

Reactie ZN op wet GDI (consultatie)

VWS heeft ZN (ons) gevraagd om te reageren op het wetsvoorstel GDI (eerste tranche). Wij geven daar graag gehoor aan. We hebben het wetsvoorstel beoordeeld op de consequentie voor zorgverzekeraars, maar zijn niet voorbij gegaan aan de impact op zorgaanbieders. Deze memo is het resultaat van een workshop in de werkgroep identificatie & authenticatie op 16 februari.

Samenvatting

Het wetsvoorstel geeft invulling aan het kabinetsvoornemen tot een volledig digitaal werkende overheid. Om digitale dienstverlening in het publieke domein te intensiveren, is veilige en betrouwbare toegang daartoe door burgers en bedrijven nodig. De zorgsector in het algemeen en de verzekeraars in het bijzonder onderschrijven het belang van veilige en betrouwbare digitale dienstverlening. De zorg heeft behoefte aan hoog-betrouwbare identificatie- & authenticatiemiddelen die grootschalig door verzekerden en patiënten gebruikt kunnen worden. Middelen die door hen begrepen worden en betaalbaar zijn.

Wij juichen het initiatief om te komen tot hoog betrouwbare identificatie- en authenticatiemiddelen toe en dragen daar graag aan bij. We constateren dat het succes van dit initiatief voor een substantieel deel bepaald wordt door de geschiktheid voor de zorgsector. Wij zien dat op dit punt verbetering van het wetsvoorstel nodig is.

In deze memo stellen we verbeteringen in het wetsvoorstel voor. In de bijlage geven we per vraag onze reactie¹.

Samenvatting verbetervoorstellen:

- Wij stellen voor de acceptatieplicht niet toe te passen op de zorgsector. De acceptatieplicht leidt tot een de-facto oligopolie voor de aanbieders qua prijsvorming. Het aantal inlogs in de zorg is per maand in te schatten op groter dan 10 miljoen keer hetgeen tot substantiële kosten kan leiden.
- Wij stellen voor het verbod op inzet van niet-erkende middelen niet toe te passen op de totale zorgsector maar proportioneel.
- Wij staan een vrije keuze van authenticatieoplossingen voor. Mits de authenticatiediensten aantoonbaar voldoen aan de in de wet GDI te stellen eisen.
- Wij stellen voor de eisen aan de dienstverleners toe te spitsen op de zorgsector en aan te sluiten bij de waarborgen die de sector al ingebouwd heeft.
- Wij vinden het essentieel dat de wet eisen ten aanzien van privacy formuleert, niet de oplossing. In het belang van een betaalbaar eID stelsel dat innovatie stimuleert – en niet belemmert.

Wij achten effectuering van deze voorstellen noodzakelijk voor succes in de zorgsector en daarmee brede uitrol van passende authenticatieoplossingen.

¹ Zie Consultatie Wet Generieke Digitale Infrastructuur en Uniforme Set van Eisen eID, Ministerie van VWS, d.d. 20 januari 2017.

Consultatie

Het hart van het wetsvoorstel is de acceptatieplicht voor dienstverleners. Dienstverleners moeten elk erkend middel accepteren en mogen geen andere middelen toestaan. Wij constateren:

1. Er ontstaat een scheve markverhouding tussen dienstverlener en erkende authenticatiediensten. Hierdoor ontstaat geen passende prijsvorming en ontbreekt een stimulans voor kostenefficiëntie en innovatie bij erkende authenticatiediensten. Wij zien het als zeer onwenselijk dat de authenticatiedienst – via de ontsluitende dienst – aan de dienstverlener kosten in rekening kan brengen. Het (nog steeds niet heldere) business model is naar onze mening te complex. Zorg dat het simpel blijft en dat partijen in de zorg het middel daadwerkelijk gaan gebruiken. Laat zeker niet per transactie betalen, maar bijvoorbeeld door integraal bedrag per tijdsperiode (jaar/ jaren).
2. Proportionaliteit ontbreekt bij de acceptatie van middelen in de zorg. De verwachting is dat een beperkt aantal authenticatiediensten (maximaal 3) de gehele zorgsector kunnen en moeten bedienen. De acceptatieplicht confronteert de zorgpartners met extra kosten voor contractering, aansluiting in compliance als de zorg alle erkende authenticatiediensten moet aanbieden. De acceptatieplicht is voor de zorg te breed en te ongericht.
3. Kleine dienstaanbieders kunnen niet voldoen aan de acceptatieplicht. De sector kent veel zelfstandige zorgaanbieders, zoals tandartsen en fysio's. Zij kunnen gezien hun omvang, financiële slagkracht en (technische) kennisniveau niet aan de acceptatieplicht gehouden worden. Tenzij er voor hen volledige procedurele, contractuele, technische en financiële ontzorging plaatsvindt.
4. Het verbod op inzet van specifieke (niet erkende) I&A oplossing in de zorg brengt continuïteit van de digitale dienstverlening in gevaar. De zorg maakt gebruik van verschillende zorgspecifieke middelen voor identificatie & authenticatie van personen, professionals en organisaties. Niet alleen voor online dienstverlening op portalen, maar ook voor machine-naar-machine dienstverlening en mobiele apps. Deze middelen lenen zich niet voor erkenning vanwege de specifieke doelgroep c.q. het specifieke kanaal waarvoor ze ontwikkeld zijn, ook al zouden ze voldoen aan de uniforme set van eisen. Door het verbod deze middelen na het in werking treden van de wet nog in te zetten, is de continuïteit van de digitale dienstverlening in gevaar. Bovendien is onvoldoende helder hoe Persoonlijke Gezondheids Omgevingen (PGO's) die moeten voldoen aan het MedMij-afsprakenstelsel hier inpassen.

Wij stellen voor (1) de acceptatieplicht niet toe te passen op de zorgsector en (2) het verbod op inzet van niet-erkende middelen niet toe te passen op de zorgsector. Wij staan een vrije keuze van authenticatieoplossingen voor. Mits de authenticatiediensten aantoonbaar voldoen aan de Uniforme eisen.

De wet GDI biedt de kaders voor het stellen van eisen aan de digitale toegangverlening door dienstverleners. Wij constateren de eisen voor tot een onevenredige lastenverzwaring voor zorgpartners leiden:

5. De eis dat de zorgsector externe auditors inzet past niet in de auditarrangementen in de zorgsector. Zorgverzekeraars maken gebruik van – door DNB als onafhankelijk gekwalificeerde - interne auditdiensten. De wet GDI moet de ruimte bieden om dat zo te houden.
6. De zorgsector krijgt een dubbele meldplicht voor datalekken. De zorgsector moet datalekken aan zowel AP als BZK gaan melden. Dat vinden wij niet passend en niet acceptabel.
7. De zorgsector lijkt met dit wetsvoorstel ook onder de WOB te vallen. Dat vinden wij onwenselijk en moet expliciet uitgesloten worden.
8. Registratieplicht van inlogs geeft negatieve beeldvorming. De registratieplicht van inlogs staat op gespannen voet met de WBP en leidt tot negatieve beeldvorming bij verzekerden en patiënten. Wij dringen er op aan deze registratieplicht bij de dienstverlener te laten vervallen.

Wij stellen voor de eisen die de wet aan dienstverleners stelt toe te spitsen op de zorgsector en aan te sluiten bij de waarborgen die de sector al ingebouwd heeft.

De MvT en USvE stellen eisen aan de werking van het eID stelsel. Wij constateren dat deze eisen de eIDAS verplichtingen overstijgen en de kosten van authenticatie verhogen en innovatie beperken:

9. Kosten van polymorfe pseudonimisering
Kennis van polymorfe pseudonimisering is zeer schaars en authenticatiediensten voorzien aanzienlijke kosten bij het implementeren en beheren terwijl er voldoende technische alternatieven zijn.
10. Dataveiligheid bij polymorfe pseudonimisering
De reikwijdte van een hack op de polymorfe pseudonimisering is – door de stelselbrede toepassing – enorm. We dringen er op aan dit risico te ondervangen door niet één oplossing voor te schrijven, maar de eisen te formuleren waaraan de oplossing moet voldoen.
11. SPOF BSNk
De inzet van het BSNk in de dienstverlening leidt tot een onwenselijke afhankelijkheid (single point of failure). Wij vinden het belangrijk dat de toegang tot de zorg niet afhankelijk wordt van één schakel in de keten.

Wij vinden het essentieel dat de wet eisen ten aanzien van privacy beschrijft, niet de oplossing. In het belang van een betaalbaar eID stelsel dat innovatie stimuleert – en niet belemmert.

Tenslotte constateren we dat de kosten voor uitvoering van de wet GDI bepaald worden door de uitvoeringsregelingen die daaronder gaan vallen. De zorgsector kan de impact van de wet nu niet kwantificeren.