Handreiking Patiëntauthenticatie

Versie 1.0

Een uitgave van het platform “Patiënt en eHealth”

Datum: 23 september 2013
Referentie: ID13002

Inhoudsopgave

Versielijst

Datum	Versie	Wijzigingen
6 nov 2012	Concept	Eerste concept voorgelegd binnen werkgroep patiëntauthenticatie
11 dec 2012	Concept	Verwerking eerste ronde schriftelijk reviewcommentaar van werkgroep
20 dec 2012	Concept	Verwerking reviewcommentaar na bespreking in werkgroep.
11 feb 2013	Concept voor publieke review	Verwerking eerste ronde extern reviewcommentaar van buiten werkgroep na bespreking in werkgroep
23 sep 2013	Versie 1.0	Verwerking tweede ronde extern reviewcommentaar

1 Inleiding

Steeds vaker richten zorgaanbieders voor patiënten een webportaal in, om hen te ondersteunen met digitale diensten, zoals het maken van afspraken of het geven van inzage in het eigen medisch dossier[1]. Daarnaast zijn er ook aanbieders van webportalen die aan zorgconsumenten de mogelijkheid bieden om een eigen medische dossier aan te leggen en bij te houden (Heldoorn, van Herk en Veereschild, 2011).

Voor de toegang tot een webportaal heeft de patiënt of zorgconsument een middel nodig om zijn identiteit te bewijzen. Deze handreiking gaat over de keuze van de methode en het middel waarmee de patiënt dit kan doen.

1.1 Aard en doelgroep van dit document

Dit document is een handreiking voor het kiezen van een geschikte methode van patiëntauthenticatie, in het geval dat de patiënt via een webportaal voor patiënten toegang krijgt tot de eigen persoonsgegevens in het algemeen en tot de eigen medische gegevens in het bijzonder[1].

De handreiking is gericht op aanbieders van patiëntportalen. Deze aanbieders kunnen zowel zorgaanbieders zijn die een patiëntportaal aanbieden onder de verantwoordelijkheid van de eigen organisatie, als onafhankelijke aanbieders van patiëntportalen, zoals 'personal health records' of websites voor lotgenotencontact.

De handreiking is opgesteld door de werkgroep patiëntauthenticatie van het overlegplatform Patiënt en eHealth.

Het platform Patiënt en eHealth

In 2011 is Nictiz gestart met het organiseren van bijeenkomsten rond het thema 'Patiënt en eHealth'. Op deze bijeenkomsten wordt kennis en ervaring gedeeld. Deelnemers zijn tot de conclusie gekomen dat samenwerking essentieel is om de uitdagingen die een opschaling van internetzorg in de weg staan het hoofd te bieden. Om deze reden is het platform 'Patiënt en eHealth' (voorheen platform Internetzorg en Patiëntportalen) opgericht. Het platform bestaat uit bijna 100 partijen (zorgaanbieders, zorgverleners, koepels, ICT-leveranciers en patiëntvertegenwoordiging). Vanuit het platform worden werkgroepen ingericht rondom thema's die relevant zijn voor het implementeren van eHealth-oplossingen voor patiënten.

1.2 Authenticatie

Authenticatie is het proces waarbij wordt nagegaan of een 'subject' (in deze handreiking een natuurlijk persoon) daadwerkelijk degene is die hij beweert te zijn. Hiervoor heeft de betrokkene een authenticatiemiddel nodig, waarmee hij zijn identiteit kan aantonen. Dit kan bijvoorbeeld een wachtwoord zijn, of een pasje met een unieke digitale sleutel.

Omdat niet alle authenticatiemiddelen even betrouwbaar zijn (een eenvoudig wachtwoord kan bijvoorbeeld geraden worden), zijn bij authenticatie verschillende niveaus van betrouwbaarheid mogelijk. Hoe betrouwbaarder het authenticatiemiddel, hoe hoger het betrouwbaarheidsniveau van de authenticatie. Daarbij hangt de betrouwbaarheid van een authenticatiemiddel niet alleen af van het middel zelf, maar ook van de manier waarop het wordt uitgegeven en de controles die daarbij worden uitgevoerd.

[1] Dit document bevat een begrippenlijst (paragraaf 1.7) waarin onze uitleg is opgenomen van enkele voor dit document relevante begrippen.

1.3 Aanleiding voor deze handreiking

Er is in de afgelopen jaren veel publieke discussie gevoerd rondom de toegang van patiënten tot de eigen medische gegevens en de daarbij passende[2] methode van authenticatie (Jacobs et al., 2008; Radboud Universiteit Nijmegen en PriceWaterhouseCoopers, 2010; PWC, 2011).

De meest concrete aanwijzingen op het gebied van authenticatie bij elektronische communicatie in de zorg zijn opgenomen in de NEN 7512 (NEN, 2005)[3]. Hierin wordt de methode van authenticatie gekoppeld aan de risico's die met elektronische communicatie gepaard gaan.

Ondanks het bestaan van de NEN 7512 is in het overlegplatform Patiënt en eHealth gebleken dat aanbieders van patiëntportalen in de praktijk worstelen met de vraag welke authenticatiemiddelen men kan inzetten om enerzijds een goede gebruikservaring van de patiënt mogelijk te maken en anderzijds risico's van identiteitsfraude te beheersen. Deze handreiking biedt aanbieders van patiëntportalen hierbij een handvat in de vorm van een methode voor het wegen van risico's van concrete gebruikssituaties en het kiezen van een bijpassend niveau van authenticatie. Het doen van een risicoanalyse is gebruikelijk bij beveiligingsvraagstukken en is ook van toepassing bij de beveiliging van persoonsgegevens (College bescherming persoonsgegevens, 2013)[4].

1.4 Doel

Het doel van deze handreiking is het bieden van houvast aan aanbieders van patiëntportalen bij het kiezen van een authenticatiemiddel en authenticatiemethode die een *passend* beveiligingsniveau bieden, gelet op:

- de risico's van het portaalgebruik (gelet op de aard van de gegevens en de vorm van gegevensverwerking);
- het gebruiksgemak van de patiënt;
- de stand der techniek;
- de kosten van de te nemen maatregelen.

1.5 Scope / Reikwijdte

Deze handreiking gaat over authenticatiemiddelen en -methoden voor patiënten en zorgconsumenten, voor het verkrijgen van toegang tot medische gegevens via een webportaal. Daarbij kunnen de medische gegevens zijn geregistreerd door de patiënt zelf of door een zorgaanbieder. In het laatste geval heeft de zorgaanbieder (in overleg met patiënten) een keuze gemaakt ten aanzien van de aan de patiënt beschikbaar te stellen gegevens.

De handreiking beperkt zich tot authenticatieaspecten. Andere aspecten, zoals de structuur of presentatiewijze van de aan te bieden gegevens of andere beveiligingsaspecten zoals autorisatie, komen in deze handreiking niet aan de orde. Ook het aspect van machtigingen valt buiten de reikwijdte van dit document, omdat dit in

---

[2] De term 'passend' komt uit de wet bescherming persoonsgegevens, die aangeeft dat een balans moet worden gezocht tussen risico, stand der techniek en kosten: "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." (artikel 13 WBP).

[3] De NEN 7512 wordt momenteel herzien.

[4] Het College bescherming persoonsgegevens (CBP) heeft in 2013 nieuwe richtsnoeren uitgebracht voor de beveiliging van persoonsgegevens (CBP, 2013), waarin de risicobenadering centraal staat. In deze nieuwe richtsnoeren staat het volgende over de verhouding tot de oude richtsnoeren: "De Registratiekamer, de voorloper van het CBP, bracht in 2001 een publicatie uit over de beveiliging van persoonsgegevens (hierna: a&v 23). Deze richtsnoeren vervangen a&v 23. a&v 23 schreef op basis van een risicoclassificatie beveiligingsmaatregelen voor. De risicoclassificatie was gebaseerd op de aard van de verwerkte persoonsgegevens in combinatie met de hoeveelheid verwerkte persoonsgegevens en de complexiteit van de verwerking. Een risicogerichte benadering, waarbij op basis van analyse van de risico's gericht beveiligingsmaatregelen worden getroffen, ontbrak. Als gevolg daarvan is a&v 23, in ieder geval waar het gaat om het concreet treffen van beveiligingsmaatregelen, in de loop der jaren steeds verder af komen te staan van de beveiligingspraktijk. In deze richtsnoeren is daarom gekozen voor een methodiek die aansluit bij de gangbare praktijk van de informatiebeveiliging en die verantwoordelijken de flexibiliteit biedt om die beveiligingsmaatregelen te treffen die in hun situatie het meest passend zijn."

feite een *autorisatie*aspect is en de keuze voor het authenticatiemiddel van de gemachtigde in het algemeen niet anders is dan de keuze voor het authenticatiemiddel van de persoon namens wie de gemachtigde handelt.

Authenticatiemiddelen voor *zorgverlener*s (of eventuele andere eindgebruikers) worden hier niet besproken omdat dit buiten de opdracht van de werkgroep lag. Wel kan worden opgemerkt dat voor de keuze van authenticatiemiddelen voor zorgverleners in principe dezelfde use-case-gebaseerde risicobenadering kan worden gevolgd als in deze handreiking, al zullen de use cases verschillen van de use cases in dit document.

Als het gaat om de *beveiliging* van patiëntportalen, dan spelen - naast de keuze van het authenticatiemiddel voor patiënten - ook talrijke andere zaken een rol, zoals:

- het opleggen van eventuele beperkende eisen aan de portaalsoftware, indien deze aangesloten wordt op bronsystemen van patiëntgegevens;
- de manier waarop het gebruik van het authenticatiemiddel in de software wordt ingeregeld (bv. het instellen van de periode dat een authenticatie geldig blijft);
- authenticatie voor machine-naar-machine-koppelingen voor het vullen van het portaal (denk aan koppelen van bijvoorbeeld meetapparatuur);
- het eventueel maken van een 'real-time' risicoanalyse bij inloggen op basis van de context (denk aan aspecten als tijd, locatie, en gebruiksfrequentie);
- procedures, bijvoorbeeld voor de uitwerking van face-to-face identiteitscontroles, vastleggen van audit-trails, etc.

