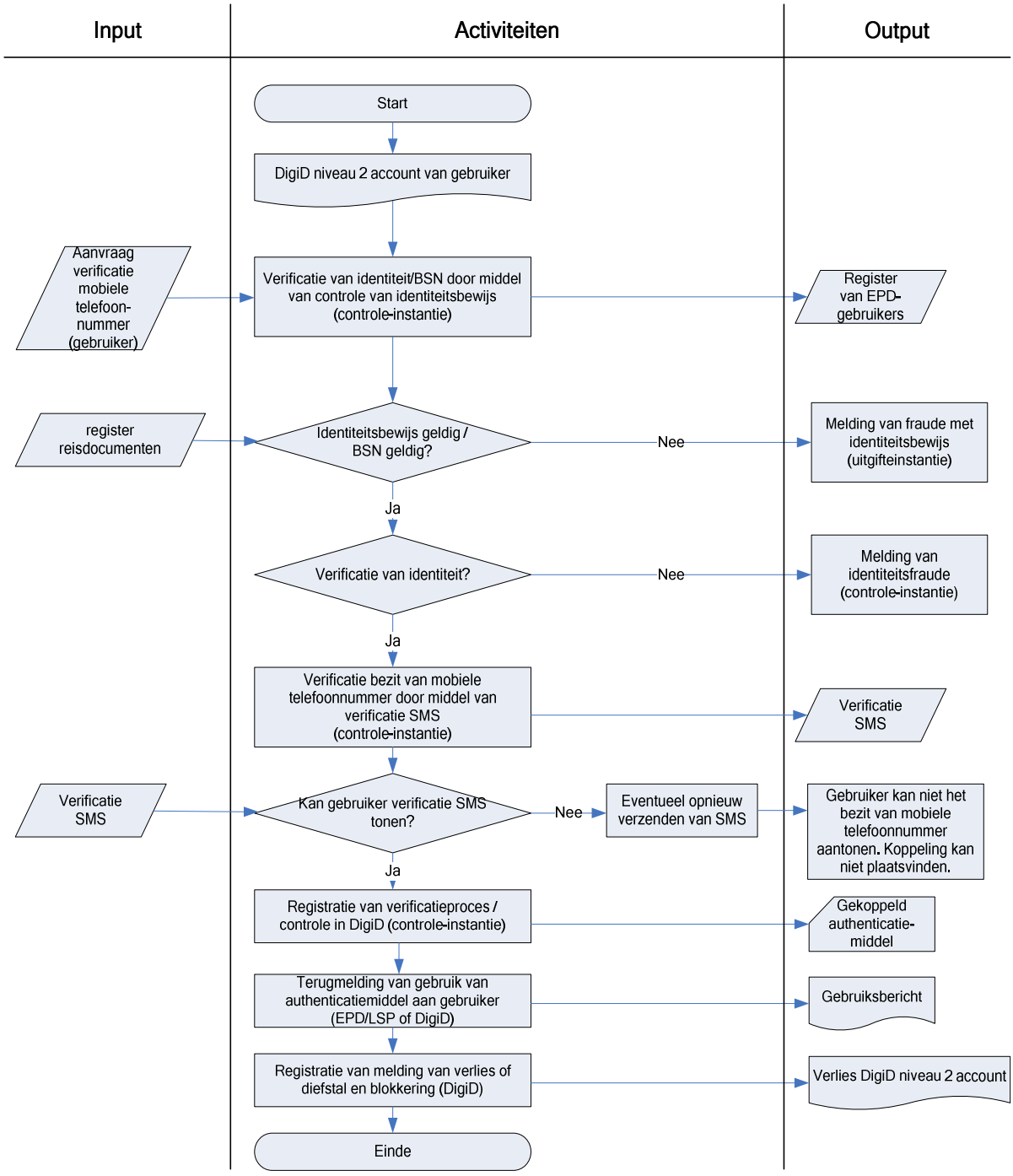
Ref	Kostenaspect	SMS+ (variant 1)	SMS+ (variant 2)	RTDA
K.5	Uitvoeringskosten voor DigiD organisatie	Bieden van ondersteuning aan controle-instantie ten aanzien van het gebruik van de verificatieapplicatie van DigiD.	Verwerking van verkregen verklaringen van zorgconsumenten over het bezit van het mobiele telefoonnummer. Hieronder valt ook de afhandeling van fouten en vragen ten aanzien van de ingevulde verklaringen (schrijffouten zorgconsument, scanfouten bij DigiD) en fouten bij de verzending van verklaringen van controle-instantie naar de DigiD-organisatie.	- Voeren van beheer van RTDA functionaliteit binnen de DigiD-omgeving. - Supportprocessen voor vragen en fouten omtrent het gebruik van RTDA door zorgconsumenten.
K.6	Kosten voor VWS	- Registratie van laatste moment van inloggen door de zorgconsument binnen het EPD. - Implementatie van DigiD als inlogmechanisme voor identificatie en authenticatie binnen EPD.	- Registratie van laatste moment van inloggen door de zorgconsument binnen het EPD. - Implementatie van DigiD als inlogmechanisme voor identificatie en authenticatie binnen EPD.	- Registratie van laatste moment van inloggen door de zorgconsument binnen het EPD. - Implementatie van DigiD als inlogmechanisme voor identificatie en authenticatie binnen EPD. - Eventuele kosten voor het versneld beschikbaar maken van een nieuw reisdocument aan alle zorgconsumenten.
		Tevens kan gedacht worden aan: - Kosten voor centrale regievoering (project- en programmamanagement) vanuit VWS voor de implementatie van toegang tot het EPD door de zorgconsumenten en van het te gebruiken authenticatiemiddel. Afstemming tussen VWS, de controle-instantie en de DigiD-organisatie is immers noodzakelijk. - Voorlichting aan alle zorgconsumenten in Nederland over de beschikbare functionaliteiten en de wijze waarop toegang tot het EPD voor zorgconsumenten beveiligd wordt. - Kosten voor toezicht op naleving van gemaakte afspraken ten aanzien van de uitvoering van het identificatie- en verificatieproces door controle-instanties.		

5.3 High-level procesbeschrijving verificatie- en uitgifteproces

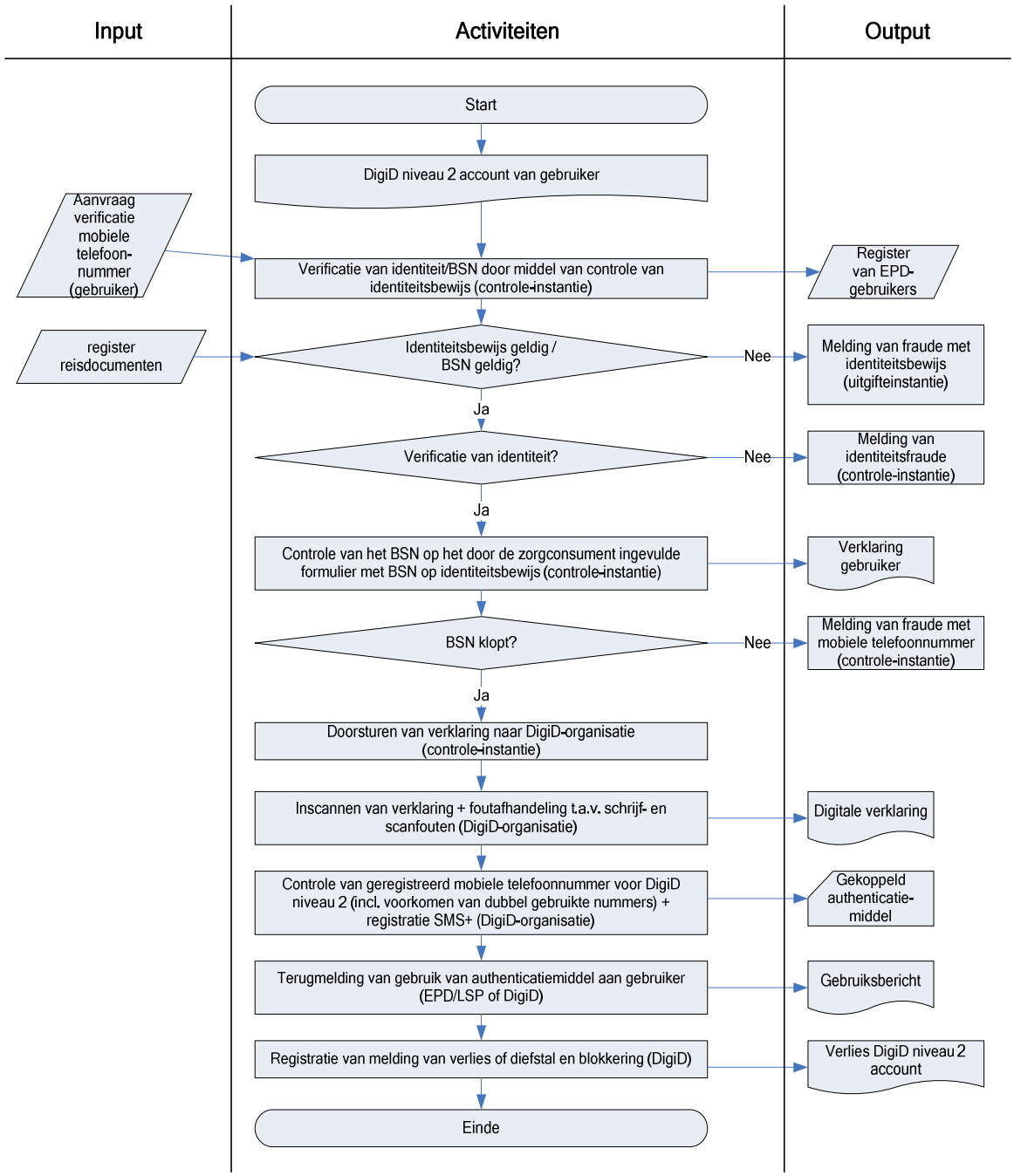
5.09 In de onderstaande procesbeschrijvingen zijn de inrichting van het verificatie- en uitgifteproces voor zowel de beide varianten van SMS+ als dat voor RTDA beschreven. Hierbij wordt opgemerkt dat het verificatie- en uitgifteproces zoals beschreven voor RTDA gelijk is aan het verificatie- en uitgifteproces voor het reisdocument zoals dit momenteel in Nederland is ingericht, echter dat het versneld kan worden uitgevoerd om iedereen voor 2011 van een reisdocument met RTDA te voorzien. Het verificatie- en uitgifteproces voor RTDA wordt per definitie uitgevoerd door de Nederlandse gemeenten.

5.10 Het beschreven verificatie- en uitgifteproces voor SMS+ bestaat momenteel nog niet en de beschrijving is daarom ook vooral suggestie voor de implementatie van het verificatie- en uitgifteproces voor dit authenticatiemiddel. Hoewel in dit hoofdstuk de eisen en wensen aan het verificatie- en uitgifteproces voor SMS+ zijn beschreven voor zowel de uitvoering van dit proces door de gemeenten als de apotheken, is de procesbeschrijving generiek beschreven omdat er in de uitvoering van het proces weinig tot geen verschillen bestaan tussen de twee verschillende controle-instanties.

