Privacy en de COVID-19-app; Laten we het zelf doen, dit zijn de fundamenten!

Gisteren heb ik de APPathon gevolgd, georganiseerd door het ministerie van VWS. De APPathon was onder andere te volgen via YouTube. Ik kom met een alternatief voorstel omdat ik mij niet aan de indruk kan onttrekken dat ze het, alles bij elkaar, nog steeds veel te ingewikkeld maken. Het proces is tot nu toe enorm rommelig verlopen. Het is daarnaast onduidelijk welke bedrijven de apps, laat staan de data, in handen hebben of gaan krijgen. Bovendien weten we niet wat het de burger gaat kosten. Met dit stuk nodig ik burgers, bedrijven, overheid, experts, universiteiten uit om mee te gaan doen aan dit Open Source "COVID-19 Testing Support APP. Voordat ik dat ga uiteenzetten eerst nog iets meer over mijn beleving bij de Appathon.

Leeswijzer:

- ***Beleving Appathon Proces van het Ministerie van VWS***
- ***Visie op de App bezien vanuit de burger, hoe zou het moeten werken?***
- ***Laten we het zelf doen, samen, open source met transparantie in gebruik!***
- ***Ontwerp van de App in detail, niet in beton, help mee en geef commentaar?***

Komende dagen meer informatie via: Open Source COVID-19 Testing Support APP

Beleving Appathon Proces van het ministerie van VWS
Ruim voor tien uur zit ik er klaar voor. Het duurt even voordat de stream live is. Het eerste deel van de Appathon bestaat uit presentaties van de geselecteerde kandidaat-apps; 7 in totaal. Het wordt al snel duidelijk dat maar weinig kandidaten een echt live werkende app kunnen demonstreren. Presenteren kon wel, maar dat geeft weinig vertrouwen en ook geen enkel inzicht wat het nog betekent om de *a*pps *fit for use* te maken.

Wat verder opvalt is dat een aantal partijen echt wel data verzamelen. Ze vragen je mobiele nummer uit om te beginnen. Encrypted of in een 'kluis'. 'Deze vallen alvast af' dacht ik direct. Het opslaan van dergelijke gegevens is immers helemaal niet nodig. Encryptie van telefoonnummers is ook een schijnveiligheid, want die beginnen vrijwel altijd met 06 en dan zijn er niet zo heel veel mogelijkheden meer over.

Tijdens de pauzes blijven de vragen komen: op welke criteria heeft de selectie eigenlijk plaatsgevonden? Hoe kunnen partijen zo nonchalant omgaan met het begrip 'open source'? Regel 1 van *privacy by design* is toch: nooit meer gegevens gebruiken dan je strikt nodig hebt? 'Privacy by Design' en 'Open Source' zijn geen vakjes die je zomaar even aan kruist. Ze zijn onderdeel van de ethiek van de bedenker, ontwikkelaar, toetser en gebruiker en horen zich daarom door te vertalen in een gedetailleerde solution architectuur.

Zouden we daar dan niet ook met z'n allen naar moeten kijken? Misschien is het voldoen aan echt privacy by design en echt open source wel belangrijker dan het snel een presentatie kunnen geven. Wat is hier eigenlijk het belangrijkst? De APPathon geeft hier geen uitsluitsel over.

Het is lastig om bij de les te blijven: al die commerciële belangen aan tafel, zo weinig verrassingen. De overtuiging zit inmiddels vast in mijn hoofd: er zijn vast nog andere oplossingen die alleen al op bovenstaande punten beter uit de bus komen.

Denk aan de Noorse Smittstopp app is al meer dan een miljoen keer gedownload in de eerste vier uur na publicatie; gefileerd door de tech community en nog steeds niet te licht bevonden en aantoonbaar

GDPR compliant. De Noren gebruiken een generieke back-end en een hele lichte front-end, waarbij de laatste machine learning algoritmes op de data worden losgelaten. De Italianen richten zich meer op de front-end met echt hele slimme algoritmen.

Hoeveel service kun je krijgen met een gelegenheidscoalitie van banken, consultants en wetenschappers, zonder aantoonbare ervaring met schaalbaarheid.

