DEUS - Antwoord op Vragenlijst covid19 app van Security panel

DEUS specifieke vragen

- Wat voegt DEUS toe aan het DP3T protocol

Zoals al kort toegelicht in de expertsessie maakt DEUS op dit moment geen wijzigingen of toevoegingen aan het protocol zelf.
Wel maken wij gebruik van de basis mobiele applicatie zoals deze in de Github van het DP3T project te vinden is. In de mobiele applicatie code maken wij wel wijzigingen. Hierbij valt te denken aan het toevoegen van accessibility functionaliteiten.
Wij zijn momenteel in contact met de initiatiefnemers van het DP3T protocol om te kijken hoe wij deze verbeteringen weer terug kunnen 'geven' aan het initiatief, zodat dit door de bredere gemeenschap gebruikt kan worden.

Algemene vragen

- Hebben jullie een overzicht beschikbaar van de complete user lifecycle?
    - Per stadium in de versleuteling, hoe ontsleuteld, en wie heeft toegang tot welke gegevens?

1) Gebruiker download de applicatie uit de appstore [de app zal gepubliceerd worden onder het officiële overheidsaccount]
2) Gebruiker start de app en wordt gevraagd om het gebruik van Bluetooth toe te staan. Dit zal nodig zijn voor de werking van de app. Zonder deze toestemming zal de app niet werken.

Een gebruiker met een Android device zal gevraagd worden om toegang te geven tot zijn/haar locatie. Dit is helaas niet uit te zetten (zie android specs en reported issue samen met Google's antwoord hierin) en dient goed uitgelegd te worden aan de gebruiker. De locatie zal namelijk nooit opgevraagd worden door de app.

Op iOS zal de gebruiker worden gevraagd om notificaties toe te staan. Ook dit is nodig voor een goede werking van de app. Let wel dat de notificaties lokaal zijn en dus niet via een server worden verstuurd.

3) De gebruiker krijgt een korte handleiding te zien van de app en komt vervolgens op het hoofdscherm. De enige data die de applicatie verzendt is de EphIDs. Deze worden verzonden via Bluetooth. Daarnaast zal de app luisteren naar andere toestellen die EphIDs uitzenden en deze opslaan [waarbij de periode beperkt is - in dit voorbeeld 14 dagen, maar dit is te configureren].

4) De app zal regelmatig een lijst met Secret Keys ophalen van de backend server. De backend bevat alleen Secret Keys van andere app gebruikers die als geïnfecteerd zijn

gemarkeerd door medisch specialisten. Op basis van deze Secret Keys zullen de EphIDs geregenereerd worden en wordt er gekeken of er een match is tussen de ontvangen EphIDs op het lokale toestel en de gegenereerde EphIDs van de geinfecteerde personen. Als hier daadwerkelijk een match is, dan zal de gebruiker een lokale notificatie ontvangen dat hij/zij in contact is geweest met een geïnfecteerd persoon. De gebruiker krijgt dan vervolgens tips over vervolgstappen.

5) Indien een gebruiker zelf positief getest wordt , dan zal de gebruiker een TAN code krijgen van de medisch expert die de test heeft afgenomen en gevraagd worden door deze expert om deze code in te voeren. Deze code wordt geverifieerd door een systeem van de GGD [specificaties nog te ontvangen].
Zodra de TAN is geverifieerd zal de Secret Key van de huidige dag van de gebruiker worden geupload naar de backend.
In de app zal nu direct een nieuwe Secret Key worden aangemaakt om tracking te voorkomen [zodra Secret Key is gedeeld zou het anders in theorie mogelijk zijn om toekomstige EphIDs te voorspellen van iemand die geïnfecteerd is]

6) De backend zal de Secret Key opslaan en deze zal gedeeld worden met alle andere app gebruikers [zie stap 4].

- Bluetooth sniffing?