Dit document concentreert zich op authenticatie en gaat niet in op deze overige beveiligingsaspecten. Het is wel noodzakelijk om de keuze van een authenticatiemiddel in een breder verband te bezien en ook ten aanzien van overige beveiligingsmaatregelen en werkprocedures een consistente keuze te maken, zodat de verschillende beveiligingsmaatregelen met elkaar in evenwicht zijn wat betreft niveau van betrouwbaarheid.

Ook moet men rekening houden met het feit dat de keuze voor een bepaald authenticatiemiddel in sommige gevallen ook tot secundaire beveiligingsrisico's kan leiden, die indirect aan het gebruik van het middel zijn gekoppeld. Zo kan bijvoorbeeld het gebruik van wachtwoorden worden ondersteund door het inrichten van een tabel met (versleutelde) wachtwoorden, die vervolgens weer eigen kwetsbaarheden introduceert. Ook kunnen bijvoorbeeld 'reset'-procedures voor wachtwoorden gevoelig zijn voor misbruik (Honan, 2012). Deze handreiking gaat *niet* in op dergelijke specifieke risico's verbonden aan individuele middelen, omdat dergelijke risico's erg implementatiespecifiek kunnen zijn.

1.6 Status

Deze handreiking heeft de status van 'versie 1.0'. Deskundigen en belanghebbenden die geen lid waren van de werkgroep patiëntauthenticatie van het platform Patiënt en eHealth, zijn tussen februari en mei 2013 in de gelegenheid gesteld om op deze handreiking te reageren, waarna het binnengekomen commentaar is besproken in de werkgroep en naar het inzicht van de werkgroep in de huidige versie is verwerkt. Deze handreiking zal worden herzien, wanneer ontwikkelingen daartoe aanleiding geven.

Commentaar kan worden ingediend bij Nictiz ter attentie van het platform Patiënt en eHealth via communicatie@nictiz.nl. Dit commentaar wordt meegewogen bij een volgende herziening.

1.7 Begrippen

Voor een juiste interpretatie van deze handreiking, geven we voor enkele (in deze handreiking veelgebruikte) begrippen aan wat we er mee bedoelen.

Authenticatie - het proces waarbij iemand nagaat of een gebruiker van een dienst degene is, die hij beweert te zijn.
Betrouwbaarheidsniveau – een semi-kwantitatieve waardering van het gewenste niveau van zekerheid over de identiteit van de gebruiker van een informatiesysteem, uitgedrukt in een numerieke waarde van 1 tot 4. Het betrouwbaarheidsniveau wordt gekozen op basis van een risicoprofiel dat is verbonden aan een bepaalde gebruikssituatie van een informatiesysteem.

Identiteitsfraude - het ongeoorloofd gebruik maken van iemands persoonsgegevens, met het doel om deze gegevens te misbruiken om ongeoorloofd toegang te krijgen tot producten, informatie of diensten.

Medisch dossier – de verzameling van medische gegevens die een zorgverlener of zorginstelling over een patiënt bijhoudt *of* de verzameling van medische gegevens die een zorgconsument over zichzelf bijhoudt. Vanwege het onderwerp van dit document beperken we ons hierbij tot de *digitaal vastgelegde* informatie en laten we niet digitaal vastgelegde informatie buiten beschouwing.

Medische gegevens - gegevens over de gezondheidstoestand van de patiënt of zorgconsument. In de Wet bescherming persoonsgegevens (Wbp) wordt deze bijzondere categorie van persoonsgegevens aangeduid als ‘persoonsgegevens betreffende iemands gezondheid’.

Patiënt – iemand die onder behandeling staat van een zorgverlener of zorginstelling of daar staat ingeschreven.
Patiëntportaal - webportaal waarmee patiënten of zorgconsumenten toegang krijgen tot diensten op het gebied van gezondheid of zorg, waarvan deel uit kan maken de toegang tot de eigen persoonsgegevens in het algemeen en tot de eigen medische gegevens in het medisch dossier (aangelegd door de zorgverlener of door de zorgconsument) in het bijzonder.
Risicoprofiel – een kwalitatieve opsomming van een verzameling van risico’s die samenhangen met een bepaalde gebruikssituatie van een informatiesysteem. Op basis van een risicoprofiel kan een betrouwbaarheidsniveau worden vastgesteld.
Webportaal – een website die dienst doet als toegangspoort tot een voor een gebruiker praktische combinatie van samenhangende diensten, met de mogelijkheid om deze diensten af te stemmen op de individuele gebruiker van het portaal.
Zorgconsument – een persoon die toegang heeft tot de Nederlandse gezondheidszorg (maar niet noodzakelijkerwijs ook patiënt is).

2 Hoe werkt deze handreiking?

2.1 Het stappenplan

Een aanbieder van een patiëntportaal kan deze handreiking gebruiken om te komen tot de keuze van een middel en methode voor patiëntauthenticatie. Daartoe doorloopt hij de volgende vijf stappen, zoals schematisch weergegeven in Figuur 1:

1. **Kies de use cases** - De portaalaanbieder stelt vast welke concrete gebruiksscenario's ('use cases') hij via het patiëntportaal wil ondersteunen. Met andere woorden: hij besluit wat patiënten met het patiëntportaal moeten kunnen doen. Om hierbij te helpen is in deze handreiking een (niet uitputtende) set van acht veel voorkomende 'use cases' opgenomen.
2. **Bepaal het risicoprofiel** - Voor elk van de vastgestelde use cases beoordeelt de portaalaanbieder vervolgens de risico's die met het beoogde gebruik samenhangen aan de hand van een aantal vaste criteria. Om hierbij te helpen wordt in deze handreiking een set van criteria gepresenteerd waartegen de voorgenomen gebruiksscenario's kunnen worden gewogen. Het gaat hier om het vaststellen van de risico's die samenhangen met authenticatie, met name de ongewenste effecten die zouden kunnen optreden ten gevolge van identiteitsfraude.
3. **Stel vast of er risicoverhogende of risicoverlagende factoren zijn** – Er kunnen, los van de in de vorige stap gebruikte criteria, bijzondere omstandigheden zijn die maken dat de risico's zwaarder moeten worden gewogen of juist lichter. Deze handreiking helpt daarbij door een aantal veel voorkomende risicoverhogende en risicoverlagende factoren aan te voeren. Dit kan leiden tot het vaststellen van een hoger of lager betrouwbaarheidsniveau in stap 4.
4. **Kies het betrouwbaarheidsniveau dat past bij de risico's** - Aan de hand van de gemaakte risicobeoordeling kiest de portaalaanbieder een gewenst betrouwbaarheidsniveau voor de authenticatie. Om hierbij te helpen koppelt deze handreiking een aantal veel voorkomende risico's aan een viertal betrouwbaarheidsniveaus. Deze betrouwbaarheidsniveaus zijn afgeleid van een Europees raamwerk voor authenticatie, het STORK-raamwerk (zie hoofdstuk 3 voor een nadere uitleg).
5. **Kies een bijpassende authenticatiemethode en authenticatiemiddel** – Op basis van het gewenste betrouwbaarheidsniveau kunnen nu een authenticatiemethode en authenticatiemiddel worden gekozen. Daarbij kan men desgewenst rekening houden met kosten van het middel en met de bijkomende kosten van randapparatuur (bv. paslezers) en van het uitgifteproces van het middel. Ook de context van de eindgebruiker kan in deze stap worden meegewogen (bv. de noodzaak voor gebruikers om randapparatuur aan te schaffen). Op basis hiervan is het nog mogelijk, onder strikte voorwaarden, om gemotiveerd te kiezen voor een middel dat een lager betrouwbaarheidsniveau biedt, in combinatie met aanvullende risicocompenserende maatregelen.

Figuur 1: het gebruik van de handreiking in vijf stappen

In hoofdstuk 3 wordt een korte toelichting gegeven op de betrouwbaarheidsniveaus volgens STORK. Vervolgens worden in hoofdstuk 4 van deze handreiking de stappen van het stappenplan verder uitgewerkt.

2.2 Opmerkingen bij de methodiek

Deze methodiek is afgeleid van de handreiking 'Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten' van het Forum Standaardisatie (Forum standaardisatie, 2012). De door het Forum Standaardisatie gepresenteerde methodiek is eenvoudig en transparant en ook bruikbaar voor andere elektronische diensten dan overheidsdiensten.

De risicobeoordeling vraagt daarbij echter wel om andere criteria, omdat het leveren van een overheidsdienst aan burgers iets anders is dan het leveren van een gezondheids(informatie)dienst door een zorgaanbieder aan een patiënt of door een portaalaanbieder aan een zorgconsument. Criteria als 'rechtsgevolg' of 'formeelrechtelijke eisen' zijn in de context van patiëntportalen bijvoorbeeld minder makkelijk praktisch bruikbaar dan in de context van overheidsdiensten. We beschouwen deze handreiking dan ook niet zozeer als een 'dochter' of 'specialisatie' van de handreiking van het Forum Standaardisatie, omdat de toepassingscontext een andere is. Wel volgen we een vergelijkbare methodiek.

Voor het inrichten van overheidsdiensten waarbij toegang tot medische gegevens van de burger aan de orde zou kunnen zijn (dit is bijvoorbeeld voorstelbaar in de context van gemeentelijke diensten in het kader van de Wet maatschappelijke ondersteuning) verwijzen we naar de handreiking van het Forum Standaardisatie.

3 Betrouwbaarheidsniveaus van authenticatie en STORK

In het stappenplan voor het kiezen van authenticatiemethode en middel wordt bij stap 4 een betrouwbaarheidsniveau gekozen. Hierbij wordt gebruik gemaakt van de vier niveaus van het STORK-raamwerk. Voordat het stappenplan nader wordt toegelicht, verklaren we kort de STORK-niveaus. Voor een uitgebreide uitleg verwijzen we naar de eerder genoemde handreiking van het Forum Standaardisatie.

STORK (dit staat voor 'secure identity across borders linked' – het acroniem is *niet* afgeleid van de eerste letters van elk woord) is een Europees project dat zich tot doel stelt om nationale elektronische identiteiten van Europese burgers op internationaal niveau binnen Europa interoperabel te maken. Hiertoe is een raamwerk opgesteld dat elektronische identiteiten indeelt in vier betrouwbaarheidsniveaus.

