KIN+CARTA
Create

Bijlage 1 Vraag- en antwoordformulier

Gegevens Uitnodiging	
Titel	Uitnodiging slimme digitale oplossingen Corona
Opdrachtgever	De Staat der Nederlanden (ministerie van Volksgezondheid, Welzijn en Sport)

Gegevens Ondernemer	
Naam Ondernemer	Kin + Carta Create (voorheen The App Business)
Adresgegevens Ondernemer	The Spitfire Building , 1 Collier Street , London N1 9BE **Let-op:** Hoofdkantoor in London maar hub met capaciteit in Amsterdam.
Contactpersoon Ondernemer	(10)(2e)
Functie contactpersoon	(10)(2e)
E-mailadres Ondernemer	(10)(2e)@theappbusiness.com
Telefoonnummer Ondernemer	NL: (10)(2e) / UK: (10)(2e)
Website Ondernemer	https://www.kinandcarta.com/en/services/create/

Verklaring	
Ondernemer verklaart dat:	*Doorstrepen wat niet van toepassing is*
De aangeboden oplossing voldoet aan de in de uitnodiging geschetste uitgangspunten en is per 28 april 2020 productierijp	Ja / ~~Nee~~
De aangeboden oplossing is per 18 april 2020 beschikbaar voor een publieke proef.	Ja / ~~Nee~~

Omwille van een efficiënte werkwijze vragen we u om een compacte beantwoording en/of beschrijving van uw mogelijkheden ten aanzien van de beoogde oplossing. We verzoeken u dringend om informatie die niet direct de kern van de oplossing raakt, niet in het hoofddocument te verwerken maar als bijlage op te nemen.

Alle voorgestelde oplossingen voldoen aan de uitgangspunten en voorwaarden die uitgelijnd zijn in de uitnodiging maar houden ook rekening met de bezwaren van veiligtegencorona.nl.

1	
Doelstelling	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:
Wireframes: zie appendix | **Data flows**: zie appendix | **Release schedule:** zie appendix

De aanbevolen oplossing is outcome-driven en houdt rekening met de verschillende partijen en huidige ontwikkelingen in de markt:

Nederlandse overheid / GGD

- Een oplossing die snel uitgerold kan worden en die een deel van de inspanningen voor het traceren van eventueel contact automatiseert en de effectiviteit van isolatiemaatregelen vergroot.
- Om effectief te zijn, moet een aanzienlijk deel van de bevolking de app hebben gedownload. Eenvoudige onboarding en sociale functies die een snelle opname en verspreiding van het product mogelijk maken, zijn van cruciaal belang.

Eindgebruikers

- Nederlanders willen helpen bij het opsporen van contact opsporing, met behoud van hun eigen privacy en informatiebeveiliging.

Technische ontwikkelingen in de markt

- Er zijn wereldwijd meerdere open source-inspanningen die gebruikmaken van de bluetooth-technologie van smartphones om dit te bereiken. Bluetrace is momenteel de toonaangevende optie voor het handhaven van gegevensprivacy en het leveren van effectieve contactopsporing.
- Apple en Google ontwikkelen een gedeelde oplossing op OS-niveau om hetzelfde resultaat te bereiken. Zodra deze standaarden beschikbaar zijn gemaakt, adviseren wij dat dat het omschakelen van de onderliggende bluetooth-tracking technologie naar deze standaarden de datakwaliteit en inzichten zou verbeteren. We hebben onze oplossing gebouwd met deze transitie in gedachten.
- De technologie alleen is niet genoeg - intelligent product- en service ontwerp is vereist om mogelijke uitdagingen het hoofd te bieden (bijv. Frauduleus of nep gebruik, effectieve integratie met medische test inspanningen, beheer van berichten en waarschuwingen om een 'information overload' te voorkomen)

Op korte termijn maakt een succesvolle oplossing gebruik van het beste van bestaande open source-frameworks (in lijn met de voorwaarden van Veiligtegencorona.nl), op een door de Nederlandse overheid goedgekeurde manier die onze culturele en sociale normen, lokale volksgezondheid en politieke context weerspiegelt. Andere succesfactoren zijn:

- Opbouwen van vertrouwen door volledig transparant te zijn:
  - De applicatie is alleen effectief wanneer er een hoge adoptie plaatsvindt. Om vertrouwen te krijgen van de eindgebruiker is het noodzakelijk om volledige transparantie te bieden (bv. wat voor data wordt gebruikt, wanneer en waar het voor wordt gebruikt). We raden ook aan om aan te geven hoeveel mensen al gebruik maken van de app om op deze manier mond-op-mond reclame te versnellen.
- Relevantie
  - Geef eindgebruikers relevante informatie over de huidige situatie
- Gebruiksvriendelijkheid
  - Door middel van kwalitatieve en kwantitatieve onderzoeken, kunnen we de app verder ontwikkelen en verbeteringen doorvoeren om zo de adoptie van de app te maximaliseren

- Nederlandse en engelse versie beschikbaar.

Zo gaat dit in zijn werk:

Registratie

1. Installeer de applicatie op je telefoon
2. Open de applicatie
3. Accepteer de voorwaarden & geef toestemming voor push notificaties
4. Een notificatie ID is gecreëerd via de push notificatie provider SDK en opgeslagen op je telefoon.
5. De notificatie ID is verstuurd naar de push notificatie provider

Opmerking: de notificatie ID wordt de "'Gebruikers ID' en is beschreven en uitgelegd in de BlueTrace paper.