Wij hebben nog geen specifieke maatregelen geïmplementeerd die Bluetooth sniffing blokkeren. Daar de token-data volledig willekeurige reeksen cijfers zijn, zal het risico van sniffing voor wat betreft de applicatie beperkt zijn.

- Waar wordt de data encrypted/decrypted, on device of in de cloud?

De data wordt niet encrypted/decrypted, maar de werking is gebaseerd op willekeurige tokens en hashing.

Het 1e deel van informatie heet de Secret Key. Dit is een 32 bytes lang getal dat volledig willekeurig gekozen wordt door de telefoon tijdens installatie. Het getal is niet gebaseerd op persoonlijke informatie. Deze Secret Key zal gedeeld worden indien een besmetting geconstateerd wordt. Elke dag zal de app een nieuwe Secret Key genereren op basis van de Secret Key van de dag ervoor.

Het 2e deel van informatie heet de EphID, dit is een 16 bytes lang getal wat berekend wordt op basis van de Secret Key, en aangezien de Secret Key niet gebaseerd is op persoonlijke informatie, is de EphID dit ook niet. Deze EphID wordt elke paar minuten gedeeld met telefoons in de buurt.

De data die we nodig hebben om de app te laten functioneren [de security keys en de EphIDs] worden lokaal op het toestel voor een beperkte periode (periode te bepalen in overleg met GGD) opgeslagen in een afgesloten locatie op het toestel. Deze locatie is encrypted door het besturingssysteem.

De data die wordt verzonden via Bluetooth [de EphIDs] zullen unencrypted worden verzonden naar andere telefoons. Dit zodat de andere telefoons de EphIDs kunnen oppakken. Nogmaals de EphIDs zijn volledig anoniem.

Mbt de cloud; Hier wordt de Secret Key opgeslagen van de gebruikers die hebben aangegeven dat zij besmet zijn geraakt. Deze secret key wordt unencrypted opgeslagen.

- Wat voor encryptie wordt toegepast en op welke momenten en locaties wordt de data decrypted?

Zie antwoord hierboven

- Welke data wordt opgeslagen?

De app is ontwikkeld met privacy als prioriteit. Er zal dan ook nooit opslag of uitwisseling van persoonlijke data plaatsvinden. De enige data die gebruikt wordt, zijn willekeurige (dus anonieme) secret keys en gegenereerde, niet traceerbare "tokens" [EphIDs] die telefoons naar elkaar sturen. Zo kunnen telefoons elkaar laten weten dat ze bij elkaar in de buurt zijn geweest en kunnen gebruikers gewaarschuwd worden wanneer zij in de buurt van een corona besmetting zijn geweest. Ook deze anonieme data willen wij graag zo kort mogelijk bewaren, daarom worden al deze tokens automatisch na 14 dagen verwijderd. De 14 dagen is een door ons gekozen termijn en is te bepalen in overleg met de instanties.

- Waar wordt de data opgeslagen en verwerkt?

Er zijn twee soorten data die opgeslagen wordt:

1. *SecretKey (om tokens mee te maken)*
2. *EphID.*

De SecretKey worden op de eerste dag van gebruik van de app opgemaakt uit een willekeurig getal. Elke dag wordt een nieuw sleutel gemaakt op basis van de oude SecretKey. Deze SecretKey worden 14 dagen (of langer of korter op basis van advies van de GGD) opgeslagen op de telefoon (lokaal dus). De hash functie waarmee de nieuwe SecretKeys worden gemaakt werkt slechts 1 kant op, waardoor je met een nieuwe SecretKey niet een oude SecretKey kunt herleiden.

De EphID die gemaakt worden op basis van de hiervoor genoemde sleutels worden ook slechts opgeslagen voor 14 dagen en daarna verwijderd. Net zoals bij de SecretKeys, kan er vanwege

een hash function die slechts 1 kant op gebruikt kan worden, niet vanuit een EphID naar een sleutel berekend worden.