Deze indeling is gebaseerd op vijf aspecten, waarvan twee gerelateerd zijn aan het authenticatiemiddel en drie aan de registratie en uitgifte:

- Registratie en uitgifte:
  - Kwaliteit van het identificatieproces
  - Kwaliteit van het uitgifteproces van de identiteit
  - Kwaliteit van de uitgever van de identiteit
- Middel:
  - Type en robuustheid van het middel
  - Kwaliteit van het authenticatiemechanisme

Afhankelijk van de invulling van deze vijf aspecten zijn in het STORK-raamwerk vier niveaus van betrouwbaarheid te bereiken, waarbij niveau 1 het laagste en niveau 4 het hoogste niveau is.

In grote lijnen kunnen de vier niveaus worden beschreven zoals weergegeven in Tabel 1. Dit is een enigszins vereenvoudigde weergave, zie de STORK-documentatie voor meer detail (STORK-eID consortium, 2009).

Tabel 1: vereenvoudigde uitleg van betrouwbaarheidsniveaus volgens STORK

Niveau	Authenticatiemiddel	Proces van uitgifte van het middel	Voorbeeld
1	"één-factor", dat wil zeggen één van de volgende factoren[5]: - iets dat je hebt - iets dat je weet - iets dat je bent Voorbeeld: alleen een wachtwoord	Op basis van de eigen bewering van de gebruiker, alleen check op geldigheid van het e-mailadres[6]	Facebook, Google, bol.com
2	"twee-factor", dat wil zeggen twee van de volgende factoren: - iets dat je hebt - iets dat je weet - iets dat je bent *Voorbeeld 1:* wachtwoord + eenmalige code via SMS *Voorbeeld 2:* wachtwoord + vingerafdruk	Registratie via bekend gegeven, bijvoorbeeld het woonadres uit de Gemeentelijke Basisadministratie (GBA)	DigiD Midden (DigiD met wachtwoord en eenmalige code via SMS)
3	Eén van de volgende middelen in combinatie met een tweede factor (bv. pincode of wachtwoord): - smartcard - 'soft certificates' (certificaat bewaard op de computer) - 'one time password (OTP) device token' (bv. OTP via sms).	Proces met identiteitsbewijs en meer checks, bijvoorbeeld fysiek verschijnen bij de uitgifte ('face-to-face' controle).	DigiD Midden, aangevuld met persoonlijke registratie bij een balie; online bankieren
4	Smartcard uitgegeven onder overheidstoezicht. Hierbij is ook een tweede factor nodig (bv. een pincode).	Idem, met altijd fysiek verschijnen bij uitgifte; uitgevoerd door partij die namens overheid gecontroleerd wordt.	PKIoverheid, UZI-pas

[5] Bij elk type factor zijn verschillende sterktes mogelijk. Een lang wachtwoord met bijzondere tekens is bijvoorbeeld moeilijker te kraken dan een kort password zonder bijzondere tekens. Echter, de methode van aanval kan ongevoelig zijn voor dit verschil: een 'key logger' achterhaalt een lang wachtwoord net zo eenvoudig als een kort wachtwoord. Ook biometrische factoren zijn, in tegenstelling wat soms gedacht wordt, niet ongevoelig voor aanvallen: ook een vingerafdruk kan gekopieerd worden. Daarom zijn twee-factor methoden veiliger, mits beide factoren niet tegelijkertijd met dezelfde methode achterhaald kunnen worden.

[6] Dit niveau geeft dus geen enkele zekerheid over de identiteit van de gebruiker, omdat deze niet gecontroleerd wordt.

4 Uitvoering van het stappenplan

4.1 Stap 1 – De keuze van use cases

In stap 1 inventariseert de portaalaanbieder hoe patiënten gebruik zullen maken van het patiëntportaal.

Om hierbij te helpen, heeft de werkgroep patiëntauthenticatie bij het opstellen van deze handreiking een aantal veel voorkomende use cases van patiëntportalen geïnventariseerd. Tabel 2 beschrijft deze use cases. Natuurlijk zijn er naast deze use cases ook nog andere mogelijk.

Tabel 2: veel voorkomende use cases voor patiëntportalen

Nr.	Use case titel	Korte beschrijving
1	Patiënt controleert inschrijvingsgegevens	De patiënt controleert zijn inschrijfgegevens zoals die bij de portaalaanbieder bekend zijn, zoals naam/adres/woonplaats (NAW) en andere gegevens die geen betrekking hebben op de gezondheid van de patiënt. Het betreft hier alle gegevens die nodig zijn om de patiënt te identificeren of met hem te communiceren.
2	Patiënt wijzigt inschrijvingsgegevens	De patiënt wijzigt zijn inschrijfgegevens zoals die bij de portaalaanbieder bekend zijn, zoals NAW en andere gegevens die geen betrekking hebben op de gezondheid van de patiënt. Het betreft hier alle gegevens die nodig zijn om de patiënt te identificeren of met hem te communiceren.
3	Patiënt maakt/wijzigt afspraak met zorgverlener	De patiënt maakt een afspraak met een zorgverlener, bijvoorbeeld voor het spreekuur van huisarts of medisch specialist of voor het uitvoeren van een bepaald onderzoek bij een ziekenhuis. Hierbij worden vastgelegd: de identificerende gegevens van de patiënt, datum en tijdstip van het bezoek, behandelend specialist/specialisme en (zo nodig) het doel van het bezoek.
4	Patiënt raadpleegt zijn medisch dossier	De patiënt raadpleegt langs elektronische weg zijn medisch dossier (huisartsdossier, laboratoriumuitslagen, beeldverslagen, medicatie, zorgplan, e.d.).
5	Patiënt maakt aanvullingen op zijn medisch dossier	De patiënt maakt (al dan niet op verzoek van zijn zorgverlener) aanvullingen op zijn medisch dossier, bijvoorbeeld door het doorgeven van resultaten van zelfmetingen van parameters zoals bloedsuikerspiegel, bloeddruk, gewicht, etc. De zorgverlener krijgt op deze wijze inzicht in de actuele situatie van de patiënt en kan bij afwijkingen van de normaalwaarden de patiënt oproepen voor een consult. Dit kan het bezoek van de arts voor routinecontroles doen verminderen, hetgeen een voordeel kan zijn voor zowel patiënt als zorgverlener. Andere voorbeelden van aanvullingen zijn antwoorden op vragenlijsten, ervaringen, gezondheidsklachten, etc.
6	Patiënt vraagt herhaalrecept aan	De patiënt vraagt voor zichzelf een herhaalrecept aan bij zijn zorgaanbieder (bijvoorbeeld de huisarts). Hierbij gaat het om medicijnen waarvoor al eerder een recept is verstrekt.
7	Patiënt heeft online contact met zorgverlener via tekstmedium (e-mail/chat) of beeldverbinding voor een consult of coaching-sessie.	De patiënt heeft via een online omgeving contact met een zorgverlener. Dit contact kan zowel asynchroon (uitwisseling van teksten, vragenlijsten, gezondheidsinformatie, adviezen, instructie) als synchroon (chatcontact of directe beeldverbinding) zijn.

Nr.	Use case titel	Korte beschrijving
8	Patiënt neemt deel aan een forum op een online community voor patiënten binnen het portaal van zorgaanbieder. Aan het forum kunnen ook zorgverleners deelnemen.	De patiënt neemt deel aan een forum waarbij hij informatie kan uitwisselen met andere patiënten en eventuele deelnemende zorgverleners en/of familieleden. Afhankelijk van de gekozen opzet kan sprake zijn van (semi-)anonieme deelname (onder een alias, waarbij de ware identiteit van de gebruiker nog wel bij de forumbeheerder bekend kan zijn) of van deelname onder de eigen naam van de gebruiker. In het algemeen worden deze fora gemodereerd.

4.2 Stap 2 – Het bepalen van het risicoprofiel

In deze stap worden de use cases (elk afzonderlijk) getoetst aan een aantal criteria, die helpen om het risicoprofiel van de use case te bepalen. De werkgroep patiëntauthenticatie heeft voor deze toetsing een lijst opgesteld van criteria die relevant kunnen zijn. Deze lijst is opgenomen in Tabel 3. Het beoordelen van elk van deze criteria leidt tot een risicoprofiel voor iedere use case, dat de basis vormt voor het kiezen van een betrouwbaarheidsniveau voor authenticatie in stap 4.

Het beoordelen van deze criteria kan worden gezien als een vereenvoudigde vorm van risicoanalyse. Hierbij worden de kans dat een risicogebeurtenis optreedt en het effect van de risicogebeurtenis niet kwantitatief uitgedrukt. Het vinden van een betrouwbare onderbouwing voor het kwantificeren van kans en effect is veelal lastig, waardoor een kwantificering van kans en effect een arbitrair karakter kan krijgen.

In plaats daarvan is een lijst van criteria voor use cases opgesteld, waarbij elk criterium een aspect van de use case behandelt waarbij bepaalde risico's horen. De redenering hierbij is dat naar mate meer van deze aspecten in een bepaalde use case een rol spelen, het risico verbonden aan de use case groter wordt. Zo is bv. een use case waarbij wijziging van gegevens mogelijk is, in principe meer risicovol dan een use case waarbij alleen sprake is van inzage in gegevens.[7]

We concentreren ons hier op risico's die samenhangen met de methode van patiëntauthenticatie en niet op andere beveiligingsrisico's die te maken kunnen hebben met het aanbieden van een portaal. Het kan bijvoorbeeld om allerlei redenen zeer interessant zijn om op beheerdersniveau toegang te krijgen tot een portaal om zo eventueel ook andere systemen in de organisatie te kunnen benaderen, maar dit heeft in principe geen samenhang met de keuze voor het niveau van patiëntauthenticatie (zie ook hoofdstuk 1.5).