Contact

1. De gebruiker komt in de buurt van een andere gebruiker die ook de app geïnstalleerd heeft.
2. Het apparaat maakt een oproep naar de backend van de applicatie om een lijst van TempIDs te genereren met een bijbehorende timestamp en geldigheidsduur.
3. De server genereert verschillende, toekomst gedateerde, TempIDs, door de notificatie ID (gebruikers ID) te versleutelen met de begin- en einddatum en tijd. Deze data is vervolgens base64 gecodeerd en versleuteld met een private key opgeslagen in de backend.
4. De applicatie gebruikt Bluetooth Low Energy om de andere gebruiker te detecteren en de TempIDs worden uitgewisseld.
5. Beide apparaten slaan de TempIDs op met de timestamp van de uitwisseling en de afstand (tot 2 meter).

Veranderen van je status (:besmet)

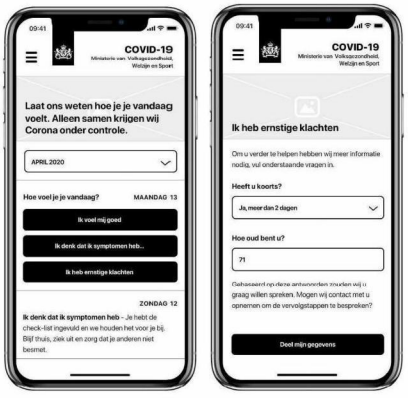
1. De gebruiker geeft via de app aan dat hij/zij denkt besmet te zijn.
2. De gebruiker wordt gevraagd om een aantal gegevens te delen zodat de juiste hulpinstantie contact kan opnemen.
3. De gebruiker krijgt een telefoontje van een GGD medewerker om dit verder te onderzoeken.
4. De GGD medewerker genereert een tijdelijke code dat niet uniek hoeft te zijn aan de gebruiker.
5. De GGD medewerker geeft de code aan de gebruiker en deze toets de code in via de applicatie
6. De gebruiker wordt ge-redirect naar de DigiD app en voert de relevante inloggegevens in.
7. De DigiD app redirect de gebruiker terug naar de applicatie
8. De applicatie zal vervolgens de recente contactinformatie uploaden (templDs + timestamp).
9. De backend valideert de authenticatie token en code.
10. De backend slaat de contactinformatie op met de gebruikers ID (vernomen via de authenticatie token) en het tijdstip van het schrijven (zodat het later nog verwijderd kan worden)
11. De back-end haalt de notificatie IDs eruit van de gebruikers die in contact zijn gekomen met de "besmette" gebruiker.
12. De applicatie filtert de TempIDs om zo ongeldige IDs te verwijderen (bijvoorbeeld van kwaadaardige gebruikers)
13. De data wordt vervolgens gegroepeerd op notificatie ID. Een berichtenstructuur (niveau) is gebaseerd op een logica van doorgebrachte tijd en afstand. Deze structuur bepaald vervolgens de waarschijnlijkheid dat the infectie is overgedragen.
14. Indien gewenst, kunnen wij een handmatige validatie stap toevoegen, dit is echter niet vereist.
15. Via de notificatie provider, verstuurd de back-end van de applicatie verstuurd een push notificatie bericht naar de notificatie ID. Het push bericht is aangepast afhankelijk van het "niveau" van het bericht.

Let:op: De gegevens die worden verwerkt zijn en blijven niet tot individuen herleidbaar tenzij a) de gebruiker hier toestemming voor geeft b) er sprake is van contact- of bron onderzoek als bedoeld in art.6

Data verwijderen

1. Het verwijderen van data gebeurd periodiek. De applicatie kan met toestemming van de gebruiker zelf worden geïnstalleerd en verwijderd.
2. Data ouder dan een specifieke dag wordt automatisch verwijderd

2	
Doelstelling	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	**Release schedule:** zie appendix De aanbevolen oplossing is outcome-driven en houdt rekening met de verschillende partijen en huidige ontwikkelingen in de markt: **Nederlandse overheid / GGD** Door burgers betere begeleiding op afstand te bieden (bijvoorbeeld bij besmetting, vermoeden van besmetting, of voortdurende zorgbehoeften) wordt verwacht dat er efficiënter en effectiever kan worden omgegaan met de beschikbare capaciteit in de huidige gezondheidszorg. **Eindgebruikers** ● Burgers willen 1) hun toestand volgen en begrijpen en 2) toegang hebben tot hulp als ze die nodig hebben **Technische ontwikkelingen in de markt** ● Zowel iOS als Android hebben bestaande 'monitoring-frameworks'. Deze kunnen snel benut worden voor het effectief volgen en monitoren van symptomen of aanbevolen zeitzorg. We hebben ook een artikel geschreven waarin we uitleggen hoe je deze APIs het beste kan toepassen (iOS Healthkit, Carekit en ResearchKit). Hulp op afstand kan snel worden aangeboden met eenvoudige beslisbomen en veelgestelde vragen. ● Op middellange termijn voorzien we de mogelijkheid om een chat-interface consultatiefunctie te bieden, of om te integreren met een derde partij om Nederlanders medisch consult op afstand aan te bieden. **Dit ziet er vervolgens zo uit: (zie onderstaande wireframes)** 1. Digitale zelfmonitoring stelt de gebruiker in staat om snel en gemakkelijk te identificeren of ze symptomen van het virus hebben en zo toegang te krijgen tot relevante overheids advies over vervolgstappen. 2. Zelfmonitoring op afstand maakt gericht advies en eventuele escalatie naar deskundigen in de gezondheidszorg mogelijk. 3. Het geeft de gebruiker / de Nederlandse burger het gevoel dat er voor hen 'gezorgd' wordt en dat als je medische hulp nodig hebt, dit snel geconstateerd zal worden en geëscaleerd waar nodig.. 4. Met toestemming van de gebruiker kunnen deze gegevens gedeeld worden met de daartoe bevoegde instanties om verder onderzoek naar het virus mogelijk te maken.