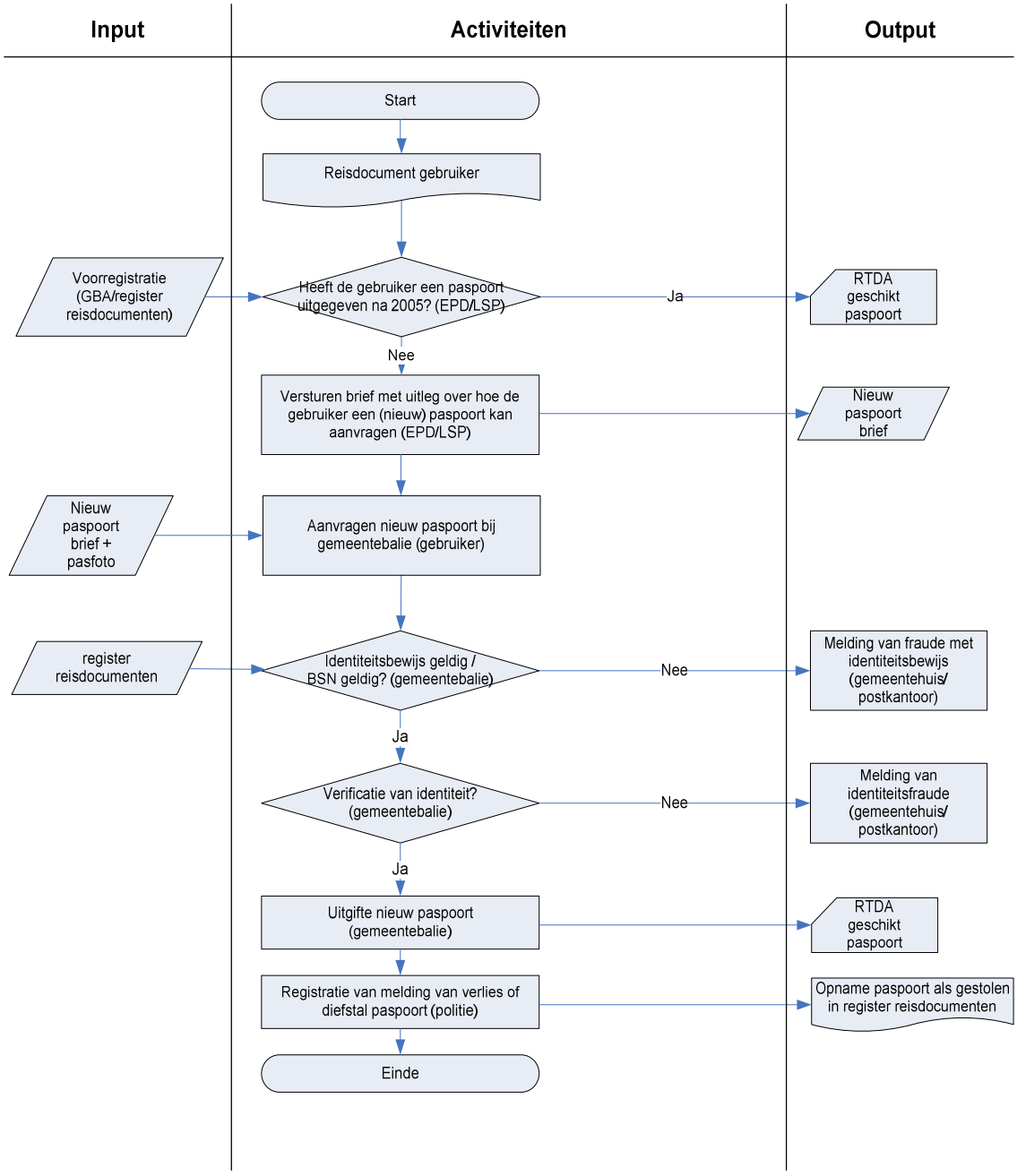
5.3.1 Suggestie voor verificatie- en uitgifteproces voor SMS+ (variant 1)



5.3.2 Suggestie voor verificatie- en uitgifteproces voor SMS+ (variant 2)



5.3.3 Versneld verificatie- en uitgifteproces voor reisdocumenten in Nederland



5.4 Analyse inrichting verificatie- en uitgifteproces

5.11 Deze paragraaf analyseert de uitkomsten van het hiervoor ingevulde referentiekader. De resultaten zijn gerangschikt naar:

- Inrichting van verificatie- en uitgifteproces zelf.
- Gebruikersvriendelijkheid.
- Kosten van implementatie.
- Technische aspecten.

5.4.1 Inrichting van verificatie- en uitgifteproces zelf

5.12 Ten aanzien van de inrichting van het verificatie- en uitgifteproces zelf blijkt dat voor wat betreft RTDA voor een groot gedeelte gesteund kan worden op bestaande processen terwijl deze voor zowel de varianten 1 als 2 van SMS+ nog geheel ingericht dienen te worden.

5.13 Het verificatie- en uitgifteproces voor RTDA is immers gelijk aan het al bestaande proces van uitgifte van identiteitsbewijzen door gemeenten. Tegelijkertijd veronderstelt RTDA wel de aanwezigheid van een kaartlezer. Dit heeft tot gevolg dat voor RTDA wel een uitgifteproces moet worden ontworpen en geïmplementeerd voor de distributie van kaartlezers. Naast de logistiek geldt dat ook ondersteuning zal moeten worden georganiseerd voor installatie en gebruik.

5.14 Voor SMS+ geldt dat het verificatieproces speciaal voor het gebruik van DigiD niveau 2 voor het EPD vormgegeven moet worden. Dit vergt vanzelfsprekend additionele inspanningen en middelen ten opzichte van het gebruik van RTDA. Denk hierbij ook aan de verificatieapplicatie die benodigd is voor SMS+ (variant 1) of de scanapplicatie voor SMS+ (variant 2).

5.15 Tevens kan het verificatieproces voor SMS+ zowel door het gemeentehuis als de apotheek worden uitgevoerd. Het gemeentehuis lijkt meer ervaring te hebben met identiteitscontrole maar dit is niet doorslaggevend. Een verantwoorde keuze tussen gemeentehuis en apotheek vergt de afweging van beschikbare middelen en van voorkeuren voor de inrichting van de bijbehorende processen.

5.16 Voor een keuze tussen deze twee instanties dient verder meegewogen te worden dat de Nederlandse gemeenten als publiekrechtelijke instanties beschikken over de middelen voor de verificatie van de identiteit van de zorgconsument. Daarnaast beschikken Nederlandse gemeenten over een actuele Gemeentelijke Basis Administratie (GBA). De beschikbaarheid van een actuele GBA kan van invloed zijn op de kwaliteit van terugkoppelgegevens.

5.4.2 Gebruiksvriendelijkheid

5.17 Enerzijds lijkt de gebruiksvriendelijkheid van het verificatie- en uitgifteproces voor RTDA groter te zijn dan in het geval van SMS+. Immers een gebruiker moet voor het laten activeren van SMS+ speciaal naar een controle-instantie terwijl in het geval van RTDA het verificatie- en uitgifteproces aansluit bij het huidige verificatie- en uitgifteproces voor reisdocumenten.

5.18 Zonder te stellen dat iedere zorgconsument binnen de doelgroep beschikt over een persoonlijk mobiel nummer, lijkt de *directe* beschikbaarheid van RTDA als authenticatiemiddel lager dan die van SMS+.

5.19 Het gebruiksgemak kan nog niet worden onderzocht. Geadviseerd wordt in de praktijkproef de diverse leeftijdsgroepen (ouderen, jongeren) nadrukkelijk te onderscheiden.

5.20 Tot slot geldt bij toepassing van SMS+ dat de waarde van de mobiele telefoon in het maatschappelijk verkeer toe zal nemen als deze in toenemende mate ook als authenticatiemiddel wordt gebruikt. De gevolgen van diefstal of vermissing van een mobiele telefoon nemen dan toe.

5.4.3 Kosten van implementatie

5.21 Ten aanzien van het kostenaspect geldt voor de onderscheiden alternatieven dat deze niet zonder additionele kosten (zowel initieel als structureel) ingevoerd kunnen worden.

5.22 Voor een zestal kostenaspecten zijn deze kosten kwalitatief beschreven. Een nadere bestudering van deze kostenaspecten door VWS zal uitsluitsel moeten geven over de vraag of de kosten voor een nieuw in te richten verificatie- en uitgifteproces opwegen tegen de kosten voor het vroegtijdig breed beschikbaar maken van RTDA als authenticatiemiddel.

5.4.4 Technische aspecten

5.23 Voor SMS+ lijkt het momenteel mogelijk om een mobiel telefoonnummer te gebruiken voor meerdere DigiD accounts. Hierdoor kan met SMS+ niet voldaan worden aan de eis van de 1-op-1 koppeling tussen gebruikersaccount en het authenticatiemiddel. Het gevolg hiervan is dat het authenticatiemiddel in voorkomende gevallen per definitie niet meer persoonlijk is waardoor de toegangsbeveiliging gereduceerd wordt tot de sterkte van een gebruikersnaam en wachtwoordcombinatie.

5.24 Voor SMS+ (zowel variant 1 als 2) en voor RTDA dient nieuwe functionaliteit te worden ontwikkeld. Voor SMS+ (variant 1) dient een verificatieappliatie voor de controle-instantie te worden ontwikkeld. Voor SMS+ (variant 2) dient een scanapplicatie te worden ontwikkeld voor

het verwerken van de verklaringen van zorgconsumenten. Tenslotte dient voor RTDA functionaliteit ontwikkeld te worden voor de communicatie tussen de chip op het reisdocument en de wireless cardreader ten behoeve van de authenticatie van de zorgconsument. Deze functionaliteit kan wellicht worden toegevoegd aan de reeds bestaande webservices binnen de DigiD-omgeving.

5.4.5 Advies inrichting verificatie- en uitgifteproces

5.25 Voor de uiteindelijke keuze door VWS voor één van de twee voorgestelde authenticatiemiddelen, wordt geadviseerd ook de gebruiksvriendelijkheid, de implementatiekosten, externe afhankelijkheden en technische aspecten mee te wegen. Nadere bestudering van deze aspecten aan de hand van een uit te voeren impactanalyse moet uitsluitsel geven over welke van de alternatieven de meest interessante optie blijkt voor VWS.

5.26 Wanneer gekozen wordt voor SMS+, dient VWS in samenspraak met BZK te waarborgen dat SMS+ als authenticatiemiddel 1-op-1 gekoppeld is met een DigiD account waardoor de vertrouwelijkheid van dit middel initieel vergroot wordt.

5.27 Tot slot geldt dat het verificatieproces voor SMS+ zowel door het gemeentehuis als de apotheek kan worden uitgevoerd. Het gemeentehuis lijkt meer ervaring te hebben met identiteitscontrole maar dit is niet doorslaggevend. Een verantwoorde keuze tussen gemeentehuis en apotheek vergt de afweging van beschikbare middelen en van voorkeuren voor de inrichting van de bijbehorende processen.

A Geraadpleegde documentatie

Document	Versie / datum
Masterplan Toegang voor de patiënt tot het elektronische patiëntendossier 2008/2009/2010	NICTIZ, versie 0.70, 16 juli 2008
Verslag Workshop Identificatie en Authenticatie rond Toegang Patiënt	Intern verslag, 20 mei 2008
Brief aan CBP inzake Identificatie en authenticatie bij toegang patiënt tot het EPD	Kenmerk MEVA/I&I-2865877, 7 augustus 2008
Antwoordbrief van het CBP	z2008-01021, 26 augustus 2008
Impact Analyse Toegang patiënt, Hedde van der Lugt	versie 1.0, juli 2008
Kamerstukken II	2007/08, 31 466
NEN - Nederlands Normalisatie-Instituut, Nederlandse norm NEN 7510 (nl). Medische Informatica – Informatiebeveiliging in de zorg – Algemeen.	Delft: Nederlands Normalisatie-Instituut, april 2004
NEN - Nederlands Normalisatie-Instituut, Nederlandse norm NEN 7512 (nl). Medische Informatica – Informatiebeveiliging in de zorg – Vertrouwensbasis voor gegevensuitwisseling.	Delft: Nederlands Normalisatie-Instituut, 2005
Kamerstukken II 2004/05, 29 800 hoofdstuk XVI, nr. 2, p. 135.	Vaststelling van de begrotingsstaten van het Ministerie van Volksgezondheid, Welzijn en Sport (XVI) voor het jaar 2005 (Memorie van Toelichting)
Wel, J.A. van der (eindred.), Informatiebeveiliging in de zorg. Schriftelijke praktijkleergang.	Eindhoven: International Management Forum, mei 2007
Brief minister Klink van Volksgezondheid, Welzijn en Sport aan de Voorzitter van de Tweede Kamer der Staten Generaal, d.d. 8 september 2008, inzake Invoering landelijk elektronisch patiëntendossier.	Kenmerk MEVA/ICT-2875251
H.J.J. Leenen, J.K.M. Gevers, J. Legemaate, Handboek Gezondheidsrecht. Deel I. Rechten van mensen in de gezondheidszorg.	Houten: Bohn Stafleu Van Loghum, 2007. Vijfde, geheel herziene druk
Karin Spaink, Medische geheimen. Risico's van het elektronisch patiëntendossier.	Nijgh & Van Ditmar / XS4ALL, 2005
Staatstoezicht op de Volksgezondheid, Inspectie voor de Gezondheidszorg, ICT in ziekenhuizen. Beveiliging van informatie nog onvoldoende voor een betrouwbare papierloze patiëntenzorg. Een inventariserend onderzoek bij twintig ziekenhuizen, uitgevoerd najaar 2003.	Den Haag, augustus 2004
"ICT levert gevaar op voor patiënt", de Volkskrant.	19 augustus 2004

Kamerstukken II.	1989/90, 21 561, nr. 3, p. 18
Europese Hof voor de Rechten van de Mens, van 7 juli 1989, in de zaak Gaskin, Series A, Publications of the Court.	Vol. 160 en NJCM 15-2 (1990)
J.M. Witmer, R.P. de Roode, Van wet naar praktijk. Implementatie van de Wgbo. Deel 4 Toegang tot patiëntengegevens. Utrecht.	KNMG 2004
Koninklijke Nederlandse Maatschappij ter Bevordering der Geneeskunst, Gedragsregels voor artsen.	Laatstelijk vastgesteld door de Algemene Vergadering van de federatie KNMG op 25 juni 2002
Blarkom, G.W. van , Borking, drs. J.J., Beveiliging van persoonsgegevens Registratiekamer.	april 2001. Achtergrondstudies en Verkenningen 23

B Geraadpleegde personen

Naam	Functie / Rol	Organisatie
Drs. M. Samson	Adviseur Informatica	Nederlandse Vereniging van Banken
Dr. M. Oostdijk	Onderzoeker	Telematica Instituut
Prof.dr. E. Verheul	Bijzonder Hoogleraar / Principal Manager	Radboud Universiteit Nijmegen / PwC Advisory
Drs. W. Kegel	Senior architect / Lead architect DigiD	GBO Overheid
Mw. Drs. L. Nijland	Beleidsmedewerker Informatie Infrastructuur Directie Innovatie- en Informatiebeleid Openbare Sector	Ministerie van BZK
Mw. B. Willems	-	KNMP

C Wet- en regelgeving: Toegang tot het EPD

C.1. Achtergrond

C.1.1 Recht op toegang tot het EPD

Als het aan minister Klink ligt, moeten eind 2009 alle zorgaanbieders aangesloten zijn op het landelijke Elektronisch Patiënten Dossier (EPD).[33] Het EPD is geen dossier dat alle gegevens van een zorgconsument bevat op een centrale plek. Feitelijk is het slechts een virtueel dossier. Een Landelijk Schakelpunt (LSP) functioneert als 'verkeerstoren' die veilige, landelijke elektronische uitwisseling van patiëntgegevens mogelijk maakt. Via het Landelijk Schakelpunt kunnen zorgverleners gegevens over hun zorgconsumenten opvragen bij andere ziekenhuizen, apotheken en huisartsen.

