Reactie op internetconsultatie Wet digitale identificatie en authenticatie in de zorg (Wet Diaz)

Steller: F.H.B. Kersten (op persoonlijke titel)
Datum: 8 augustus 2023

---

1. Essentieel voor het kunnen beoordelen van dit wetsvoorstel is NEN-7518. Deze norm is echter nog niet beschikbaar. Hierdoor kan niet goed beoordeeld worden wat het effect is op de in de praktijk gehanteerde inlogmiddelen.
2. De focus lijkt te liggen op de vervanging van de UZI-pas. Zoals ook blijkt uit de toelichting wordt in veel zo niet de meeste gevallen door zorgmedewerkers gebruik gemaakt van een personeelspas (in de MVT aangeduid met ziekenhuispas). Deze pas wordt niet alleen gebruikt voor logische maar ook voor fysieke toegangsbeveiliging. Hierbij voldoet de pas aan internationale standaarden (Mifare en opvolgers). Uit het voorstel annex MvT blijkt onvoldoende of rekening is gehouden met:
- het feit dat deze passen in de huidige situatie ook al gebruikt worden voor identificatie en authenticatie (2FA) waarmee - bijvoorbeeld via ZIS/EPD - toegang wordt verkregen tot elektronische berichtuitwisselingssystemen: denk aan Zorgplatform van ChipSoft en TWINN voor XDS (beelden);
- mate waarin deze passen voldoen aan de (nieuwe) normen;
- de vraag of de (internationale) fabrikanten/leveranciers wel bereid zijn deze aan te bieden voor certificering tegen NEN-7518.
3. In diverse onderdelen wordt onvoldoende rekening gehouden dat het uiteindelijke betrouwbaarheidsniveau niet alleen afhankelijk is van het fysieke middel of software maar ook van de procedures daar omheen. Alleen certificeren van het middel/software is dan niet genoeg. Verwijzen naar DigID is dan ook een slecht voorbeeld: de basis toepassingen zonder specifiek ID voldoen niet aan betrouwbaarheidsniveau hoog. Ik denk dat er in Nederland dagelijks vele onrechtmatige inzages in patiëntendossiers plaatsvindt aan de kant van de patiënt, doordat ouders inloggen of kinderen of anderen dan de de patiënt zelf ook toegang hebben tot diens DigID gegevens.
4. Er is onvoldoende rekening gehouden met diverse praktische complicaties:
- Geen duidelijkheid of de overgangsperiode ook geldt voor bestaande personeelspassen; de verwijzing naar huidig artikel 15 lid 3 Wabvpz lijkt alleen gericht te zijn op de UZI-pas;
- Onboarden van nieuwe medewerkers is nu al een lastig proces, zeker bij spoed. Het gaat niet werken om dan dagen te moeten wachten op een centrale registratie; ga eens te raden bij (implementatie van) I&AM toepassingen.
- Wisseling van werkgever: veiligste methode is dan om de oude rechten c.q. koppeling te verwijderen; wat echter als werknemer ook daar in dienst blijft. Hoe is het bewijs geregeld;
- Als een zorgverlener een uniek ID moet krijgen, dan moet dit ook op diverse plekken geregistreerd worden: HR-systeem, Active Directory, logging van het EPD-systeem; dit laatste vergt strikt genomen een aanpassing van NEN-7513; kosten van dit soort aanpassingen zijn niet meegenomen;
- zeker in ziekenhuizen heeft niet iedere medewerker een door de werkgever verstrekte telefoon;
- het is absoluut onwenselijk om meer dan 1 inlogmiddel per medewerker te verstrekken, zeker geen combinatie met een middel dat feitelijk privé is.
5. Indien de bestaande personeelspassen niet gehandhaafd kunnen blijven, zijn de inschattingen van de kosten veel en veel te laag. Bij mijn werkgever speelt momenteel de vervanging van deze passen. Daarbij blijkt dat een generatie passen ca 10 jaar meegaat en je daarna alles zou moeten vervangen. Dus ook de paslezers naast de computer of medische apparatuur en die voor fysieke beveiliging van ruimten. Dan praat je over enkele tonnen voor een ziekenhuis van gemiddelde omvang en ca 2500 passen. Dit dan nog zonder de kosten van licenties voor koppelingen tussen systemen en de eventuele vervanging van het pasbeheersysteem. Hier staat overigens wel tegenover dat er geen kosten zijn per gebruik (tik).
6. De ervaring heeft helaas geleerd dat medici maar beperkt geschikt zijn om informatiesystemen en toepassingen te beoordelen. Zij kunnen hoogstens een uitspraak doen over het gebruiksgemak. Zij geen geen idee wat er vaak achter zit en nodig is om tot een praktisch werkende oplossing te komen.
7. Het zou prettig zijn als er gestopt wordt met 'Window dressing' rond de feitelijke beveiliging van patiëntgegevens. Uiteraard draagt toegang via passende middelen daartoe bij. Echter, er wordt in veel situaties door het gebruik van ZIBs meer informatie uitgewisseld dan op grond van de Wgbo toegestaan is. Voorts is de beveiliging elders in de zorgketen vaak veel lager dan bijvoorbeeld een ziekenhuis (hoe is het bij gemeenten?). Zijn alle patiënten wel in staat om een PGO goed te beheren of verstrekken zij gemakkelijk gegevens aan wie er om vraagt?