Tabel 3: Criteria voor het bepalen van het risicoprofiel

Nr	Criterium	Toelichting
1	Is er inzage in (tot de persoon herleidbare) persoonsgegevens van niet bijzondere aard?	Hiermee worden alle gegevens bedoeld die betrekking hebben op een specifieke persoon en in het kader van de use case ook op die persoon herleidbaar zijn, maar die niet vallen onder de 'bijzondere persoonsgegevens'. Dit kunnen bijvoorbeeld iemands adresgegevens of telefoonnummer zijn. In dit criterium bedoelen we geen bijzondere gegevens in de zin van de Wet bescherming persoonsgegevens (Wbp), zoals gegevens over godsdienst, ras, politieke gezindheid, gezondheid of strafrechtelijke verleden. Onbevoegde toegang tot persoonsgegevens van niet bijzondere aard kan hinderlijk zijn voor de betrokkene en kan in sommige gevallen zelfs serieuze consequenties hebben voor de persoonlijke levenssfeer, bijvoorbeeld indien een geheim adres of telefoonnummer terecht komt bij iemand die hiervan misbruik kan maken. Dit kan ook indirect misbruik zijn, bijvoorbeeld doordat via de verkregen gegevens ook andere gegevens elders kunnen worden achterhaald (zo vragen dienstverlenende bedrijven bij telefonisch contact vaak de geboortedatum, huisnummer en postcode ter controle van iemands identiteit). Mogelijke waarden voor dit criterium zijn: • Nee, er is geen inzage in tot de persoon herleidbare persoonsgegevens.

[7] Deze methodiek bouwt voort op de methodiek die is gehanteerd in de handreiking 'Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten' van het Forum Standaardisatie (zie hoofdstuk 2.2).

Nr	Criterium	Toelichting
		• Ja, er is inzage in tot de persoon herleidbare persoonsgegevens. In vrijwel alle use cases voor patiëntportalen zal sprake zijn van inzage in tot de persoon herleidbare persoonsgegevens, tenzij sprake is van anonieme toegang tot het portaal (als tenminste door in te breken op het anonieme account niet alsnog gegevens over de betrokkene kunnen worden achterhaald, zoals een e-mailadres).
2	Kunnen er persoonsgegevens (van niet bijzondere aard) gewijzigd worden?	In sommige use cases kunnen er door de patiënt persoonsgegevens gewijzigd worden, bijvoorbeeld contactgegevens. Bij de mogelijkheid tot wijziging van gegevens kan het effect van onbevoegde toegang in principe groter zijn dan in andere gevallen. Er kunnen bijvoorbeeld door een onbevoegde onjuiste gegevens worden doorgegeven over de betrokkene, waardoor bijvoorbeeld post die bedoeld was voor de patiënt naar een verkeerd adres kan worden gestuurd. Een ex-partner zou bijvoorbeeld op een dergelijke manier gezondheidsinformatie kunnen achterhalen. Mogelijke waarden voor dit criterium zijn: • Nee, wijzigen van persoonsgegevens is niet mogelijk. • Ja, er kunnen persoonsgegevens gewijzigd worden.
3	Wordt het burgerservicenummer verwerkt en/of getoond?	Het burgerservicenummer (BSN) wordt bij uitwisseling van informatie tussen zorgverleners verplicht gebruikt (op grond van de Wet gebruik burgerservicenummer in de zorg) om persoonsverwisseling te voorkomen. In veel gevallen zal ook bij het delen van informatie met de patiënt het BSN wordt gebruikt.[8] Het BSN is bedoeld om foutloze uitwisseling van gegevens tussen overheidsorganisaties (en in de zorg en het onderwijs) te ondersteunen, het BSN is dan ook een middel om gegevens uit verschillende gegevensbronnen aan elkaar te koppelen. Daarom kan onbevoegde toegang tot iemands BSN consequenties hebben voor de privacy van de betrokkene, als de persoon die inzicht heeft in het BSN zich ook tot andere gegevensbronnen waarin het BSN is opgeslagen toegang kan verschaffen. Het BSN kan in een patiëntportaal ‘onder de oppervlakte’ worden gebruikt om gegevens te koppelen aan de juiste persoon, maar het kan ook aan de patiënt getoond worden in het portaal. Als het BSN behalve verwerkt ook wordt getoond, is de kans op onbevoegde toegang tot het BSN groter. Mogelijke waarden voor dit criterium zijn daarom: • Nee, het BSN wordt niet verwerkt. • Ja, het BSN wordt verwerkt, maar niet getoond. • Ja, het BSN wordt verwerkt en getoond.

[8] NB: het verwerken van het BSN is toegestaan aan zorgaanbieders op grond van de Wet gebruik burgerservicenummer in de zorg. Het gebruik van BSN is echter niet toegestaan aan niet-zorgaanbieders. Indien een portaal dus niet wordt aangeboden onder de eindverantwoordelijkheid van een zorgaanbieder is het in principe niet toegestaan om het BSN te verwerken.

Nr	Criterium	Toelichting
4	Is er inzage in gezondheidsgegevens (of andere bijzondere persoonsgegevens)?	Use cases waarbij gezondheidsgegevens worden getoond zijn risicovoller dan use cases waarbij dit niet het geval is. Gezondheidsgegevens zijn gevoelige gegevens en vallen daarom in de Wet bescherming persoonsgegevens onder de bijzondere gegevens. De privacy van de betrokkene kan ernstig geschaad worden indien deze gegevens onbevoegd worden geraadpleegd. Dit kan serieuze consequenties hebben voor de persoonlijke levenssfeer. Voor de zorgverlener geldt dat de gegevens die hij opneemt in zijn dossier onder het medisch beroepsgeheim vallen. Op grond van de Wet op de Geneeskundige Behandelingsovereenkomst (WGBO) mag hij deze gegevens niet delen met anderen dan de patiënt en de direct betrokkenen bij de uitvoering van de behandelingsovereenkomst, tenzij sprake is van toestemming van de patiënt.[9] Het is om die reden belangrijk dat hij substantiële zekerheid heeft over de identiteit van de raadpleger van gegevens. In sommige gevallen is het niet onmiddellijk duidelijk is of sprake is van *gezondheidsgegevens*, maar kan gezondheidsinformatie uit andere persoonsgegevens worden *afgeleid*. Voorbeelden zijn de gegevens over inschrijving bij een bepaalde instelling (zoals een instelling voor verslavingszorg) of over een afspraak met een specifieke zorgverlener. Mogelijke waarden voor dit criterium zijn: • Nee, er is geen inzage in gezondheidsgegevens. • Nee, er is geen inzage in gezondheidsgegevens, maar deze zijn mogelijk wel afleidbaar uit andere persoonsgegevens. • Ja, er is inzage in gezondheidsgegevens.
5	Kunnen er wijzigingen (zoals aanvullingen op het medisch dossier) worden gemaakt die invloed kunnen hebben op het medisch handelen?	In sommige gevallen kan de patiënt (al dan niet op verzoek van de zorgverlener) zelf gegevens leveren die onderdeel worden van het medisch dossier, zoals de resultaten van thuismetingen. Dergelijke aanvullingen kunnen in sommige gevallen (mede) de basis vormen voor het medisch handelen, bijvoorbeeld het besluit om iemand voor controle op te roepen. Indien een onbevoegde zich toegang zou weten te verschaffen tot de functies om aanvullingen door te geven, dan zouden in theorie onjuiste gegevens kunnen worden geregistreerd. Mogelijke waarden voor dit criterium zijn: • Nee, er kunnen geen wijzigingen of aanvullingen worden gemaakt die invloed zouden kunnen hebben op het medisch handelen of nalaten. • Ja, er kunnen wijzigingen of aanvullingen worden gemaakt die invloed zouden kunnen hebben op het medisch handelen of nalaten.

[9] Voor een uitgebreide bespreking van de juridische aspecten van patiëntportalen verwijzen we naar Krabben, 2013.

Nr	Criterium	Toelichting
6	Kan de patiënt via het portaal anderen autoriseren?	In sommige gevallen heeft de patiënt de mogelijkheid om via het portaal anderen te autoriseren tot inzage of gebruik van een deel van zijn account, bijvoorbeeld aan een ander (bv. een mantelzorger) via het portaal inzage geven (in een deel van) de gegevens die hem via het portaal ter beschikking staan. In een dergelijk geval heeft een persoon die onbevoegd toegang krijgt de mogelijkheid om namens de eigenlijke patiënt autorisaties uit te delen aan anderen. Afhankelijk van de inrichting van het portaal kan dit mogelijk een tijd lang niet worden opgemerkt. Mogelijke waarden voor dit criterium zijn: • Nee, de patiënt kan geen autorisaties toekennen aan derden. • Ja, de patiënt kan autorisaties toekennen aan derden.
7	Zijn er gegeven de aard van de use case aannemelijke motieven denkbaar die identiteitsfraude in het algemeen aantrekkelijk maken?	Identiteitsfraude wordt waarschijnlijker als er ook iets mee te winnen valt. Daarom zijn use cases waarbij identiteitsfraude winst kan opleveren voor een fraudeur risicovoller dan andere. Een voorbeeld is het gebruik maken van online therapie door een onverzekerde op naam van een verzekerde. In dit voorbeeld geldt overigens dat indien de verzekerde hier zelf aan meewerkt, authenticatie hiervoor geen barrière opwerpt omdat de verzekerde zijn authenticatiemiddel - in strijd met de regels – kan ‘uitlenen’. Een ander mogelijk voorbeeld is het bestellen van herhaalrecepten op naam van iemand anders, indien later in het proces geen identiteitscontrole meer plaatsvindt. Dit wordt overigens pas werkelijk interessant indien men dit kan doen voor grotere aantallen patiënten, bv. alle patiënten van een huisartsenpraktijk. In dit criterium doelen we op motieven die van toepassing zijn op de use case in het algemeen, dus inherent zijn aan de use case. Als het motief zich alleen voordoet in een bijzondere context, dan is er eerder sprake van een risicoverhogende factor. Zo kan het bv. interessant zijn om zich toegang te verschaffen tot de gegevens van een SOA-kliniek om te kijken of er bekende Nederlanders staan ingeschreven, om met deze informatie iemand te chanteren. Daarmee is dit motief echter niet van toepassing op de algemene use case ‘patiënt raadpleegt zijn medisch dossier’ (de use case is immers niet ‘bekende patiënt raadpleegt zijn dossier bij de SOA-kliniek’). Bij het afwegen van motieven voor fraude kan in algemene zin worden gedacht aan zaken als: - geldelijk gewin, of toegang tot zorgdiensten of middelen waardoor indirect geldelijk gewin kan worden verkregen; - criminele motieven zoals chantage of reputatiebeschadiging; - misbruik maken van informatie vanwege conflicten in de persoonlijke sfeer. Mogelijke waarden voor dit criterium zijn: • Nee, er zijn gezien de aard van de use case geen aannemelijke motieven denkbaar die identiteitsfraude aantrekkelijk maken. • Ja, er zijn gezien de aard van de use case aannemelijke motieven denkbaar die identiteitsfraude aantrekkelijk maken.