Zo gaat dit in zijn werk:

1. Met behulp van 'built in frameworks', kunnen gebruikers verschillende symptomen (dagelijks) bijhouden via de applicatie.
2. Informatie kan veilig op het toestel worden opgeslagen met protocollen die zijn ontwikkeld door Apple en Google.
3. Alle gegevens over eventuele symptomen worden op het apparaat bewaard terwijl een gebruiker zijn gezondheid blijft monitoren.
4. Op basis van door de door de gebruiker ingevoerde symptomen, biedt het systeem advies aan over (eventuele) escalatie.
5. Op basis van het advies in de app, kan de gebruiker een formulier invullen om contact op te nemen. Dit kan door middel van het weergeven van een telefoonnummer, het verzenden van een e-mail of het integreren met bestaande API's. (zoals callcenter-wachtrijen).

3	
Doelstelling	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 afschalingsstrategie en begeleiding op afstand?

Antwoord:

Wireframes: zie appendix | **Data flows**: zie appendix | **Release schedule:** zie appendix

De aanbevolen oplossing is outcome-driven en houdt rekening met de verschillende partijen en huidige ontwikkelingen in de markt:

Nederlandse overheid / GGD

- Er zijn een aantal voorgestelde beleidsveranderingen om van de huidige Intelligente Lock-down terug naar een 'normale samenleving' te gaan - op een manier die de openbare veiligheid handhaaft, maar de economie weer laat functioneren. Het is daarom noodzakelijk dat deze digitale oplossing toestaat snel te reageren op de laatste beleidsvoering m.b.t. de transitiestrategie.
- Door onze uitgebreide ervaring in het bouwen van software, zijn we in staat snel te reageren op opkomende beleids- of volksgezondheids veranderingen. We zullen samenwerken met het Outbreak Management team (OMT) om prioriteiten te stellen en snel de vereiste functies te leveren om de gewenste beleidsresultaten mogelijk te maken.
- We hebben een 'immuniteit paspoort' en een 'gelokaliseerde lock-down' onderzocht als twee belangrijke nieuwe functies van een mobiel product die de overgang zal helpen.
- Een 'Immuniteit Paspoort' biedt de mogelijkheid voor Nederlanders om hun eerdere testresultaten veilig en anoniem aan hun DigID te koppelen en deze te tonen of te laten gelden bij een controlerende autoriteit. Dit kan in een aantal situaties worden gebruikt, bijvoorbeeld bij personen die positief zijn getest op het virus (of virus antilichamen) die willen solliciteren voor een functie waarvoor het noodzakelijk is dat een persoon volledig hersteld is.
- Een 'gelokaliseerde lockdown' kan worden ingezet om lokale uitbraken te monitoren. Een mobiele app kan gebruikers een manier bieden om te controleren welke gebieden vergrendeld zijn en te waarschuwen als er ergens in de buurt quarantaine controles plaatsvinden.
- Daarnaast is er een mogelijkheid voor Nederlandse autoriteiten (centrale overheid, gemeente en politie) om geaggregeerde en anonieme data in real-time te verwerken. Bijvoorbeeld om aan te geven waar nieuw gerapporteerde infecties ontstaan.
- Deze informatie kan gebruikt worden om verdere beslissingen te maken met bijpassende beperkingen, om zo een volledige lock-down voorkomen.

Hoe ziet dit er dan uit?

1. Als de overheid een individu getest heeft, kan een QR-code of uniek ID gecombineerd worden met andere authenticatie factoren, om een 'immuniteit paspoort' weer te geven.Gebruikers met virus immuniteit kunnen zich vervolgens met minder beperkingen kunnen verplaatsen.
2. Door slim gebruik te maken van animatie, de smartphone accelerometer en gyroscoop, kunnen we een 'digitaal hologram' maken.Dit biedt een hoger beveiligingsniveau dan eenvoudig en statisch scherm, waardoor er meer vertrouwen in de applicatie ontstaat.
3. De app kan de gebruiker relevante informatie blijven geven over welke beperkingen er momenteel gelden, afhankelijk van hun status en het huidige overheidsadvies. Dit zal bijdragen tot de transitiestrategie.

Hoe gaat dit in zijn werk?
We leggen de bovengenoemde concepten in meer detail uit.
Het immuniteit paspoort

We raden een eenvoudig systeem aan dat een burger kan laten zien om te bewijzen dat hij van het virus is hersteld, beveiligd door een moeilijk te vervalsen 'digitaal hologram'. Om het immuniteits paspoort te verkrijgen, doorloopt de gebruiker de volgende stappen:

1. Wanneer een gebruiker een positief antilichaamtest resultaat van de GGD ontvangt, genereert een GGD-moderator een hash-code van een individu's unique overheids-ID in combinatie met de status van de gebruiker met behulp van het back-end systeem
2. De gebruiker logt in op de app en voert de hash-code in
3. Het backend systeem ontvangt de hash van de gebruiker en hun authenticatietoken
4. De back-end haalt het gebruikers-ID uit het verificatie token en hasht dit met de immuniteitsstatus
5. Als deze overeenkomen, bevestigd de app dit door middel van een een bevestigde status aan de gebruiker.
6. De app kan vervolgens de bevestigde status weergeven, samen met een 'digitaal hologram' en de huidige "datetime".

Een digitale hologram
We zouden gebruik maken van een bestaande aanpak die wij eerder hebben geïmplementeerd voor de Rail Delivery Group in het Verenigd Koninkrijk - door een beveiligd scherm te creëren dat een gebruiker kan laten zien aan een controlerende partij.

