

# e-identity: zorgeloze identificatie van zorgconsumenten



KENNIS, IDENTIFICATIE

Betere zorg door betere informatie

**Datum**  
23 april 2010

**ID nummer**  
KA10002

**Auteur(s)**  
drs. Maarten Wegdam (Novay)

**Dit kennisartikel geeft een beschrijving van de ontwikkelingen op het gebied van e-identity in de zorg. De nadruk ligt op de zorgconsument. Andere e-identity vraagstukken binnen de zorg, zoals e-identity voor zorgprofessionals in de zorgketen of binnen de zorginstelling, worden buiten beschouwing gelaten. De primaire doelgroep van dit artikel zijn beslissers en beleidsmakers in de zorg die affiniteit hebben met ICT.**

**U vindt informatie over de rol van e-identity in online dienstverlening en de relatie met privacy. Daarna wordt ingegaan op de veiligheidsproblematiek en de ontwikkeling rondom e-identity op het internet. Tot slot de gevolgen van e-identity ontwikkelingen voor de ICT roadmap en architectuur voor online dienstverlening.**

## Samenvatting

De communicatie tussen zorginstellingen en zorgconsumenten verloopt steeds meer via het internet. Internet wordt niet alleen ingezet voor relatief simpele zaken als een afspraak, maar ook voor geavanceerde Health 2.0 tele-medicine applicaties. Voorwaarde voor verantwoord gebruik van internet is een goede e-identity voor zorgconsumenten.

De trend is hergebruik van bestaande identiteiten en bijbehorende authenticatiemiddelen voor verschillende diensten. Zorgverleners dienen te letten op veiligheid, gebruikersgemak, kosten en beschikbaarheid van e-identity oplossingen. De meest voor de hand liggende keuzes zijn DigiD of oplossingen gebaseerd op open standaarden zoals OpenID.

De keuze voor de Nederlandse gezondheidszorg voor DigiD of OpenID wordt in dit Nictiz kennisartikel verduidelijkt.

# Introductie

Een e-identity is een digitale representatie van een identiteit. Deze bestaat uit een serie van attributen, zoals naam, geboortedatum, geslacht, adres of een Burger Service Nummer (BSN). Aan een e-identity zijn één of meer authenticatiemiddelen gekoppeld, zoals een gebruikersnaam en een wachtwoord of een smartcard.

De veiligheid van een e-identity oplossing is niet alleen afhankelijk van de veiligheid van het authenticatiemiddel. Maar ook van het uitgifteproces waarmee iemand een e-identity krijgt. Een voorbeeld van een uitgifteproces is het authenticatiemiddel per post naar een bekend adres sturen, of een 'face2face' controle van het paspoort tijdens de uitgifte.

## Health2.0: online dienstverlening in de zorg

Ook in de zorg neemt het gebruik van internet steeds verder toe, een ontwikkeling die vaak wordt aangeduid met de term Health2.0. Denk hierbij aan applicaties in de tele-medicine sfeer; Personal Health Records en online zelfzorg voor chronische aandoeningen. Maar denk ook aan simpele interacties tussen zorginstellingen en zorgconsumenten voor het maken van een afspraak of het verstrekken van informatie. Hierbij is het belangrijk te weten wie de zorgconsument is. Dit vereist een e-identity oplossing die de zorgconsument identificeert op een voldoende veilige manier, en de relevante persoonsattributen hierbij doorgeeft; zoals de naam, geboortedatum, geslacht of BSN.

E-identity is onlosmakelijk verbonden met privacy. E-identity is hierbij tegelijkertijd zowel een gevaar voor de privacy van de zorgconsument, als een middel om de privacy van de zorgconsument te beschermen. Het gevaar bestaat dat een e-identity oplossing wordt gebruikt om online gedrag van individuele patiënten te monitoren en het gedrag op verschillende websites met elkaar

in verband te brengen, zonder dat hiervoor een directe noodzaak bestaat. Daarnaast bestaat het gevaar dat een dienst aanbieder meer persoonsattributen opvraagt dan nodig is. Belangrijk is alleen die attributen van een patiënt te verstrekken die strikt noodzakelijk zijn voor de specifieke dienst.

