Memo

Aan: leden AcZie

[redacted]

Datum: 28 februari 2017

Betreft: **Advies wetsvoorstel Generieke Digitale Infrastructuur (GDI)**

Gezien mijn rol als vertegenwoordiger/gebruiker in het Tactisch Beraad eID / Idensys namens de zorg is mij door AcZie gevraagd een advies aan NFU uit te brengen inzake de consultatievraag aangaande het wetsvoorstel GDI. De materie rond de wet GDI en het project eID is dermate omvangrijk en complex, dat ook anderen (SIG Informatiebeveiliging & persoonsbeschermening, informatiemanagement, beleidsafdelingen) om een advies gevraagd zou moeten worden.

Inleiding
De wet GDI richt zich op de invoering van een generieke digitale infrastructuur die de identificatie en authenticatie van afnemers van digitale diensten op een betrouwbare manier mogelijk maakt. Daarbij richt de wet zich vooral, maar niet uitsluitend, op digitale diensten die door de overheid worden aangeboden. Onder afnemers van diensten worden in hoofdzaak verstaan burgers en vertegenwoordigers van organisaties.

Relaties
Project eID
Onder regie van het ministerie van BZK wordt in Nederland gewerkt aan het kunnen aanbieden van identificatie en authenticatie middelen aan burgers en vertegenwoordigers van organisaties met verschillende betrouwbaarheidsniveaus (standaard, substantieel en hoog). Dit wordt in een publiek-private samenwerking tot stand gebracht. De overheid is verantwoordelijk voor de infrastructuur en het toezicht, de private partijen geven middelen uit en kunnen optreden als makelaar. In de makelaarsrol wordt de verbinding gelegd tussen de afnemer en de aanbieder van digitale diensten. De makelaar toetst - op basis van vereiste specificaties van de dienstaanbieder - de afnemer van de digitale dienst op diens identiteit en andere vereisten, zoals het betrouwbaarheidsniveau, leeftijd, machtigingen etc. De middelenuitgevers en de makelaars moeten voldoen aan de Uniforme Set van Eisen. Naar deze USvE wordt in de stukken rond het wetsvoorstel GDI af en toe verwezen.
Middelen en concurrentie
Door de overheid is naast DigiD (betrouwbaarheidsniveau "standaard") ook eHerkenning (voor vertegenwoordigers van organisaties met betrouwbaarheidsniveaus "substantieel" en "hoog") en Idensys (voor burgers met betrouwbaarheidsniveau "substantieel" en "hoog") ontwikkeld. De merken eHerkenning en Idensys zijn feitelijk gebaseerd op dezelfde techniek en infrastructuur en hebben in de praktijk bewezen betrouwbaar te zijn. In Europees verband wordt gezorgd dat eHerkenning en Idensys voldoen aan eIDAS, het Europese stelsel voor digitale identificatie en authenticatie.
Er zijn vele methoden voor identificatie en authenticatie in gebruik. De meesten zijn gericht op slechts één dienstverlener, zoals het aanmelden bij een webwinkel of een bank. Sinds kort bieden de banken hun middelen (bankpassen/random readers) onder de merknaam iDIN ook aan voor identificatie en authenticatie bij andere dienstverleners.
BurgerServiceNummer (BSN)
De overheid biedt met het BSN koppelregister in relatie tot eHerkenning en Idensys de mogelijkheid om net als bij DigiD het BSN beschikbaar te krijgen bij het gebruik van deze identificatie en authenticatie systemen.

Zorgsector

Verwacht wordt dat in de zorg steeds meer informatie uitwisseling langs digitale weg zal plaatsvinden, zowel tussen zorgprofessionals onderling als tussen zorgprofessional en zorggebruiker. Medische informatie moet worden verwerkt op betrouwbaarheidsniveau 4 van het STORK model ofwel betrouwbaarheidsniveau "hoog" zoals genoemd in het wetsvoorstel GDI. Alleen de UZI pas voor zorgprofessionals voldoet aan dit betrouwbaarheidsniveau. Alle overige gebruikte middelen als DigiD en specifieke identificatie en authenticatie methoden van bijvoorbeeld EPD leveranciers voldoen hier niet aan. Een belangrijk aandachtspunt als het gaat om betrouwbare identificatie en authenticatie van gebruikers van de informatiesystemen in de zorg.

Overwegingen

Privacy en security

Voor de UMC's is het borgen van privacy van patiënten en het kunnen vertrouwen op een goede beveiliging van gegevens in het algemeen en persoonsgebonden medische gegevens in het bijzonder van uitermate hoog belang. Het op een betrouwbare manier kunnen vaststellen van de identiteit van gebruikers van de informatiesystemen van de UMC's is daarbij evident. De huidige wetten stellen nu al hoge eisen op het gebied van betrouwbaarheid, waar de UMC's (nog) niet aan kunnen voldoen. Daarom is het aansluiten bij een (inter-)nationale infrastructuur voor identificatie en authenticatie zeer aan te bevelen.

Middelen

De gebruikers van de digitale diensten van de UMC's zullen zelf hun middelen voor identificatie en authenticatie kunnen kiezen. Alleen met middelen met betrouwbaarheidsniveau "hoog" kan gebruik worden gemaakt van de diensten van UMC's om medische gegevens te kunnen benaderen. De gebruikers zijn zelf verantwoordelijk voor de bekostiging van de gekozen middelen. Daarom is het wel belangrijk dat eenmaal aangeschafte middelen breed te gebruiken zijn, van belastingdienst tot UWV, van ziekenhuis tot verzekeraar, etc.