Om te bewijzen dat dit afkomstig is van een gezaghebbende bron (en geen zelf-gegenereerde afbeelding, video of nep-app is,) wordt een digitaal hologram gegenereerd met een animatie als reactie op beweging van het toestel (gedetecteerd met de accelerometers en gyroscopen in het toestel).

Door de app te kantelen, kan de gebruiker aan de controlerende partij laten zien dat het de officiële immuniteit paspoort-app is, en zo dat de controlerende partij zien dat de digitale hologram reageert op beweging van het toestel om te verifiëren dat het echt is.

De hologram vervangen door validatie met een unieke QR-code
Als er meer robuuste beveiliging nodig is, kunnen we in de loop van de tijd het digitale hologram uitbreiden met een systeem dat voor elke gebruiker unieke, tijdgevoelige QR-codes genereert. Deze kunnen door de autoriteiten worden gescand als bewijs van immuniteit.

Om dit mogelijk te maken, zou de back-end-server een reeks voortdurend tijdgevoelige codes updaten voor de app. De app is dan in staat om codes van een halve dag downloaden voor toekomstig offline gebruik. Deze codes zijn de ID, de status van de gebruiker en een tijdstempel gecodeerd met een sleutel.

Met dezelfde applicatie (of een aanvullende applicatie voor autoriteiten die immuniteit paspoorten moeten verifiëren) zou een functie kunnen hebben waarmee gebruikers de QR-codes kunnen scannen en deze ter verificatie naar de server kunnen sturen. Hiervoor zou de app online moeten zijn.

Eenmaal ingediend, kan de server vervolgens de QR-code decoderen en de gebruikers-ID, status en tijdstempel identificeren, waardoor de code wordt gevalideerd en de geldige status werd teruggestuurd naar de app van de controlerende partij. Op deze manier heeft de controlerende partij geen identificerende informatie van de gebruiker, maar kan hij zeker zijn van de status, omdat deze wordt gevalideerd door een centrale autoriteit.

Deze oplossing heeft als bijkomend voordeel dat de centrale server geen database met gebruikersidentificatie gegevens zal bevatten, aangezien de codes direct met sleutels kunnen worden gegenereerd en gevalideerd.

Hoe een regio gerichte lock-down technisch te werk gaat:
Een regionale lock-down zou een eenvoudige content en mapping gebaseerde oplossing zijn, waarbij een gebruiker op een kaart zou kunnen kijken, of door een regio selecteren om de regels of richtlijnen voor zijn gebied te kiezen.

Content kan regelmatig worden bijgewerkt vanuit een openbare of unauthenticated API, waarbij de gegevens worden gelezen uit een database die regelmatig kan worden bijgewerkt met een content management system. Als de gebruiker hiermee instemt, kan de app proactieve mobiele notificaties sturen.

4	
Doelstelling	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?

Wireframes: zie appendix
Release schedule: zie appendix

- Om de applicatie effectief te laten zijn, moeten gebruikers gegevens veilig worden opgeslagen, verwerkt en verzonden worden om gehoor te geven aan de bezorgdheid over Privacy en het gebruik van data.
- Deze benadering van beveiliging en privacy moet effectief worden gecommuniceerd via de gebruikerservaring in de app. Dit moet transparant en duidelijk zijn over privacy en in elke fase, om bezorgde burger ervan te verzekeren dat de applicatie kan helpen met de verspreiding het virus, maar zeker niet ten koste van de privacy. Dit zal ook bijdragen tot een brede acceptatie bij het publiek.

Technologie en implementatie
We raden aan om native applicaties te bouwen met Kotlin (Android) en Swift (iOS) om ervoor te zorgen dat de applicatie-ontwikkeling veilig, flexibel en snel is. Door een native applicatie te bouwen, kunnen we snel reageren op veranderingen in de technologie en de gezondheidszorg, terwijl we gebruik maken van de nieuwste native frameworks, features en standaarden. We bouwen en testen met behulp van DevOps-principes, waarbij we continue integratie- en leveringssystemen implementeren om de kwaliteit, productiviteit en doorlooptijden van het product te ondersteunen.

Hosting
De beveiliging wordt ook gehandhaafd en verbeterd door effectief gebruik van één van de grootste cloud providers. We zijn zeer ervaren in het ontwerpen en ontwikkelen van back-end systemen op AWS, Google Cloud Platform en Microsoft Azure, en met behulp van toonaangevende cloud-native technologieën.
Via overleg met jullie technische teams, zullen wij een light-touch verkenning doen van de providers van jullie voorkeur - met bijzondere aandacht voor beveiliging en privacy vereisten. We kunnen de applicatie opzetten en hosten binnen onze eigen accounts, maar we kunnen ook binnen bestaande accounts hosten of de accounts na verloop van tijd naar jullie te migreren met het oog op duidelijk eigendom en controle.

Operational Support
We kunnen technische helpdesk ondersteuning bieden (ook buiten kantoortijden) via een toegewijd team. Zowel infrastructuur- als applicatie ondersteuning en onderhoud gedurende de gehele levensduur van de applicatie.

Privacy en gegevensbeveiliging
We hebben deze vraag als een privacy-FAQ gestructureerd voor bezorgde burgers. Daarnaast hebben wij een data flow diagram opgenomen in de bijlage voor oplossing 1 en 3.

Hoe wij eventuele vragen van bezorgde burgers zouden beantwoorden:

1- Hoe zorgt u voor beveiliging tegen kwaadaardige aanvallen?
De applicatie wordt vóór penetratie getest op penetratie door een externe leverancier. Bovendien zal alle broncode van de app, met uitzondering van het digitale paspoort 'digitaal hologram' en alle cryptografische

geheimen, open source zijn, zodat het kan worden gecontroleerd door betrokken personen, zonder dat dit ten koste gaat van privégegevens.