Het toepassen van de risicoprofielen kan geïllustreerd worden aan de hand van de in stap 1 geïdentificeerde use cases. In tabel 4 is per use case door de werkgroep patiëntauthenticatie een invulling gegeven aan elk van de criteria. Daarbij konden enkele criteria niet in algemene zin worden beoordeeld, omdat de algemene use case op verschillende wijze kan worden ingevuld. Zo staat voor niet alle use cases vast dat het burgerservicenummer (BSN) wordt verwerkt; dit hangt af van de gemaakte keuze voor invulling van de use case. In deze gevallen is voor de beoordeling van het criterium een vraagteken in de tabel opgenomen.

Deze uitwerking is bedoeld als voorbeeld en *niet* om zonder verdere analyse te worden overgenomen, aangezien de uitwerking van een use case in een specifiek geval tot een andere beoordeling kan leiden. De tabel maakt wel duidelijk dat de geïdentificeerde use cases onderling verschillen qua risicoprofiel.

Tabel 4: voorbeelduitwerking risicoprofielen van use cases (? = afhankelijk van implementatie)

Risicoprofiel van voorbeeld use cases		**Use case**							
		1 controle inschrijvingsgegevens	2 wijzigen inschrijvingsgegevens	3 afspraak maken	4 medisch dossier raadplegen	5 medisch dossier aanvullen	6 herhaalrecept aanvragen	7 online contact met zorgverlener	8 deelname online forum
Criterium	Is er inzage in (tot de persoon herleidbare) persoonsgegevens van niet bijzondere aard?	Ja	Ja	Ja	Ja	Ja	Ja	Ja	?
	Kunnen er persoonsgegevens (van niet bijzondere aard) gewijzigd worden?	Nee	Ja	Ja	Nee	Nee	Nee	Ja	Nee
	Wordt het burgerservicenummer verwerkt en/of getoond?	?	?	Ja	?	Ja	Ja	?	Nee
	Is er inzage in gezondheidsgegevens (of andere bijzondere persoonsgegevens)?	Nee	Nee	Moge-lijk afleid-baar	Ja	Ja	Ja	Ja	?
	Kunnen er wijzigingen (zoals aanvullingen op het medisch dossier) worden gemaakt die invloed kunnen hebben op het medisch handelen?	Nee	Nee	Nee	Nee	Ja	Ja	Ja	Nee
	Kan de patiënt via het portaal anderen autoriseren?	Nee	?	?	?	?	?	?	?
	Zijn er gegeven de aard van de use case aannemelijke motieven denkbaar die identiteitsfraude in het algemeen aantrekkelijk maken?	Nee	Ja	Nee	Ja	Nee	Ja	Ja	Nee

4.3 Stap 3 – Bepaal risicoverhogende en risicoverlagende factoren

Nadat de use cases in algemene zin beoordeeld zijn op de verschillende criteria, wordt in deze stap gekeken of er nog specifieke omstandigheden zijn die maken dat de algemene use cases in het specifieke geval meer of minder risico met zich meebrengen dan anders het geval zou zijn.

Voorbeelden van veel voorkomende risicoverhogende of risicoverlagende factoren zijn opgenomen in onderstaande tabellen. Voor het vaststellen van risicoverhogende of risicoverlagende factoren is de specifieke context erg belangrijk, daarom blijft het belangrijk om over de waarde van deze factoren in de eigen situatie een goede afweging te maken.

Tabel 5: Risicoverhogende factoren

Risicoverhogende factoren
De portaalaanbieder of het portaalinitiatief staat onder grote publieke belangstelling. Dit kan extra risico's op reputatieschade met zich meebrengen.
Er nemen bekende personen deel aan het portaal, zonder dat er beleid is vastgesteld met speciale maatregelen ter bescherming van bekende personen.
Het portaalinitiatief heeft een zeer grote schaal (bv. alle klanten van een grote verzekeraar).
De aard van de portaalaanbieder of het portaal maakt dat onbevoegde toegang tot persoonsgegevens extra gevoelig is (bv. een portaal van een verslavingscentrum of SOA-kliniek).
De aard van de portaalaanbieder of het portaal maakt het portaal extra interessant voor aanvallen (bv. een verslavingskliniek waarvan bekend is dat deze veel bekende personen behandelt)?
Er worden genetische gegevens ontsloten, waardoor ook de privacy van anderen dan de patiënt (familieleden) in het geding kan zijn.

Indien een risicoverhogende factor van toepassing is, dan kan dat een reden zijn om het gewenste betrouwbaarheidsniveau te verhogen of om extra maatregelen te nemen. Dit kunnen maatregelen zijn die identiteitsfraude bemoeilijken en/of ertoe leiden dat een eventuele identiteitsfraude zo snel mogelijk wordt ontdekt. Voorbeelden hiervan staan in Tabel 6.

Tabel 6: Risicoverlagende factoren

Risicoverlagende factoren
In de werkprocessen rondom het gebruik van het patiëntportaal zijn veel stappen opgenomen die de kans op identiteitsfraude verkleinen[10]. Voorbeelden van dergelijke stappen zijn: • De patiënt krijgt bij ieder toegangsmoment te zien wanneer hij voor het laatst toegang heeft gehad. • De patiënt krijgt van iedere aanvulling of wijziging meteen een bevestiging via een ander kanaal dan het portaal zelf (bv. via e-mail of sms). • Bij iedere actie die ten gevolge van de acties in het patiëntportaal worden uitgevoerd (bv. verstrekken van een herhaalrecept) is een identiteitscontrole aan de hand van een identiteitsdocument in het proces ingebouwd (bv. bij het ophalen van medicatie op basis van een herhaalrecept). • Er is sprake van een visuele herkenning van de gebruiker (bv. in het geval van online therapie via beeldcontact).
Er is beleid vastgesteld waarbij speciale maatregelen zijn genomen voor de bescherming van de gegevens van bekende personen die deelnemen aan het portaal (bv. gebruik van pseudoniemen en/of aanvullende beveiligingsmaatregelen in de procedurele sfeer).[11]
Het portaalinitiatief is zeer kleinschalig (bv. beperkte cliëntengroep van één ziekenhuis)[12].
Toegang is gelimiteerd in tijd en plaats (bv. binnen een wachtkamer waar toezicht aanwezig is), of er worden algoritmes toegepast om onwaarschijnlijke gebruikspatronen te ontdekken.

Als een risicoverlagende factor van toepassing is, dan is onder omstandigheden verlaging van het resulterende betrouwbaarheidsniveau met één stap mogelijk. Verlaging naar een betrouwbaarheidsniveau lager dan 1 is niet mogelijk.

[10] Sommige maatregelen beperken weliswaar de omvang van de gevolgen van identiteitsfraude voor de groep portaalgebruikers als geheel doordat verder misbruik wordt voorkomen, maar niet voor de individuele portaalgebruiker, wiens gegevens mogelijk al zijn ingezien.

[11] Dergelijk beleid is vaak niet afdoende bij plotseling optredende bekendheid, bijvoorbeeld in geval van betrokkenheid bij een incident dat veel publieke aandacht krijgt.

[12] Voor wat een grote of kleine schaal is moet de context in aanmerking worden genomen; absolute getallen zijn hiervoor niet te geven.

4.4 Stap 4 – keuze van het betrouwbaarheidniveau

In stap 4 wordt aan de hand van het vastgestelde risicoprofiel per use case en de eventuele risicoverhogende en/of risicoverlagende factoren het gewenste betrouwbaarheidsniveau bepaald. Zoals eerder vermeld, wordt hierbij uitgegaan van STORK-niveaus.

Tabel 7 geeft een aanbeveling ten aanzien van de keuze van het betrouwbaarheidsniveau op basis van de invulling van de risicocriteria zoals bepaald in stap 2. De risicoverhogende en risicoverlagende factoren zoals bepaald in stap 3 kunnen leiden tot een betrouwbaarheidsniveau dat een stap hoger of een stap lager ligt.

Tabel 7: Criteria voor het bepalen van het betrouwbaarheidsniveau

Criterium	**Keuze van betrouwbaarheidsniveau (STORK)**
• Wel inzage in (tot de persoon herleidbare) persoonsgegevens van niet bijzondere aard • Geen wijziging van persoonsgegevens (van niet bijzondere aard) • Geen verwerking van het burgerservicenummer • Geen inzage in gezondheidsgegevens (of andere bijzondere persoonsgegevens) • Geen wijzigingen die invloed kunnen hebben op het medisch handelen • De patiënt kan geen autorisaties geven aan derden • Geen aannemelijke motieven die identiteitsfraude aantrekkelijk maken • Geen risicoverhogende factoren	1
• Wel inzage in (tot de persoon herleidbare) persoonsgegevens van niet bijzondere aard • Wel wijziging van persoonsgegevens (van niet bijzondere aard) • Wel verwerking van het burgerservicenummer (maar niet zichtbaar) • Geen inzage in gezondheidsgegevens (of andere bijzondere persoonsgegevens) • Geen wijzigingen die invloed kunnen hebben op het medisch handelen • De patiënt kan geen autorisaties geven aan derden • Geen aannemelijke motieven die identiteitsfraude aantrekkelijk maken	2
• Wel inzage in (tot de persoon herleidbare) persoonsgegevens van niet bijzondere aard • Wel wijziging van persoonsgegevens (van niet bijzondere aard) • Wel verwerking van het burgerservicenummer (ook zichtbaar voor patiënt) • Wel inzage in gezondheidsgegevens (of andere bijzondere persoonsgegevens) • Wel wijzigingen die invloed kunnen hebben op het medisch handelen • De patiënt kan autorisaties geven aan derden • Mogelijk aannemelijke motieven die identiteitsfraude aantrekkelijk maken	3
• Wel inzage in (tot de persoon herleidbare) persoonsgegevens van niet bijzondere aard • Wel wijziging van persoonsgegevens (van niet bijzondere aard) • Wel verwerking van het burgerservicenummer (ook zichtbaar voor patiënt) • Wel inzage in gezondheidsgegevens (of andere bijzondere persoonsgegevens) • Wel wijzigingen die invloed kunnen hebben op het medisch handelen • De patiënt kan autorisaties geven aan derden • Mogelijk aannemelijke motieven die identiteitsfraude aantrekkelijk maken • Risicoverhogende factoren aanwezig (bijvoorbeeld gevoelige context, grootschalig initiatief met veel zichtbaarheid, bekende personen doen mee)	4

Als *voorbeeld* geven we hier een uitwerking per use case op basis van de eerder getoonde risicoanalyse (zie Tabel 8). Deze uitwerking is *niet* bedoeld om zonder verdere analyse te worden overgenomen, aangezien de uitwerking van een use case in een specifiek geval tot een andere beoordeling kan leiden. Het is belangrijk dat bij het toepassen van deze handreiking binnen de zorgpraktijk of zorginstelling de discussie over de inschatting van de risico's grondig wordt gevoerd.
Een goed oordeel valt alleen te geven met inachtneming van de specifieke eigen context. Met name de aanwezigheid van risicoverhogende factoren is in dit voorbeeld nog niet meegenomen.