Het enige moment dat de data van lokaal zich tijdelijk verplaatst, is als een persoon een (ddor de GGD verstrekte) TAN-code invoert om aan te geven dat zij positief getest zijn voor COVID-19. Zoals reeds aangegeven dienen wij de specificaties van het Tan-code systeem nog te ontvangen.

Concluderend kan er dus gezegd worden dat de data (SecretKey en EphID) lokaal (op de telefoons van gebruikers) opgeslagen wordt voor 14 dagen en ook daar verwerkt wordt.

- Is de data op enige wijze herleidbaar?

Het aanmaken van data (zowel de Secret key voor de nieuwe dag als de EphID's gebeurt dmv een 1-richting wiskundige formule/hash. Het resultaat is te berekenen aan de hand van de invoerwaarde, maar de invoerwaarde is niet te herleiden aan de hand van het resultaat. De data is dus niet herleidbaar.

- Is de data gepseudonimiseerd of geanonimiseerd?

  Data is geanonimiseerd op het moment dat de data op geen enkele manier terug te herleiden is naar een individu. Echter, als dit via een andere weg wel kan, denk aan versleuteling, ontsleuteling, andere contextuele data of welke weg dan ook, is het gepseudonimiseerd. In het geval van ons voorstel WelZijNL is op geen enkele manier terug te herleiden welke sleutels bij welk individu horen. Dit betekent dat in ons systeem de data geanonimiseerd is.

  Wat wel kan gebeuren is dat er vanuit de GGD of de overheid een verzoek komt om de backend en de GGD inzicht in elkaar te geven wat betreft data. Als dit gebeurt kan in theorie de medicus die een TAN-code geeft aan de patiënt later zien aan welke sleutel de TAN-code gelieerd is, waardoor alleen die medicus een persoon aan sleutel zou kunnen linken. Echter, de hoeveelheid moeite samen met het feit dat noch de overheid noch de GGD verzocht heeft om inzicht in de backend te krijgen, doet ons denken dat dit niet zal gebeuren.

- Met wie worden de resultaten gedeeld en onder welke voorwaarden?

  De EphID's zijn de tokens die tussen gebruikers van de applicaties worden uitgewisseld. Deze tokens zijn volledig anoniem en bevatten geen persoonlijke data.
  Op het moment dat een gebruiker positief wordt getest, dan zal hij/zij een TAN code ontvangen van een medisch specialist. Na invoering van de TAN code zal

de Secret Key van het eerste moment van besmettelijk zijn gedeeld worden met de backend. De backend stelt vervolgens deze Secret Key beschikbaar voor andere apps zodat matchmaking gedaan kan worden.
Daar de data volledig anoniem is is er geen enkele manier om te weten wie de besmette persoon is.

- Wie is de eigenaar van de data?

  De gebruiker van de applicatie is de eigenaar van de data op zijn of haar telefoon, daar hij/zij ten alle tijden er voor kan kiezen de app weer te verwijderen. Zodra de app wordt verwijderd wordt alle data gewist van het toestel. Het verwijderen is onomkeerbaar.
  De data die op de backend opgeslagen wordt is niets anders dan een set secret keys die niet aan een gebruiker gekoppeld kunnen worden.

  Indien een gebruiker zich reeds al besmet heeft aangemeld [en dus dat zijn/haar secret key is gedeeld met de backend] en vervolgens de app verwijderd, dan zal de secret key op de backend blijven bestaan. Dit is geen probleem, daar de key anoniem is.
Secret Keys ouder dan X dagen zullen worden verwijderd van de server.

- Statelijke actoren?
  - Hoe borgen jullie onbedoelde bij-effecten van de inzet van de apps?