Bij het EPD zijn de volgende onderdelen van belang vanuit een oogpunt van beveiliging:

- Het identificeren van zorgconsumenten met het burgerservicenummer (BSN).
- Het identificeren en authenticeren van zorgverleners met de Unieke Zorgverlener Identificatie (UZI).
- Het veilig en betrouwbaar uitwisselen van informatie via het Landelijk Schakelpunt (LSP).
- Het authenticeren van zorgconsumenten voor het verlenen van toegang tot hun eigen gegevens in het EPD.

Het onderhavige advies beperkt zich tot het laatste.

Het recht op toegang tot de gegevens in het eigen medisch dossier is een reeds lang erkend recht voor zorgconsumenten. Dit recht heeft zich sinds het midden van de jaren zeventig vooral ontwikkeld als rechtersrecht.[34] Inmiddels is dit inzagerecht wettelijk vastgelegd in bijvoorbeeld art. 7:456 BW (Wgbo) en in art. 35 Wet bescherming persoonsgegevens (Wbp). In de Wet EPD (zie par. 2.1) is het recht op inzage geregeld in artikel 13e. Het inzagerecht van cliënten, door tussenkomst van de beheerder van het LSP, strekt zich volgens dat artikel uit over "de indexgegevens" en "de centrale gebruiksregistratie". Artikel 13a, tweede lid, van de Wet EPD voorziet in een nadere regeling bij AMvB waarin voorzieningen worden getroffen waarmee cliënten rechtstreeks toegang kunnen krijgen tot het LSP. Volgens de memorie van toelichting wordt daarbij gedacht aan "de eNik of een toegangsmiddel met een vergelijkbaar beveiligingsniveau".[35]
De toegang voor zorgconsumenten tot hun eigen gegevens in het EPD dient op een passende wijze te geschieden om misbruik te voorkomen en te garanderen dat de juiste persoon toegang krijgt tot de juiste gegevens. Het belang van een goede informatiebeveiliging in de zorg wordt hieronder geïllustreerd.

---

[33] Brief minister Klink van Volksgezondheid, Welzijn en Sport aan de Voorzitter van de Tweede Kamer der Staten Generaal, d.d. 8 september 2008, inzake Invoering landelijk elektronisch patiëntendossier. Kenmerk MEVA/ICT-2875251.

[34] H.J.J. Leenen, J.K.M. Gevers, J. Legemaate, *Handboek Gezondheidsrecht. Deel I. Rechten van mensen in de gezondheidszorg*. Houten: Bohn Stafleu Van Loghum, 2007. Vijfde, geheel herziene druk, p. 260.

[35] *Kamerstukken II*, 2007/08, 31 466, nr. 3, p. 24-25.

C.1.2 Kwetsbaarheid van elektronische patiëntendossiers

"Medische dossiers niet goed beveiligd", kopte NRC Handelsblad van zaterdag 3 en zondag 4 september 2005. Tijdens een onderzoek, dat werd verricht in opdracht van publiciste Karin Spaink, wist een aantal specialisten van drie internetbeveiligingsbedrijven zich binnen enkele dagen toegang te verschaffen tot de elektronische dossiers van 1,2 miljoen zorgconsumenten van twee Nederlandse ziekenhuizen. De ziekenhuizen gaven hun medewerking aan het onderzoek, onder de voorwaarde dat zij anoniem zouden blijven. De onderzoekers kregen onder andere toegang tot de namen van de zorgconsumenten, hun polisnummers, de ziekten waaraan zij leden en hun medische voorgeschiedenis. De gegevens in de dossiers konden worden gekopieerd en gewijzigd. Karin Spaink publiceerde in 2005 tevens haar boekje "Medische geheimen", over risico's van het elektronisch patiëntendossier.[36] Daarin waarschuwt zij ervoor dat het elektronisch patiëntendossier volgens haar - in tegenstelling tot de gedachte die overheerst bij de politiek - niet het antwoord is op het brede scala aan problemen in de gezondheidszorg. Zij wijst er bovendien op dat de invoering van elektronische patiëntendossiers zelf ook weer nieuwe problemen en risico's met zich meebrengt. Een van die risico's is dat artsen mogelijk meer gefocust zullen raken op de informatie in het dossier (die fouten kan bevatten of onvolledig kan zijn) en minder op het doen van lichamelijke onderzoeken bij de zorgconsument zelf. Voorts wijst zij op het gevaar dat landelijke geautomatiseerde patiëntendossiers interessant kunnen zijn voor spionage en diefstal. Met een beetje creativiteit is het voorstelbaar dat terroristen de toegang tot elektronische patiëntendossiers van belangrijke Nederlandse politici zouden kunnen misbruiken door hun medische gegevens daarin te wijzigen en aldus hun gezondheid in gevaar te brengen.

In de conclusie van haar boekje wijst Spaink op het belang van draagvlak voor het elektronisch patiëntendossier bij de gebruikers. Succes lijkt eerder verzekerd wanneer de gebruikers zelf betrokken zijn bij het oplossen van een praktijkprobleem, dan wanneer de overheid van bovenaf een standaard wil opleggen. In het verlengde daarvan kan met het oog op de informatiebeveiliging in de zorg worden verdedigd dat het ook daarbij belangrijk is om de gebruikers in een vroeg stadium te betrekken bij nieuwe ontwikkelingen.

C.1.3 ICT gevaar voor zorgconsument?

In augustus 2004 publiceerde de Inspectie voor de Gezondheidszorg (IGZ) het rapport "ICT in ziekenhuizen".[37] In het rapport doet de IGZ verslag van een inventariserend onderzoek onder twintig ziekenhuizen over de invulling van verantwoorde toepassing van ICT. Ondanks dat bij steeds meer processen ICT het papier vervangt, is er nog onvoldoende aandacht van de ziekenhuizen voor de risico's van ICT. De IGZ concludeerde dan ook dat de beveiliging van informatie in ziekenhuizen nog onvoldoende is voor een betrouwbare papierloze patiëntenzorg. De IGZ ging nog een stap verder door te concluderen dat zorgconsumenten zelfs fysiek gevaar lopen

[36] Karin Spaink, Medische geheimen. Risico's van het elektronisch patiëntendossier. Nijgh & Van Ditmar / XS4ALL, 2005.

[37] Staatstoezicht op de Volksgezondheid, Inspectie voor de Gezondheidszorg, ICT in ziekenhuizen. Beveiliging van informatie nog onvoldoende voor een betrouwbare papierloze patiëntenzorg. Een inventariserend onderzoek bij twintig ziekenhuizen, uitgevoerd najaar 2003. Den Haag, augustus 2004.

als gevolg van de gebrekkige aandacht voor informatiebeveiliging in de zorg en het onjuist en ondeskundig gebruik van ICT.[38]

Over informatiebeveiliging (hoofdstuk 3.14) concludeert de Inspectie:
"Het informatiebeveiligingsbeleid in ziekenhuizen kan veel beter nu er een norm voor de informatiebeveiliging in de zorg is geformuleerd. Ziekenhuizen moeten daarom alle deze norm volgen."

De conclusies over privacybescherming (hoofdstuk 3.15) luiden:
"De bescherming van de privacy van de patiënt in ziekenhuizen is met het gebruik van ICT niet in orde. Er bestaan teveel mogelijkheden dat onbevoegden kennis nemen van patiënteninformatie. De vigerende privacywetgeving moet daarom in de ziekenhuizen beter geïmplementeerd worden dan nu het geval is."

De IGZ kondigde aan in de toekomst vaker en op systematische wijze aandacht te schenken aan het gebruik van ICT in ziekenhuizen en in andere zorginstellingen. In het bijzonder zal worden nagegaan of die instellingen wel voldoen aan de NEN norm voor informatiebeveiliging in de zorg: NEN norm 7510.

[38] Zie ook "ICT levert gevaar op voor patiënt", de Volkskrant, 19 augustus 2004.

C.2. Wet- en regelgeving over informatiebeveiliging

C.2.1 Wet algemene bepalingen burgerservicenummer (Wabb)

Op 26 november 2007 is de Wet algemene bepalingen burgerservicenummer (Wabb) in werking getreden. Deze wet introduceert het BSN-stelsel, dat bestaat uit voorzieningen waarmee een BSN kan worden aangemaakt, waarmee de nummers kunnen worden beheerd en waarmee het gebruik ervan kan worden ondersteund. Het BSN is gelijk aan het sociaal-fiscaalnummer. Het verschil zit hem in het bereik en stringenter beheer ervan en de wijze waarop wettelijk is vastgelegd wat er mag met het BSN. De bedoelde 'voorzieningen' zijn een nummergenerator en een nummerregister waarin het BSN met een aantal administratieve gegevens wordt vastgelegd. Het nummerregister wordt geraadpleegd voor de verificatie van een BSN.

De Wabb regelt dat alle overheidsorganen het BSN kunnen gebruiken voor de uitvoering van hun publiekrechtelijke taken. Daarnaast kunnen bij of krachtens de wet ook andere dan overheidsorganen worden aangewezen die het BSN mogen gebruiken, zoals zorgaanbieders, onderwijsinstellingen en werkgevers. Beide categorieën worden 'gebruiker' genoemd. Tenzij bij wet iets anders is voorgeschreven, zijn 'gebruikers' verplicht om het BSN als identificerend nummer te gebruiken bij de uitwisseling van persoonsgegevens. Wanneer een gebruiker intern een ander persoonsnummer hanteert, dan moet dat nummer aan het BSN gerelateerd kunnen worden, bijvoorbeeld door een koppeltabel. Door transparantie, bijvoorbeeld via de 'Landkaart' die aangeeft wie gebruikers zijn van het BSN, tracht de Wabb vertrouwen te wekken in de wijze waarop de overheid met de persoonsgegevens van burgers omgaat.

De categorie 'gebruikers' in de zin van de Wabb is beperkt tot degenen die bij of krachtens de wet verplicht zijn het BSN te gebruiken. In de memorie van toelichting wordt dat als volgt uitgelegd: *"Het gaat daarbij met name om de toegang tot de faciliteiten van het BSN-stelsel, en hetgeen met die toegang samenhangt. Die toegang is beperkt tot (enerzijds) overheidsorganen en (anderzijds) anderen dan overheidsorganen, die verplicht zijn het burgerservicenummer te gebruiken. Hierbij speelt onder meer de beheersbaarheid van het stelsel een rol. In het onderhavige voorstel van wet wordt het begrip «gebruiker» derhalve voornamelijk gebruiktin de context van de faciliteiten die aan de hier bedoelde gebruikers ter beschikking staan ten behoeve van de verificatie van burgerservicenummers."*

Deze beperking heeft tot gevolg dat de burger zelf niet als 'gebruiker' van het BSN kan worden beschouwd. Een burger valt niet onder de categorie 'overheidsorgaan', waardoor niet de Wabb maar de Wbp van toepassing zou zijn. Daarmee valt de burger onder de beperking van art. 24 Wbp dat het "slechts" toelaat om wettelijk voorgeschreven identificatienummers (zoals het BSN) te gebruiken ter uitvoering van de betreffende wet of voor doeleinden bij de wet bepaald. Dat burgers voorzichtig dienen om te springen met het BSN (en bijvoorbeeld niet zelf op internet moeten zetten) volgt ook uit de memorie van toelichting bij art. 24 Wbp, die vermeldt dat persoonsnummers

de koppeling van verschillende bestanden aanzienlijk vergemakkelijken en daarmee een extra bedreiging voor de persoonlijke levenssfeer vormen. Deze dreiging is toegenomen, aldus de memorie van toelichting, sinds het sofinummer (thans BSN) mede door de inwerkingtreding van de Wet op de identificatieplicht, ook ter kennis van particulieren kan komen.

