

Hf 5.1.2e all (en 5.1.2e in cc ivm Nieuwsuur vragen van vandaag)

Excuses voor de long read, maar achtergrond is echt relevant in deze discussie

De principiële discussie is of we vinden dat er één testbewijsapp (van overheidswege) moet zijn of juist meerdere apps. Die hebben we zojuist ook intern gevoerd.

Wij neigen naar:

- als wij als overheid testbewijzen gaan verplichten (via wet) dan hebben we ook zorgplicht om er voor te zorgen dat de het testbewijs betrouwbaar is én dat de persoonsgegevens van de houder van het testbewijs beschermd worden.
- communicatief is het eenvoudiger voor zowel houder als controleur als er één systeem is.
- als we private aanbieders van testbewijsapps toestaan moet er een toelatingskader komen voor deze apps. In komende kamerbrief schrijven we hierover: "Gezien de uitvoeringslasten van een dergelijk kader, waaronder de toelating en toetsing van private testbewijzen en het toezicht en de handhaving hierop, richt ik op dit moment de aandacht op door de overheid gerealiseerde toepassingen voor zowel digitale als niet digitale testbewijzen."
- dat betekent wel dat we er voor moeten zorgen dat andere testaanbieders toegang moeten krijgen tot het systeem zodat het mogelijk wordt dat hun uitslagen ook omgezet worden (middels CoronaCheck) in een testbewijs.
- NB ook Apple en Google hebben recent hun voorwaarden voor toelating in appstore aangepast waarin staat dat ze dit soort type apps alleen toestaan als die van de overheid komen.

Tav wel of geen foto op of in het testbewijs (en daar komt stellingname van 5.1.2e om de hoek kijken):

Wij hebben onze keuze om geen foto te gebruiken gebaseerd op de volgende redentatie:

- De belangrijkste afweging is het vinden van de juiste balans tussen de mate van bescherming van persoonsgegevens en het tegengaan van misbruik.
- Testbewijzen zijn bedoeld om toegangscontrole mogelijk maken voor mensen die kunnen aantonen dat ze recent negatief getest zijn. Dergelijke negatieve testuitslagen bevatten in de regel veel gevoelige persoonsgegevens, zoals adresgegevens, telefoonnummers, burgerservicenummers en de testuitslag zelf.
- Voorkomen moet worden dat dergelijke persoonsgegevens worden overgedragen aan de controleur van het bewijs, terwijl de betrokkene geen controle heeft over waar die gegevens daarna verder voor worden gebruikt.
- Ook is niet voorzien dat kan worden gecontroleerd of iedereen bij toegang is gecontroleerd. Dit is namelijk niet goed mogelijk zonder dat door de controleur een verzameling wordt aangelegd van alle gescande testbewijzen, hetgeen in het kader van gegevensbescherming onwenselijk is. Een dergelijke controle kan ook anders. Bijvoorbeeld door de inzet van mystery guests of door steekproefsgewijs mee te kijken of de controle daadwerkelijk wordt uitgevoerd aan de ingang van een evenement.
- Tegelijkertijd is er de wens om misbruik te voorkomen om zo de risico op verspreiding van het virus zo klein mogelijk te houden. Het verkleinen van de kans op misbruik moet daarom worden afgewogen tegen de verwerking van kwetsbare persoonsgegevens zoals het Burgerservicenummer en medische gegevens. Temeer omdat met het verplicht testbewijs ook het verplicht tonen ontstaat van de gegevens in dit bewijs.
- We neigen er naar om het belang van privacy en informatieveiligheid in dit geval zwaarder te laten wegen dan het volledig uitsluiten van alle mogelijke misbruik. Dit omdat het gaat om uiterst gevoelige gegevens die zouden worden getoond aan private controleurs bij toegang tot allerlei voorzieningen of activiteiten. Die controleurs zijn niet te controleren (of per definitie te vertrouwen).
- De vraag is of we willen dat er een identificatieplicht komt in combinatie met het tonen van een testbewijs met daarop identificerende persoonsgegevens. Wij zijn er tot vandaag vanuit gegaan dat die plicht er niet is.

Als we wel foto zouden toevoegen dan moeten we ons afvragen waar het tegen helpt, hoe we de foto verkrijgen en wat de privacy consequenties zijn.

