DEMO Coronatester app

1e -very basic- prototype

28-01-2021

Er wordt gekeken om -als de situatie het toelaat- de samenleving weer gedeeltelijk te openen d.m.v. de invoering van een testbewijs. De context bepaalt of het gebruik van een testbewijs passend is.

Wanneer een testbewijs gevraagd mag worden om toegang te verlenen is een beleidsmatige keuze.

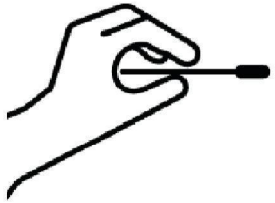
Om deze beleidsmatige keuzes te faciliteren ontwikkelen we 2 applicaties die de invoering van een testbewijs technisch mogelijk maken, in alle contexten die realistisch zijn.

Vandaag concentreren we ons primair op het middel, niet op de toepassing.

Situatie: als burger wil ik naar een social event: concert, horeca, theater, voetbal, ... (ntb)

Ik wil naar een event

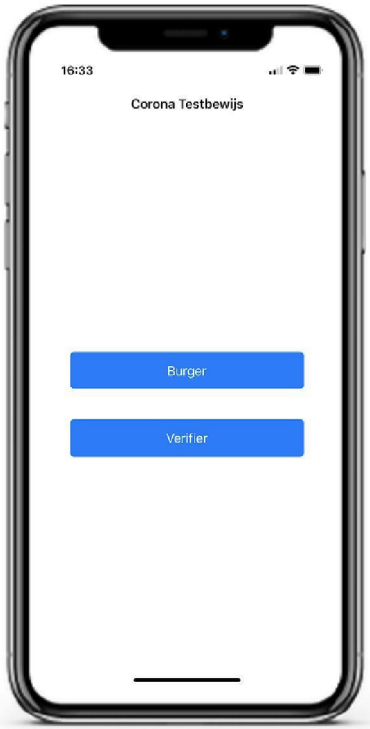
- Ik wil naar een evenement en/of locatie waarbij een testbewijs nodig is om toegang te verkrijgen
- TBD of, voor wie en wanneer een testbewijs vereist gaat zijn



Ik laat mij testen

- Voor aanvang van mijn bezoek laat ik mij testen via de GGD of commerciële testlocatie
- Ik ontvang een negatief testresultaat
- Dit testresultaat kan binnen 48/72 (tbd) uur worden gebruikt om een negatief testbewijs te genereren

We bouwen 2 apps: 1 voor de burger en 1 voor de controleur



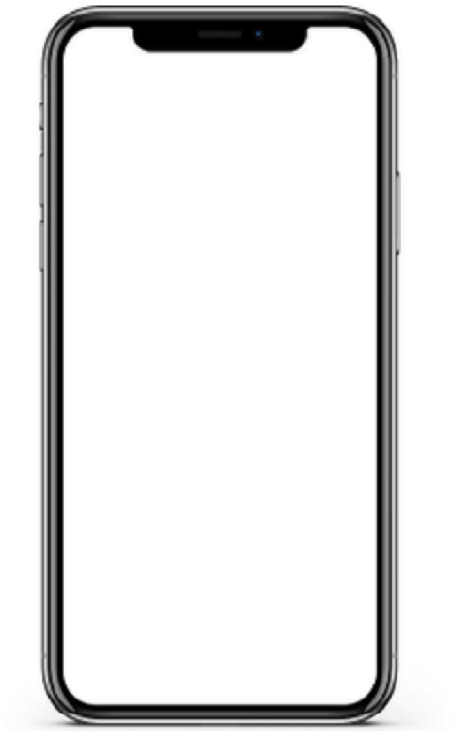
De burger heeft de **'Burger app'**

De controleur heeft de **'Verifier app'**

Er wordt overwogen om beide functionaliteiten in 1 app te combineren (keuze)

Voor demo doeleinden laat dit prototype beide functies zien

Na zijn test haalt de burger zijn test*resultaat* op



De burger haalt het negatieve testresultaat op van de GGD of van een commerciële testaanbieder

Dit doet hij door in te loggen via DigID of door een QR te scannen

Het resultaat is ondertekend met handtekening met een ‘private key’. Niemand kan dit resultaat lezen behalve jouw app.

In het testresultaat wat de app ophaalt, staat - encrypted*- alleen: negatief resultaat, test tijdstip en evt type test (wellicht spoor 2 requirement)

In de burgerapp wordt het testresultaat cryptografisch omgezet in een QR

De handtekening wordt ‘gerandomiseerd’, waardoor de burger zelfs niet te herkennen is aan de handtekening

M.b.v. ‘zero knowledge proof’ bewijst de app dat de handtekening nog wel geldig is.

De QR wordt aangemaakt en opnieuw versleuteld

De QR is hiermee alleen uit te lezen door de verifier app

De verifier app wordt gebruikt door de controleur

De verifying app scant de QR code in de burger app

In de verifying app wordt vervolgens berekend of de handtekening en de ‘zero knowledge proof’ echt is

Zo ja, dan wordt wordt er rood of groen getoond

M.b.v. de verifier app wordt de QR van de burger gescand

Groen = er is een geldig negatief testbewijs. U mag naar binnen.

Rood: er is geen geldig negatief testbewijs.

(bv te oud, of het is geen echt bewijs)

Verdere beveiliging

Voorbeeld van animatie van de Israëlische Corona tester app

We verwerken bewegend beeld rondom de QR zodat duidelijk zichtbaar is dat de QR in de Coronatest app staat - voorkomt het doorsturen van screenshots (of filmpjes bij interactieve animaties)

Daarnaast checkt de verifier app of de tijd in de QR klopt met de actuele tijd. Ook hiermee maken we misbruik door doorsturen van de QR erg lastig

De enige kopie van het testresultaat en testbewijs staat op de drager van de burger

In de Qr code staan geen leesbare persoonsgegevens (geen initialen of naam bijv). Dit is een beleidskeuze.