Samenvattend over de Appathon
- Het is veel show en enthousiasme en complimenten over de organisatie, dit overschaduwt de inhoud;
- Het is wel een open maar geen *transparante* procedure. Er is geen academisch toetsproces, en er zijn vage criteria en geen duidelijke uitgangspunten;
- de RFI (Request For Information) vragen van het VWS zijn veelomvattend, de overheid wil te veel en veel van wat ze vragen lijkt onnodig;
- Op welke criteria zijn de 743 andere partijen afgevallen?
- Wie zijn de experts en beoordelaars in de verschillende rondes en wat maakt ze expert?
- Een aantal van de betrokken experts is het openlijk oneens met de procedure en gang van zaken, en neemt afstand van de selectieprocedure (zie https://www.veiligtegencorona.nl). Hiermee is het draagvlak nu al verloren bij de burger;
- Het heeft op z'n minst de schijn van doorgestoken kaart door het toevoegen van de 'bekende grote ICT spelers uit de overheids wereld' die er dus blijkbaar sowieso bij zitten;
- De apps zijn géén open source. Er is op zijn minst vaagheid over de broncode en er is geen ontwikkeling in een community van experts;
- Transparantie over wat het mag kosten of gaat kosten heb ik niet vernomen, maar ook niet verwacht;
- Teveel commercieel belanghebbenden aan tafel. Het zijn veel mooie praatjes maar op inhoud is het gebrekkig.

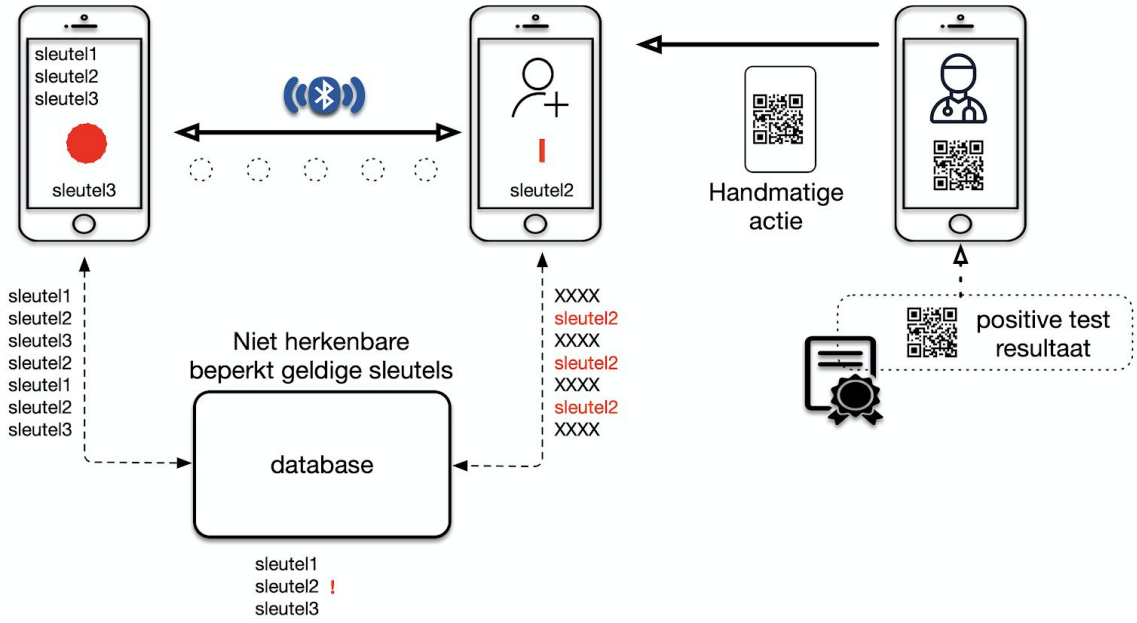
Komende dagen meer informatie via: Open Source COVID-19 Testing Support APP

Visie op de App bezien vanuit de burger, hoe zou het moeten werken?

Mijn uiteenzetting begint met mijn visie om een ethisch en dus ook privacy verantwoorde "COVID-19 Testing Support APP" te delen met een groter publiek. Hopelijk zijn lezers, autoriteiten, journalisten hiermee weer een stapje verder geholpen.