Technologie is een middel, nooit een doel. Wij geloven erin dat de applicatie kan helpen bij de bron- en contactopsporing. Het succes van de app zal ook vallen en staan met de adoptie ervan. Wij geloven erin dat een goede user-interface hierin cruciaal zal zijn, zodat de gebruikers de app leren 'vertrouwen'. Het vertrouwen van het Nederlandse volk winnen is de grootste hindernis om te nemen.
We zullen dan ook na uitrol van de applicatie continue moeten monitoren welke feedback er komt vanuit de gebruikers en hierin op in moeten spelen door regelmatig nieuwe releases uit te brengen.

Er zijn meerdere scenario's te bedenken waarin de app beter of minder goed zal werken. Dit komt voort uit de beschikbare technologie. Het ene toestel zal een sterker Bluetooth signaal uitzenden dan een ander toestel. Dit is zeer hardware afhankelijk en derhalve niet te ondervangen. We zullen dan ook, in overleg met de GGD en het RIVM, moeten bepalen wanneer een gebruiker redelijkerwijs gewaarschuwd dient te worden dat er mogelijk contact is geweest. Dit om het gevoel van schijnveiligheid zoveel mogelijk te voorkomen.

Verder zijn er meerdere edge-cases te verzinnen die wederom in overleg met de instanties zo goed mogelijk moeten worden ingevuld.

Een ander potentieel risico wat te verzinnen is, is een Ddos aanval op de backend server. Onze aanbeveling blijft dan ook om een gedegen, reeds door de overheid gefiatteerde hosting oplossing te kiezen, waarbij er reeds oplossingen voor Ddos mitigatie zijn geïmplementeerd.

Om dit te borgen raden wij aan om code-audits en pentests te laten uitvoeren op de code.

- Pen-testen?

In de afgelopen dagen is de opgeleverde code door KPMG gepentest. Wij zijn nog in afwachting van de resultaten hiervan, maar staan volledig open voor elke test die kan bijdragen aan het veiliger maken van de app en backend code.

- 2 Factor Authentication voor gebruikers

De gebruiker hoeft niet in te loggen om de applicatie te gebruiken. Er zal dus ook geen 2-factor authenticatie zijn.

Een overweging is om de app te beveiligen met vingerafdruk [voor toestellen die dat ondersteunen]. Dit is een OS functionaliteit die verder geen invloed heeft op de werking van de app of de data in de app, maar die wel nog een extra laag beveiliging zou kunnen toevoegen. Dit zullen wij toevoegen aan de roadmap.

- Wordt alle data gedeeld, of alleen infected data?

Zie antwoorden hierboven. De applicaties zullen anonieme EphIDs uitwisselen en ontvangen. Dit wordt dus tussen apps onderling gedeeld.
Verder zal de Secret Key alleen naar een server geupload worden na invoering van de TAN code. Deze TAN codes worden alleen verstrekt door de officiële instanties.

- Wordt data centraal opgeslagen?

De Secret Keys die worden geupload naar de backend worden centraal opgeslagen. Voor de werking hiervan verwijzen we naar de eerder gegeven antwoorden.

- Wat is de definitie van een 'contactmoment'

Dit zal in consultatie met het RIVM en GGD moeten worden bepaald. Op dit moment is er sprake van een contactmoment als er een EphID is uitgewisseld tussen toestellen. Op basis van input van de medische instanties willen we deze criteria verder aanscherpen. Denk hierbij aan 'minimaal 5 minuten contact via Bluetooth' of gemeten afstand binnen 1.5 meter.

- Met hoeveel gebruikers is er al getest?

Zoals reeds aangegeven maakt DEUS gebruik van het bestaande DT3P protocol. Dit protocol [waarvan de documentatie hier te vinden is: https://github.com/DP-3T/documents] is reeds door een grote community getest [en wordt nog steeds getest].

Echter zal de definitieve oplossing van DEUS nog veel meer getest moeten worden. Dit niet alleen om eventuele bugs te fixen, maar juist ook om nog meer zichtbaarheid te ontwikkelen op de edge cases.