De beheerder van het LSP is wel gebruiker in de zin van de Wabb. Dat betekent dat de beheerder van het LSP verplicht is de identiteit en het BSN van een cliënt te controleren alvorens deze inzage te verlenen in de indexgegevens of de centrale gebruiksregistratie of alvorens te voldoen aan een verzoek tot afscherming of vernietiging van de indexgegevens.

C.2.2 Wet gebruik burgerservicenummer in de zorg (Wbsn-z)

Een aparte wet, de Wet gebruik burgerservicenummer in de zorg (Wbsn-z) regelt het gebruik van het BSN in de gezondheidszorg. Behalve de overheid moet ook de zorgsector het BSN gebruiken bij het uitwisselen van gegevens met andere zorgaanbieders, indicatieorganen en in het declaratieverkeer. Alleen deze zorgaanbieders, indicatieorganen en zorgverzekeraars mogen (en moeten) het BSN gebruiken. Zorgverzekeraars waren reeds verplicht om het sofinummer te gebruiken op grond van de Zorgverzekeringswet en de AWBZ. De Wbsn-z vervangt dit gebruik van het sofinummer door gebruik van het BSN waarbij tegelijkertijd de waarborgen voor het gebruik van dat nummer worden versterkt.

Zorgaanbieders en indicatieorganen mogen het BSN gebruiken vanaf 1 juni 2008. Een jaar daarna is gebruik van het BSN ook voor hen verplicht. Het BSN moet in de zorgsector een eind maken aan de verschillende persoonsnummers die zorgaanbieders, indicatieorganen en zorgverzekeraars nu nog gebruiken. De Wbsn-z regelt onder meer dat gegevens over een cliënt worden bewaard en uitgewisseld door middel van het BSN. De wet beoogt de betrouwbaarheid te waarborgen door te regelen dat een cliënt moet worden geïdentificeerd door middel van een wettelijk identificatiemiddel als bedoeld in art. 1 WID en diens BSN moet worden gecontroleerd (dat laatste is niet nodig als het BSN afkomstig is van iemand die het nummer al heeft moeten controleren). Hierdoor moet gegarandeerd kunnen worden dat de persoonsgegevens op de desbetreffende cliënt betrekking hebben.

In par. 1.26 is reeds ingegaan op de cliënten zonder BSN. In de memorie van toelichting bij de Wbsn-z wordt bevestigd dat er situaties zijn waarin het BSN of de identiteit van een cliënt niet kan worden vastgesteld. Om daaraan tegemoet te komen bevat art. 11 Wbsn-z de mogelijkheid om bij AMvB nadere regels te stellen voor zorgaanbieders die gegevens moeten verwerken over cliënten van wie het vaststellen van de identiteit of het BSN onmogelijk blijkt of een onevenredige inspanning kost. Hoewel de memorie van toelichting bij de Wbsn-z niet ingaat op de toegang door cliënten tot de eigen persoonsgegevens, zou wellicht via dezelfde AMvB nadere regels kunnen worden gesteld voor de toegang door cliënten zonder BSN.

C.2.3 Wet EPD[39]

C.2.3.1 Algemeen

Op 20 mei 2008 is het voorstel voor de Wet EPD ingediend bij de Tweede Kamer. Deze wet bevat de randvoorwaarden voor een veilig en betrouwbaar gebruik van het landelijke EPD.
De Wet EPD regelt de volgende aspecten:

- De (verplichte) aansluiting van zorgaanbieders op het Landelijk Schakelpunt.
- Het elektronisch beschikbaar stellen van patiëntgegevens via het Landelijk Schakelpunt.
- De gegevens op veilige en betrouwbare wijze via het Landelijk Schakelpunt uitwisselen.

De verplichte aansluiting van zorgaanbieders op het Landelijk Schakelpunt moet garanderen dat de zorgaanbieders hun systemen aanpassen aan het landelijk EPD-systeem. Daarnaast bevat de Wet EPD juridische waarborgen om te zorgen dat de gegevens veilig en betrouwbaar via het Landelijk Schakelpunt worden uitgewisseld. Daarmee moet worden voorkomen dat patiëntgegevens die door zorgaanbieders zijn aangeleverd - en die daar zelf verantwoordelijk voor blijven - in handen van onbevoegden vallen.

De Wet EPD, die zal worden aangehaald als Kaderwet elektronische zorginformatieuitwisseling, wordt dus een kaderwet en zal sober van opzet zijn. De minister heeft laten weten dat de Wet EPD niet zal zijn bedoeld om de wettelijke bepaling van het medisch beroepsgeheim te doorbreken als gevolg van meer ICT-verkeer, maar dat deze juist zal aangeven wat de waarborgen zijn voor het medisch beroepsgeheim in verband met de mogelijkheden van ICT.

Voor zover relevant voor de toegang van zorgconsumenten (in de wet “cliënten” genoemd) zijn de volgende bepalingen uit de Wet EPD van belang.

C.2.3.2 Landelijk Schakel Punt (artikel 13a)

Er is een Landelijk Schakel Punt (LSP), dat wordt beheerd door NICTIZ, en dat een landelijke verwijsindex bevat met “indexgegevens” die desgewenst door de cliënt mogen worden ingezien.
De indexgegevens bestaan uit:

1. Een vermelding dat een zorgaanbieder beschikt over patiëntgegevens van een cliënt.
2. Het burgerservicenummer van de cliënt.
3. Het UZI-abonneenummer en andere gegevens of persoonsgegevens van de zorgaanbieder die de vermelding heeft opgenomen.
4. Het UZI-nummer, de titels en andere persoonsgegevens van de beroepsbeoefenaar die de vermelding heeft opgenomen.
5. De categorie van de patiëntgegevens.
6. Gegevens betreffende de vermelding.

De beheerder van het LSP (NICTIZ) houdt ook een centrale gebruiksregistratie bij. Daarin wordt

[39] Wijziging van de Wet gebruik burgerservicenummer in de zorg in verband met de elektronische informatieuitwisseling in de zorg. Kamerstukken II, 2007/08, 31 466. Hierna te noemen: Wet EPD.

het gegevensverkeer (opvragingen door zorgaanbieders) geregistreerd.

Naast voorzieningen voor zorgaanbieders, kan bij AmvB worden bepaald dat het LSP tevens voorzieningen dient te bevatten waarmee een cliënt:

a. Zijn elektronisch patiëntendossier elektronisch kan opvragen en raadplegen;
b. De hem betreffende centrale gebruiksregistratie kan opvragen en raadplegen;
c. Zijn indexgegevens volledig kan afschermen voor het opvragen en raadplegen door een zorgaanbieder of een categorie van zorgaanbieders.

Medewerkers van de beheerder van het LSP (NICTIZ) hebben een geheimhoudingsplicht (lid 5).

C.2.3.3 Recht op inzage, afschermen, vernietigen, opvragen, raadplegen (artikel 13e)

De beheerder van het LSP (NICTIZ) is verplicht op verzoek van de cliënt:

1. De cliënt inzage te verlenen in de indexgegevens van de cliënt en de centrale gebruiksregistratie met betrekking tot de cliënt (art. 13e, lid 1).
2. De indexgegevens van de cliënt volledig af te schermen voor het opvragen en raadplegen door een zorgaanbieder of een categorie van zorgaanbieders (art. 13e, lid 2 sub a).
3. Gehele of gedeeltelijke vernietiging van de indexgegevens van de cliënt (art. 13e, lid 1 sub b).

Bij de realisatie van deze rechten van de cliënt is de beheerder van het LSP verplicht de identiteit van de cliënt en diens BSN op een deugdelijke wijze vast te stellen (art. 13e, lid 3).

Het LSP zal – op grond van een in art. 13a, tweede lid van het wetsvoorstel aangekondigde algemene maatregel van bestuur – tevens voorzieningen aanbieden waarmee een cliënt zelf:

a. Zijn elektronisch patiëntendossier elektronisch kan opvragen en raadplegen.
b. De hem betreffende centrale gebruiksregistratie kan opvragen en raadplegen.
c. Zijn indexgegevens volledig kan afschermen voor het opvragen en raadplegen door een zorgaanbieder of een categorie van zorgaanbieders (art. 13e, lid 5).

C.2.3.4 Recht op informatie, inzage, vernietiging via de zorgaanbieder (artikel 13g)

Een cliënt heeft het recht om de zorgaanbieder te verzoeken om algemene informatie over het EPD (lid 1). Daarnaast mag een cliënt de zorgaanbieder verzoeken om inzage in de door deze zorgaanbieder in het EPD van de cliënt opgenomen gegevens en in de decentrale gebruiksregistratie met betrekking tot die cliënt (lid 3). Een cliënt heeft voorts het recht om de zorgaanbieder te verzoeken om diens door de zorgaanbieder in het EPD vastgelegde gegevens geheel of gedeeltelijk te vernietigen (lid 4).

C.2.3.5 Beveiligingseisen (artikel 13i)

Bij of krachtens een AmvB kunnen nadere eisen worden gesteld aan de gegevensverwerkingen bedoeld in de artikelen 13d tot en met 13h, met name met betrekking tot de beveiliging van persoonsgegevens, bijvoorbeeld door middel van een doorlopende controle op gegevensverwerkingen, de beschikbaarheid van persoonsgegevens en de inrichting en het beheer van de bij de gegevensverwerkingen te gebruiken zorginformatiesystemen. Die eisen zijn er op

gericht om te voorzien in passende waarborgen ter bescherming van de persoonlijke levenssfeer van de cliënt en om te waarborgen dat uitsluitend gegevens over één cliënt in een EPD worden verwerkt (lid 3).

C.2.3.6 Uitoefenen rechten via Klantenloket (artikel 13j)

Voor een aantal van zijn rechten kan een cliënt ook terecht bij het Klantenloket. Het Klantenloket verschaft op verzoek aan eenieder algemene informatie over het EPD (lid 1, sub a). Voorts helpt het Klantenloket cliënten bij het verschaffen van inzage in de indexgegevens en de hem betreffende centrale gebruiksregistratie. Tevens helpt het Klantenloket cliënten bij de afscherming van diens indexgegevens tegen opvragen door een zorgaanbieder of een categorie zorgaanbieders en bij de geheel of gedeeltelijke vernietiging van diens indexgegevens (lid 1, sub b).

Een cliënt heeft bovendien het recht om bij het Klantenloket bezwaar te maken tegen de verwerking van diens indexgegevens of patiëntgegevens in het EPD (lid 1, sub c). Tevens biedt het Klantenloket een cliënt ondersteuning bij het herstellen of beëindigen van verwerkingen van persoonsgegevens die niet voldoen aan een wettelijk voorschrift voor het EPD.
Medewerkers van het Klantenloket hebben een geheimhoudingsplicht (lid 6).

C.2.4 Wet geneeskundige behandelingsovereenkomst

C.2.4.1 Algemeen

De Wet op de geneeskundige behandelingsovereenkomst (Wgbo) is geen zelfstandige wet, maar is een onderdeel van het Burgerlijk Wetboek (BW). De Wgbo is te vinden in boek 7, titel 7, afdeling 5 van het BW en regelt de juridische relatie tussen een zorgverlener en degene die de opdracht geeft tot een geneeskundige behandeling (zorgconsument of een derde). De Wgbo bevat ook een aantal wettelijke voorschriften ter bescherming van de privacy van zorgconsumenten. De privacy van zorgconsumenten bestaat voor een belangrijk deel uit de vertrouwelijke omgang met patiëntengegevens. Informatiebeveiliging kan die vertrouwelijkheid bevorderen.
Vooropgesteld moet worden dat de regeling van de overeenkomst inzake de geneeskundige behandeling in het BW niet primair is gericht op bescherming van de privacy van zorgconsumenten. Deze regeling is vooral bedoeld om de privaatrechtelijke verhouding tussen zorgconsumenten en zorgverleners in te vullen, ter verbetering van de materiële rechtspositie van zorgconsumenten. De persoonlijke levenssfeer in verband met medische persoonsgegevens is daarvan slechts een onderdeel. In het BW zijn daarover wel enkele wetsbepalingen opgenomen. Deze aan privacy gerelateerde bepalingen vormen een aanvulling op de bepalingen in de Wet bescherming persoonsgegevens (Wbp). De Wbp bepalingen en de BW bepalingen zijn beide - naast elkaar - van toepassing op de verwerking van medische persoonsgegevens.

