Een digitaal vaccinatiebewijs riskeert onze privacy

opinie

Evert Mouw

2021-03-03

Veel partijen hebben vanwege uiteenlopende redenen de wens neergelegd om een digitaal vaccinatiepaspoort te ontwikkelen. Vooral voor COVID-19 heeft dat nu spoed. Dat brengt echter wel risico's naar voren op het gebied van gegevensbescherming en privacy.

Zo ging het al behoorlijk fout toen bleek dat mogelijk de persoonsgegevens (naam, geboortedatum, adres, BSN) van grote aantallen burgers, verzameld door de GGD t.b.v. de testregistratie, in verkeerde handen gevallen zijn [1]. De systemen van de GGD bleken slecht beveiligd te zijn [2]. Zulke incidenten kunnen negatieve consequenties hebben voor de test- en vaccinatiebereidheid onder de bevolking.

De afgelopen tientallen jaren werd een papieren vaccinatiebewijs gebruikt, het zgn. "gele boekje". Vaccins werden met datum en stempel opgenomen in dit vaccinatieboekje, dat ook voor internationale reizen gebruikt kan worden. Dit papieren vaccinatiebewijs werkt goed en is via de Sdu (staatsdrukkerij) ook in coronatijd beschikbaar [3].

Toch zijn er diverse initiatieven richting een digitaal vaccinatiebewijs:

- Op dit moment ontwikkeld het team dat eerder de coronamelder maakte een vaccinatiepaspoort in opdracht van de overheid. De eerdere coronamelder werd geen succes en het ontwikkelproces werd gekenschetst door uitstel en slechte overheidscommunicatie.
- Het RIVM zal in maart of april dit jaar een soort "Mijn RIVM" presenteren waar je met DigiD kunt inloggen om je vaccinatiestatus in te zien. Dit is ontstaan vanuit het COVID-vaccinatie Informatie- en Monitoringsysteem (CIMS). Misschien is het mogelijk de achterliggende database te koppelen aan een digitaal vaccinatiepaspoort.
- De EU ontwikkeld een eigen digitaal vaccinatiepaspoort, waarbij het voorstel van de EC gepland staat voor 2022.
- Enkele commerciële partijen ontwikkelen digitale vaccinatiepaspoorten.

Het team van TechTegenCorona heeft het advies gegeven papier als basis te nemen, met optioneel digitale middelen erbij. Behalve veiligheid was ook een argument dat niet iedereen een smartphone heeft. Het ministerie wilde echter hoe dan ook een app voor smartphones – er komt nog vervolgoverleg. Inmiddels zijn er al vijf apps gemaakt of gepland. Het initiatief om tot nieuwe digitale oplossingen te komen is mooi, maar kan ook werken als stoorzender als al bestaande oplossingen daardoor buiten zicht raken.

Ook de Begeleidingscommissie Digitale Ondersteuning Bestrijding Covid-19 heeft luid en duidelijk van zich laten horen in Advies 16: Veiligheid & privacy van Covid-19 test en- vaccinatie data [4]. Daarbij refereerden ze in een voetnoot naar een advies van de eerder genoemde TechTegenCorona en riepen ze op tot een *sense of urgency*:

> Expliciet adviseert de commissie een veiligheid- en privacy-inventarisatie bij alle huidige en nieuwe SARS-CoV-2 en Covid-19 gerelateerde datak-nooppunten/registratiesystemen, en een verhoging van het veiligheid & privacy bewustzijn zowel bij verantwoordelijke beheerders van deze data-knooppunten/registratiesystemen als bij degenen die toegang tot deze data hebben. Daarnaast adviseert de commissie een publieke campagne op te starten die de huidige problemen en oplossingen beschrijft, en zodra deze datasystemen daadwerkelijk weer privacy-proof zijn dit kenbaar te maken opdat het vertrouwen van de Nederlandse burger kan worden (her)wonnen.

Zo'n oproep tot *sense of urgency* komt niet uit het luchtledige. In informatiebeveiligingskringen[pc] werd de vraag opgeworpen of niet het hele BSN systeem vervangen moet worden na het grote GGD datalek. Onbekend is hoeveel gegevens door hoeveel personen bemachtigd zijn, maar het is *niet uit te sluiten* dat sinds het datalek bij de GGD de gegevens van miljoenen mensen bemachtigd zijn door onbevoegden. Zulke gegevens kunnen gebruikt kunnen worden voor marketing, maar ook voor identiteitsfraude, afpersing en dies meer, ook vele jaren na de diefstal. Desondanks blijkt regelmatig uit contacten met GGD-medewerkers[pc] dat het "vullen van de database" grote prioriteit heeft, zonder dat er veel besef is van de risico's.

Papier is een goede informatiedrager. Zeker in tijden dat er al genoeg problemen zijn is het experimenteren met mobiele apps eerder een stoorzender dan een oplossing. Waarom niet nu even focussen op het al bestaande vaccinatieboekje? Op dit moment zijn niet eens meer altijd stempels beschikbaar als mensen bij coronavaccinatie door de GGD hun gele boekje meenemen, omdat alle aandacht naar databases gaat.