- Wie heeft momenteel toegang tot de data? IAM rollen
    - Wie heeft toegang tot de encryption keys?

Momenteel maken wij gebruik van Github als repository en Amazon AWS voor de hosting van de backend. Voor beide systemen staat two-factor authentication aan.
Onze CTO is admin voor Github en kan dus gebruikers toevoegen/verwijderen etc.
De CTO en COO zijn de enige met toegang tot de AWS omgeving.

- Mini-sanity check:
    - Waar en hoe wordt de app ontwikkeld en zijn de hard drives van eventuele werklaptops encrypted?

Van alle laptops waarop wordt ontwikkeld zijn de disks encrypted. De app [en backend] wordt ontwikkelt obv de open source oplossing van DP3T en is derhalve beschikbaar voor de community.

Indien er nieuwe ontwikkelingen zijn mbt het protocol, dan zullen wij deze eerst reviewen [code review] alvorens te besluiten deze wijzigingen te adopteren.

    - Wat is het wachtwoordwijzigingsprotocol voor medewerkers?

DEUS werkt niet met een active directory. Wel worden onze medewerkers verplicht om elke 75 dagen hun password van hun e-mail te wijzigen. De e-mail wordt gebruikt als single sign-on voor SAAS toepassingen, dus wijzigingen in wachtwoorden propageren direct ook voor deze tools.
Verder zijn kritische omgevingen [zoals een AWS] beschermd door de toegang te beperken tot een zeer summiere groep - zie hierboven.

    - Welke ISO certificeringen of protocollen zijn er om interne data-breaches te minimaliseren?

Daar DEUS pas recent is opgericht zijn wij nog niet in het bezit van ISO certificeringen. Wel zijn wij vanuit onze 12 jarige mobiele technologies expertise (MOBGEN & Accenture) gewend om op basis van dergelijke protocollen te werken.

Ons advies voor deze app is om de app te hosten om een reeds door de overheid goedgekeurde hosting oplossing.

- NEN normen compliance

Idem als hierboven - ons proces is compliant aan de gestelde normen, echter is er geen certificering aanwezig.

- Uberhaupt de eisen uit de lijst uit de uitvraag van VWS

  De app voldoet aan de voorwaarden zoals gesteld in de tender briefing door VWS en ook aan de criteria voorgesteld door [redacted] *van de Waag Society: tijdelijk, transparant, volledig anoniem, vrijwillig, gebruiksvriendelijk, niet commercieel en kan onder de regie van onafhankelijke deskundigen worden geïmplementeerd.*

- Op welke geëiste uitgangspunten wijken jullie af, en waarom?

  Niet van toepassing

- 2 factor authentication voor remote werk over VPN?

DEUS maakt geen gebruik van een intern netwerk en derhalve werken wij niet met een VPN. De tools die wij gebruiken zijn SAAS based, marktstandaard [denk Slack, G-Suite, Github] en maken gebruik van de security en authenticatie methodes van deze tools.

- Wanneer wordt de app code open source gemaakt?
  - Kunnen externe partijen de code auditen/reviewen

De code is reeds gedeeld en derhalve beschikbaar ter review.
Github link: http://github.com/DEUS-BV/

- Lopen er IP procedures mbt de technologieën

Voor zover wij weten lopen er geen IP procedures mbt de gebruikte technologieën.

- Hoe is GDPR met inzage tot de data en recht om vergeten te worden geïmplementeerd?

Belangrijk om hier te bespreken dat de gebruiker in controle is van zijn of haar data en dat dit ook betekent dat zij op ieder moment ervoor moeten kiezen om vergeten te kunnen worden. Als de app wordt verwijderd verdwijnt ook alle data (zie eerdere informatie over dataretentie).

Vanuit het GDPR staat centraal dat de gebruiker (in dit geval de Nederlandse burger) controle heeft over zijn of haar data. Dit betekent ook dat zij ervoor zullen moeten kunnen kiezen om 'vergeten te worden'. Wat dit inhoudt dat er geen data meer is van diegene die wenst vergeten te worden.