Ook dient, waar mogelijk, gebruik gemaakt te worden van anonimisering en pseudonimisering. Hiermee wordt de privacy van de zorgconsument beschermd.

Zo zal het voor een online patiëntenforum vaak niet nodig zijn om bezoekers te identificeren met hun echte naam. Wel kan het nuttig zijn een eerdere bezoeker te herkennen aan de hand van een browser cookie (pseudonimisering).

Naast bovenstaande maatregelen om de privacy te beschermen, hoort een e-identity oplossing ook de privacy te beschermen door simpelweg de identiteit van een zorgconsument op voldoende veilige manier te verifiëren, met name als er toegang wordt gegeven tot gezondheidsinformatie van een patiënt.



# De uitdaging

Op dit moment gebruiken de meeste internetgebruikers voor elke online dienstverlener veelal een afzonderlijke identiteit. Voor deze vele digitale identiteiten zijn evenveel gebruikersnamen en wachtwoorden (of andere authenticatiemiddelen) nodig. Deze situatie wordt ook wel aangeduid als de 'silo-benadering'. De combinatie van de vele gebruikersnamen en of wachtwoorden en het hergebruik van wachtwoorden is een kwetsbare plek in de bescherming van onze digitale identiteiten<sup>1</sup>.

Uit onderzoek, gedaan in 2009 in het Verenigd Koninkrijk, blijkt dat één derde van de internetgebruikers hetzelfde wachtwoord gebruikt voor alle websites en dat ongeveer de helft gebruik maakt van slechts enkele wachtwoorden.<sup>2</sup> Criminelen maken hier dankbaar gebruik van voor identity theft. Kortweg: Het stelen van persoonsgegevens.

Indien een wachtwoord kan worden achterhaald, kan hiermee toegang worden verkregen tot persoonlijke informatie en de e-identity van de gebruiker worden aangenomen. De gevolgen kunnen desastreus zijn: er wordt geld afgeschreven van de bankrekening, persoonlijke informatie wordt veranderd, de gebruiker wordt gehanteerd, etc.

Veelgebruikte technieken door criminelen om wachtwoorden te pakken te krijgen zijn phishing en het gebruik van malware.

Bij phishing wordt een website door criminelen nagebouwd om gebruikers hun wachtwoord te ontfrutselen. Bij malware draait er kwaadwillende software op de PC van een gebruiker om bijvoorbeeld gebruikersnaam en wachtwoord door te sturen naar de hacker.

Deze veiligheidsproblematiek kan voor een deel worden opgelost door gebruik te maken van veiligere authenticatieoplossingen. Voorbeelden van veiligere authenticatieoplossingen zijn smartcards. Zoals de UZI pas die in Nederland door zorgprofessionals gebruikt wordt, en zogenaamde one-time-password tokens die telkens een ander, tijdelijk wachtwoord genereren. Veiligere authenticatieoplossingen voor consumenten zijn in Nederland wel gebruikelijk voor online banking, maar voor andere toepassingen (nog) niet. Een andere maatregel om de veiligheid te verhogen is het loggen van de toegang en het gebruik van online diensten. Dit biedt de mogelijkheid om te detecteren dat er ongewenste toegang heeft plaatsgevonden. Deze detectie kan handmatig gebeuren, maar ook geautomatiseerd door intelligente algoritmes die de logdata analyseren.



<sup>1</sup> Zie bv. ENISA rapport *Web 2.0 Security and Privacy*, 10 december 2008, <http://www.enisa.eu>.

<sup>2</sup> Zie *Web users stick to one password, survey reveals*, Computer Weekly, 10 maart 2009.