2 - Lijkt dit op de andere methoden waarover ik in het buitenland heb gehoord - b.v. BlueTrace?

Dit zal in eerste instantie gebaseerd zijn op de BlueTrace-methodologie, maar zal vervolgens worden aangepast om gebruik te maken van de aanstaande API's op besturingssysteem niveau die door Apple en Google zijn gemaakt. Een onmiddellijke wijziging van de methode die in het BlueTrace-document wordt gebruikt, is om een gegenereerde push-notificatie-ID te gebruiken in plaats van een telefoonnummer voor tracering. Dit heeft het voordeel dat het minder persoonlijk identificeerbare informatie vereist (met name geen telefoonnummer van een gebruiker vereist) om een gebruiker te informeren over mogelijk contact met geïnfecteerde personen.

3- Heeft de overheid of andere gebruikers toegang tot mijn privégegevens om te horen dat ik mogelijk in contact ben gekomen met geïnfecteerde personen?

Nee. Voor de applicatie zijn uw privégegevens niet nodig. Het verzendt geen privégegevens naar andere gebruikers of naar de overheid voor het traceren van contacten.

Andere gebruikers waarmee u in contact bent gekomen, worden op de hoogte gebracht dat ze in contact zijn gekomen met een persoon die positief heeft getest, maar ze zullen geen details over uw identiteit of andere informatie ontvangen.

Uw contactgegevens worden alleen gedeeld met de GGD en gebruikt om de verspreiding van het virus op geaggregeerd niveau te volgen. Dit betekent dat de autoriteiten beslissingen kunnen nemen over de beste manier om de bevolking als geheel te beschermen, maar geen toegang hebben tot de gegevens of gegevens van een specifieke persoon.

Als u de immuniteit paspoort functionaliteit wilt gebruiken, moet u zich ook aanmelden met de DigiD-app. Uw ID wordt niet gedeeld met andere gebruikers ten behoeve van deze paspoort functionaliteit, het wordt alleen gebruikt om te verifiëren dat u het virus heeft gehad en nu is getest als hersteld of immuun.

4 -De app maakt gebruik van Bluetooth, kan iemand dan niet nagaan waar ik heen ga?

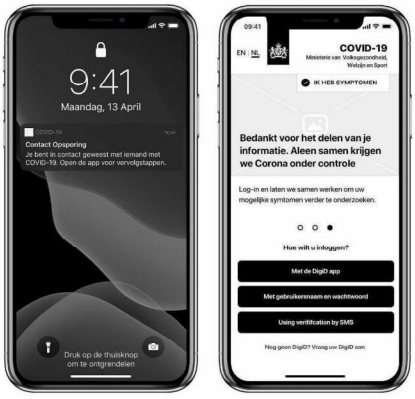
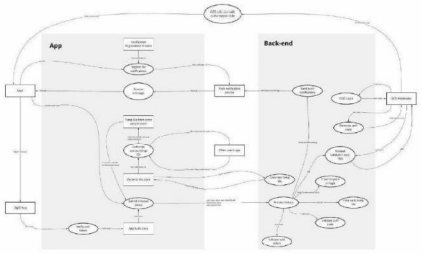
De applicatie is bovenop BlueTooth gebouwd, maar zendt zijn eigen tijdelijke ID's uit die voortdurend worden gewijzigd. Deze constante verandering maakt het onmogelijk om een specifieke ID in de tijd te traceren. Het is voor andere gebruikers of waarnemers niet mogelijk om tijdelijke ID's aan elkaar te koppelen om na verloop van tijd een enkele persoon of apparaat te identificeren..

De onderliggende BlueTooth-technologie van uw apparaat maakt ook zeer waarschijnlijk gebruik van adres randomisatie om te voorkomen dat uw apparaat wordt gevolgd.

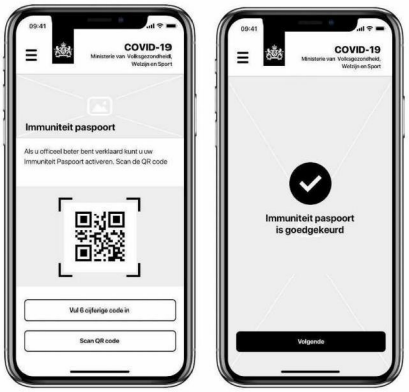
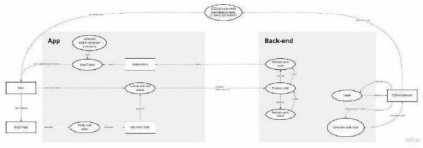
5 - Voldoet deze AVG?

Ja. Dit systeem voldoet aan alle AVG-vereisten om wettig, eerlijk en transparant te zijn, inclusief maar niet beperkt tot:

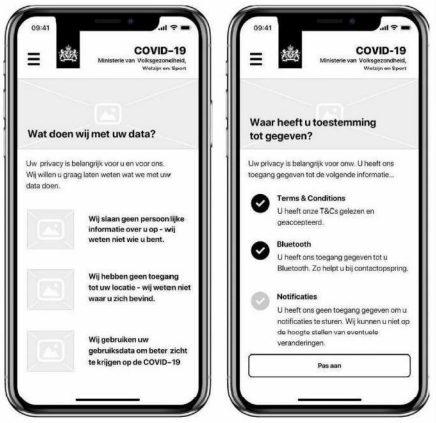
- Minimalisatie - we verzamelen alleen de minimale gegevens om de verspreiding van het virus te voorkomen. Als u bijvoorbeeld positief heeft getest, vragen we optioneel naar uw locatiegegevens op het algemene postcode niveau - we vragen GEEN specifieke, doorlopende GPS
- Nauwkeurigheid en rectificatie - we kunnen uw gegevens op verzoek bijwerken om ervoor te zorgen dat ze correct zijn
- Opslag - alle gegevens worden alleen opgeslagen voor de tijd dat ze nodig zijn, gegevens worden regelmatig opgeschoond
- Transparantie en toestemming - de algemene voorwaarden en het privacybeleid beschrijven duidelijk het gebruik van gegevens en vereisen uitdrukkelijke toestemming
- Wissen - als u contact met ons opneemt, zullen we uw gegevens binnen 28 dagen wissen
- Draagbaarheid - uw gegevens kunnen op verzoek naar u worden verzonden als u voldoende bent geïdentificeerd

Appendix oplossing 1	
Wireframes	
Data flow diagram	 The following data flow diagram shows the data flow for contact tracing.

