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

PRICEWATERHOUSECOOPERS

UNIVERSITEIT VAN TILBURG

Radboud Universiteit Nijmegen

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)