In essentie zou je een app maar om één reden willen lanceren en dat is ondersteuning van de GGD bij het testen van mensen die in potentie COVID-19 hebben. Iedereen weet het telefoonnummer van de GGD of autoriteiten te vinden dus meer is er niet nodig.

"Als we landelijk niet bereid zijn op grote schaal te gaan testen op COVID-19 heeft een App geen enkele toegevoegde waarde"



Laten we de app gaan gebruiken. We downloaden in de iOS en Android store de “COVID-19 Testing Support APP”, verder te noemen APP-C19. Het bovenstaande plaatje geeft een schematisch overzicht van de oplossing met de APP-C19.

Nadat we de APP-C19 hebben gedownload is hij direct operationeel. We hebben geen persoonsgegevens hoeven afstaan aan APP-C19. Hij staat gewoon *AAN*. Willen we de APP-C19 niet meer gebruiken dan verwijderen we hem van onze telefoon. Wanneer je Bluetooth tracking uitzet werkt hij overigens ook niet meer.

Alternatief voor Bluetooth - Bluetooth tracking kan tot security problemen leiden en mogelijk zal er dienen te worden samengewerkt met telecommunicatiebedrijven die met terugwerkende kracht de locatie van je geanonimiseerde telefoon van de afgelopen twee weken pushed naar de eveneens geanonimiseerde telefoons die in die tijd bij jou in de buurt geweest zijn. We hoeven dan slechts een toestemming (consent) te geven die een unieke eenmalige sleutel genereert om het FEIT van de besmetting te melden, niet de PATIENT. Dit is een voorbeeld van Zero Knowledge Proof en anonimisering die ook niet-smart phones mee laat doen in de dataset.

De enige andere garantie die we willen hebben is dat de app ons niet kan tracken en traceren maar alleen vasthoudt wie (andere smartphone) de afgelopen dagen vanaf het moment dat ik besmet werd mijn pad heeft gekruist binnen een bepaalde afstand. Daarbij kunnen we ook meegeven hoe lang de persoon in mijn beurt is geweest, maar meer informatie is niet zinvol.

Wanneer ik denk COVID-19 klachten te hebben dan bel ik de GGD en word ik getest.
Wanneer de GGD mij positief test moet ik in quarantaine.

De GGD of andere autoriteit kan met een CORONA-Token via APP-C19 een bericht sturen naar mijn APP-C19 door fysiek en dus handmatig een QR code te scannen. Dit CORONA-Token informeert via het systeem de mensen die in mijn buurt zijn geweest via hun APP-C19 met de melding “U was de afgelopen dagen in de buurt van een Corona besmet persoon voor de duur van 14 min en 2 seconden, u kunt zich laten testen bij de GGD daarmee helpt u COVID-19 te bestrijden”. Bij voorbaat dank!

Kunnen we mensen dwingen zich te laten testen? Nee!!

Omdat de App alleen zin heeft als we hem op grote schaal toepassen, zal het moeten werken op basis van verantwoordelijkheid. De burger heeft de verantwoordelijkheid door middel van de app om contacten bij te houden.De GGD heeft de verantwoordelijkheid om te testen en zo de besmetting vast te stellen. Verder dienen ze ons patiëntendossier bij te werken, zoals dat gebruikelijk is. Uiteraard kunnen en mogen ze, zoals ze nu ook doen, tellen hoeveel mensen besmet zijn en weer gezond verklaart zijn.

De GGD kan op basis van de anonieme data een sociogram (een patroon analyse van sociale netwerken van personen) samenstellen om zo de besmettingsgraad en verdeling / over tijd van de besmettingen te monitoren, waarop dan weer beslissingen kunnen worden genomen in het opschalingsproces. De Britten gebruiken dit soort informatie voor het op kaarten aangeven van geofenced rode zones, waar je de komende 24 uur even niet zou moeten komen. De kaartinfo is ook ideaal voor het finetunen waar de schaarse test capaciteit het meest efficiënt kan worden ingezet. Door het toevoegen van bakens op gedefinieerde plaatsen kan ook geheel anoniem locatie informatie bij dit patroon worden toegevoegd. Denk aan het investeren in iBeacons die nu al in winkels gebruikt worden en goede diensten doen op congrescentra en tijdens SAIL, op openbare knooppunten zoals stations en pleinen. Dat zou in elk geval een investering zijn die ook economisch bijdraagt.