	Note: There is no start and end point for data flow diagrams, nor segregation of use cases, therefore the following notes may be useful in interpreting the diagram: • View the Appendix 2 flow for step-by-step flows for each use case • Login is only required to report infected status • Notification IDs/tokens are used in place of phone numbers as unique identifiers in the BlueTrace reference implementation

Appendix oplossing 3	
Wireframes	
Data flow diagram	 The following data flow diagram shows the data flow for the immunity passport.

	Note: There is no start and end point for data flow diagrams, nor segregation of use cases, therefore the following notes may be useful in interpreting the diagram: • The flows start with the moderator on the right, then the user logs in, enters the code, submits status to the back-end before eventually viewing the status **Moderator code generation flow** 1. The GGD moderator enters the user's government user id/number into the back-end, with their status (e.g, immune) 2. The back-end hashes the user id and status with a key and returns the hash - a unique number 3. The GGD moderator calls the user or emails them the hash **Registration flow** 1. The user obtains the hash from the GGD moderator 2. The user installs the app 3. The user logs in with DigiD to obtain an auth token that contains their user id 4. The user inputs the hash into the app 5. The app submits the hash and auth token to the server 6. The back-end receives user id in the auth token and hashes this with the status to generate a new hash 7. The back-end compares the new hash with the received hash to check they match 8. If they match, the confirmed status is returned to the app 9. The app stores the status **View status flow** 1. The user opens the app 2. The app reads the status and shows it alongside the timestamp and a 'digital hologram' 3. The user shows this screen to the person requiring their status. This user can see that the status is authentic, as its 'digital hologram' shows it is not an image or a video

Appendix oplossing 4	
Wireframes	

Appendix overig	
Vraag:	**Wie zijn wij?**
Antwoord:	- Wij zijn Kin+Carta Create - Wij bouwen digitale producten voor bedrijven zoals Unilever, Shell en ING maar ook Tesco, M&S en Kingfisher. - Wij leveren een complete end-to-end service - vanaf een digitale innovatie strategie, het lanceren van nieuwe proposities tot aan het versnellen van product delivery. - Het oplossen van problemen door middel van software, is wat wij al meer dan 10 jaar heel succesvol doen. - Wij zijn een team van 200+ mensen met hubs in London, Edinburgh en Amsterdam en 2000+ mensen wereldwijd. - Ons doel is om producten en services te ontwikkelen die de wereld beter doen werken (We exist to make world work better).
Vraag:	**Waarom zijn wij de juiste partner voor het (verder) ontwikkelen van slimme digitale oplossingen voor** 1) bron- en contactopsporing 2) zelfmonitoring en 3) begeleiding op afstand?
Antwoord:	1 - Experts in digitale platforms & aanbevolen software partners (e.g Microsoft, Google en Apple) - We hebben een lange relatie met Microsoft Google en Apple - We zijn een van Apple's 1 op 7 wereldwijde mobiliteitspartners 2 - Vertrouwd met het bouwen van kritische applicaties voor de gezondheidszorg & die werken op schaal - We hebben op grote schaal zorg op afstand geleverd voor Xenzone (meer dan 4 miljoen gebruikers, zeer vertrouwelijke gegevens over geestelijke gezondheid en peer-to-peer-interactie), - Remote monitoring en hulp propositie voor CareUK met Apple Watch, HealthKit en CareKit - We hebben geholpen met de symptomen volger-app van Zoe Coronavirus te schalen naar de lancering in de UK en nu meer dan 2 miljoen gebruikers - waar wij de beveiliging en robuustheid hebben verbeterd. 3 - We bouwen software die het Outbreak Management Team (OMT) volledige controle geeft - We bouwen software op maat voor 's werelds grootste organisaties en bedrijven - In tegenstelling tot een start-up of grote tech-bedrijven, betekent samenwerking met K + C dat de Nederlandse overheid alle intellectuele eigendom en volledige controle behoudt over wat we creëren. We zullen met u samenwerken om ervoor te zorgen dat de prioriteiten van ons team precies leveren wat er nu en in de komende maanden in Nederland nodig is - niet wat een start-up of een groot internationaal technologiebedrijf prioriteit heeft gegeven.
Vraag:	**Wat zijn drie relevante case-studies?**
Case studies:	**Case study 1**: Peer to Peer (P2P) in de digitale geestelijke gezondheidszorg (Meer hier) Achtergrond: Xenzone biedt online veilig, toegankelijk en betaalbare begeleiding voor de geestelijke gezondheid. Zowel volwassenen (18+) als kinderen (11-18) kunnen via het