Bij deze voorbeelduitwerking is in sommige cellen een vraagteken opgenomen. De reden hiervoor is dat voor de desbetreffende vragen meerdere antwoorden mogelijk zijn en het van de specifieke implementatie afhangt welke keuze in de praktijk wordt gemaakt. Zo is het bijvoorbeeld bij de use case 'controle van inschrijvingsgegevens' mogelijk om al dan niet het burgerservicenummer te verwerken en/of te tonen. Het antwoord op deze vraag is dus afhankelijk van de uitwerking die aan de use case wordt gegeven.

Tabel 8: voorbeelduitwerking van de keuze van STORK-niveaus per use case

Risicoprofiel van voorbeeld use cases		**Use case**							
		1 controle inschrijvingsgegevens	2 wijzigen inschrijvingsgegevens	3 afspraak maken	4 medisch dossier raadplegen	5 medisch dossier aanvullen	6 herhaalrecept aanvragen	7 online contact met zorgverlener	8 deelname online forum
Criterium	Is er inzage in (tot de persoon herleidbare) persoonsgegevens van niet bijzondere aard?	Ja	Ja	Ja	Ja	Ja	Ja	Ja	?
	Kunnen er persoonsgegevens (van niet bijzondere aard) gewijzigd worden?	Nee	Ja	Ja	Nee	Nee	Nee	Ja	Nee
	Wordt het burgerservicenummer verwerkt en/of getoond?	?	?	Ja	?	Ja	Ja	?	Nee
	Is er inzage in gezondheidsgegevens (of andere bijzondere persoonsgegevens)?	Nee	Nee	Afleid-baar	Ja	Ja	Ja	Ja	?
	Kunnen er wijzigingen (zoals aanvullingen op het medisch dossier) worden gemaakt die invloed kunnen hebben op het medisch handelen?	Nee	Nee	Nee	Nee	Ja	Ja	Ja	Nee
	Kan de patiënt via het portaal anderen autoriseren?	Nee	?	?	?	?	?	?	?
	Zijn er gegeven de aard van de use case aannemelijke motieven denkbaar die identiteitsfraude in het algemeen aantrekkelijk maken?	Nee	Ja	Nee	Ja	Nee	Ja	Ja	Nee
	STORK-niveau	2	2/3	3	3	3	3	3	1/2

4.5 Stap 5 – keuze van de authenticatiemethode en het authenticatiemiddel

In stap 5 wordt de uiteindelijke keuze gemaakt voor de authenticatiemethode en het bijbehorende authenticatiemiddel. Deze keuze volgt uit het in stap 4 vastgestelde STORK-niveau, waarbij op alle niveaus kan worden gekozen uit meerdere beschikbare alternatieve authenticatiemiddelen.

In Tabel 9 zijn per STORK-niveau concrete voorbeelden opgenomen. Bij het gebruik van deze voorbeelden moet worden aangetekend dat hun geschiktheid om een bepaald STORK-niveau te behalen kan veranderen in de tijd. Of een bepaald authenticatiemiddel geschikt is om een gewenst (STORK-)betrouwbaarheidsniveau te bereiken, is afhankelijk van zowel het middel zelf als van de procedures die worden gehanteerd bij uitgifte en bij het authenticatieproces zelf. In het geval van het gebruik van via SMS verstuurde codes bijvoorbeeld, hoort daar ook bij hoe wordt omgegaan met de procedures voor opgeven/wijzigen van het telefoonnummer waarop de codes ontvangen zullen worden. Verschillende authenticatiemiddelen kennen elk hun specifieke risico's (soms gerelateerd aan het middel zelf, soms aan de procedures rondom uitgifte en gebruik van het middel) die mede bepalend zijn voor het STORK-niveau waarvoor ze geschikt zijn. Het valt buiten de scope van deze handreiking om in detail de risico's te bespreken die verbonden kunnen zijn aan specifieke middelen.[13]

[13] Een relevante ontwikkeling op het gebied van authenticatiemiddelen is eHerkenning. eHerkenning is ontwikkeld voor toegang tot overheidsdiensten en biedt een set met afspraken waarbinnen authenticatiemiddelen voor verschillende STORK-niveaus door verschillende aanbieders worden. De middelen die worden aangeboden in het kader van eHerkenning zijn in principe ook bruikbaar voor authenticatie van personen bij niet-overheidsdiensten. Zie voor het overzicht van middelen die worden uitgegeven in het kader van eHerkenning het overzicht van eHerkenningsmiddelen op www.eherkenning.nl. Hierbij moet wel worden opgemerkt dat eHerkenning zich momenteel richt op bedrijfsmatige authenticatie. Gebruik van eHerkenning voor individuele burgers is op dit moment nog niet aan de orde.
In de indeling van de STORK-niveaus heeft eHerkenning tevens een aanpassing gemaakt, door splitsing van het niveau 2 in 2 en 2+, waarbij niveau 2, anders dan STORK-niveau 2 op één-factor authenticatie gebaseerd is. Het is nog niet duidelijk of deze wijziging in de STORK-systematiek zal worden opgenomen.

Tabel 9: concrete authenticatiemiddelen en procesaanwijzingen per STORK-niveau

Niveau	Authenticatiemiddel	Proces van uitgifte van het middel	Voorbeeld
1	"één-factor", dat wil zeggen één van de volgende factoren: - iets dat je hebt - iets dat je weet - iets dat je bent Voorbeeld: alleen een wachtwoord	Op basis van de eigen bewering van de gebruiker, geen controle op identiteitsbewijs; alleen controle op geldigheid van het e-mailadres.	Facebook-id Windows-live-id Eigen gebruikersnaam en wachtwoord verstrekt door zorgaanbieder.
2	"twee-factor", dat wil zeggen twee van de volgende factoren: - iets dat je hebt - iets dat je weet - iets dat je bent *Voorbeeld 1:* wachtwoord + eenmalige code via SMS *Voorbeeld 2:* wachtwoord + vingerafdruk	Registratie via bekend gegeven, bijvoorbeeld het woonadres uit de Gemeentelijke Basisadministratie (GBA).	DigiD Midden (met wachtwoord en eenmalige code via SMS); Diverse commerciële aanbieders: gebruikersnaam en wachtwoord aangevuld met TAN-code via SMS of one-time-password responder. Gebruikersnaam en wachtwoord aangevuld met token via mobiele app.
3	Eén van de volgende middelen in combinatie met een tweede factor (bv. pincode of wachtwoord): - smartcard - 'soft certificates' (certificaat bewaard op de computer) - 'one time password (OTP) device token' (bv. OTP via sms).	Proces met identiteitsbewijs, en meer checks, bijvoorbeeld fysiek verschijnen bij de uitgifte ('face-to-face' controle).	DigiD Midden in combinatie met een enrollment procedure[14]. Diverse commerciële aanbieders: gebruikersnaam en wachtwoord aangevuld met TAN-code via SMS of one-time-password responder, aangevuld met controle van de legitimatie bij aflevering.
4	Smartcard uitgegeven onder overheidstoezicht. Hierbij is ook een tweede factor nodig (bv. een pincode).	Idem, met altijd fysiek verschijnen bij uitgifte; uitgevoerd door partij die namens overheid gecontroleerd wordt.	Commerciële aanbieders, door OPTA gecertificeerd als aanbieder van gekwalificeerde certificaten.

[14] Een enrollment procedure houdt in dat een manier wordt gevonden om aan de portaalaanbieder te bewijzen dat de eindgebruiker zelf beschikt over een geldig DigiD, bv. door de gebruiker een activeringscode mee te geven, waarmee een account na inloggen met DigiD op basis van de meegegeven activeringscode gekoppeld en geactiveerd kan worden.

Naast het gewenste STORK-niveau, kan men bij de keuze tussen beschikbare alternatieven tevens de aspecten van gebruiksvriendelijkheid, algemene beschikbaarheid en kosten betrekken.

4.5.1 Gebruiksvriendelijkheid

Het aspect van gebruiksvriendelijkheid is in het geval van patiëntportalen van bijzonder groot belang. In het algemeen zijn patiëntportalen gericht op zorgconsumenten in de thuisomgeving en niet op een specifieke beroepsgroep in de zakelijke markt. Men kan daarom minder vooronderstellingen doen over de bekendheid met specifieke middelen en methoden voor informatiebeveiliging (zoals smartcards en smartcardreaders). Middelen die in een zakelijke omgeving redelijk geaccepteerd zijn, kunnen voor patiënten aanzienlijke hindernissen opwerpen voor acceptatie.