# Werkwijze

## Recente ontwikkelingen: identity federatie en user-centric identity

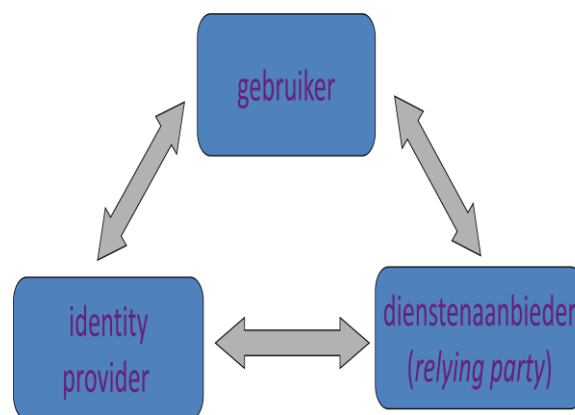
De silo-benadering kent naast bovenstaande veiligheidsrisico's ook andere nadelen. In de eerste plaats worstelen gebruikers met lijsten van gebruikersnamen en wachtwoorden, die moeilijk te onthouden zijn. Een veilige uitgifte van identiteiten is daarnaast kostbaar en complex, waardoor dit vaak wordt nagelaten. Ten slotte zijn veilige authenticatiemiddelen duur, waardoor deze vaak niet gebruikt worden.

Er zijn twee belangrijke en aan elkaar gerelateerde ontwikkelingen rondom identiteitsoplossingen op het internet die tegemoet komen aan deze problemen: identity federatie en user centric identity.

### Identity federatie

Als reactie op bovenstaande nadelen van silo-oplossingen is sinds enkele jaren de federatieve benadering van e-identity sterk in opkomst. Gartner beschouwt deze technologie als early mainstream en als goed gepositioneerd om als basis voor consumenten identificatie gebruikt te gaan worden.<sup>3</sup> In een federatieve benadering van e-identity vertrouwt de online dienstverlener (ook relying party genoemd) op een andere partij (de identity provider) om de gebruiker te identificeren (zie ook Figuur 1).

De identity provider fungeert hier als een Trusted Third Party, die zowel door de online dienstverlener als de gebruiker vertrouwd moet worden. Om dit vertrouwen verder te vergroten kan ook een vierde, toezichhoudende, partij in het proces worden betrokken.



Figuur 1 - Drie partijen e-identity federatie model

De voordelen van dit federatieve model zijn evident: het is potentieel goedkoper, veiliger en gebruikersvriendelijker. Er hoeven immers minder authenticatiemiddelen te worden gebruikt en de kosten worden gedeeld door meer partijen. Afhankelijk van de implementatie biedt het ook de mogelijkheid voor een single sign-on ervaring bij de gebruiker, waardoor hij zich niet telkens opnieuw hoeft te authenticeren. Federatieve benaderingen worden overigens ook vaak gebruikt binnen grotere organisaties om single sign-on te leveren.

### User-centric identity

De tweede belangrijke ontwikkeling op het gebied van e-identity heet user-centric identity. In de federatieve aanpak is het voor gebruikers vaak onduidelijk welke informatie over hen wordt uitgewisseld. User-centric identity is een extensie van de federatieve benadering waarbij een gebruiker, veel meer dan nu het geval is, inzicht en controle krijgt over welke data er potentieel uitgewisseld gaat worden tussen de identity provider en de dienstenaanbieders. Uitwisseling van e-identity informatie vindt pas plaats na expliciete toestemming van de gebruiker.

Er is geen harde scheidslijn te trekken tussen welke identity federatie benaderingen wel en welke niet user-centric zijn. Uitgangspunten zijn in ieder geval, naast inzicht en controle over uit te wisselen data, dat alleen die data

<sup>3</sup> Gartner, *Hype Cycle for Identity and Access Management Technologies*, 2009, 16 juli 2009.

<sup>4</sup> Creative Commons Naamsvermelding-Gelijk delen 3.0 Nederland Licentie is van toepassing op dit werk <http://creativecommons.org>

uitgewisseld wordt die strikt noodzakelijk is (minimal disclosure), dat pseudoniemen ondersteund worden en dat er een consistente en begrijpelijke interactie met de gebruiker is.