Personeel en zorgprofessionals

De verwachting is, dat op termijn de rol van de UZI pas voor zorgprofessionals kan worden overgenomen door de middelen zoals die nu bij eHerkenning en Idensys worden ingezet. Dat impliceert uiteindelijk dat ook medewerkers en zorgprofessionals gebruik zullen gaan maken van erkende identificatiemiddelen. Daarmee ontstaat een uniforme en gestandaardiseerde infrastructuur voor identificatie en authenticatie, ook binnen de UMC's, die inzetbaar is voor in- en externe gebruikers.

Provisioning

Omdat de overheid een multi-middelen strategie hanteert is het zeer aan te bevelen dat UMC's gebruik gaan maken van zogenaamde makelaars, die de toegang tot de UMC informatiesystemen al of niet mogelijk maken voor de gebruikers (dit mechanisme wordt "provisioning" genoemd). Daarmee wordt niet alleen gegarandeerd dat alle erkende identificatie middelen kunnen worden aangeboden, maar worden ook de Europese varianten ondersteund, bijvoorbeeld voor burgers uit onze buurlanden bij het noodzakelijk gebruik van UMC informatiesystemen.

Identity & Access Management (IAM)

Het wetsvoorstel GDI, de Uniforme Set van Eisen en de in dit advies genoemde relaties en overwegingen hebben betrekking op enkel een betrouwbare identificatie en authenticatie van gebruikers van digitale informatiediensten, waarbij met de identificatie enkele kenmerken kunnen worden meegegeven (bv. betrouwbaarheidsniveau, leeftijd, BSN, registratie in een beroepenregister, etc.). Naast identificatie en authenticatie blijft autorisatie een belangrijke verantwoordelijkheid voor de instelling, die digitale informatiediensten beschikbaar stelt aan in- en externe gebruikers. Daarom is het hebben van een goed ingericht en gefaciliteerd Identity & Access Management systeem van cruciaal belang.

Advies

- Organisaties die op dit moment onder de Wet BSN in de zorg vallen dienen ook onder de wet GDI te vallen en dus op aangeven van de eigen minister moeten worden opgenomen in de bijlage van de wet GDI
- In het memo van het ministerie van Volksgezondheid, Welzijn en Sport inzake de consultatie wet Generieke Digitale Infrastructuur en Uniforme Set van Eisen eID van 20 januari 2017 worden een flink aantal vragen gesteld. Per vraag treft u mijn voorstel voor antwoorden, opmerkingen of advies:
    1. Zie eerste bullit van dit advies;
    2. Dit betekent voor UMC's dat zij zelf en de leveranciers van de UMC informatiesystemen (o.a. EPD systemen) om moeten kunnen gaan met provisioning technieken vanuit de makelaars. Het roept ook vragen op betreffende financiering van deze makelaarsdiensten en de financiering van middelen (voor de beroepsuitoefening) voor eigen medewerkers;
    3. Zie mijn teksten hiervoor;
    4. Voldoende leesbaar en begrijpelijk, hoewel omvangrijk;
    5. Duidelijkheid over tijdslijnen, kosten, consequenties voor digitale informatiediensten vanuit de UMC's;
    6. Hoe kom ik aan een geschikt middel? Wat kost dat? Wat heb ik er aan? Bij wie kan ik terecht? Waarom moet dit op deze manier? Is het makkelijk in gebruik?
    7. Een goede governance voor de besturing van het stelsel eID is hiervoor evident;
    8. Deze vraag is te stellen aan SIG TacZie en SIG IB;
    9. Idem;
    10. De gevolgen heb ik o.a. geschetst bij de paragraaf "overwegingen" en bij vraag 2.
    11. M.i. is het belangrijk dat niet alleen UMC's, maar alle ziekenhuizen (e.a. zorginstellingen) als aangewezen organisatie gaan gelden;
    12. Daarvoor is een impact analyse nodig. Mijn verwachting is dat het stevige consequenties heeft, maar niet onuitvoerbaar;
    13. Nu gelden al NEN 7510 en ISO 2700x als veldnorm of certificeringskader. Kortom, niet onoverkomelijk, mits realistisch tijdspad wordt gehanteerd;
    14. Een multimiddelen strategie houdt in dat alle erkende middelen gebruikt moeten kunnen worden om diensten te ontsluiten. Als aan deze voorwaarde niet wordt voldaan, zal er beperkt draagvlak zijn voor het gebruik van de erkende middelen. Een UMC zal derhalve een makelaar (ontsluitende dienst) willen, die de volledige multimiddelenstrategie kan volgen;
    15. In het algemeen zal het betrouwbaar ontsluiten van digitale diensten door een UMC op basis van eigen infrastructuur meer kosten met zich meebrengen (infrastructuur/beheer) dan gebruik maken van een generieke digitale infrastructuur. Echter in alle gevallen is sprake van meerkosten, omdat nog lang niet alle digitale diensten nu worden aangeboden vanuit de UMC's. De baten van deze digitale diensten zijn (nog) onduidelijk;
    16. Het doorberekenen van digitale diensten op zich is m.i. nog een onontgonnen terrein binnen de UMC's. Hier ligt ook een relatie met de zorgverzekeraars, digitale diensten versus fysieke diensten, efficiënt (digitaal) werken, etc.;
    17. Hier is sprake van marktwerking, waarbij aanbieders (de makelaars, ontsluitende diensten) net als aanbieders van informatiesystemen of telefoniediensten voor de zorg een passende propositie kunnen doen. Prima;
    18. Deze vraag moet nog worden beantwoord door de technische commissie van de umc's;
    19. Er zijn zorgen over het draagvlak voor de wet GDI en de multimiddelen strategie bij de gewone burger. Een goede voorlichting naar burgers over het waarom en voor welke diensten toepasbaar is noodzaak. Als een burger straks moet betalen voor een middel moet deze kunnen vertrouwen op een zeer brede en veilige toepasbaarheid;