We zullen of een groot deel van onze bevolking moeten overtuigen (17 miljoen mensen) wanneer we geen persoonsgegevens op willen geven aan de app en de app onze locatiegegevens niet mag gebruiken. Of we moeten diezelfde populatie snel scholen in de verschillen tussen anonimiteit, pseudonimiteit en veronimiteit en cruciale technieken als verifieerbare claims. Privacy kent namelijk vele lagen, net als identiteit, net als zekerheid en net als vertrouwen. We willen geen informatie delen. Het gaat alleen om data die nodig is om het probleem op te kunnen lossen. Het is niet mogelijk om de privacy discussie op emotionele gronden te voeren. Het is ook een juridische, ethische en uiteindelijk data technische discussie, die in volstrekt logische verhoudingen gevoerd moet worden. APP-C19 houdt alleen bij wie ons pad heeft gekruist vanaf het moment dat ik besmettelijk kan zijn geweest. Het enige wat er hoeft te gebeuren is dat mensen die in de buurt zijn geweest bij deze persoon ook getest worden om verdere verspreiding tegen te gaan.

Komende dagen meer informatie via: Open Source COVID-19 Testing Support APP

Laten we het zelf doen, samen, opensource met transparantie in gebruik

Mijn inziens moet de burger zelf het heft in de openheid in eigen handen nemen, hoe doen we dat?

A. We storten als samenleving giften op een derdenrekening van een onafhankelijk te bepalen notaris en accountancy kantoor die toezien op de boekhouding, partijen mogen zich melden bij mij. De accountant betaalt de rekeningen van leveranciers en er wordt door hen wekelijks een transparante rapportage opgeleverd met inkomsten en uitgaven De accountant werkt hierbij strikt en alleen kostendekkend en wordt als sponsor gekenmerkt;
B. We werken op basis van giften die alleen bij gebruik van de App door de centrale en decentrale overheden en GGD tegen betaling van 8% rente van moment van starten van een gift als een lening wordt afgelost, geldt ook voor buitenlandse overheden. Omdat er strikt en alleen kosten mogen worden opgevoerd en er mag geen marge gemaakt mag worden neemt de overheid dus alleen de kosten voor haar rekening;
C. De ontwikkeling van de App kost € 250.000 exclusief BTW dat is een groot bedrag maar we willen wel binnen 6 a 8 weken live kunnen zijn. Het geld dat overblijft gaat naar de

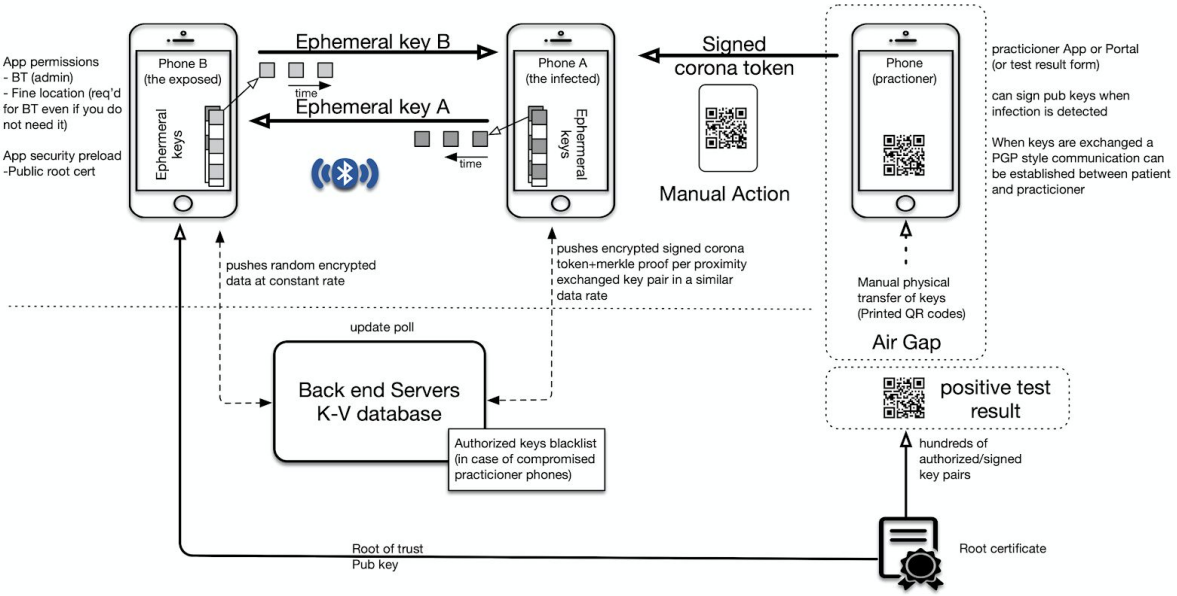
doorontwikkeling van de App na live-gang, blijft er meer over dan kunnen we dat storten op een door de overheid te open rekeningnummer. voor mondkapjes;