	digitale platform direct toegang krijgen tot professionals voor één-op-één gesprekken of participeren in een online forum. Project: Middels een P2P model, wil Xenzone kinderen (11-18) die geen bestaande gebruiker zijn, ook toegang geven tot deze community. Om jonge mensen in staat te stellen en aan te moedigen om hier online gebruik van te maken, zijn verschillende proposities ontwikkeld. Een aantal van deze proposities zijn vertaald naar digitale concepten en vervolgens getest via een uitgebreid kwantitatief onderzoek. Resultaat: Een eerste versie van het P2P platform is gebouwd en is inmiddels live. De data wordt gebruikt door een lokale universiteit voor verder wetenschappelijk onderzoek. Afhankelijk van de onderzoeksresultaten wordt de applicatie verder ontwikkeld en landelijk gepromoot. **Case study 2:** Snellere, betere real-time besluitvorming wereldwijd voor Unilever (Meer hier) Achtergrond:OneView maakt snellere, betere besluitvorming mogelijk binnen Unilever wereldwijd, door real-time, zeer gevoelige informatie in handen te geven van besluitvormers op elk niveau van de organisatie. Project: Unilever OneView is de slimste en veiligste business intelligence-tool in de boardroom. OneView, een platformonafhankelijk, end-to-end Executive Information System (EIS), gebruikt mobiel om business intelligence krachtig contextueel te maken. OneView haalt informatie uit heel Unilever en biedt precies de juiste gegevens op het juiste moment. Unilever heeft TAB consequent vertrouwd om zijn koersgevoelige gegevens te beheren in OneView, het hoogste niveau van gegevensclassificatie voor het bedrijf. OneView maakt onder andere gebruik van federatieve authenticatie, MFA, aangepaste toegangscontrole, TLS / SSL-pinning, beheer van digitale rechten en andere vormen van codering om ervoor te zorgen dat gegevens in rust en onderweg veilig zijn en alleen toegankelijk voor geautoriseerde gebruikers. Het beveiligingsteam van Unilever erkent dat de technici van TAB veel barrières voor Unilever hebben doorbroken, aangezien OneView het eerste project was dat aan al hun nieuwe beveiligingscontroles voldeed, en het eerste dat hun hoogste gegevensclassificatie in de cloud haalde. We hebben vroeg en samengewerkt met het beveiligingsteam van Unilever. Resultaat:De eerste OneView-pilot werd in slechts 12 weken in heel Europa gelanceerd en wereldwijd uitgerold. De huidige generatie van dit product wordt gebruikt in 111 landen en onze samenwerking met Unilever heeft 7 jaar geduurd. Met een 100% acceptatie van de CEO naar beneden, verlopen alle Unilever-vergaderingen nu met OneView. **Case study 3:** Covid Symptom tracker for King's College London (Meer hier) Achtergrond: Help de COVID-19-uitbraak te vertragen door gebruikers 1 minuut de tijd te laten nemen om uw gezondheid dagelijks te melden, zelfs als het goed met u gaat. Project: We hebben samen met Zoe gewerkt aan de ontwikkeling van een coronavirus-app voor het volgen van symptomen, in samenwerking met King's College London. We hebben hen ondersteund bij het ontwikkelen en implementeren van een CI / CD-pijplijn die een snelle implementatie van nieuwe iteraties van de app mogelijk maakt. Dit maakt snelle prestatie-

	en functionaliteit upgrades mogelijk, ondersteunt het opschalen van het product naar miljoenen gebruikers en het uitbreiden van de bijgehouden symptomen. We hebben Zoe ook ondersteund met overleg over Open Sourcing van de app, waardoor een breder team van vrijwillige software developers kunnen bijdragen aan het ontwikkelen van de app als onderdeel van wereldwijde vrijwilligers inspanningen. <u>Resultaat</u> De Covid Symptom Tracker heeft momenteel 4,8 sterren op Android en 4,7 sterren op iOS en staat momenteel # 12 in de app store in de categorie Medical.
Vraag	**Wat zijn onze plannen om de applicatie verder te ontwikkelen?**
Antwoord	- De iOS & Android applicatie kan getest worden door een gesloten groep voor 18 April 2020. De privacy altijd gewaarborgd zal blijven. - Het onderstaand overzicht geeft een korte weergave van de geplande werkzaamheden om de applicatie verder door te ontwikkelen (afhankelijk hoe de situatie zich ontwikkeld). - Fases aangegeven met een (*) zijn gebaseerd op informatie waarover wij nu beschikken. Wij werken graag met jullie samen om deze goed in te vullen.

Potentieel release plan						
	Product vereisten	Gewenst resultaat van gebruiker	Gewenst resultaat van de overheid	**App te downloaden in de store:** 28 April	**Volgende release***	**Volgende release***
1	Niet herleidbare Bron- en contactopsporing	Ik wil weten of ik in contact ben geweest en of ik maatregelen moet nemen	Wij willen geïnformeerd worden over potentiële nieuwe gevallen en verdere verspreiding voorkomen	Bluetooth tracking	Google + Apple open source APIs	Google + Apple platform software integratie
2	Mogelijkheid van het delen van I persoonlijke gegevens	Ik wil het gevoel hebben dat ik meehelp in de strijd tegen corona	Wij willen de gemelde gevallen beter begrijpen en beslissingen maken gebaseerd op data.	Contact formulier	DigiD integratie	
3	Zelfmonitoring	Ik neem de verantwoordelijkheid en controle over de situatie	Wij willen de meldingen beter filteren om de belasting op de zorg te verkleinen	Dagelijks bijhouden hoe gebruikers zich voelen	Slimme inzichten die bijdragen aan het maximaal controleren van het virus	
4	Begeleiding op afstand	Ik wil hulp zonder dat ik mijn huis hoef te verlaten	Wij willen de belasting op de zorg verkleinen	Vraag en antwoord op basis van een beslisboom	Chat bot	Slimme chat bot
5	Transitie strategie	Ik wil op een verantwoordelijke manier terug naar 'normaal'.	Wij willen de kans op verspreiding verkleinen zodat ons land en de economie weer op gang	Basisversie van Immuniteit Paspoort + Push notificaties	QR code generatie + regionaal advies.	