C.2.4.2 Recht op inzage en afschrift (artikel 7:456 BW)

In beginsel dient de zorgverlener aan de zorgconsument die dat wenst, zonder tussenkomst van

derden, inzage te verlenen in en afschrift te verstrekken van de bescheiden uit het medisch dossier van die zorgconsument. Er bestaat slechts één uitzondering op deze regel. Daarvan is sprake wanneer de persoonlijke levenssfeer van een ander erdoor zou worden geschaad. Het belang van die derde moet dan wel een overwegend karakter hebben[40]. Het recht op inzage en afschrift strekt zich overigens niet uit tot de persoonlijke werkaantekeningen van de zorgverlener, daar deze geacht worden geen deel uit te maken van het medisch dossier.

De regels in Boek 7 van het BW, inzake de geneeskundige behandeling, hebben betrekking op alle soorten van gegevensverzamelingen: al dan niet geautomatiseerd of gestructureerd. Wanneer het niet-systematisch toegankelijke verzamelingen betreft, kan het meer tijd kosten om de gegevens waarom is verzocht terug te vinden. Volgens de *Modelrichtlijn toegang tot patiëntengegevens* moet een zorgverlener zo snel mogelijk en in ieder geval binnen twee tot vier weken gehoor geven aan het verzoek van de zorgconsument om toegang tot diens eigen gegevens.[41]

Voor de verstrekking van een afschrift mag de zorgverlener een “redelijke vergoeding” in rekening brengen (art. 7:456 BW). Wat een redelijke vergoeding is, kan worden afgeleid uit het Wbp-Kostenvergoedingenbesluit.[42] Bij de redactie van artikel 2 en 3 van het Wbp - Kostenvergoedingenbesluit is aansluiting gezocht bij artikel 7:456 BW.

Voor een afschrift van gegevens uit een dossier mag € 0,23 per pagina in rekening worden gebracht, tot een maximum van € 4,50 per bericht.
Voor een afschrift op een andere gegevensdrager dan papier, bijvoorbeeld op diskette, per e-mail of een röntgenfoto, mag een redelijke vergoeding (kostprijs) worden gevraagd, tot een maximum van € 4,50.
Voor een afschrift dat uit meer dan honderd pagina’s bestaat, mag een vergoeding worden gevraagd van maximaal € 22,50.
Voor een afschrift uit een moeilijk toegankelijke registratie mag ook maximaal € 22,50 worden gevraagd. Men moet hierbij denken aan gevallen waarin het technisch gezien moeilijk is om een afschrift te verstrekken, bijvoorbeeld van een microfilm.

Volgens een uitspraak van de Registratiekamer van 25 juli 2001 (z2001-0979), is het vragen om een vergoeding voor administratiekosten alleen toegestaan in situaties waarin geen sprake is van een verzoek om een afschrift in de zin van artikel 39 Wbp of artikel 7:456 BW, al dan niet via een bemiddelende organisatie.

---

[40] *Kamerstukken II*, 1989/90, 21 561, nr. 3, p. 18, alwaar tevens wordt gewezen op de uitspraak van het Europese Hof voor de Rechten van de Mens, van 7 juli 1989, in de zaak Gaskin, *Series A, Publications of the Court*, Vol. 160 en NJCM 15-2 (1990).

[41] J.M. Witmer, R.P. de Roode, *Van wet naar praktijk. Implementatie van de Wgbo. Deel 4 Toegang tot patiëntengegevens*. Utrecht: KNMG 2004, Bijlage 1.

[42] Besluit van 13 juni 2001 tot vaststelling van de vergoeding van de kosten als bedoeld in de artikelen 39 en 40 van de Wet bescherming persoonsgegevens (Besluit kostenvergoeding rechten betrokkene Wbp), *Stb.* 2001, 305.

Een verzoek tot inzage of afschrift dat op de Wbp is gebaseerd, dient te worden gericht aan de verantwoordelijke voor de gegevensverwerking. In de gezondheidszorg zal de inzage meestal verlopen via de zorgverlener die de betreffende gegevens heeft aangeleverd. Op grond van het BW kan een zorgconsument zich met een beroep op het inzagerecht dus rechtstreeks wenden tot de zorgverlener met wie hij een behandelingsovereenkomst heeft gesloten. Via deze zorgverlener ('zorgaanbieder') kan de cliënt op grond van art. 13g, lid3 van de Wet EPD inzage krijgen in de in het EPD van de cliënt opgenomen gegevens en in de decentrale gebruiksregistratie met betrekking tot de cliënt. Volgens art. 13e, lid 1 van de Wet EPD zou de cliënt ook inzage kunnen krijgen door tussenkomst van de beheerder van het LSP voor wat betreft de inzage in de indexgegevens van de cliënt en de centrale gebruiksregistratie met betrekking tot de cliënt. Inzage in de indexgegevens en in de centrale gebruiksregistratie is ook mogelijk door tussenkomst van het Klantenloket (art. 13j, lid 1 van de Wet EPD).

C.2.4.3 Verstrekking van gegevens aan derden (artikel 7:457 BW)

In beginsel mag de zorgverlener aan anderen dan de zorgconsument geen informatie over die zorgconsument verstrekken noch inzage in of afschrift van de in diens medisch dossier opgenomen bescheiden.

Dit vloeit voort uit het medisch beroepsgeheim van de zorgverlener. Het medisch beroepsgeheim is van oudsher van invloed geweest op de omgang met medische persoonsgegevens. Wij vinden dit geheim reeds terug in de Eed van Hippocrates. Ook in de Gedragsregels voor artsen[43] treffen we het beroepsgeheim aan. Artikel 88 van de Wet beroepen in de Individuele Gezondheidszorg (BIG)[44] bevat voor geregistreerde en voor niet geregistreerde beroepsbeoefenaren een wettelijke geheimhoudingsplicht. Degenen die wel betrokken zijn bij de behandeling van de zorgconsument, maar zich niet kunnen beroepen op een wettelijk erkende geheimhoudingsplicht - zoals medische studenten, secretaressen, en dergelijke - hebben een afgeleid beroepsgeheim[45]. De hoofdregel in de Wgbo (art. 7:457 BW) houdt in, dat de geheimhoudingsplicht van een zorgverlener, behoudens in bij of krachtens de wet geregelde gevallen of in noodsituaties, alleen met toestemming van de zorgconsument kan worden opgeheven.

De zwijgplicht voor een zorgverlener is echter niet absoluut, maar kan in een aantal gevallen worden doorbroken:

- Met toestemming van de zorgconsument.
- Als gegevens worden verstrekt aan degenen die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst (mits die verstrekking noodzakelijk is).
- Als gegevens worden verstrekt aan de vervanger of waarnemer van de zorgverlener (mits die verstrekking noodzakelijk is).

---

[43] Koninklijke Nederlandse Maatschappij ter Bevordering der Geneeskunst, *Gedragsregels voor artsen.* Laatstelijk vastgesteld door de Algemene Vergadering van de federatie KNMG op 25 juni 2002, artikel II.15.

[44] Wet van 11 november 1993, houdende regelen inzake beroepen op het gebied van de individuele gezondheidszorg. *Stb.* 655.

[45] H.J.J. Leenen, *Handboek gezondheidsrecht. Deel I. Rechten van mensen in de gezondheidszorg.* Houten/Diegem: Bohn Stafleu Van Loghum, 2000, vierde geheel herziene druk, p. 224.

- Als gegevens worden verstrekt aan de vertegenwoordiger van de zorgconsument.
- Als de verstrekking wettelijk verplicht is.
- Als gegevens worden verstrekt op basis van een conflict van plichten.

Doet een van deze omstandigheden zich voor, dan mogen gegevens aan derden worden verstrekt voorzover althans de persoonlijke levenssfeer van een ander daar niet door wordt geschaad.
De rol van informatiebeveiliging in de zorg is te waarborgen dat het beroepsgeheim bijvoorbeeld niet door technische gebreken wordt doorbroken. Ook is aandacht nodig bij organisatorische aanpassingen. Zo zijn een aantal jaren geleden de meldkamers van politie brandweer en ambulance geïntegreerd. Als nu iemand 112 belt voor een ambulance, dan kan het in bepaalde omstandigheden gebeuren dat de telefonist gelijk maar een politieagent meestuurt.

C.2.5 Wet bescherming persoonsgegevens

C.2.5.1 Algemeen

De Wet bescherming persoonsgegevens (Wbp) is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens en op handmatig beschikbare gegevens, voorzover deze in een bestand voorkomen of bestemd zijn om daarin te worden opgenomen (art. 2, lid 1). Voldoende duidelijk is dat het EPD een geautomatiseerde verwerking van persoonsgegevens is en dat de Wbp daarop van toepassing is.

De Wbp stelt een aantal voorwaarden waaraan moet worden voldaan om rechtmatig persoonsgegevens te verwerken. Een van die voorwaarden is dat de ‘verantwoordelijke’ voor de gegevensverwerking passende technische en organisatorische maatregelen treft om de persoonsgegevens voldoende te beveiligen (art. 13 Wbp).

De beveiligingsplicht in artikel 13 Wbp is - dat zal duidelijk zijn - erg ruim geformuleerd. Wat zijn immers “passende technische en organisatorische maatregelen” om persoonsgegevens “voldoende” te beveiligen? Om de toetsen of in de praktijk een juiste invulling is gegeven aan deze algemene norm kan een rechter te rade gaat bij ICT-deskundigen die daarop de rechter kunnen adviseren met een beroep op erkende ICT-literatuur en de norm voor informatiebeveiliging in de zorg (NEN norm 7510).

Een andere voorwaarde betreft het gebruik van nummers, zoals het BSN. Het gebruik van persoonsnummers kan de koppeling van verschillende bestanden aanzienlijk vergemakkelijken maar vormt daardoor tegelijkertijd een extra bedreiging voor de persoonlijke levenssfeer. Wettelijk voorgeschreven nummers (art. 24 Wbp) bestaan in verschillende varianten. Een bekend voorbeeld is het burgerservicenummer (BSN). Omdat het gebruik van persoonsnummers extra bedreigend kan zijn voor de persoonlijke levenssfeer is het verwerken van persoonsnummers voor andere doeleinden dan de uitvoering van de betreffende wet alleen toegestaan voor zover dat bij de wet is bepaald. Alleen de minister mag via een algemene maatregel van bestuur gevallen aangeven

waarin een persoonsnummer mag worden gebruikt, waarbij tevens nadere voorschriften voor het gebruik van zo een persoonsnummer kunnen worden gegeven.

De Wbp kent de betrokkenen van wie persoonsgegevens worden verwerkt voorts diverse rechten toe. Deze rechten bestaan met name uit het inzagerecht (art. 35), het correctierecht, het recht op aanvulling, verwijdering en afscherming (art. 36) en het recht op verzet (art. 41 en 42).

C.2.5.2 Beveiligingsplicht

Op een 'verantwoordelijke' rust een beveiligingsplicht. Ter voorkoming van onrechtmatige verwerkingen, zoals onbevoegde toegang tot of verlies van patiëntengegevens, moet een verantwoordelijke 'passende technische en organisatorische maatregelen' treffen. Een organisatorische maatregel is bijvoorbeeld het treffen van een regeling voor de toegang tot de gegevens. In een overzicht kan worden aangegeven welke functionaris tot welke gegevens toegang heeft. Zo een voorbeeldmatrix is opgenomen in een van de rapporten die in het kader van het Implementatieprogramma Wgbo in juni 2004 zijn gepubliceerd.[46] Een technische maatregel is bijvoorbeeld het gebruik van een wachtwoord om toegang tot de gegevens te kunnen krijgen.

Een belangrijk hulpmiddel bij de concretisering van passende maatregelen is de NEN-norm 7510. In april 2004 is deze norm onder de titel 'Medische Informatica - Informatiebeveiliging in de zorg - Algemeen' gepubliceerd door het Nederlands Normalisatie Instituut (NEN). In aanvulling op deze norm zijn extra hulpmiddelen beschikbaar ter ondersteuning van de implementatie van de norm in de zorgsector. De hulpmiddelen zijn beschikbaar voor huisartsen, fysiotherapeuten, ziekenhuizen, thuiszorg, streeklaboratoria en netwerkorganisaties.
Volgens de minister van Volksgezondheid,Welzijn en Sport is de NEN-norm 7510 een geschikt hulpmiddel om invulling te geven aan de algemene plicht om te zorgen voor passende beveiligingsmaatregelen.[47]

Als uitwerking van NEN 7510 zijn in november 2005 NEN 7511-1, -2 en -3 gepubliceerd. Deze bevatten zogeheten 'toetsbare voorschriften' die, indien toegepast samen met de norm, een passende beveiliging rondom het gebruik van het identificatienummer in de zorg kunnen bevorderen. NEN 7511 is daartoe in drie zorgclusters ingedeeld: complexe organisaties (ziekenhuizen, universitaire medische centra, gezondheidscentra, GGD- en GGZ-instellingen), samenwerkende organisaties (thuiszorginstellingen, verpleeghuizen, bloedbanken, ambulances en revalidatie-instellingen) en solopraktijken (apotheken, alleen praktiserende en in samenwerking praktiserende huisartsen, fysiotherapeuten, psychiaters, psychologen en tandartsen).
NEN 7512 is eveneens een uitwerking van NEN 7510, maar dan met betrekking tot de vertrouwde gegevensuitwisseling. Deze uitwerking geeft een aanzet tot risicoclassificatie en een uitwerking van de eisen over identificatie en authenticatie die samenhangen met een bepaalde risicoklasse.