D. De doorontwikkeling kost € 25.000 exclusief BTW per maand voor het eerste jaar en € 10.000 exclusief BTW per maand voor de jaren daarna zolang we hem als maatschappij in productie willen houden.
E. De infrastructuur voor de “achterkant van de App” (met name de database): Om te garanderen dat het systeem voor potentieel 17 miljoen mensen kan blijven draaien dient deze bij een Nederlandse infrastructuur partij komen te liggen. Die partij heeft geen toegang tot de App of de gegevens. Infrastructuur Partijen mogen zich melden bij mij. Er mag geen marge gemaakt worden op de dienst. De partij wordt als sponsor gekenmerkt.
F. Het project is open source, zodat ook derdewereldlanden hem nagenoeg kosteloos in gebruik kunnen gaan nemen. De broncode is door iedereen direct in te zien, er wordt vanuit een openbare repository gewerkt en wijzigingen vanuit de gebruikersgroep kunnen direct worden toegepast.
G. De app wordt ontwikkeld conform de Normalized Systems Theory; een wetenschappelijk bewezen werkwijze van de Universiteit van Antwerpen die afdwingt dat de ontwikkelaar zich aan vier wetmatigheden houdt. Als die vier ontwerp wetten in samenhang worden gevolgd is onderhoudbaarheid en schaalbaarheid van de app volstrekt gegarandeerd.
H. Voor de ontwikkeling hebben we een team met ongeveer 10 rollen nodig en iedereen krijgt € 70 per uur exclusief BTW. We starten met ontwerpen en bouwen zodra de eerste giften binnen komen.
I. Er werken 10 rollen (1 UX/UI Designer, 1 Back-End Scala, 1 Security Specialist, 2 React Native, 1 Native Kotlin en 1 Native Swift, 1 Technisch Tester, 1 Infrastructuur Expert, 1 Lead & Solution) niet fulltime aan van 10 verschillende MKB bedrijven die zullen worden gekenmerkt als sponsoren. Deze personen mogen zich bij mij melden en wanneer ze de juiste profiel en ervaring kunnen leveren mogen ze aansluiten. Wie het eerst komt die het eerst maalt.
J. De app staat structureel open voor alle security specialisten in de wereld. Zij mogen proberen zwakheden te vinden.
K. Ook zijn alle experts vanuit de wetenschappelijke en gezondheid wereld welkom hun eisen aan de app te stellen, aanpassingen te doen en mee te denken, GGD, RIVM, Universiteiten, etc.
L. Gebruik van de App is voor iedereen gratis. Wanneer het project slaagt zou het mooi zijn als de regering de kosten overneemt en iedereen die gesponsord heeft een rente geeft van 10% op de gift/lening.

Komende dagen meer informatie via: Open Source COVID-19 Testing Support APP

Ontwerp van de App in detail, commentaar door alle experts welkom!?

Vragen door het VWS gesteld en door App bouwers beantwoord! Hierbij mijn een ontwerpvoorstel. De onderstaande figuur laat schematisch zien welke elementen we kunnen onderscheiden en hoe het voorgestelde systeem werkt.



Doel 1
Het verkrijgen van een voorstel voor slimme digitale oplossingen, zoals bijvoorbeeld apps die kunnen bijdragen aan bron- en contactopsporing, waarbij stringente eisen gelden voor onder meer snelle beschikbaarheid, privacy en informatiebeveiliging.