Daarnaast blijkt in de praktijk dat de manier van werken met patiëntportalen zorgvuldig moet worden afgestemd op de behoeften en verwachtingen van de gebruiker om acceptatie te vergroten. Dit geldt ook voor de aanmeldingsprocedure en de beveiligingsaspecten daarvan. Overigens is het daarbij van belang om te beseffen dat de gebruiker naast wensen op het gebied van gebruiksgemak ook verwachtingen heeft op het gebied van beveiliging van zijn gegevens.[15]

Met het oog op de gebruiksvriendelijkheid verdient het verder aanbeveling om samen met andere portaalaanbieders (bijvoorbeeld in de regio) tot afstemming te komen over de te gebruiken middelen, aangezien patiënten in het algemeen snel te maken zullen krijgen met meerdere portaalaanbieders.

4.5.2 Beschikbaarheid

Niet alle authenticatiemiddelen zijn op eenvoudige wijze beschikbaar te maken voor een groot publiek. De gemiddelde zorgconsument beschikt niet over een smartcardreader die geïntegreerd is met de PC en evenmin over een paspoortlezer. Dit maakt authenticatiemiddelen die dergelijke apparatuur vereisen minder geschikt voor de zorgconsumentenmarkt.

Er zijn ook voorbeelden van laagdrempelige authenticatiemiddelen die geen aanvullende bijzondere randapparatuur vereisen aan de kant van de gebruiker. Het bekendste voorbeeld is DigiD (dit vereist in het geval van gebruik van een SMS-code wel een mobiele telefoon). Voordelen van DigiD zijn dat het voor burgers gratis is, dat burgers het voor verschillende diensten kunnen gebruiken en dat het relatief veel gebruikers heeft. Op het moment van publicatie van deze handreiking is STORK-niveau 4 echter niet bereikbaar met DigiD. Er zijn ook andere (commerciële) aanbieders van laagdrempelige authenticatiemiddelen, waarvoor geen speciale randapparatuur nodig is. Op het moment van publicatie van deze handleiding werden voor de consumentenmarkt middelen op niveau 4 aangeboden door enkele van de bedrijven die door de OPTA erkend zijn als aanbieder van gekwalificeerde certificaten[16].

Bij de keuze van een authenticatiemiddel is het verder verstandig om rekening te houden met de eventuele wens om een portaal ook aan te bieden via mobiele devices. Voor mobiele devices zijn deels andere oplossingen beschikbaar dan voor webportalen (denk bijvoorbeeld aan het gebruik van een digitaal certificaat dat is opgeslagen op een mobiele telefoon).

Voor zorgaanbieders in de grensstreek die eventueel te maken hebben met buitenlandse patiënten, kan het wellicht onverstandig zijn om uitsluitend DigiD als enige authenticatiemiddel te kiezen, aangezien buitenlandse patiënten niet hierover kunnen beschikken.

[15] Er leven niet alleen verwachtingen bij de daadwerkelijke eindgebruiker, maar ook bij maatschappelijke groepen, zoals organisaties die de belangen van patiënten vertegenwoordigen of politieke partijen. Het is daarom verstandig om maatschappelijke groepen, voor wiens achterban het portaalinitiatief relevant kan zijn, bij keuzes over beveiligingsaspecten te betrekken, bv. als klankbord.
[16] Zie http://www.opta.nl/nl/registraties/geregistreerde-ondernemingen

4.5.3 Kosten

Het kostenaspect speelt een belangrijke rol bij het aanbieden van patiëntportalen aan zorgconsumenten. In het geval dat het authenticatiemiddel door de zorgaanbieder/portaalaanbieder wordt bekostigd, kan dit bij grotere aantallen gebruikers tot niet verwaarloosbare kosten leiden, zeker indien de zorgconsument ook bijzondere randapparatuur nodig heeft, zoals smartcardlezers.

Indien de bekostiging moet plaatsvinden door de zorgconsument zelf, kan dit een drempel opwerpen voor het gebruik, zeker als de aanschaf van het authenticatiemiddel en randapparatuur alleen bedoeld is voor toegang tot het portaal (en elders niet gebruikt kan worden voor een voor de zorgconsument interessante dienst).

Vooralsnog is DigiD het meest bekende voorbeeld van een authenticatiemiddel dat gratis wordt verstrekt.

4.5.4 Algemene aanbevelingen ten aanzien van de gemaakte keuze voor een middel

Ten aanzien van de gemaakte keuze bevelen we het volgende aan:

1. Documenteer zorgvuldig de gemaakte afweging.
2. Neem maatregelen (ook procedureel) die identiteitsfraude bemoeilijken en die borgen dat een eventuele identiteitsfraude zo snel mogelijk ontdekt wordt; enkele voorbeelden van dergelijke maatregelen zijn gegeven onder het kopje ‘risicoverlagende factoren’ in Tabel 6.
3. Maak een actieplan dat het mogelijk maakt om zo snel mogelijk adequaat in te grijpen in het geval van concrete verdenking van identiteitsfraude. Oefen de procedures die in dit plan zijn opgenomen.
4. Informeer patiënten voorafgaand aan deelname aan het patiëntportaal op heldere wijze (in voor hen begrijpelijke taal) over eventuele risico’s en hoe hiermee wordt omgegaan. Besteedt daarbij ook aandacht aan de maatregelen die de patiënt zelf kan nemen, zoals het alert zijn op berichten over toegang tot zijn account.
5. Herzie op gezette tijden de gemaakte keuze en ga na of inmiddels een beter middel beschikbaar is.
6. Wees transparant over geconstateerd misbruik en verschaf hierover heldere openbare rapportages. Informeer getroffen gebruikers onmiddellijk (Ekker, 2012). Dit vereist het voeren van een actief auditbeleid.

4.5.5 Eventuele keuze voor een lager betrouwbaarheidsniveau

Het kan voorkomen dat men op het beoogde betrouwbaarheidsniveau geen middel kan vinden dat bruikbaar is in de beoogde context van de eindgebruiker[17] en in voldoende mate beschikbaar gemaakt kan worden voor de doelgroep tegen acceptabele kosten. In dit geval staat men voor de lastige keuze om (tijdelijk) te kiezen voor een lager betrouwbaarheidsniveau dan men ideaal zou vinden of om voorlopig geheel van het beoogde initiatief af te zien.

Let wel: de Wet bescherming persoonsgegevens (Wbp) vereist een *passend* beveiligingsniveau, rekening houdend met de risico’s, de stand van de techniek en de kosten van de tenuitvoerlegging. Men kan dus rekening houden wat gezien de stand der techniek haalbaar is tegen redelijke kosten. Echter, men kan dit niet als excuus gebruiken om risicovolle situaties langere tijd te laten bestaan.

Bij het kiezen van een (tijdelijk) lager betrouwbaarheidsniveau moet sprake zijn van zwaarwegende argumenten. Men dient de mogelijkheid om in plaats daarvan voorlopig van de voorgenomen dienst af te zien serieus te overwegen. Immers, men kan de doelgroep onbedoeld blootstellen aan privacyrisico’s. Echter, daar kunnen andere zwaarwegende belangen van de doelgroep tegenover staan (bv. een beter geïnformeerde patiënt).

Belangrijk hierbij is dat men een bewuste risicoafweging maakt op het juiste niveau in de organisatie. De bestuurlijk verantwoordelijke moet een evenwichtig oordeel kunnen vormen over de risico’s voor patiënten en organisatie die samenhangen met de gemaakte keuzes.

17 In het kader van deze handreiking zal dit meestal de thuisomgeving van de patiënt zijn.

Daarom dient men bij de eventuele keuze om tijdelijk een authenticatiemiddel van een lager dan gewenst niveau te gebruiken, ten minste alle aanbevelingen te volgen zoals genoemd in hoofdstuk 4.5.4. Besteed hierbij nog extra aandacht aan het nemen van zoveel mogelijk compenserende maatregelen die extra waarborgen kunnen bieden tegen identiteitsfraude en aan het goed informeren van patiënten over de risico's. Herzie regelmatig de gemaakte keuze en ga na of inmiddels een beter middel beschikbaar is.

4.6 Tot slot

Misbruik of diefstal van authenticatiemiddelen is slechts één van de mogelijke beveiligingsrisico's.

In de praktijk zijn – helaas steeds meer - voorbeelden bekend van ongeautoriseerde toegang door misbruik van softwarelekken, zwakheden in (verouderde) infrastructuur, databases, fabrieksinstellingen van beheeraccounts en dergelijke.

Een zorgaanbieder kan onevenredige aandacht en middelen besteden aan authenticatieaspecten (met bijbehorende nadelige consequentie voor het gebruikersgemak), in vergelijking met andere beveiligingsmaatregelen (zoals inzet van anti-virussoftware, actueel houden van infrastructurele software, configuratie van firewalls).

Het is belangrijk om bij de afweging van risico's de keuze van authenticatiemiddelen ook vanuit deze context te bezien en naar een balans te zoeken tussen de verschillende beveiligingsmaatregelen.

5 Relevante bronnen

1 College Bescherming Persoonsgegevens; *CBP Richtsnoeren – Beveiliging van persoonsgegevens*; College Bescherming Persoonsgegevens, Den Haag, februari 2013
2 Forum standaardisatie; *Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten – een handreiking voor overheidsorganisaties*; Forum standaardisatie, januari 2012
3 Ekker, A.H.; *In vier stappen voldoen aan de meldplicht datalekken*; Nictiz, 20 september 2012, ID-nummer 12015
4 Hulsebosch, B., Lenzini, G. en Eertink, H.; *D2.3 Quality authenticator scheme*, STORK-eID consortium, 3 maart 2009
5 Heldoorn, M., van Herk, E. en Veereschild, S.; *Online inzage in mijn medische gegevens – Patiëntportalen in Nederlan*d; Nictiz, 16 mei 2011, ID-nummer RP 110013.
6 Honan, M.; *Kill the password, why a string of characters can't protect us anymore*; Wired, 15 november 2012; geraadpleegd op 28 augustus 2013 op http://www.wired.com/gadgetlab/2012/11/ff-mat-honan-password-hacker/all/
7 Jacobs, B., Nouwt, S., de Bruijn, A., Vermeulen, O., van der Knaap, R., de Bie, C.; *Beveiligingseisen ten aanzien van identificatie en authenticatie voor toegang zorgconsument tot het Elektronisch Patiëntendossier (EPD)*; PriceWaterhouseCoopers, Universiteit van Tilburg, Radboud Universiteit Nijmegen, 2 december 2008
8 Krabben, J.A.L.; *Een juridisch kader voor Patiëntportalen*; Nictiz en NPCF, Den Haag, juli 2013.
9 NEN 7512:2005, *Medische informatica – Informatiebeveiliging in de zorg – Vertrouwensbasis voor gegevensuitwisseling*; NEN, Delft, 1 oktober 2005
10 PWC; *Digitale toegang tot het eigen medisch dossier: mogelijkheden voor een elektronische sleutel*; PWC, 25 november 2011; Referentie A-2011-2087/OV/cdb/mp
11 Radboud Universiteit Nijmegen en PriceWaterhouseCoopers; *Risicoanalyse EPD-DigiD naar aanleiding van de A5/1 kwetsbaarheid in GSM*; Radboud Universiteit Nijmegen en PriceWaterhouseCoopers, 30 juni 2010; Referentie 2010-1400/OV/ev/mp