Een foto toevoegen maakt een visuele inspectie door de controleur mogelijk en voegt iets toe in betrouwbaarheid in de volgende twee meest voor de hand liggende misbruik-scenario's:

- A) dat persoon a zijn testbewijs overdraagt aan persoon b (die zich niet heeft laten testen) en beiden willen naar binnen
 - Tegen A) hebben we allerlei maatregelen getroffen die simpel kopiëren van de QR code zinloos maakt: App staat maken van screenshot niet toe, de QR code verandert elke 3 minuten en is daarna niet meer geldig, de QR code wordt voorzien van bewegende elementen, we signaleren als een QR code meerdere keren gebruikt wordt.
- B) persoon a laat zich testen maar draagt zijn inlog / digid code over aan persoon b die daarmee het testresultaat van a ophaalt en er een geldig testbewijs van genereert

o Allereerst: als a zijn code overdraagt aan b is dat een vorm van samenspanning die niet toegestaan is. Let wel als a dat doet kan hij zelf niet naar binnen, dus hoeveel mensen laten zich daadwerkelijk testen voor een ander. Neemt niet weg dat het kan. Ten tweede : een DigiD zal iemand wellicht naar verwachting minder snel overdragen want kent veel breder toepassingsgebied. Maar ook niet waterdicht. Een foto of andere persoonsgegevens toevoegen op het testbewijs geeft hier de controleur meer zekerheid.

Let wel, de betrouwbaarheid van het hele systeem hangt echter ook af van de wijze waarop de persoon aan de deur de controle doet. Als die persoon iedereen toelaat zonder het testbewijs te controleren, is de discussie over het wel / niet toevoegen van een foto water under the bridge. En we hebben er ook bewust voor gekozen om de controleur niet continue te gaan controleren.

Waar wordt de foto gemaakt? Om het systeem betrouwbaar te laten zijn moet dat gebeuren op het moment van testen én moet het niet mogelijk zijn om later een andere foto in te voegen. Dat is nu nergens het geval en zal vergen dat iedereen die een test ondergaat vooraf toestemming moet geven om zich te laten fotograferen als hij later een testbewijs wil. PS de GGD en commerciële testpartijen vragen nu niet om zo'n foto. Ik vermoed dat de GGD dat niet wil gaan doen.

Derde punt is privacy. Een foto is een gevoelig persoonsgegeven in termen van de AVG. Zoals gezegd de persoon zal toestemming moeten geven om een foto te laten maken. Die toestemming is niet helemaal vrijwillig, want vereist vanwege testbewijs. Dat betekent dat we in onze wetsaanpassing ook de verwerking van dit gegeven moeten regelen.

Consequentie hiervan is dat we niet meer kunnen volhouden dat de CoronaCheck geen persoonsgegevens verwerkt én dat we langs de Autoriteit Persoonsgegevens moeten. Reken op maanden vertraging!

Groeten,

5.1.2e

Van: 5.1 5.1.2e) < 5.1.2e @minvws.nl >

Verzonden: maandag 22 februari 2021 11:05

Aan: 5.1.2e) < 5.1.2e @minvws.nl >; 5.1.2e) < 5.1.2e @minvws.nl >; 5.1.2e) < 5.1.2e @minvws.nl >

Onderwerp: app of apps?

Ha 5.1.2e

5.1.2e gaf vanmorgen aan in het BO met MVWS/MEZK/MOCW en VNO dat hij zich als opdrachtnemer verantwoordelijk voelt op grond van zijn opdracht voor de end-to-end ICT oplossing, inclusief een werkende testbewijs app. Naast de VWS-app kijkt hij ook naar een alternatief. Hij is daar positiever over dan over de VWS-app omdat er een fotootje bij de QR code zit, zodat ID-bevestiging mogelijk is.

Dit verraste mij. Kunnen jullie aangeven:

-wat hierover is afgesproken tot nu toe in de opdrachtverstrekking?

-welke voor- en nadelen zitten er aan het alternatief waar 5.1.2e is naar kijken? Als deze in staat stelt een ID-check te doen, is dat wel een pre natuurlijk dus wel graag even serieus naar kijken.

-graag het alternatief in beeld brengen tbv het gesprek met de minister a.s. woensdag. Hij moet erover geïnformeerd worden omdat hij het anders alleen van 5.1.2e /VNO hoort.

Mvg

5.1.2e

5.1.2e

5.1.2e

5.1.2e @minvws.nl

5.1.2e