Vraag: Welke slimme digitale oplossing kunt u leveren die bij kunnen dragen aan bron- en contactopsporing?

Antwoord: Een smartphone-app (Android / iOS) voor 100% anonieme contact tracering. De app is gebaseerd op een (voor de gebruiker bezien) 'black box'-mechanisme dat peer-to-peer-meldingen mogelijk maakt tussen apparaten die in de buurt zijn. Het centrale systeem kent relaties die elk apparaat opbouwt niet.
Door echter bluetooth-bakens (eigenlijk bluetooth scanners die lijken op apparaten zoals die al in gebruik zijn op veel publieke plaatsen) die op bijvoorbeeld treinstations, treinen, trams, metro, bus en kantoren te plaatsen, wordt het mogelijk om de beweging van (positief geteste) Corona-patiënten anoniem te volgen. Dit zou antwoorden kunnen geven als: 'Tussen Tiel en Geldermalsen was er op deze datum / tijd verkeer van een Corona-patiënt, alle mensen die in de directe omgeving van deze patiënt zijn geweest, worden geïnformeerden moeten contact opnemen met de autoriteiten om op Corona te worden getest'.

Artsen, beoefenaars of ander door de overheid geautoriseerd personeel dienen als kwaliteitscontrole-mechanisme voor het systeem. Alleen zij mogen een diagnose stellen en persoonlijke gegevens opvragen / communiceren die via reeds bestaande kanalen. Via hen kan de data (uiteraard na toestemming van betrokkene) worden gebruikt voor verder (pandemisch) onderzoek.

Het vertrouwensmodel tussen de app en zorgverleners is 'air gapped'. Dit betekent dat er geen potentiële beveiligingslekkende informatie ooit de apparaten (electronisch) kan verlaten, communicatie is door ondertekende berichten verzonden via QR-codes.

Doel 2
Het verkrijgen van een voorstel voor slimme digitale oplossingen zoals bijvoorbeeld apps die kunnen bijdragen aan zelfmonitoring en begeleiding op afstand, waarbij stringente eisen gelden voor onder meer snelle beschikbaarheid, privacy en informatiebeveiliging

Vraag: Welke slimme digitale oplossing kunt u leveren die bij kunnen dragen aan zelfmonitoring en begeleiding op afstand?

Antwoord: De app is inherent voor zelfcontrole. De app is gebaseerd op de aanname dat als je het installeert, je bereid bent om deel te nemen en de instructies van de app te volgen. De app laat u weten wanneer u in de buurt van een positief geteste patiënt bent geweest en vraagt u om uzelf te controleren en anders contact op te nemen met uw zorgverlener.

Hulpverlening op afstand kan worden ingesteld tussen de zorgverlener en geteste patiënten nadat de sleutels zijn uitgewisseld.

Monitoring-instructies via actuele informatie over corona, behandeling, RIVM-nieuws kunnen worden toegevoegd. Naast deze informatie zou het niet nodig moeten zijn om informatie over de gezondheid van de app-gebruiker te vragen, maar het is essentieel om ze naar een geraadpleegde arts te leiden voor testen op Corona.

Doel 3
Het verkrijgen van voorstellen voor overige digitale oplossingen, zoals bijvoorbeeld apps, die kunnen bijdragen aan de transitiestrategie en het bestrijdingsbeleid.

Vraag: Welke slimme digitale oplossingen kunt u leveren die bij kunnen dragen aan de afschalings strategie en begeleiding op afstand?

Antwoord: Onze voorgestelde bluetooth- en bakens strategie stelt ons in staat om een transitie te maken om langzaam economisch verkeer op te bouwen, het effect te monitoren en maakt het daarom mogelijk om de downscaling snelheid aan te passen.

Een controlebeleid betekent dat mensen die positief getest zijn op het hebben van het virus, gedwongen / aangeraden moeten worden thuis te blijven, wat leidt tot schending van de privacy. Daar kunnen wij niet achter staan. Mensen luisteren al naar de overheid. Op basis van sociale druk blijven ze thuis als ze symptomen vertonen zoals ze al doen.

Doel 4
Het verkrijgen van voorstellen voor voorwaarden waaronder digitale oplossingen kunnen worden ingezet (met betrekking tot techniek, inhoud, werking, implementatie, de privacy en informatieveiligheid)

Vraag: Welke voorstellen voor het op technische en organisatorische wijze borgen van privacy en informatieveiligheid kunt u doen?