Vraag	**Specifiek ten aanzien van oplossingen voor Bron en contactopsporing**
Antwoord	1 - Het huidige proces van bron- en contactopsporing is uitgangspunt ter ondersteuning (REFF) Klopt. 2 - De gegevens die worden verwerkt zijn en blijven niet tot individuen herleidbaar Zelfs met het inloggen met DigiD, zullen we alleen de auth-token transactie gebruiken en geen data opslaan 3 - Daarbij moet het onmogelijk zijn, om met de gegevens, die door de oplossing worden verzameld, gebruikers te deanonimiseren Klopt 4 -De oplossing slaat zo min en zo kort mogelijk gegevens op Klopt 5 - Oplossingen kunnen met toestemming van de gebruiker zelf worden geïnstalleerd en verwijderd Klopt 6 - Gegevens mogen uitsluitend uitgelezen of gedeeld worden als er sprake is van a) contact- of brononderzoek als bedoeld in art. 6 Wpg of b) toestemming van de gebruiker Klopt 7 - Gegevens die het apparaat verlaten mogen op geen enkele wijze iets zeggen over verplaatsingsgedrag, tijdstip, locatie of sociale netwerk van die persoon Klopt 8 - Valse positieven moeten zoveel mogelijk beperkt worden door de oplossing Klopt - we hebben een DigiD check toegevoegd om dit te bewijzen 9 - De inzet van de applicatie is per definitie tijdelijk. Klopt 10 - De oplossing moet zoveel mogelijk rekening houden met de ontwikkelingen van slimme digitale oplossingen uit andere EU-lidstaten (met name in de grensregio's), zodat mogelijk op termijn grensoverschrijdende interoperabiliteit kan worden bewerkstelligd Klopt 11 - De oplossing voorziet in een informatieportal voor de gebruikers waarin fouten en kwetsbaarheden kunnen worden gemeld Ja, via de app store. We hebben ook crashrapporten geïmplementeerd. Ook zullen de fouten en kwetsbaarheden via de open-source issue tracker. (zoals Github issue tracker)
Vraag	**Uitgangspunten en voorwaarden alle voorstellen**
	1 - Oplossingen voldoen aan gangbare beveiligingsstandaarden voor: - Gebruik een veilige verbinding en sla gegevens veilig op - Volg hierbij NCSC TLS-richtlijnen

	- Volg hierbij de NCSC-richtlijnen voor mobiele app - Code review, gebruikerstest en pen-test (de app mag het aanvalsprofiel van de smartphone niet vergroten) - Geen datalek bij verlies/diefstal van de smartphone - Voldoet aan standaarden Informatiebeveiliging in de zorg NEN 7510, NEN 7512 en NEN 7513 Klopt, we zullen de standaarden volgen en samen werken met jullie team om er voor te zorgen dat wij hier aan voldoen. 2 - Oplossingen voldoen aan ISO/IEC 25010 Kwaliteit van Software: proceskwaliteit, systeemkwaliteit, gegevenskwaliteit Klopt 3- Als er oplossingen worden aangeboden moeten deze reeds bestaan, uitontwikkeld zijn en werken in een productie omgeving Klopt. Wij stellen voor om deze per datum te bespreken. 4- De oplossing moet binnen enkele dagen breed uitgerold kunnen worden naar burgers in Nederland Klopt 5 -De opzet, bestaan en werking van de beveiliging van de oplossing wordt gecontroleerd op basis van onafhankelijke audits Klopt 6 -In de oplossing wordt gebruik gemaakt van begrijpelijke taal voor alle niveaus in zowel het Nederlands en Engels Klopt 7- De oplossing adresseert een helder omschreven probleem en helder omschreven doelgroep en richt zich op slechts één doel (doelbinding) 8 - Het gebruik moet gericht zijn op het vereenvoudigen van contactonderzoek en/of zelfmonitoring en daarmee het informeren en beschermen van individuen Klopt 9 -De inzet van de oplossing en de daarmee verzamelde gegevens moet gebaseerd zijn op wetenschappelijke kennis en zo mogelijk al aantoonbaar bijdragen aan het maximaal controleren van het virus Klopt 10 - De oplossing moet het mogelijk maken om vooraf te testen op een beperkte groep gebruikers, zodat op basis hiervan beoordeeld kan worden dat deze noodzakelijk, effectief en proportioneel is Klopt 11 - De oplossing is interoperabel op basis van gangbare en open standaarden Klopt 12 - Beschrijving van controleerbaarheid van de daadwerkelijk gebruikte oplossing Klopt

	13 - Als de oplossing niet meer effectief of noodzakelijk is, moet de uitrol kunnen worden teruggedraaid en data kunnen worden verwijderd Klopt 14 - Dataminimalisatie is uitgangspunt Klopt 15 - Beschreven aantoonbare aandacht voor vertrouwelijkheid en integriteit Klopt 16 - Gebruiksvriendelijk met duidelijke handleiding en instructie Klopt 17 - De oplossing is breed toegankelijk en ondersteunt meertaligheid (conform de WCAG 2.0) Klopt 18 - De oplossing is efficiënt, waaronder zo min mogelijk beslag op batterij- en opslagcapaciteit Klopt 19 - De oplossing dient eenvoudig te kunnen worden geüpdatet om bijvoorbeeld crashes te verhelpen Klopt 20 - De oplossing voldoet aan alle geldende wet en regelgeving, waaronder de AVG Klopt 21- De oplossing is voorzien van een verwerkingsregister en een DPIA (Privacy Impact Assessment) van de voorgenomen verwerking Klopt