Doordat alle data na 14 dagen verwijderd zal worden, hoeft de gebruiker eigenlijk niks te doen behalve wachten tot de 14 dagen om zijn. Echter, de wens kan bestaan om per direct vergeten te worden. De gebruiker kan dan de app verwijderen. De SecretKey zal dan ook verwijderd worden. Het enige dat nog zal blijven bestaan zijn de (anonieme) EphID's op telefoons van andere gebruikers. Ook deze zullen automatisch na 14 dagen verwijderd worden.

Waar rekening mee gehouden moet worden is dat als gebruiker de TAN-code al ingevoerd heeft en zijn SecretKeys al naar de backend gestuurd zijn, deze op een dusdanig anonieme manier versleuteld zijn dat ook wij de SecretKeys niet kunnen herleiden naar hen, waardoor wij deze niet op verzoek kunnen verwijderen.

- Wat is het vernietigingsprotocol voor de data?

Er bestaat geen vernietigingsprotocol, daar de data anoniem is. Wel wordt de data na 14 dagen verwijderd. Ook op het moment dat de gebruiker de app verwijderd zal de data worden verwijderd. Zoals eerder aangegeven zal een reeds gerapporteerde Secret Key niet verwijderd worden van de backend bij het verwijderen van de app, daar er op dat moment geen communicatie plaatsvindt tussen app en backend.

- Wat is de team samenstelling en team grootte? (Data Privacy Officer, Information Security, testers, testers, testers)

DEUS is een Nederlandse start-up met een vast team van 25 specialisten in mobile app development en design. Daarnaast werken wij met een vaste flexibele schil van 30 specialisten waarmee wij in de afgelopen 10 jaar (met 7 jr MOBGEN en 3 jr Accenture) ruime ervaring hebben opgebouwd. Verder hebben we ervaring in het snel scalen van een organisatie. MOBGEN groeide in 7 jaar tijd van een start-up naar een organisatie van 200 mensen.

- Is de app te downloaden en testen? == zie alleen mock-ups, niet te downloaden in store

Zoals hierboven al is aangegeven is de broncode vrijgegeven. De app en backend kunnen derhalve getest worden.

- Wat is de lanceerstrategie (inclusief testplan)

Het lanceerplan zal in overleg met de overheid en de medische instanties moeten worden opgesteld. Wij bevelen een gefaseerde roll-out aan, waarbij de app eerst in een kleine, gecontroleerde groep wordt getest op de werking.

Wij geloven dat dit van enorm belang is om de werking en vooral ook de edge-cases goed in kaart te brengen. De resultaten van deze tests kunnen openbaar gemaakt worden om het vertrouwen in de app te stimuleren. Grote adoptie [kritische massa] zal namelijk essentieel zijn om de app goed te laten functioneren. Hier zal een marketingcampagne voor nodig zijn met actieve push vanuit de overheid.

DEUS wil transparant zijn mbt haar test-capaciteit. Deze is onvoldoende en hulp zal hierbij nodig zijn. Dit gaat niet alleen om de werking van de app en/of back-end, maar ook mbt het testen van de app/backend op vele verschillende toestel-modellen en verschillende versies van besturingssystemen.

- Wat is het dataverbruik van deze app?

Het dataverbruik van de app zal beperkt zijn.
- *Uitgaande van 1.000 gemelde besmettingen per dag zullen er dus ook 1.000 Secret Keys worden verstuurd naar de back-end. De Secret-Key is 32 bytes lang.*
- *Uitgaande dat de app elke 4 uur een check doet naar de backend voor nieuwe Secret Keys is dit dus 6x per dag*

Dit komt dan neer op een orde van grootte van circa 250KB aan data. Uiteraard, indien de data vaker opgehaald wordt [of er meer besmettingen zijn gerapporteerd], dan zal het data verbruik stijgen.

