



Beveiligingseisen 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



Inhoud

Management samenvatting	4
1 Inleiding.....	7
1.1 Achtergrond en aanleiding.....	7
1.2 Doelstelling en reikwijdte	8
1.3 Randvoorwaarden en uitgangspunten.....	9
1.3.1 Gebruik BSN.....	10
1.4 Aanpak.....	11
1.5 Leeswijzer.....	12
2 Samenvatting onderzoek	13
2.1 Fase 1: Het opstellen van minimale (beveiligings)eisen aan identificatie- en authenticatiemiddelen.....	13
2.2 Fase 2: Het inventariseren en beoordelen van identificatie- en authenticatiemiddelen.....	13
2.3 Fase 3: Verificatie- en uitgifteproces	16
3 Fase 1: Minimale (beveiligings)eisen identificatie- en authenticatiemiddelen	19
3.1 Juridische eisen.....	19
3.2 Technische eisen.....	20
3.3 Eisenpakket	24
4 Fase 2: Inventarisatie en beoordeling van identificatie- en authenticatiemiddelen	25
4.1 Geschiktheid van DigiD voor identificatie	25
4.2 Beschikbare authenticatiemiddelen.....	27
4.2.1 Authenticatie door middel van extra code/wachtwoord, aangetekend verstuurd.....	27
4.2.2 Face-to-face authenticatie van mobiel nummer (SMS+).....	28
4.2.3 Authenticatiemiddelen van internetbankieren	31
4.2.4 eNIK.....	32
4.2.5 Elektronisch rijbewijs	32
4.2.6 UZI pas	32
4.2.7 Reisdocument (RTDA)	33
4.3 Gebruik van een chipkaart.....	36
4.4 Advies ten aanzien van het te implementeren authenticatiemiddel	37
5 Fase 3: Inrichting en minimale eisen aan het verificatie- en uitgifteproces	39
5.1 Referentiekader voor het verificatie- en uitgifteproces	39
5.1.1 Eisen en wensen voor het verificatie- en uitgifteproces	39
5.1.2 Kostenaspecten voor het verificatie en uitgifteproces.....	40
5.2 Referentiekader ingevuld voor SMS+ en RTDA.....	41
5.2.1 Eisen en wensen voor het verificatie en uitgifteproces ingevuld voor SMS+ en RTDA..	42
5.2.2 Kostenaspecten voor verificatie- en uitgifteproces ingevuld voor SMS+ en RTDA	48
5.3 High-level procesbeschrijving verificatie- en uitgifteproces.....	52



	5.3.1 Suggestie voor verificatie- en uitgifteproces voor SMS+ (variant 1)	53
	5.3.2 Suggestie voor verificatie- en uitgifteproces voor SMS+ (variant 2)	54
	5.3.3 Versneld verificatie- en uitgifteproces voor reisdocumenten in Nederland	55
	5.4 Analyse inrichting verificatie- en uitgifteproces	56
	5.4.1 Inrichting van verificatie- en uitgifteproces zelf.....	56
	5.4.2 Gebruiksvriendelijkheid	57
	5.4.3 Kosten van implementatie	57
	5.4.4 Technische aspecten.....	57
	5.4.5 Advies inrichting verificatie- en uitgifteproces	58
A	Geraadpleegde documentatie	59
B	Geraadpleegde personen	61
C	Wet- en regelgeving: Toegang tot het EPD	62
	C.1. Achtergrond.....	62
	C.1.1 Recht op toegang tot het EPD	62
	C.1.2 Kwetsbaarheid van elektronische patiëntendossiers.....	63
	C.1.3 ICT gevaar voor zorgconsument?.....	63
	C.2. Wet- en regelgeving over informatiebeveiliging	65
	C.2.1 Wet algemene bepalingen burgerservicenummer (Wabb)	65
	C.2.2 Wet gebruik burgerservicenummer in de zorg (Wbsn-z)	66
	C.2.3 Wet EPD	67
	C.2.4 Wet geneeskundige behandelingsovereenkomst.....	69
	C.2.5 Wet bescherming persoonsgegevens.....	72
	C.2.6 Computercriminaliteit	74
	C.2.7 Normen en regels uit de beroepsgroep	74
	C.2.8 Kwaliteitswet zorginstellingen en Wet BIG	74
	C.2.9 Samenvattend	75
	C.3. Praktische interpretatie door de zorgpraktijk	76
	C.3.1 Inleiding.....	76
	C.3.2 Registratiekamer Rapport Beveiliging van persoonsgegevens	77
	C.3.3 Code voor Informatiebeveiliging en NEN 7510.....	81
	C.3.4 Modelrichtlijn Toegang tot patiëntengegevens	84



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 geïnterviewde 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-instantie¹ 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.
Management samenvatting



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 BSN² 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 invoering³. 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 beveiligingseisen 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
Inleiding



- 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 "vreemdelingsnummer" 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 eisen⁶ waaraan identificatie en authenticatie middelen dienen te voldoen:

- De identificatie van zorgconsumenten vindt plaats door middel van het **BSN**.
- Het authenticatieniveau moet **Sterk** zijn.
- Identificatoren⁷ 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."