Figuur 2 illustreert hoe inzicht en consent kunnen werken door middel van een fictief voorbeeld van een screenshot waarin een gebruiker consent moet geven bij het inloggen op het patiëntenportaal van ziekenhuis Waddenburg.

**Toestemming**  
www.mijnZiekenhuisWaddenburg.nl wil graag het volgende van je weten:

- je voor- en achternaam (*Maarten Wegdam*)
- je adres (*Brouwerijstraat 1, 7523 XC, Enschede*)
- je emailadres (*maarten.wegdam@novay.nl*)
- je geboortedatum (*01-01-1901*)

Vink hierboven uit welke informatie niet mag worden doorgegeven.

Doe dit voortaan automatisch.

**Figuur 2 - Fictief voorbeeld van gebruikersconsent.**

User-centric identity oplossingen werken nu nog vaak met zogenaamde self-asserted identities, waarbij de identity provider de attributen niet geverifieerd heeft. De betrouwbaarheid van de hierdoor verschaft attributen is vanzelfsprekend laag, maar het is desalniettemin al wel veiliger en gebruikersvriendelijker dan een silo-benadering. User-centric identity principes kunnen echter ook heel goed gebruikt worden in situaties waarin de identity provider wel geverifieerde attributen verschaft en dit zal naar verwachting ook in toenemende mate gebeuren.

## Standaarden

Er zijn verschillende federatiestandaarden. De meeste gebruikte zijn OpenID en SAML. OpenID (<http://openid.net>) is in relatief korte tijd de meest populaire user-centric identity specificatie geworden op het internet. OpenID wordt ondersteund door grote internet bedrijven, inclusief sociale netwerk partijen. Een grote partij in Nederland die OpenID ondersteunt is Hyves (ongeveer 8 miljoen

gebruikers), maar ook bijvoorbeeld Yahoo en Google zijn OpenID identity providers.

Hierdoor beschikt een meerderheid van de consumenten, en zeker het overgrote deel van de jeugd, reeds over een OpenID identiteit. OpenID is een relatief simpele standaard, maar heeft als grootste nadeel dat het beperkte veiligheid biedt. Het is daarmee alleen geschikt voor online diensten waarbij het gaat om personalisatie en minder voor privacy- of fraudegevoelige diensten. SAML (<http://www.oasis-open.org>) bestaat langer en wordt veel als identiteit oplossing binnen en tussen grote organisaties gebruikt, en voor e-overheid. Het is veiliger dan OpenID en daarmee ook geschikt voor meer kritische toepassingen. Andere standaarden zijn het nog veelbelovende maar nog weinig gebruikte Information Cards en het met name door Microsoft gebruikte WS-Federation.

## e-identity door de overheid

Ook bij elektronische dienstverlening door de overheid is een veilige e-identity oplossing noodzakelijk. In Nederland is hiervoor DigiD ontwikkeld. Hierbij is er één centrale identity provider, namelijk de rijksoverheid. DigiD is momenteel nog gebaseerd op een proprietary protocol, maar zal overgaan op het eerder genoemde SAML protocol.

DigiD kent verschillende niveaus voor authenticatie. Het laagste, en meest gebruikte, maakt gebruik van een wachtwoord en gebruikersnaam-combinatie. Het middelste niveau gebruikt SMS als authenticatiemiddel. Hierbij wordt een SMS met een eenmalig geldig wachtwoord (one-time-password) verstuurd naar de burger. Het hoogste niveau is nog niet ingevuld, hiervoor zal typisch smartcard technologie gebruikt gaan worden.

Een DigiD is aan te vragen door iedereen die beschikt over een BSN-nummer en woonachtig is in Nederland. Sinds kort kunnen klanten van de Sociale Verzekeringsbank die woonachtig zijn in het buitenland daarnaast ook een DigiD aanvragen. Omdat het gebruik van DigiD zoveel mogelijk voor iedereen

mogelijk te maken voor iedereen die een relatie heeft met de Nederlandse overheid, werkt de overheid ten slotte aan de zogenaamde Registratie Niet Ingezetenen (RNI). Denk hierbij bijvoorbeeld aan Nederlanders die net over de grens in België of Duitsland wonen, werken, naar school gaan en mogelijk ook gebruik maken van zorg in Nederland.

