Reactie op "Tijdelijke wet testbewijzen covid-19"

Den Haag, 14 maart 2021

Stichting uNLock

De Stichting uNLock en de daarbij aangesloten partijen hebben kennisgenomen van de "Tijdelijke wet testbewijzen covid-19". Het is een goede zaak dat (snel)testen (later wellicht uitgebreid met vaccinatiebewijzen) nu worden ingezet om de maatschappij gecontroleerd weer meer open te maken door veilige bubbels te creëren waarin de maatregelen als afstand houden en beperking van groepsgrootte tijdelijk kunnen worden losgelaten. De Fieldlab Evenementen experimenten hebben ook laten zien dat dit een succesvolle aanpak kan zijn waarmee de maatschappij weer een stukje opener kan worden op een veilige wijze.

Bij een dergelijke aanpak hoort ook een systeem waarbij testbewijzen privacy-vriendelijk en fraudebestendig gebruikt kunnen worden door geteste individuen. Het ligt voor de hand hier een digitale oplossing voor aan te bieden met een papieren variant om inclusie te waarborgen (je wilt geen mensen uitsluiten die geen smartphone kunnen of willen gebruiken hiervoor, bijvoorbeeld omdat ze niet voldoende digitaal vaardig zijn).

Het uitgangspunt dat de overheid gekozen heeft is om een dergelijke aanpak maximaal privacy-vriendelijk te laten plaatsvinden. Dat is lovenswaardig en is een uitgangspunt dat wij ook onderschrijven. Hierbij past een technologische invulling die zorgt voor maximale decentralisatie. Geen centrale databases maar een persoonlijke "datakluis" voor iedereen die op basis van negatieve testresultaten ergens toegang toe wil krijgen. Wij staan daarom een aanpak voor waarbij blockchain als onderliggend fundament gebruikt wordt. De onderliggende blockchain infrastructuur wordt dan gebruikt om de geldigheid van de testbewijzen te controleren en om vast te stellen dat testbewijs en persoon bij elkaar horen. Zonder dat persoonsgegevens op de blockchain geschreven worden, omdat dat in strijd zou zijn met de AVG. Een dergelijke op blockchain gebaseerde oplossing wordt momenteel ook in andere landen ontwikkeld, zoals in Duitsland.

De stichting uNLock, ondersteund door de Dutch Blockchain Coalition en een aantal vooraanstaande publieke en private organisaties, is van mening dat het gebruik van blockchain technologie waarde kan toevoegen aan de ontwikkeling die VWS voorstaat. De DBC is in het leven geroepen met de Nederlandse overheid als drijvende kracht om het gebruik van de blockchain technologie te promoten en verder door te ontwikkelen, om zo grote maatschappelijke problemen te helpen oplossen. Bij uitstek heeft de Nederlands overheid nu een use-case die zich leent om van blockchain technologie gebruik te maken en deze in te zetten voor een breed maatschappelijk doel.

De rol van de overheid (i.c. VWS) zou o.i. moeten zijn om criteria te definiëren waar dergelijke "testresultaat-ontsluitingsoplossingen" aan moeten voldoen. Partijen kunnen deze oplossingen dan ontwikkelen, specifiek voor dit vraagstuk en/of met meer generieke toepassingen. Zo wordt de totale intellectuele ontwikkelcapaciteit in Nederland ook optimaal gebruikt. Veel van de organisaties die nu actief zijn op dit front, werken hier al jaren aan en hebben dus een schat aan ervaring opgebouwd. Ook als VWS de wens heeft om ook zelf een oplossing te maken, dan zou de wetgever andere oplossingen niet bij voorbaat uit moeten sluiten. Al was het maar omdat het riskant is om op één paard te wedden in deze enorme maatschappelijke en economische crisis, waarbij elke dag dat de maatschappij dankzij dit soort oplossingen eerder opener kan worden, een enorme waarde vertegenwoordigt in allerlei dimensies. De maatschappij snakt hier ook naar. De Overheid kiest in

deze ontwerp-wet echter voor een eigen snel ontwikkelde oplossing en legt deze ook in de wet vast. Dit zorgt voor een gebrek aan wendbaarheid en flexibiliteit en dreigt de innovatie- en ontwikkelpotentie van de hele ICT industrie buiten spel te zetten.

Nederland is geen eiland maar staat midden in de Europese en internationale samenleving. De oplossing die nu bij VWS in ontwikkeling is en in de wet exclusief wordt voorgeschreven houdt hier, blijkens de MvT, nu geen rekening mee: "*De inzet van testbewijzen kan het personen uit andere lidstaten minder aantrekkelijk maken om hier bijvoorbeeld diensten te verrichten of af te nemen. Een testbewijs kan vooralsnog alleen verkregen worden van een uitvoerder van testen die is aangesloten op de applicatie CoronaCheck of voldoet aan de voorwaarden voor het uitgeven van een schriftelijk testbewijs. Er is daarom sprake van een beperking van het vrij verkeer.*" Dit is een onacceptabele en onnodige beperking – er zijn al oplossingen in de Nederlandse markt beschikbaar die gebaseerd zijn op dezelfde internationale standaarden als bijvoorbeeld de oplossing die in Duitsland is aangekondigd afgelopen week.

