

**To:** [redacted] [redacted]@minvws.nl]  
**From:** [redacted]  
**Sent:** Fri 10/9/2020 8:37:05 AM  
**Subject:** RE: zelf-tests en CoronaMelder?  
**Received:** Fri 10/9/2020 8:37:05 AM

Ja  
 Behalve het laatste punt ;-)

[redacted]  
 [redacted]  
 [redacted]@minvws.nl  
 +31 6 [redacted]

---

**Van:** [redacted] <[redacted]@minvws.nl>  
**Verzonden:** vrijdag 9 oktober 2020 10:32  
**Aan:** [redacted] <[redacted]@minvws.nl>  
**Onderwerp:** FW: zelf-tests en CoronaMelder?

Ha [redacted]  
 Meer iets voor jullie denk ik?

Gr

[redacted]

Begin doorgestuurd bericht:

**Van:** "[redacted]" <[redacted]@umcutrecht.nl>  
**Datum:** 8 oktober 2020 om 16:34:07 CEST  
**Aan:** [redacted] <[redacted]@cwi.nl>, [redacted] <[redacted]>  
**Onderwerp:** Antw: zelf-tests en CoronaMelder?

Op 8 okt. 2020 om 16:09 heeft [redacted] <[redacted]@cwi.nl> het volgende geschreven:

Beste [redacted]

Vannmiddag in de DOCB ging het over het feit dat Abbott een zelftest (sneltest) heeft die van heel hoge kwaliteit is. Bij monde van [redacted] van het OMT. Eerst werd gedacht om deze in te zetten voor het opschalen van de teststraten, maar de test vereist geen lab, maar wel wat handwerk (incl 15 minuten wachten) en opschalen zo is eigenlijk niet handig in te richten en de uiteindelijke schaal die dan bereikt kan worden is veel minder dan wat je met zelftests zou kunnen bereiken. Deze Abbott test werkt het beste als echte zelftest.

Het zou goed zijn als de Nederlandse regering daar miljoenen van deze test kopen. Anders zijn ze straks uitverkocht, en krijg je een zwarte markt en chaos. Idealiter zou iedereen per post zo'n test moeten kunnen ontvangen, als je hem aan zou vragen op coronatest.nl (wensdenken nog even..)

Indien goed aangepakt, zou zoiets al over een maand de realiteit kunnen zijn. En ik denk binnen drie maanden zeer waarschijnlijk.

Deze situatie zal het functioneren van CoronaMelder fundamenteel veranderen, omdat GGD PCR tests dan veel minder zullen gebruikt worden, en er ook dus geen meldingen de CoronaMelder in zouden komen.

Mijn vraag was: is het bouwteam hier over aan het nadenken??? Je moet niet in de situatie

komen dat het testbeleid snel verandert in een zelftest-distributie, en het CoronaMelder systeem daarin niet meegaat. Bijvoorbeeld: aannemen dat mensen na een positieve test zich zelf dan alsnog gaan laten hertesten bij de GGD is mijns inziens niet realistisch. Dus komt CoronaMelder dan droog te staan, en dat is jammer want CoronaMelder kan volgens mij echt een verschil maken.

Ik kan me voorstellen dat er in deze situatie een app-functionaliteit zou kunnen komen waarmee men een foto maakt van het positieve "zwangerschapstrijkje". Hopelijk staat daar een unieke ID op, zodat we kunnen voorkomen dat nummers dubbel worden gemeld, of niet bestaande nummers (ik denk even aan Putin scenario's, waarin via valse meldingen chaos gezaaid zou kunnen worden). Die foto uit de app (geen GPS erin natuurlijk) zou handmatig, of misschien met beeldherkenning geanalyseerd kunnen worden. En dan zou je op die manier de positieve melding door kunnen zetten in CoronaMelder.

graag jullie reactie!

Ondertussen rennen we richting de lockdown (dinsdag?) is de teststraat structureel overbelast (test wachttijd is nu 5 dagen en dus niet waardevol voor het stoppen van corona), is het BCO volstrekt overbelast en oppervlakkig, en lijken de dijken doorgebroken. Maar, de CoronaMelder wordt gelanceerd zaterdag, en dat is een felicitatie waard! (geen sarcasme, oprecht). Dus we gaan nog wat meemaken, maar coronabestrijding is een zaak van lange adem en CoronaMelder kan volgens mij echt een rol spelen.

met vriendelijke groeten,

5.1.2e

PS

Overigens weet de begeleidingscommissie niet wat er zaterdag precies gecommuniceerd gaat worden en hoe, en dat is eigenlijk wel raar.

----- Original Message -----

From: "5.1.2e" <5.1.2e@cw.nl>  
 To: "5.1.2e" <5.1.2e@vng.nl>  
 Cc: "5.1.2e" <5.1.2e@vng.nl>  
 Sent: Thursday, October 8, 2020 1:52:01 PM  
 Subject: Re: 'Meldcode' voor coronamelder notificaties

Beste 5.1.2e

Excuses voor de lange latency. Ik was druk, maar probeerde ook een en ander uit te zoeken.

Proof of Work gaat niet werken, volgens mijn CWI collega. Het probleem is dat een attacker ook een historie kan opbouwen (of histories kan opbouwen, of desnoods just-in-time naspelen). Het feit dat we werken met een CDN een eenzijdige communicatie maakt naspelen later in de tijd makkelijk.

Ik heb wel een nieuwe suggestie, en dat is om remote attestation te gebruiken. Als de CoronaMelder een alert ziet, neemt die contact op met de VWS server. Daar bewijst de app eerst dat het een echte app is (remote attestation). Op basis van dit bewijs, wordt een bewijs-specifieke voucher (meldcode) uitgereikt. Die leest de gebruiker op.

Ik ben zelf geen specialist op het gebied van remote attestation, maar zowel Google als Apple hebben in hun devices een chip (system-on-chip, eigenlijk) die onafhankelijk is van de rest van het systeem en een secure enclave bevat. In principe kan remote attestation zover gaan dat de SoC informatie krijgt over de code die het aanroept en daar een hash van in de berekening mee

kan nemen. Een andere app heeft een vervalste hash, dus dan krijg je een verkeerde uitkomst. De secure enclave bevat prive sleutels, die er niet uit kunnen. Je kunt er wel berekeningen mee laten doen. Je moet iemand hebben die hier echt veel van weet, bovendien moet datgene wat we evt zouden gebruiken een equivalent hebben op zowel Android en iOS. Maar beiden hebben zo'n SoC, al een paar jaar. Dus dit zou volgens mij wel kunnen werken op de telefoonmodellen die nu GAEN ondersteunen.

Hadden jullie hier zelf aan gedacht (remote attestation)? In de tussentijd probeer ik hier nog een specialist op te vinden.

met vriendelijke groet,

5.1.2e