Ook voor de toegang van patiënten tot hun eigen patiëntgegevens in het landelijk EPD zal gebruik gemaakt gaan worden van DigiD. Vanwege de privacygevoeligheid van de informatie in het EPD is een hoog beveiligingsniveau nodig. Het huidige hoogst beschikbare niveau voor DigiD is niveau middel (authenticatie op basis van een via SMS verstuurd one-time-password). Het huidige uitgifteproces is echter niet veilig genoeg bevonden<sup>4</sup>. Hieraan zal daarom een face-to-face controle met een officieel legitimatiebewijs worden toegevoegd. Deze DigiD middel met face-to-face controle wordt ook wel aangeduid als EPD-DigiD (of DigiD-SMS+).

Het gebruik van DigiG is alleen toegestaan indien hiervoor een wettelijke grondslag bestaat. Dit is gekoppeld aan het gebruik van het BSN, en daarmee beperkt tot e-overheid, pensioenuitvoerders en de zorg.

Zorgverzekeraars en zorginstellingen mogen hierdoor DigiD gebruiken. CZ en Agis zijn voorbeelden van zorgverzekeraars die dit al doen. En bijvoorbeeld patiëntenportalen van mijnFlevoziekenhuis.nl, van Gezondheidscentrum Lindenholt ([www.gclindholt.nl](http://www.gclindholt.nl)) en van Erasmus MC maken gebruik van DigiD. Flevoziekenhuis.nl en het Erasmus MC maken daarnaast overigens ook nog gebruik van een specifiek ziekenhuispatiëntenaccount.

---

<sup>4</sup> Zie kamerstuk "Elektronisch patiëntendossier" van VWS, 12-12-2008 (MEVA/ICT-2899251), <http://www.minvws.nl/kamerstukken/meva/2008/elektronisch-patientendossier.asp> (gecontroleerd 13-12-2009).

Op Europees niveau vindt onder de naam STORK ([www.eid-stork.eu](http://www.eid-stork.eu)) een pilotproject plaats waarin nationale e-identity oplossingen gefedereerd worden.

Dit project moet het mogelijk maken om bijvoorbeeld met DigiD in te loggen op een e-overheid dienst in België, dus zonder een Belgische e-identity nodig te hebben. Naast technologische, architecturale en juridische uitdagingen, is een belangrijk punt hoe om te gaan met de beveiligingsniveaus van de verschillende landen. Zo kent Nederland momenteel twee niveaus (gebruikersnaam en wachtwoord en one-time-password over SMS), terwijl Oostenrijk maar één niveau in de vorm van een eID smartcard (of vergelijkbare) oplossing heeft. Met 27 EU landen met elk hun eigen niveaus is het nodig dit af te schermen van dienstenaanbieders (relying parties), zodat een dienstenaanbieder gebruik kan maken van een buitenlandse e-identity zonder de details van verschillende niveau in de verschillende landen te hoeven kennen. Hiervoor worden de niveaus in verschillende landen op elkaar "gemapped". Via de STORK infrastructuur kan bijvoorbeeld worden doorgegeven dat een Duitser met het equivalent van DigiD niveau 2 moet inloggen, zonder te hoeven weten met welk Duits niveau dit overeenkomt.

### **E-identity in de ICT roadmap & architectuur**

Deze sectie analyseert, gegeven de bovenstaande problematiek en ontwikkelingen, de plek van e-identity voor zorgconsumenten in de ICT roadmap en architectuur van zorginstellingen. Zorginstellingen die in hun interacties met zorgconsumenten het internetkanaal (gaan) gebruiken doen er in de eerste plaats verstandig aan in hun ICT architectuur de identiteitsfunctionaliteit los te koppelen van de online applicaties. Niet alleen vanuit het principe van scheiden van functies (vaak ook aangeduid met 'separation of concerns'), maar ook om flexibel gebruik te kunnen maken van externe identity providers. Dit is dan ook een tweede aanbeveling: vermijd

eigen, per zorginstelling, identiteiten en maak in plaats daarvan gebruik waar mogelijk gebruik van externe identity providers. Afhankelijk van de soort dienstverlening, en met name de benodigde veiligheid van de identiteitsoplossing, zijn de meest voor de hand liggende keuzes voor externe identiteitsaanbieders momenteel:

- **OpenID voor low-security**  
De OpenID standaard, en identity providers die daar gebruik van maken, kunnen worden ingezet bij toepassingen met een laag veiligheidsrisico. Zodoende is toegankelijkheid voor alle zorgconsumenten gewaarborgd. Zij kunnen immers zelf hun identity provider kiezen, bijvoorbeeld Hyves of Yahoo. DigiD (op niveau 1) is een alternatief, maar heeft als nadeel dat mensen niet anoniem zijn tegenover de online dienstenaanbieder. Daarnaast kunnen mensen zonder een DigiD hiervan geen gebruik maken.
- **DigiD voor high-security**  
DigiD gebruiken, met hetzelfde niveau als gebruikt gaat worden voor EPD ontsluiting (SMS one-time-password authenticatie inclusief face-to-face controle bij uitgifte). Dit gaan zorgconsumenten immers gebruiken voor EPD toegang waardoor er gewenning ontstaat. Bovendien is dit het veiligste wat er momenteel in Nederland voor zorgconsumenten op grote schaal beschikbaar is.

Aangezien identiteitsoplossingen voor burgers en consumenten nog volop in ontwikkeling zijn, is het niet ondenkbaar dat er andere identity providers, federatie standaarden of beveiligingsniveaus ontstaan. Zo bestaat de mogelijkheid dat de Nederlandse overheid een elektronische identiteitskaart gaat introduceren, om daarmee veiligheidsniveau 3 van DigiD in te vullen. Ook is het denkbaar dat identiteitsoplossingen voor online banking in de toekomst kunnen worden gebruikt in de zorgsector. Door het loskoppelen, of 'externaliseren', van de identiteitsoplossing

van de online applicaties kan hier flexibel op ingesprongen worden.

Als een aanvullende oplossing kan een zorginstelling ten slotte overwegen om zelf een identity provider te worden voor de eigen applicaties. Een dergelijke, aanvullende, silo-oplossing kan nodig zijn omdat niet alle zorgconsumenten een DigiD of OpenID identiteit hebben of willen hebben. Hierbij moet wel goed nagedacht worden over het benodigde veiligheidsniveau qua authenticatiemiddel en uitgifteproces. Qua authenticatiemiddel zal gebruikersnaam en wachtwoord vaak niet voldoende veilig zijn, en kan bijvoorbeeld SMS one-time-password authenticatie overwogen worden. Hierdoor wordt extra veiligheid t.o.v. gebruikersnaam en wachtwoord gecreëerd zonder kosten te hoeven maken voor hardware tokens.

Naast en gerelateerd aan e-identity, is in de ICT roadmap en architectuur ook aandacht nodig voor autorisatie. Bij autorisatie gaat het erom wat iemand mag. Onderdeel hiervan is of iemand ook geautoriseerd, ook wel genoemd gemachtigd, is om namens iemand anders toegang te krijgen tot bepaalde gegevens, bijvoorbeeld een mantelzorger die toegang krijgt tot privacy-gevoelige gegevens.

Nictiz is het landelijke expertisecentrum dat ontwikkeling van ICT in de zorg faciliteert. Met en voor de zorgsector voorziet Nictiz in mogelijkheden en randvoorwaarden voor elektronische informatieuitwisseling voor en rondom de patiënt. Wij doen dit ter bevordering van de kwaliteit en doelmatigheid in de gezondheidszorg.

Nictiz,  
Oude Middenweg 55  
2491 AC Den Haag  
Postbus 19121  
2500 CC Den Haag

T 070 317 3409  
E [info@nictiz.nl](mailto:info@nictiz.nl) [www.nictiz.nl](http://www.nictiz.nl)