Antwoord: Totdat een potentiële patiënt contact opneemt met de zorgverlener, is er geen inbreuk op de privacy omdat er nooit persoonlijk identificeerbare informatie wordt uitgewisseld of opgeslagen. De uitgewisselde informatie kan alleen worden gelezen door de verzender en ontvangers (end-to-end versleuteld). Er worden maatregelen genomen om netwerk en verbindings analyse binnen het systeem zelf te voorkomen.

Zodra een patiënt contact heeft met een zorgverlener, kunnen ze ervoor kiezen om deel te nemen aan onderzoek zoals momenteel mogelijk is. Het vertrouwensmodel is ‘Air gapped’.

De voorgestelde App is gebaseerd op het identifier mechanisme van het open (source) project DP3-T (code en documentatie te vinden onder https://github.com/DP-3T) waarbij tijdelijke identifiers worden gebruikt die in kleine stukjes worden gecommuniceerd.De backend afhandeling en tokenverwerking is toegevoegd op een eigen wijze.

App-functionaliteiten:

- IOS- en Android-app gebouwd op basis van één continuous delivery ontwikkelproces met één ontwikkel toolkit op basis van onder anderen react-native en native (Swift en Korlin);
- User Experience en User Interface gebaseerd op de stijlgids van de GGD;
- De app logt nooit in en vraagt zelfs niet naar persoonlijke informatie;
- De app infrastructuur heeft alleen voor deze gelegenheid een (privé) rootcertificaat;
- De app wisselt de identificatie-sleutels uit in kleine stukjes om zodoende te voorkomen dat er pas sprake is van een compleet reconstrueerbare anonieme identificatie na een zekere tijd. Dit is de tijd die de GGD noemt als tijd nodig voordat we een potentiële besmetting kunnen hebben opgelopen. De sleutels worden uitgewisseld via bluetooth en het tijdstempel wordt opgeslagen, om zodoende na de incubatietijd de sleutel weer te verwijderen;
- Sleutelparen worden gegenereerd en hun openbare sleutels worden verzameld in een merkle-boom. De merkle-boom groeit, maar kan worden gebruikt om bewijs van opname te creëren zonder additionele te onthullen;
  (zie ook: http://www.certificate-transparency.org/log-proofs-work)
- De app publiceert willekeurig versleutelde gegevens in een zekere snelheid. Dit vormt een belasting voor de back-end, maar maakt de analyse van verbindingen / activiteiten zeer lastig, zoniet onmogelijk. Maar vanwege de eenvoud van de installatie is het gemakkelijk om in korte tijd naar miljoenen gebruikers te schalen.
- De app kan speciale berichten ontvangen die zijn versleuteld met een van de uitgewisselde sleutelparen. Dit pakket bevat een ondertekende (door een geautoriseerde sleutel) merkle-root en merkle-bewijs dat bewijst dat het sleutelpaar deel uitmaakte van de ondertekende root. Dit bericht activeert het alarm in de app;
- De app zoekt voortdurend naar nieuwe updates en releases

Beoefenaars app / ruimte (is dezelfde app alleen een andere rol):

- Zorg professionals / GGD kunnen worden geactiveerd door het laden van een privésleutel die is ondertekend door het root-certificaat. Hierdoor heeft de app-eigenaar de mogelijkheid om een bericht met een openbare sleutel / merkle-root te ondertekenen;
- Het afgeven van een handtekening van een zorgverlener (autoriteit) aan het apparaat van de geïnfecteerde persoon kan worden gedaan met behulp van een speciaal vervaardigde QR-code die wordt verstrekt door de app voor artsen en kan worden gescand door de app voor geïnfecteerde personen;
- Bovendien kan hetzelfde mechanisme voor het uitwisselen van handtekeningen worden gebruikt om extra sleutels uit te wisselen voor versleutelde en geauthenticeerde communicatie in PGP-stijl (Pretty Good Privacy).