Wel geeft de GGD bij het vaccin een sticker met de productnaam, het batchnummer, de naam van de ontvanger e.d. Deze sticker kan ik het gele boekje geplakt worden, conform de RIVM LCI richtlijn COVID-19-vaccinatie [5]:

> **10.6 Registratie van vaccinatiegegevens** Als deelnemers door de GGD worden gevaccineerd ontvangen ze als vaccinatiebevestiging een brief uit het registratiesysteem van de GGD met daarop alle relevante informatie: datum toegediende vaccinatie, productnaam, batchnummer vaccin en een url die linkt naar de bijsluiter. Deze brief kan in het gele vaccinatieboekje bewaard worden. (par. 10.6, versie 25 februari 2021)

Als iemand een coronavaccinatie krijgt bij de GGD, krijg die persoon de vraag of de gegevens ook bij de RIVM in de CIMS database mogen worden opgenomen. Mensen die "nee" antwoorden, zullen dus ook geen gegevens zien in de "Mijn RIVM" omgeving die in maart of april beschikbaar komt. Een koppeling met die database is dus ook niet voor alle gevallen een werkende oplossing.

De aanlevering van de gegevens gaat volgens de eerder genoemde richtlijn bij voorkeur via het Landelijk Schakelpunt (LSP), dat oorspronkelijk een belangrijk element was van het door de Eerste Kamer verworpen landelijke Elektronisch Patiëntendossier (EPD). De onderzoeker Guido van 't Noordenende had destijds zwakheden gevonden rondom het LSP [6].

Juist computerdeskundigen, hackers en mensen betrokken bij privacy- en gegevensbeveiliging zijn vaak voorstander van papieren systemen in situaties waar privacy van groot belang is of waar de omstandigheden niet optimaal zijn om tot goede systemen en processen te komen. Hackers hebben al diverse malen kwetsbaarheden aangetoond bij digitale stemsystemen. Nog in 2019 werd tijdens Defcon in Las Vegas de sport beoefend om in zo kort mogelijke tijd diverse stemcomputers te hacken [7]. In Nederland was er de actiegroep Wij vertrouwen stemcomputers niet, opgericht door Rop Gonggrijp, voormalig hacker en mede-oprichter van internetprovider XS4ALL. Een vervolg daarop is de Stichting Tegen Hackbare Verkiezingen, waar hoogleraren cybersecurity en andere specialisten aan verbonden zijn.

De toegevoegde waarde van een digitaal vaccinatiebewijs is onduidelijk. Het raakt wellicht minder snel kwijt dan een papieren boekje, maar als – zoals nu gedaan wordt – voor een app gekozen wordt die enkel op smartphones werkt, zijn we weer terug bij iets dat kwijt kan raken of waarvan de batterijen leeg kunnen lopen. Integratie met andere diensten is met zo'n app wellicht mogelijk, maar dat zal nog ontwikkeld moeten worden en zal tevens leiden tot nieuwe risico's.

Voor het vertrouwen in de overheid en de medische zorg is het van groot belang dat er nu niet nog meer fouten gemaakt worden dan er al gemaakt zijn. Er moet worden ingezet op snelle en betrouwbare systemen.

De Sdu (staatsdrukkerij), die het gele boekje uitgeeft, heeft meer dan genoeg capaciteit om de verspreiding van het gele boekje vlot te regelen. Ook hebben ze al nagedacht over het gebruik van hun gele vaccinatieboekje voor COVID-19. Een praktische, veilige en al tientallen jaren bewezen oplossing ligt klaar voor gebruik. Laten we in tijden van nood niet experimenteren, maar kiezen voor de bewezen en beschikbare oplossing.

Over de auteur

Evert Mouw is opgeleid tot medisch informatiekundige (MSc) en politicoloog (MA). Hij is niet verbonden aan instituten of organisaties die enig belang hebben bij het onderwerp van deze opinie, heeft geen achterliggende belangen en heeft geen fondsen ontvangen voor het publiceren van deze opinie. Voor hem is dit meer een hobby en een vorm van maatschappelijke betrokkenheid.

Referenties

[pc] Persoonlijke communicatie met betrokkenen.

1. Sjaak Nouwt. *Datalek bij de GGD is een les voor ons allemaal.* (column) *In:* Medisch Contact, 2021-02-17. https://www.medischcontact.nl/nieuws/federatienieuws/federatiebericht/datalek-bij-de-ggd-is-een-les-voor-ons-allemaal-1.htm
2. Niels Klaassen / Het Parool. *De Jonge in debat over GGD-datalek: 'We hebben er onvoldoende aandacht voor gehad'.* (nieuwsbericht) 2021-02-03. https://www.parool.nl/amsterdam/de-jonge-in-debat-over-ggd-datalek-we-hebben-er-onvoldoende-aandacht-voor-gehad~bec6f44d/
3. Sdu. *Vaccinatieboekje.* (webpagina) verkregen 2021-03-01. https://www.sdu.nl/over-sdu/producten-diensten/formulieren/mijnvaccinatieboekje)
4. Begeleidingscommissie Digitale Ondersteuning Bestrijding Covid-19. *Advies 16: Veiligheid & privacy van Covid-19 test en- vaccinatie data.* (rapport) 2021-02-08. https://www.rijksoverheid.nl/documenten/publicaties/2021/02/23/advies-16-veiligheid-covid-19-test-en-vaccinatiedata
5. RIVM. *COVID-19-vaccinatie – Professionele standaard voor COVID-19-vaccinatie 2021.* (LCI richtlijn) 2021-02-25. https://lci.rivm.nl/richtlijnen/covid-19-vaccinatie#10-communicatie-uitnodiging-en-registratie
6. Guido van't Noordende. *Security in the dutch electronic patient record system.* (research article) *In:* SPIMACS '10: Proceedings of the second annual workshop on Security and privacy in medical and home-care systems. 2010-10. https://doi.org/10.1145/1866914.1866918
7. Joost Schellevis / NOS. *Hackers nemen het op tegen stemcomputers (en winnen).* (nieuwsbericht) 2019-08-11. https://nos.nl/artikel/2297115-hackers-nemen-het-op-tegen-stemcomputers-en-winnen.html