Op basis van hetgeen tot nu toe openbaar bekend is over de Corona Checker oplossing van VWS, zijn er ook technisch-inhoudelijke vragen:

- De crux zit 'm in de QR code die je moet laten zien vanuit de coronacheck app: 1) hoe weet je dat het een unieke code is? 2) hoe weet je dat die code bij (het testresultaat van) die persoon hoort? Voor 1 heb je een centrale database of een blockchain nodig. Voor 2 een credential, die dezelfde vragen met zich meebrengt. Een centrale database is in onze optiek niet wenselijk, omdat deze kwetsbaar is voor lekken en hacken (zoals we recent in vergelijkbare systemen ook gezien hebben).
- De papieren oplossing die geboden wordt, lijkt een separaat PDF spoor te zijn, dat daarmee los staat van de digitale oplossing. De vraag is hoe fraudebestendigheid en privacy voor dat papieren spoor geborgd zijn – dit verdient speciale en expliciete aandacht.
- Hoe gaat VWS om met het mogelijke issue veroorzaakt door de centrale positie van de VWS signer van schaalbaarheid en betrouwbaarheid, als 'single point of trust' en 'single point of failure'?
- Blockchain oplossingen maken eenvoudig zaken als "verify de issuer" (niet zomaar iedereen kan verklaringen/testresultaten uitgeven), "verify de verifier" (niet iedereen kan zomaar testresultaten scannen) en eventueel een "revocation scheme" (credentials kunnen om wat voor reden dan ook worden ingetrokken) toevoegen. Dit vergroot de acceptatiegraad van dergelijke oplossingen, omdat aan ethische bezwaren tegemoetgekomen kan worden dat we geen ongecontroleerde testsamenleving moeten worden en het voorkomt frauduleuze c.q. onbetrouwbare testcertificaten. Hoe wil VWS hier mee om gaan?

Het streven naar minimale inzet van persoonsgegevens is lovenswaardig. Maar de vraag is of initialen en een afgeleide van de geboortedatum voldoende zijn om fraude te voorkomen. Bovendien moet nu separaat een identiteitsbewijs getoond worden als iemand ergens naar binnen wil en dient een handmatige vergelijking gemaakt te worden. Daarbij krijgt degene die de toegangscontrole uitoefent tóch weer alle persoonsgegevens te zien terwijl dit bij gebruik van alleen een geautoriseerde pasfoto niet nodig is. In bestaande oplossingen (zoals uNLock) wordt deze pasfoto op een privacy-veilige manier gekoppeld aan het testresultaat en krijgt de controleur alleen een groen licht ("persoon voldoet aan de criteria" plus een pasfoto te zien, om vast te stellen of het groene licht ook bij de persoon hoort die voor hem staat). Het gebruik van pasfoto's voor dit soort doeleinden is al sinds jaar en dag geaccepteerd. Elke Nederlander heeft tal van pasjes voor bibliotheek, sportclub etc. met een pasfoto erop. Ook oplossingen waarbij de pasfoto digitaal gekoppeld is aan zo'n ledenpas en

waarbij de pasfoto kortstondig op een monitor verschijnt bij binnenkomst zodat de controleur kan vaststellen of betreffende persoon ook met zijn/haar eigen pasje binnen wil komen, zijn er legio.

Het (resterende) frauderisico wordt nu bij de controleur neergelegd, terwijl de controlerende organisatie door deze aanpak geen middelen heeft om ook ècht vast te stellen of degene die voor hem staat, er staat met zijn eigen testresultaat. Dit is unfair, vooral omdat er bruikbare oplossingen zijn die dit beter regelen cf. voorgaande punt.

Sowieso lijkt een behoorlijk rest-risico m.b.t. fraude hier geaccepteerd te worden. In het licht van het feit dat er oplossingen beschikbaar zijn die dit kunnen voorkomen, is dit onbegrijpelijk. Vooral omdat dit soort fraude ervoor kan zorgen dat het virus zich weer verspreidt, waardoor lockdown maatregelen weer nodig zullen zijn. Met alle maatschappelijke en economische gevolgen van dien.

De flow waarbij er naast de Corona Checker een separaat identiteitsbewijs getoond moet worden en door de toegangscontroleur gecheckt moet worden of de initialen etc. op het testbewijs kloppen, is te tijdrovend voor tijdkritische toegangsprocessen. Het toelaten van 50.000 mensen via 50 ingangen gaat minimaal 5 uur kosten op deze manier. En dat terwijl er dus goede integrale oplossingen beschikbaar zijn waar dit in 10-20% van de tijd gaat.

Resumerend zijn wij dus zeer positief over het feit dat deze wet het mogelijk maakt op basis van negatieve coronatesten toegang te krijgen tot het sociale domein, zoals in de wetstekst omschreven. Voor de digitale oplossing moet de overheid kaders en randvoorwaarden stellen en desgewenst ook een eigen oplossing uitrollen, maar deze niet tot de exclusieve standaard maken. Essentieel binnen die kaders en randvoorwaarden is dat oplossingen aan de volgende eisen moeten voldoen: veilig (dus geen centrale database), privacy-proof, fraudebestendig, interoperabel i.v.m. de interne Europese markt en ander internationaal verkeer (essentieel voor de Nederlandse open samenleving en economie) en praktisch uitvoerbaar en voldoende snel (ook bij grote evenementen met tienduizenden bezoekers).

De stichting uNLock en de daarin participerende partijen – specifiek ook de Dutch Blockchain Coalition – doet bij deze een handreiking naar VWS om gezamenlijk te kijken naar de beste mogelijke oplossing voor de Nederlandse samenleving. Het bundelen van krachten past in de tijdsgeest van nu, de farmaceutische industrie heeft hier reeds de waarde van laten zien bij de ontwikkeling van het vaccin.