6 Lijst van afkortingen

CBP	College bescherming persoonsgegevens
BSN	Burgerservicenummer
HSM	Hardware security module
NAW	Naam, adres, woonplaats
OPTA	Onafhankelijke post- en telecommunicatieautoriteit
OTP	One time password
PKI	Public key infrastructure
SOA	Seksueel overdraagbare aandoening
STORK	secure identity across borders linked (het acronym is *niet* afgeleid van de eerste letters van elk woord)
UZI	Unieke zorgverleneridentificatie
Wbp	Wet bescherming persoonsgegevens

7 Leden van de werkgroep

Deze handreiking is samengesteld door de werkgroep patiëntauthenticatie van het platform Patiënt en eHealth. Aan de werkgroep namen de volgende personen deel:

- Martijn Bakkers, directeur van MedischeGegevens.nl
- Chris Flim, eigenaar van Flim Consultancy
- Marcel Heldoorn, senior beleidsmedewerker bij de Nederlandse Patiënten en Consumenten Federatie (werkgroepvoorzitter)
- Ronald Huijgens, director biometric technology bij Unisys
- Johan Krijgsman, senior consultant bij Nictiz, het Nationaal Instituut voor ICT in de Zorg (werkgroepsecretaris)
- Marcel van Loosbroek, voorzitter van Stichting Innovatieprojecten OIZ
- Jan van der Sluis, Client Security Offer, Hewlett-Packard Nederland
- Wouter Tesink, IT-architect bij het VZVZ-Servicecentrum
- Florian Visser, projectleider bij Zorgportaal Rijnmond
- Maarten Wegdam, managing advisor bij Novay
- Poppe Wijnsma, partner bij PKI-partners.

Daarnaast danken wij diverse deskundigen die met constructieve opmerkingen en aanvullingen hebben bijgedragen aan de totstandkoming van dit document. Met name danken wij Jaap Kuipers, oprichter van het Platform Identity Management Nederland. Wij danken ook diverse deskundigen die de moeite hebben genomen om ons van (soms stevig) reviewcommentaar te voorzien, te weten René van de Assem, Rik Ernst, Leon Haszing, Peter Jurg, Jacqueline Krabben, Remco Schaar, Jan Willem Schoemaker, Ron van Troost, Ivar Vennekens, Ton Verschuren, Peter Waters en Kick Willemse. Hun commentaar is verwerkt naar het inzicht van de werkgroep; het is dan ook niet mogelijk de indieners van commentaar verantwoordelijk te houden voor de inhoud van dit document.

8 Vragen en antwoorden

In dit hoofdstuk komen vragen aan de orde die lezers van de handreiking aan de werkgroep hebben gesteld. Om andere lezers bij wie mogelijk soortgelijke vragen leven behulpzaam te zijn, heeft de werkgroep in dit hoofdstuk de antwoorden op enkele vragen opgenomen. Deze vragen en antwoorden kunnen worden gezien als een toelichting op de handreiking.

Waarom wordt niet ingegaan op de risico's die verbonden zijn aan het gebruik van bepaalde soorten authenticatiemiddelen?

De STORK-methodiek dient juist om een ontkoppeling aan te brengen tussen de use case en het specifieke authenticatiemiddel. Eerst bepaalt men op basis van de risico's van de use case welk niveau van zekerheid men wenst te hebben over de identiteit van de gebruiker. Bij dat niveau wordt dan vervolgens een passend middel gezocht. Afhankelijk van de risico's die aan een specifiek middel zijn verbonden, is het al dan niet geschikt om het gewenste zekerheidsniveau te bereiken.

We hebben het bespreken van de risico's van individuele authenticatiemiddelen (zoals phishing van wachtwoorden of kopiëren van smartcards) willen vermijden omdat een dergelijke bespreking de handreiking gevoeliger maakt voor veranderingen in de tijd. Of een bepaald authenticatiemiddel geschikt is om een gewenst (STORK-)betrouwbaarheidsniveau te bereiken, is immers afhankelijk van zowel het middel zelf als van de procedures die worden gehanteerd bij uitgifte en bij het authenticatieproces zelf. In het geval van het gebruik van SMS-tokens bijvoorbeeld, hoort daar ook bij hoe wordt omgegaan met de procedures voor opgeven/wijzigen van het telefoonnummer waarop de codes ontvangen moeten worden.

De middelspecifieke risico's kunnen in de loop der tijd veranderen. Bij elk authenticatiemiddel zou men zich eigenlijk vijf vragen kunnen stellen, gerelateerd aan de punten genoemd in hoofdstuk 3 van deze handreiking:

- Wat is bekend over de mate waarin de uitgever van het authenticatiemiddel zijn procedures op orde heeft?
- Welke eisen worden gesteld aan de identificatie van de natuurlijke persoon voorafgaand aan de uitgifte van het authenticatiemiddel?
- Hoe goed wordt bij het (her)uitgifteproces gegarandeerd dat het middel bij de juiste persoon terechtkomt? Is het middel makkelijk onrechtmatig te verkrijgen?
- Wat is bekend over de robuustheid van het middel zelf? Zijn er gedocumenteerde gevallen waarin het middel gecompromitteerd is? Is het middel makkelijk na te maken?
- Is er bij het gebruik van het authenticatiemiddel voldoende garantie dat het middel op de juiste wijze wordt aangeboden en gecontroleerd (denk ook aan ingetrokken middelen)?

Afhankelijk van de antwoorden op deze vragen, kan het middel al dan niet geschikt zijn voor het gebruik bij hogere betrouwbaarheidsniveaus.

Hoe ga ik om met een situatie waarin verschillende use cases andere betrouwbaarheidsniveaus vereisen?

Webportalen van (zorg)aanbieders zullen in veel gevallen meerdere diensten (use cases) ondersteunen. Mogelijk elk met een andere betrouwbaarheidseis (STORK). Dit roept de vraag op welk betrouwbaarheidsniveau het portaal bij inloggen vereist. De ene keer wil de patiënt alleen zijn gegevens inzien, en de volgende keer ook wijzigen.

Eén strategie is het voorschrijven van de hoogste betrouwbaarheid voor alle handelingen op het portaal. Maar dit verlaagt de gebruiksvriendelijkheid en verhoogt de kosten.

Een betere oplossing is ondersteuning voor verschillende betrouwbaarheidsniveaus, in combinatie met een mechanisme voor 'bij-authenticeren'. Vergelijk dit met het gebruik van internetbankieren. Bij sommige websites voor internetbankieren kan men binnenkomen met gebruikersnaam/wachtwoord. Op het moment dat een actie wordt ondernomen met een hoger vereist betrouwbaarheidsniveau (bijvoorbeeld een

overboeking maken) wordt een aanvullende vorm van authenticatie vereist (bv. een TAN-code van een lijst of een via SMS verstuurde code).

Waarom wordt het onderwerp machtigingen niet behandeld?

Er kunnen situaties voordoen waarin namens patiënten anderen (bv. familieleden of mantelzorgers) toegang zouden moeten kunnen krijgen tot een patiëntportaal. Er kan bijvoorbeeld sprake zijn van machtigingen, waarbij de patiënt er zelf voor kiest om iemand anders toegang te geven, of van bijvoorbeeld een ouder-kind relatie.

Hierbij kan in de uitvoering het vaststellen van bevoegdheid problematisch zijn. Het aspect machtiging is echter geen *authenticatie*aspect, maar een *autorisatie*aspect. Het gaat erom vast te stellen dat de gemachtigde geautoriseerd is om namens de machtigende partij op te treden. De keuze voor het authenticatiemiddel van de gemachtigde is (in het algemeen) niet anders dan de keuze voor het authenticatiemiddel van de machtigende partij. Als voor de patiënttoegang gekozen wordt voor twee-factor-authenticatie, zal dit voor de gemachtigde ook gelden.

Er is in zoverre een samenhang met authenticatie, dat sommige verstrekkers van authenticatiemiddelen de mogelijkheid bieden om naast het aanvragen van authenticatiemiddelen ook machtiging te regelen, als beide partijen bij de middelenverstrekker bekend zijn. Een voorbeeld is 'DigiD Machtigen'.

Wat kan ik doen om grensoverschrijdende toegang te regelen?

Hierbij is het zaak om een middel te kiezen dat in beide landen beschikbaar is of twee verschillende middelen met eenzelfde STORK-niveau. De STORK-methodiek is hierbij behulpzaam, want STORK is juist bedoeld om op Europees niveau de betrouwbaarheidsniveaus van authenticatiemiddelen met elkaar vergelijkbaar te maken. Middelen uit verschillende landen die hetzelfde STORK-niveau hebben, zijn in feite even betrouwbaar.

Waarom is 'het mogelijk zijn van een transactie met een financiële consequentie' geen apart criterium om het risico van een use case te beoordelen in hoofdstuk 4.2?

Dit aspect is opgenomen in een breder criterium dat gaat over de mate waarin fraude aantrekkelijk is. Sommige use cases zijn aantrekkelijker voor fraude dan andere, bijvoorbeeld omdat er geldelijk gewin mogelijk is, maar er kunnen ook andere motieven zijn die fraude aantrekkelijk maken (zoals het misbruik van informatie vanwege conflicten in de persoonlijke sfeer). De gebruikservaringen met deze handreiking kunnen overigens nog uitwijzen dat bepaalde criteria anders geformuleerd zouden moeten worden.