---

[46] J.M.Witmer, R. de Roode, *Van wet naar praktijk. Implementatie van de Wgbo. Deel 4 Toegang tot patiëntengegevens*, Utrecht 2004, bijlage 2, p. 73. Op internet: www.knmg.nl/wgbo.

[47] *Kamerstukken II* 2004/05, 29 800 hoofdstuk XVI, nr. 2, p. 135, Vaststelling van de begrotingsstaten van het Ministerie van Volksgezondheid,Welzijn en Sport (XVI) voor het jaar 2005; Memorie van Toelichting.

C.2.6 Computercriminaliteit

Uit het Wetboek van Strafrecht, om precies te zijn artikel 138a WvSr, vloeit ook in meer of mindere mate een beveiligingsplicht voort. Dat artikel stelt het “hacken” van “geautomatiseerde werken” strafbaar. Dat wordt “computervredebreuk” genoemd. Volgens deze strafbepaling is sprake van strafbaar binnendringen in een geautomatiseerd werk als de toegang wordt verkregen door een beveiliging te doorbreken, door een technische ingreep, met behulp van valse signalen of een valse sleutel, of door het aannemen van een valse hoedanigheid. Dat betekent dat het niet beveiligen van een geautomatiseerd werk, zoals een zorg informatie systeem, tot gevolg kan hebben dat het inbreken daarin niet strafbaar is.

C.2.7 Normen en regels uit de beroepsgroep

Door de beroepsgroep van zorgverleners, in het bijzonder de Koninklijke Nederlandsche Maatschappij tot bevordering der Geneeskunst (KNMG), zijn ook normen en regels vastgelegd die van invloed zijn op de bescherming en beveiliging van medische informatie.
De KNMG Richtlijnen inzake het omgaan met medische gegevens (het ‘groene boekje’, versie 2003) bevat bijvoorbeeld ook regels voor het beheer van medische dossiers. Volgens richtlijn 1.1.3 is de arts die een dossier aanlegt in beginsel ook verantwoordelijk voor het beheer daarvan. Is die arts in dienstverband werkzaam bij een zorginstelling, dan is de directie of Raad van Bestuur van die instelling verantwoordelijk voor de instandhouding en het beheer van die dossiers. De individuele arts blijft in dat geval echter wel mede verantwoordelijk voor het beheer van die dossiers.

De KNMG-Handleiding voor artsen “Privacy-wetgeving en het omgaan met patiëntgegevens” (2001) bevat nadere regels voor het beheer van dossiers. In deze Handleiding wordt ook uiteengezet dat de verantwoordelijke (bijvoorbeeld de Raad van Bestuur van een zorginstelling) verplicht is om passende organisatorische maatregelen te treffen. In dat verband moet bijvoorbeeld worden vastgelegd welke personen toegang mogen hebben tot welke gegevens. In een bijlage wordt een overzicht als mogelijk voorbeeld van een model toegangsregeling gegeven. Dit model is later uitgewerkt in het kader van het Implementatieprogramma Wgbo in deel 4 ‘Toegang tot patiëntengegevens’ (bijlage 2: Voorbeeldmatrix Toegang tot patiëntgegevens).

Daarnaast gelden, aldus de Handleiding, ook technische beveiligingseisen. Zo mag de toegang tot elektronische gegevens alleen mogelijk zijn via een uniek wachtwoord. En wanneer patiëntengegevens elektronisch worden verzonden over een openbaar netwerk (bijvoorbeeld per e-mail), dan moeten die gegevens eerst worden versleuteld. Aldus moet worden voorkomen dat onbevoegde derden, zoals familieleden, toegang krijgen tot de gegevens, bijvoorbeeld doordat een typefout wordt gemaakt in het e-mailadres.

C.2.8 Kwaliteitswet zorginstellingen en Wet BIG

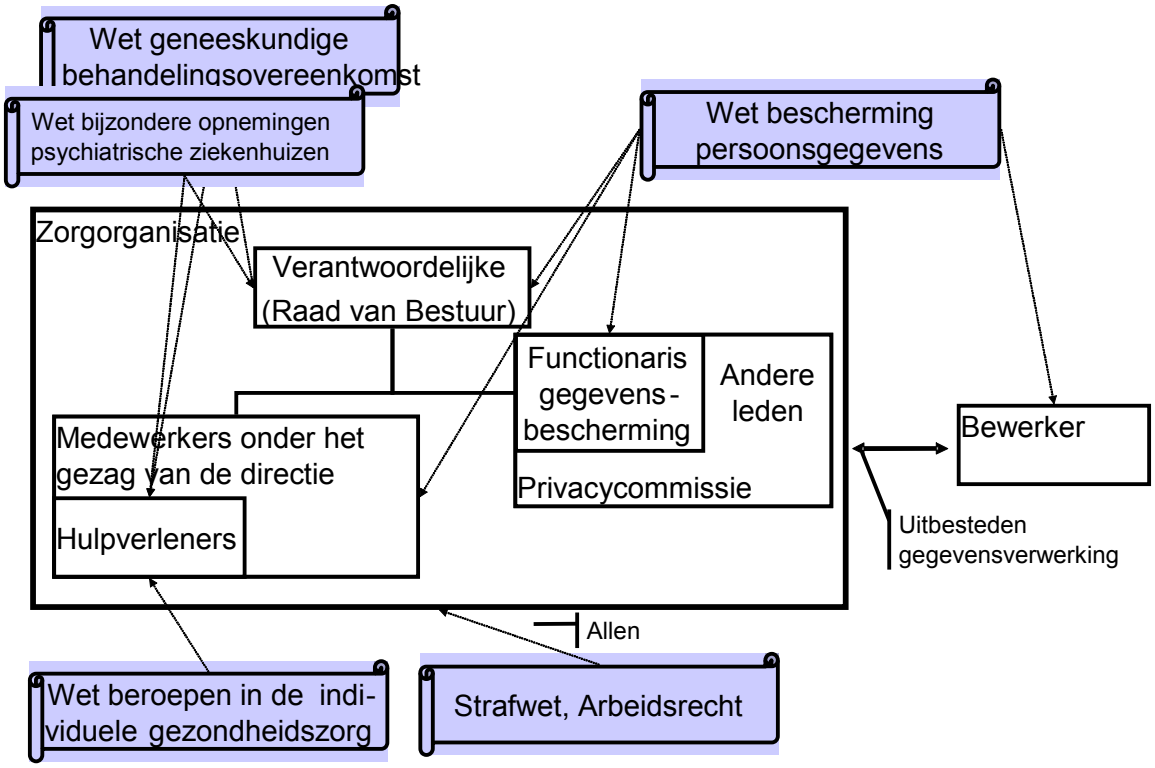
Ook op grond van de kwaliteitswetgeving voor de gezondheidszorg, zoals de Kwaliteitswet

zorginstellingen (Kwz) en de Wet beroepen in de individuele gezondheidszorg (Wet BIG) vloeit een verplichting voort tot beveiliging van medische informatie.

Artikel 2 van de Kwz en artikel 40 Wet BIG schrijven voor dat zorginstellingen, respectievelijk individuele beroepsbeoefenaren in de zorg, verplicht zijn om 'verantwoorde zorg' te leveren. Die verplichting houdt niet alleen in dat de geleverde zorg inhoudelijk verantwoord moet zijn, maar bijvoorbeeld ook dat daarbij gebruik wordt gemaakt van kwalitatief goede materialen en apparatuur. Ook is men verplicht om praktijkruimten behoorlijk in te richten. Tevens houdt verantwoorde zorg in dat patiëntendossiers zorgvuldig worden bijgehouden en beheerd.

C.2.9 Samenvattend

Het volgende plaatje geeft een overzicht van de verschillende wetten die van toepassing kunnen zijn bij de beveiliging van persoonsgegevens in de zorg.



Bron: J. van der Wel, Informatiebeveiliging in de Zorg. Academic Service, juni 2006.

Voor de informatiebeveiliging in de zorg zijn bijvoorbeeld ook de Wet bescherming persoonsgegevens en de (toekomstige) Wet op het EPD van belang. Beide wetten zijn voorbeelden van wetten die zijn lastig zijn onder te brengen in een van de bovengenoemde rechtsgebieden. De Wet op het EPD kan gerangschikt worden onder het specifieke rechtsgebied

van het Gezondheidsrecht, dat zelf ook een multidisciplinair rechtsgebied is. De Wbp kan worden gerangschikt onder het specifieke rechtsgebied van het privacyrecht. Ook het privacyrecht is multidisciplinair, aangezien het zowel terug te vinden is in het internationale recht, het staats- en bestuursrecht (grondrechten), het privaatrecht (BW) en het strafrecht (zwijgplicht en verschoningsrecht).

C.3. Praktische interpretatie door de zorgpraktijk

C.3.1 Inleiding

Het beveiligingsbeginsel is een van de algemene privacybeginselen zoals die o.a. zijn geformuleerd in de OESO-privacyrichtlijn (OECD Guidelines on the Protection of Privacy and Transborder Flow of Personal Data, Paris 1981) en in het Databeschermingsverdrag van de Raad van Europa (Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, Straatsburg 28 januari 1981).
De bescherming van de informationele privacy is in Nederland mede gebaseerd op deze internationaal - ook door ons land - erkende algemene privacybeginselen.

Deze algemene privacybeginselen vormen de grondslag voor de bescherming van persoonsgegevens (de informationele privacy) in ons land. Het Verdrag van Straatsburg is door Nederland ondertekend op 21 januari 1988 en door het Nederlandse parlement goedgekeurd op 20 juni 1990. De EU-richtlijn bescherming persoonsgegevens (95/46/EG) beoogt nadrukkelijk deze privacybeginselen verder uit te werken en te versterken. Het bestaande Nederlandse stelsel van privacybescherming bevat aldus een nadere uitwerking van de bedoelde beginselen, met name gebaseerd op de EU-richtlijn. De maatregelen die op nationaal niveau zijn getroffen kunnen worden beschouwd als middelen waarmee invulling wordt gegeven aan de doelen die zijn neergelegd in de afzonderlijke privacybeginselen.

De OESO-privacyrichtlijn en het Verdrag van Straatsburg bevatten twee categorieën algemene privacybeginselen. De eerste categorie bevat algemene voorwaarden voor rechtmatige gegevensverwerking. Het privacybeginsel dat noopt tot beveiliging van persoonsgegevens behoort tot de tweede categorie van privacybeginselen, die betrekking hebben op de verplichtingen van degenen die verantwoordelijk zijn voor de gegevensverwerking en op de rechten van geregistreerden of betrokkenen. Het beveiligingsbeginsel houdt in dat persoonsgegevens moeten worden beschermd met redelijke beveiligingsmaatregelen tegen verlies van of ongeoorloofde toegang tot gegevens alsmede tegen ongeoorloofde vernietiging, gebruik, verandering of uitlekken daarvan.

Bij het treffen van maatregelen ter beveiliging van persoonsgegevens dient onder andere te worden gelet op de mate van gevoeligheid van de gegevens, de mate waarin de toegang tot de gegevens binnen een organisatie beperkt dient te worden en de behoefte aan het kunnen bewaren van de gegevens gedurende langere tijd. Beveiligingsmaatregelen moeten zijn gebaseerd op de

gangbare methoden en technieken van gegevensbeveiliging. Wat gangbaar is hangt af van de stand van de techniek, die voortdurend voortschrijdt met de tijd. Zij worden getroffen om persoonsgegevens te beschermen tegen:

1. Verlies en onbedoeld wissen van gegevens.
2. Onbevoegde toegang tot gegevens.
3. De ongeoorloofde vernietiging van gegevens, waaronder begrepen het onbevoegd vernietigen en ontvreemden van opslagmedia.
4. Onbevoegd gebruik van persoonsgegevens inclusief het ongeautoriseerd kopiëren van gegevens.
5. Ongeoorloofde wijziging of vervalsing van gegevens, met inbegrip van het ongeautoriseerd invoeren van gegevens: iemand kan bevoegd toegang hebben tot bepaalde gegevens teneinde deze te raadplegen, hetgeen echter niet automatisch het recht inhoudt deze gegevens te wijzigen of nieuwe gegevens aan het bestand toe te voegen.
6. Ongeoorloofde verspreiding of openbaarmaking, dat een wezenlijk aspect is van het recht op informationele privacy, dat wel eens kortheidshalve wordt omschreven als ‘het recht op selectieve openbaarmaking’.