Corona-tokens:

- Dit is een ‘token’ (informatiepakket) dat is electronisch ondertekend door een arts met de sleutel die is verstrekt door de autoriteiten;
- Dit token wordt vervolgens samen met een merkle-proof naar andere apparaten verspreid. Zonder dit cryptografische bewijs is het token nutteloos. Dit betekent dat de app het uiteindelijk zelf naar elk van zijn contacten moet sturen; Dit gebeurt automatisch.
- Alleen het token zichtbaar maken, betekent niets.

Wanneer een gebruiker de app op een apparaat installeert, wordt de gebruiker gevraagd om dit token automatisch te delen wanneer de diagnose wordt gesteld.

De backend:

- De backend kan heel eenvoudig worden gemaakt, als een database met sleutels en waarden (key-value pairs) die Time-To-Live-mechanismen ondersteunt voor automatische gegevensverwijdering;
- De eenvoud van de backend maakt schaalbaarheid mogelijk;
- De backend toont altijd een lijst met openbare eindpunten die kunnen worden gebruikt met consistente hashing (op basis van openbare sleutels) om efficiënte netwerk routering en scaling te bieden zonder dat dit in een netwerkomgeving hoeft te worden opgelost.

Het meest veiligheidskritische onderdeel is het systeem dat vanaf het basis/ root certificaat) sleutels kan produceren voor artsen en beoefenaars of ander bevoegd personeel. Zij kunnen dan na het stellen van een de resultaten in het apparaat van de patiënt in te voeren. Dit systeem wat de sleutels kan produceren staat fysiek geheel los van de rest van de infrastructuur (zgn. air gapped) , en kan daardoor moeilijker (over een netwerk) gecompromitteerd worden

De technologie van het uitwisselen van tokens op basis van tijdelijke ID's en het voorkomen van drive-by-aanvallen zoals beschreven in het white paper van het DP3-T consortium (zie eerder) , is aan dit ontwerp worden toegevoegd.

Belangrijke zaken om hier rekening mee te houden zijn onder andere de eigenschappen gebruikte proximity technology. Bluetooth is in staat om door corona bestendige barrières zoals muren te dringen. Om dit te ondervangen, kan technologie op basis van voor de mens (en ook dieren) onhoorbare geluiden worden toegevoegd om valse positieve meldingen te voorkomen. Ook is de resolutie van de RSSI (signaalsterkte) van een bluetooth-signaal zoals waargenomen door een smartphone afkomstig van een andere bron vaak niet goed genoeg om een afstand van 1,5 m nauwkeurig te bepalen. Extra time-of-flight en / of triangulatie functies op laag niveau in de software kunnen de nauwkeurigheid, indien nodig, verder verbeteren, Echter, door de inherent gesloten onderlaag van de software op mobiele devices kan dit lastig zijn om correct te implementeren. Het toepassen van de door Google en Apple in ontwikkeling zijnde API kan hier helpen.

Technische zaken als backend performance, bandbreedte en schaling zijn van belang. De backend technologie (database en encryptie) kan worden opgelost met behulp van een cloud (ofwel een openbare of de Nederlandse overheid private cloud) implementatie en clustertechnologie. De cloudprovider moet voldoende bandbreedte hebben, zowel in- als uitgaand.

Ook wordt opgemerkt dat het batterijgebruik op mobiele platforms een probleem is. Zowel (mobiele) data communicatie als het gebruik van de bluetooth functie gebruiken relatief veel energie. Om dit te optimaliseren kunnen berichten op het device in de wachtrij worden geplaatst, en als batch verstuurd worden. Ook is het van belang dat de bandbreedte belasting van mobiele providers moet worden meegewogen in de communicatiestrategie.

Komende dagen meer informatie via: Open Source COVID-19 Testing Support APP

Graag nodig ik burgers, bedrijven, overheid, experts, universiteiten uit om mee te gaan doen aan dit Open Source “COVID-19 Testing Support APP” initiatief waarbij volledige transparantie en openheid wordt gegarandeerd en overheid dus een onderdeel kan worden van de ontwikkeling i.p.v. dat er bepaalt wordt voor de burger wat goed voor ons is. Ook helpen we

hiermee landen die het zelf niet kunnen opbrengen een ethisch en privacygevoelige App te financieren en te realiseren.

Met vriendelijke groeten,

Hans van Bommel, IT ondernemer
M +31628751295