- Jullie werken als het goed is allemaal Agile. Wat is jullie definition of done? (Controleren op ontbrekende punten)

Definition of Done bestaat op verschillende niveaus: voor een user story, een sprint en voor een release. Hieronder staat onze definition of done voor een release omschreven.

1. *Voldoet aan alle Definition of Done requirements van de gescopete functionaliteiten in de user stories en sprints*
2. *Functionele tests geslaagd*
3. *Voldaan aan acceptatie criteria*
4. *User acceptance testing doorstaan*
5. *Integratie tests doorstaan*
6. *Alle unit tests geslaagd*
7. *CI/CD geverifieerd en werkend*
8. *PEN test geslaagd*
9. *Load test geslaagd*
10. *Performance test geslaagd*
11. *Peer code review doorstaan*
12. *Documentatie voltooid*
13. *Compliance documentatie up to date*
14. *Voldoet aan alle niet-functionele requirements*

15. Voldoet aan wettelijke / legale regelgeving
16. Betrokken stakeholders gaan akkoord met de release

- Achten de ontwikkelaars de geëiste tijdlijn realistisch om zo'n ingrijpende applicatie m.b.t. Consumer privacy in productie te brengen?

Om een app live in de appstore te hebben op 28/04 zal de app circa 1 week van te voren gesubmit moeten worden naar Apple [review tijd]. Dit zou betekenen dat de app op 21/04 gesubmit moet worden. Dit zien wij niet als haalbaar.

Daarnaast zijn er een breed scala aan afhankelijkheden [denk van het opleveren van een door de overheid gefiatteerde hosting omgeving tot de besluitvorming door de regering] die de gestelde tijdslijn onrealistisch maken.

Onze verwachting is dat de app op 28/04 klaar is voor UAT en kan worden uitgerold naar een kleine testgroep die van te voren is bepaald. De distributie van deze test app zal via een oplossing als Firebase gaan en niet via de reguliere appstores.

Na lancering van de apps zullen er ook continue verbeteringen moeten worden doorgevoerd, dus het is van belang om te realiseren dat dit geen eenmalige oplevering betreft.

- Wat is de statistische nauwkeurigheid van het huidige tracing algoritme? (Hoeveel % van gebruikers met coronainfecties wordt correct gevlagd als gevolg van het gebruik? True Positives, True Negative, False Positives, False Negatives, balans in de dataset.) Hebben jullie dit gesimuleerd?

Nee, dit is nog niet gesimuleerd

- Welke features zijn afgerond en welke niet?

Zie gedeelde code base voor afgeronde features
Features die momenteel nog onder ontwikkeling zijn zijn verbeteringen mbt gebruikersvriendelijkheid, implementatie van meertaligheid [naast Nederlands en Engels] en accessibility features voor ouderen en mensen met een beperking en verdere requirements obv feedback van de GGD en het ministerie.

Onderzocht wordt nog de toevoeging van de vingerafdruk beveiliging [zie omschrijving in een eerder antwoord].

- Welke user stories staan er op de backlog?

Zie hierboven

- Wordt in het kader van transparantie ook de backlog beschikbaar gesteld?

Zie hierboven voor huidige backlog. Zodra er akkoord is over de finale scope van het project zal de backlog wat ons betreft beschikbaar kunnen worden gesteld.

- Hoe worden mensen die niet over geschikte mobiele telefoons beschikken hierin meegenomen?

De app vereist een smartphone. Dit is niet te omzeilen. Wij zien de app dan ook als toevoeging op de bestaande activiteiten van de GGD, om de GGD bij bron- & contact opsporing te ondersteunen en informatievoorziening te verbeteren. De groep die niet over geschikte mobiele telefoons beschikken zullen moeten worden afgevangen door de bestaande dienstverlening en procedures van RIVM en GGD.