Het beveiligingsbeginsel dient onder meer ter bescherming van persoonsgegevens tegen onbevoegd gebruik en verstrekking daarvan. Beveiligingsmaatregelen kunnen worden getroffen op het niveau van:

1. Fysieke beveiliging: gesloten deuren of identificatiepasjes.
2. Organisatorische beveiliging: bevoegdhedenregeling met betrekking tot de toegang tot gegevens.
3. Informationele beveiliging: encryptie of elektronisch toezicht op ongebruikelijke activiteiten.

Tot de organisatorische maatregelen wordt ook gerekend de geheimhoudingsplicht voor het gegevensverwerkend personeel. De maatregelen die voortvloeien uit dit beginsel vertonen deels enige overlap met de toegangs- en verstrekkingenproblematiek.

C.3.2 Registratiekamer Rapport Beveiliging van persoonsgegevens

In de Achtergrondstudie en Verkenning nr. 23: ‘Beveiliging van persoonsgegevens tegen verlies en tegen enige vorm van onrechtmatige verwerking’ (2001), publiceerde de Registratiekamer (thans College Bescherming Persoonsgegevens: CBP) de beveiligingseisen die voor het CBP de uitgangspunten vormen sinds het in werking treden van de Wbp.

De door de verantwoordelijke op grond van art. 13 Wbp te nemen beveiligingsmaatregelen zijn afhankelijk van de aard en omvang van de persoonsgegevens en van de wijze van verwerking van die persoonsgegevens. Door de verantwoordelijke dient een analyse te worden uitgevoerd teneinde te bepalen welke risicoklasse van toepassing is op de persoonsgegevens.
De Registratiekamer gaat uit van vier risicoklassen. De opbouw van de risicoklassen is cumulatief: hogere klassen geven additionele normen aan die passen bij de hogere risicoklasse.

De vier risicoklassen die in ieder geval kunnen worden onderscheiden zijn:

Risicoklasse 0: publiek niveau
Het gaat hier om openbare persoonsgegevens. In deze klasse zijn persoonsgegevens opgenomen waarvan algemeen aanvaard is dat deze, bij het beoogde gebruik, geen risico opleveren voor de betrokkene. Voorbeelden hiervan zijn telefoonboeken, brochures, publieke internet sites, et cetera. De persoonsgegevens behoeven ten aanzien van de exclusiviteit van de persoonsgegevens niet beter beveiligd te worden dan gebruikelijk is om een toereikende kwaliteit van de informatievoorziening tot stand te brengen en in stand te houden. Door de Wbp worden voor deze risicoklasse geen extra eisen ten aanzien van de beveiliging gesteld ten opzichte van wat noodzakelijk is voor een zorgvuldige bedrijfsvoering.

Risicoklasse I: basis niveau
De risico's voor de betrokkene bij verlies of onbevoegd of onzorgvuldig gebruik van de persoonsgegevens zijn zodanig dat standaard (informatie) beveiligingsmaatregelen toereikend zijn. Bij verwerkingen van persoonsgegevens in deze klasse gaat het meestal om een beperkt aantal persoonsgegevens dat betrekking heeft op bijvoorbeeld lidmaatschappen, arbeidsrelaties, klantrelaties en overeenkomstige relaties tussen een betrokkene en een organisatie.
Voorbeelden van relaties waarover veelal persoonsgegevens worden verwerkt die vallen in deze klasse zijn: school - leerling, verhuurder - huurder, hotel - gast, vereniging - lid, organisatie - deelnemer.

In deze klasse zijn de risico's zodanig dat met een basispakket van beveiligingsmaatregelen kan worden volstaan.

Risicoklasse II: verhoogd risico
In deze klasse bestaan extra risico's voor negatieve gevolgen voor de betrokkenen bij onbevoegd of onzorgvuldig gebruik van persoonsgegevens. De verwerkingen van bijzondere (gevoelige) gegevens als bedoeld in art. 16 van de Wbp vallen in ieder geval in deze risicoklasse.

Risicoklasse III: hoog risico
In deze klasse is sprake van verwerking van persoonsgegevens die in aanmerkelijke mate een risico opleveren voor onbevoegd of onzorgvuldig gebruik. Dit geldt bijvoorbeeld bij verwerking van meerdere verzamelingen van bijzondere persoonsgegevens. De beveiligingsmaatregelen die voor de beveiliging van dergelijke persoonsgegevens moeten worden genomen, moeten voldoen aan de hoogste normen. De gegevensdrager (CD-ROM, tapes, schijven, intern geheugen) van persoonsgegevens die onder deze risicoklasse vallen, moet - voor dat zover technisch mogelijk is - worden voorzien van een markering waaruit direct blijkt dat deze gegevens in risicoklasse III vallen.

De verwerking van persoonsgegevens omtrent iemands gezondheid valt in elk geval in risicoklasse II (verhoogd risico). Onder verhoogd risico wordt verstaan dat er extra negatieve gevolgen bestaan

voor de betrokkene bij verlies, onbehoorlijke of onzorgvuldige verwerking van de persoonsgegevens. Soms kan de verwerking van bijzondere gegevens vanwege een hoge gevoeligheidsgraad in het maatschappelijk verkeer, bijvoorbeeld wanneer het gegevens over levensbedreigende ziektes betreft, ondergebracht moeten worden in risicoklasse III.
Volgens de Registratiekamer valt de verwerking van persoonsgegevens waarop een bijzondere geheimhoudingsplicht van toepassing is binnen risicoklasse III. Zo een bijzondere geheimhoudingsplicht is bijvoorbeeld het medisch beroepsgeheim. Dit heeft tot gevolg dat de verwerking van persoonsgegevens over iemands gezondheid valt in risicoklasse III.

In de Achtergrondstudie en Verkenningen nr. 23 van de Registratiekamer wordt gedetailleerd weergegeven welke beveiligingseisen er gelden bij risicoklasse III.

De verantwoordelijke is verplicht te zorgen voor een niveau van beveiliging van de persoonsgegevens dat overeenkomt met de eisen die in het rapport van de Registratiekamer worden gepresenteerd. Als er sprake is van een bewerker in de zin van de wet (artikel 14 Wbp), dient de verantwoordelijke die bewerker te instrueren over de wijze waarop de persoonsgegevens moeten worden beveiligd. De uiteindelijke keuze van het stelsel van algemene maatregelen wordt bepaald door de ‘state of the art’, de kosten van de maatregelen en de continuïteit van bepaalde voorzieningen. De verantwoordelijke moet een evenwichtige afweging maken tussen deze factoren en het belang van de beveiliging van de persoonsgegevens en hij moet deze afweging ook documenteren. Het uit deze afweging voortvloeiende beveiligingsstelsel behoort permanent een evenwichtig stelsel van zowel technische als organisatorische maatregelen te zijn.
Volgens de eisen van de Registratiekamer is de verantwoordelijke verplicht met de volgende aspecten van informatiebeveiliging rekening te houden:

1. Vaststellen van beveiligingsbeleid, beveiligingsplan en implementatie van het stelsel van maatregelen en procedures.
2. Administratieve organisatie (beschrijving) van de beveiliging.
3. Bevorderen van beveiligingsbewustzijn.
4. Eisen stellen bij werving en selectie van personeel.
5. Juiste inrichting van de werkplek.
6. Beheer en classificatie van de ICT infrastructuur.
7. Toegangsbeheer en –controle.
8. Beveiliging van netwerken en externe verbindingen.
9. Voorwaarden aan het gebruik van software van derden.
10. Beveiliging bij bulkverwerking van persoonsgegevens.
11. Eisen aan het bewaren van persoonsgegevens.
12. Eisen aan de vernietiging van persoonsgegevens.
13. Opstellen van een calamiteitenplan.
14. Aandacht voor beveiliging bij uitbesteden van en overeenkomsten voor de verwerking van persoonsgegevens.

Voor de verwerking van patiëntgegevens betekent dit bijvoorbeeld dat:

- De gegevensverwerking (opslag en transport) zoveel mogelijk versleuteld dient te zijn.
- Identificatie en verificatie dienen adequaat geregeld te zijn, bijvoorbeeld door middel aan de UZI-pas van de zorgaanbieder.
- Er dient sprake te zijn van een strikte autorisatie: alleen degenen die daartoe bevoegd zijn mogen toegang hebben tot de gegevens in het patiëntendossier.

Wat de versleuteling betreft stelt de Registratiekamer dat in ieder geval moet worden voorkomen dat berichten met persoonsgegevens zonder expliciet, bewust handelen ongeoorloofd worden gelezen door onbevoegde personen. Voor de uitwisseling van persoonsgegevens in risicoklasse III geldt bijvoorbeeld dat:

- De verantwoordelijke uitsluitend datacommunicatie toepast over netwerken buiten het toezicht van zijn eigen organisatie, indien hij expliciete waarborgen (zekerheden) heeft over de kwaliteit van de geïmplementeerde beveiligingsmaatregelen.
- De verzender het berichtenverkeer zodanig vastlegt dat achteraf vastgesteld kan worden wanneer en aan wie een bericht met persoonsgegevens is verzonden en voorzieningen treft voor een vergelijkbare functionaliteit voor de ontvangen berichten.
- De verzender van een bericht (systeem of gebruiker) zich ervan vergewist dat een getransporteerd bericht ongewijzigd is overgebracht.

Het vereiste van integriteit heeft betrekking op de kwaliteit van de verwerkte persoonsgegevens. Deze dienen in het algemeen juist, volledig en actueel te zijn. Hiertoe moeten maatregelen worden getroffen die kunnen waarborgen dat de gegevens juist en nauwkeurig zijn, gelet op de doeleinden waarvoor ze zijn verzameld.

Het vereiste van beschikbaarheid houdt in dat de persoonsgegevens steeds beschikbaar moeten zijn overeenkomstig daarover gemaakte afspraken en wettelijke voorschriften. Wettelijke voorschriften bestaan bijvoorbeeld omtrent de bewaartermijnen van persoonsgegevens. Voor persoonsgegevens die zijn opgeslagen in een (elektronisch) medisch dossier geldt in beginsel de bewaartermijn van vijftien jaren (artikel 7:454, lid 3, BW). Dit vereiste houdt ook in dat de infrastructuur voldoende flexibel moet zijn zodat, op verzoek van de zorgconsument, verwijdering of vernietiging van de persoonsgegevens uit het dossier mogelijk is. Tegelijkertijd moeten, gelet op de wettelijke bewaartermijn van vijftien jaar, aanvullende eisen worden gesteld aan de mogelijkheden tot conversie naar eventuele nieuwe hard- en softwareplatforms, teneinde de toegankelijkheid van de gegevens te kunnen waarborgen.

C.3.3 Code voor Informatiebeveiliging en NEN 7510

In januari 2000 verscheen een 'draft' Code voor Informatiebeveiliging van het ministerie van Economische Zaken en het Nederlands Normalisatie Instituut (NNI, thans NEN). Inmiddels is deze definitief vastgesteld. Deze code is oorspronkelijk gepubliceerd door de British Standards Institution (BSI) als Information Security Management, (BS 7799-1:1999). Deze Code voor Informatiebeveiliging is gericht op de geautomatiseerde informatieverwerking in het algemeen. De Code bestaat uit twee delen:

- Deel 1: Code voor Informatiebeveiliging;
- Deel 2: Specificatie voor managementsystemen voor informatiebeveiliging.

De Code voor Informatiebeveiliging is oorspronkelijk uitgegeven in 1994. Die versie was ook reeds gebaseerd op de toenmalige versie van BS 7799. De Code geeft een uitgebreide verzameling maatregelen voor een goede implementatie (best practices) van informatiebeveiliging. De Code is bedoeld als een referentiepunt voor het vaststellen van de reeks beveiligingsmaatregelen die nodig zijn in de meeste situaties waarin informatiesystemen worden gebruikt in industrie en handel, maar ook in de gezondheidszorg, en kan worden gebruikt in grote, middelgrote en kleine organisaties. De Code is mede uitgangspunt geweest voor de ontwikkeling door NEN van de Nederlandse norm NEN 7510 (Medische Informatica - Informatiebeveiliging in de zorg - Algemeen), die in april 2004 is vastgesteld. Minister Hoogervorst heeft in 2004 aangegeven dat door de naleving van deze norm tegelijkertijd invulling wordt gegeven aan het vereiste van 'passende technische en organisatorische beveiligingsmaatregelen', zoals bedoeld in art. 13 Wbp:
"Een passend beveiligingsniveau is een vereiste om gegevens uit te wisselen. Als uitgangspunt daarvoor zal de recent vastgestelde norm voor informatiebeveiliging in de zorg gaan gelden, de NEN 7510."

De norm 7510 is aangevuld met de normen 7511 en 7512, waarvan 7512 het meest relevant is voor de elektronische communicatie. NEN 7512 is in twee opzichten een aanvulling op NEN 7510. Ten eerste is NEN 7512 gericht op het verkrijgen van zekerheid die partijen (bijvoorbeeld zorgconsument en beheerder LSP) elkaar moeten bieden als voorwaarde voor vertrouwde gegevensuitwisseling. Ten tweede bevat NEN 7512 een nadere invulling van een aantal richtlijnen van NEN 7510, in het bijzonder de risicoclassificatie en de uitwerking van de eisen voor identificatie en authenticatie die behoren bij een bepaalde risicoklasse.[48]

In de context van het EPD is de beveiliging van persoonlijke informatie een wettelijke verplichting. Onvoldoende beveiliging van persoonlijke informatie die in een EPD is opgeslagen, brengt risico's voor de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie met zich mee. De zorgverlener, die voor zijn EPD verantwoordelijk is, is gebonden aan zijn beroepsgeheim. Derhalve zal hij voor een goede beveiliging dienen in te staan, zodat onbevoegden geen toegang tot de patiëntgegevens hebben. Even belangrijk is echter dat het vertrouwen van de zorgconsument op het spel staat. Derhalve zijn toereikende maatregelen nodig om dergelijke informatiesystemen te

[48] Nederlands Normalisatie-Instituut, Nederlandse norm NEN 7512 (nl). Medische Informatica – Informatiebeveiliging in de zorg – Vertrouwensbasis voor gegevensuitwisseling. Delft: Nederlands Normalisatie-Instituut, oktober 2005, p. 3.

beschermen tegen hedendaagse gevaren zoals computerfraude, computervirussen, computer hacking, sabotage, vandalisme, brand, overstromingen, stroomstoringen, et cetera. Technische middelen zijn niet toereikend, maar kunnen worden ondersteund door passende beheersmaatregelen en procedures.

De Code voor Informatiebeveiliging bevat op de volgende onderdelen aanbevelingen voor het management van informatiebeveiliging, die tevens in acht genomen dienen te worden bij de beveiliging van patiëntgegevens in een EPD:

1. Het opstellen van een beveiligingsbeleid.
2. Het inrichten van een beveiligingsorganisatie.
3. Classificatie en beheer van bedrijfsmiddelen.
4. Beveiligingseisen ten aanzien van personeel.
5. Fysieke beveiliging en beveiliging van de omgeving.
6. Beheer van communicatie- en bedieningsprocessen.
7. Toegangsbeveiliging.
8. Ontwikkeling en onderhoud van systemen.
9. Continuïteitsbeleid.
10. Naleving.

Dezelfde onderdelen zijn te vinden in de NEN Norm 7510, die wat betreft structuur overeenkomt met de Code voor Informatiebeveiliging. In de NEN Norm 7510 zijn diverse formuleringen en met name het hoofdstuk over toegangsbeveiliging verder toegesneden op de gezondheidszorg. Om de NEN Norm 7510 in de praktijk toe te kunnen passen zijn implementatiehulpmiddelen ontwikkeld voor huisartspraktijken, fysiotherapiepraktijken, algemene ziekenhuizen, psychiatrische instellingen, thuiszorginstellingen, streeklaboratoria en netwerkorganisaties.

Hier zij benadrukt dat informatiebeveiliging rond het EPD als een proces moet worden beschouwd. Dit proces bestaat uit de tien hierboven genoemde onderdelen uit de Code voor Informatiebeveiliging en NEN norm 7510. Met betrekking tot de identificatie en autorisatie van cliënten is met name onderdeel 7 (Toegangsbeveiliging) relevant.

In verband met de toegangsbeveiliging dient aandacht te worden besteed aan zakelijke eisen ten aanzien van toegangsbeveiliging, management van toegangsrechten en autorisatiebeheer, de verantwoordelijkheden van gebruikers, de toegangsbeveiliging voor netwerken, de toegangsbeveiliging voor besturingssystemen, de toegangsbeveiliging voor toepassingen, de bewaking van de toegang tot en het gebruik van systemen, alsmede aan mobiele computers en telewerken.

Het stellen van zakelijke eisen ten aanzien van toegangsbeveiliging dient ter beheersing van de toegang tot informatie. De toegang tot informatie en bedrijfsprocessen dient te worden beheerst op grond van zakelijke behoeften en beveiligingseisen. Daarbij dient men rekening te houden met het

geldende beleid ten aanzien van informatieverspreiding en autorisatie.

Management van toegangsrechten en autorisatiebeheer heeft tot doel het voorkomen van ongeautoriseerde toegang tot informatiesystemen. Daartoe dienen formele procedures te bestaan voor het beheer van autorisaties voor informatiesystemen en -diensten. Het is van belang dat in deze procedures alle fasen in de levenscyclus van een autorisatie worden vastgelegd, van de registratie van nieuwe gebruikers tot en met het formeel afmelden van gebruikers die niet langer toegang behoeven te hebben tot informatiesystemen en -diensten. Indien van toepassing dient bijzondere aandacht te worden besteed aan de toewijzing van speciale bevoegdheden (zoals noodprocedures) waarmee gebruikers de normale beveiliging in een systeem kunnen omzeilen. Ook voldoende aandacht voor de verantwoordelijkheden van gebruikers dient ongeautoriseerde toegang zoveel mogelijk te voorkomen. Een effectieve beveiliging vereist de medewerking van geautoriseerde gebruikers. Zij dienen op hun verantwoordelijkheid te worden gewezen voor het handhaven van effectieve toegangsbeveiliging, met name met betrekking tot het gebruik van wachtwoorden en de beveiliging van gebruikersapparatuur.

De toegangsbeveiliging voor netwerken is van belang voor de bescherming van netwerkdiensten. Daartoe dienen interne en externe netwerkdiensten te worden beheerd. Dat is nodig om ervoor te zorgen dat gebruikers die toegang hebben tot netwerken of netwerkdiensten de veiligheid daarvan niet in gevaar brengen. Deze maatregelen dienen onder andere te bestaan uit:

1. De juiste interfaces tussen het netwerk van de organisatie en netwerken van andere organisaties, of openbare netwerken.
2. De juiste verificatiemethoden voor gebruikers en apparatuur op afstand.
3. Toegangsbeveiliging tot informatiediensten.

De toegangsbeveiliging voor besturingssystemen heeft tot doel het voorkomen van ongeautoriseerde toegang tot computers. Op het niveau van het besturingssysteem dienen de voorzieningen daartoe in staat te zijn tot:

a. Het identificeren of authenticeren van elke geautoriseerde gebruiker en zo nodig het werkstation of de locatie.
b. Het registreren van geslaagde en mislukte pogingen tot toegang tot het systeem.
c. Het bieden van een passend authenticatiesysteem (bijvoorbeeld wachtwoordbeheer).
d. Indien nodig dient de verbindingstijd van de gebruikers te worden beperkt.

Toegangsbeveiliging voor toepassingen heeft tot doel het voorkomen van ongeautoriseerde toegang tot informatie in computersystemen. De logische toegang tot programmatuur en gegevens moet worden beperkt tot geautoriseerde gebruikers. Daartoe dienen toepassingssystemen:

a. De toegang tot gegevens en systeemfuncties te beheren overeenkomstig het vastgestelde toegangsbeleid van de organisatie.
b. Bescherming te bieden tegen ongeautoriseerde toegang tot alle hulpprogramma's en programmatuur van het besturingssysteem waarmee beheersmaatregelen in systemen of

toepassingen kunnen worden doorbroken.

c. De beveiliging niet in gevaar te brengen van andere systemen die ook van dezelfde faciliteiten gebruik maken.
d. In staat te zijn om alleen de gebruiker, andere aangewezen geautoriseerde personen of vastgestelde groepen gebruikers toegang te bieden tot gegevens.

Bewaking van de toegang tot en het gebruik van systemen heeft tot doel het opsporen van ongeautoriseerde activiteiten. Daartoe dienen systemen te worden bewaakt om afwijkingen van het toegangsbeleid te kunnen detecteren en de te controleren gebeurtenissen te registreren, als bewijs bij beveiligingsincidenten. Systeembewaking maakt het mogelijk om de doeltreffendheid van de genomen maatregelen te bepalen en zeker te stellen dat wordt voldaan aan het vastgestelde toegangsbeleid.

Toegangsbeveiliging heeft ook betrekking op mobiele computers (laptops) en telewerken. Aldus dient de informatiebeveiliging bij het gebruik van mobiele computers en voorzieningen voor netwerken te zijn gewaarborgd. De vereiste beveiliging dient in overeenstemming te zijn met de risico's die verbonden zijn aan deze manieren van werken. Bij het gebruik van mobiele computers moet rekening worden gehouden met de risico's van het werken in een niet beveiligde omgeving en dient de juiste beveiliging te worden aangebracht. In het geval van telewerken dient de organisatie een beveiliging aan te brengen op de locatie waar het telewerken plaatsvindt en ervoor te zorgen dat er adequate voorzieningen zijn voor deze manier van werken. (Code voor Informatiebeveiliging 2000, deel 1, p. 50-65; NEN Norm 7510, p. 25-28)

In de NEN Norm 7510 is als extra onderdeel aandacht besteed aan Beveiligingsincidenten. In dat verband wordt het van belang geacht dat alle eigen en externe medewerkers bekend gemaakt moeten worden met de procedure voor het rapporteren van beveiligingsincidenten. Zij moeten ook worden verplicht om alle incidenten die zij ontdekken of vermoeden, zo snel mogelijk te rapporteren bij de verantwoordelijke contactpersoon.

C.3.4 Modelrichtlijn Toegang tot patiëntengegevens

Als resultaat van de evaluatie van de Wgbo werd een Implementatieprogramma opgezet, dat in juni 2004 heeft geleid tot de publicatie van een viertal rapporten die concrete hulpmiddelen bevatten voor de naleving van de WGBP in de praktijk. Een van die rapporten handelt over de "Toegang tot patiëntengegevens" (deel 4). In dat rapport staan het privacybelang van zorgconsumenten en de noodzaak van beschikbaarheid van (toegang tot) patiëntengegevens centraal.[49]

Het rapport Toegang tot patiëntengegevens gaat in op de mogelijkheden en beperkingen van het verlenen van toegang tot patiëntengegevens. Het verlenen van toegang omvat niet alleen het verstrekken van patiëntengegevens, maar ook het bekend maken of op andere wijze ter beschikking stellen van patiëntengegevens.

[49] Alle delen van het Implementatieprogramma Wgbo zijn in pdf-formaat te downloaden van www.knmg.nl/wgbo.

Een belangrijke conclusie is, dat het verlenen van toegang tot patiëntengegevens voor curatieve zorgdoeleinden in veel situaties is toegestaan op grond van de veronderstelde toestemming van de zorgconsument.

Het rapport besteedt eerst aandacht aan de grenzen van het beroepsgeheim en de mogelijkheden om dat geheim te doorbreken. Naast deze mogelijkheden wordt gewezen op de voorwaarden die daarbij in acht genomen moeten worden. Ook voor het verlenen van toegang op basis van de veronderstelde toestemming van de zorgconsument geldt een aantal voorwaarden.
Voorts gaat het rapport in op de vraag in hoeverre een nieuw fenomeen, de generieke toestemming, in dit kader gehanteerd zou kunnen worden. Vervolgens komt ook het belang van zorgconsumentenvoorlichting aan de orde, de controle op toegang en het toezicht op de naleving van de regels voor de toegang tot patiëntengegevens.

Tot slot wordt aandacht besteed aan een tweetal actuele omstandigheden waarin de toegang tot patiëntengegevens vanwege het gecompliceerde karakter bijzondere aandacht verdient. Het betreft hier de zogeheten ketenzorg en het elektronisch medicatiedossier.
Bij dit rapport horen enkele concrete hulpmiddelen voor de praktijk die als bijlagen bij het rapport zijn opgenomen. Die hulpmiddelen zijn: een Modelrichtlijn Toegang tot Patiëntengegevens, een Voorbeeldmatrix Toegang tot Patiëntengegevens, een Stroomschema Toegang tot Patiëntengegevens met toelichting en een Pakket van eisen Patiëntenvoorlichting en Informatieverstrekking.

Het rapport wijst onder andere op de mogelijkheid van controle op het gebruik van patiëntgegevens door zorgconsumenten zelf, wanneer zorgconsumenten toegang zouden hebben tot de logbestanden waarin is vastgelegd wie, wanneer, voor welk doel welke gegevens heeft geraadpleegd.[50]

[50] J.M. Witmer, R.P. de Roode (red.), Van wet naar praktijk. Implementatie van de Wgbo. Deel 4 Toegang tot patiëntengegevens. Utrecht: KNMG, juni 2004, p. 39.