

TNO PUBLIEK

TNO-rapport

TNO 2021 R10134 | 0.1

**uNLock voor coronaveilige toegang - eisen en
vergelijking met alternatieven**

Anna van Buerenplein 1
2595 DA Den Haag
Postbus 96800
2509 JE Den Haag

www.tno.nl

T +31 88 866 00 00

Datum	5 februari 2021
Auteur(s)	Sterre den Breeijen Dr. Oskar van Deventer Hidde-Jan Jongsma Victor Li Pieter Verhagen

Exemplaarnummer	
Oplage	
Aantal pagina's	16 (incl. bijlagen)
Aantal bijlagen	
Opdrachtgever	Stichting uNLock
Projectnaam	uNLock toegangstesten
Projectnummer	060.48109

Alle rechten voorbehouden.

Niets uit deze uitgave mag worden vermenigvuldigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm of op welke andere wijze dan ook, zonder voorafgaande toestemming van TNO.

Indien dit rapport in opdracht werd uitgebracht, wordt voor de rechten en verplichtingen van opdrachtgever en opdrachtnemer verwezen naar de Algemene Voorwaarden voor opdrachten aan TNO, dan wel de betreffende terzake tussen de partijen gesloten overeenkomst.

Het ter inzage geven van het TNO-rapport aan direct belanghebbenden is toegestaan.

© 2021 TNO

TNO PUBLIEK

Samenvatting

concept

Dit document is een *living document*. Dit is de versie van 5 februari 2021.

TNO is een van de medeontwerpers van het uNLock systeem voor coronaveilige toegangsverlening. Dit document maakt een analyse van uNLock, hoe het werkt in de praktijk, de eisen waar een dergelijk systeem aan moet voldoen en risico's voor een dergelijk systeem. Ook wordt uNLock tegen de door VWS opgestelde eisen voor een dergelijk digitaal coronabewijs gehouden, en worden er aanvullende eisen geformuleerd.

De doelgroep van dit document is een breed technisch-geïnteresseerd publiek dat inzicht wil in de waarborgen die het uNLock systeem biedt.

Met de inzichten van 5 februari 2021 zijn de conclusies als volgt:

- het uNLock systeem onderscheidt zich positief op alle eisen van een centralistisch en een papieren alternatief en van het nulscenario, en voldoet aan vrijwel alle eisen die tot op heden vanuit VWS en andere mogelijke stakeholders worden gesteld.
- Er is een gebrek aan een eenduidige en gedragen set aan eisen en criteria rondom coronaveilig toegang verlenen. Het uitblijven daarvan draagt niet bij aan een snelle en veilige heropening van de Nederlandse samenleving. In dit rapport worden suggesties gedaan voor aanvullende eisen en criteria, welke in onze ogen noodzakelijk zijn voor een privacy-vriendelijke, veilige en schaalbare oplossing.

Inhoudsopgave

Managementuittreksel.....	Error! Bookmark not defined.
Samenvatting	2
1. Probleemstelling en oplossingsrichting	4
Wat is het probleem?	4
Wat is uNLock?	4
Wat is de stichting uNLock?	4
Welke ideeën liggen ten grondslag aan uNLock?	4
Kan dit probleem ook worden opgelost met een andere aanpak?	5
Hoe ver is uNLock?	6
2. Impact in de praktijk.....	7
2.1 Hoe werkt uNLock in de praktijk?	7
2.2 Kan iedereen uNLock gebruiken?	7
2.3 Wat is de rol van uNLock voor het doen van coronatesten en verwerking van deze data?	7
2.4 Welke pilots zijn er al geweest?	8
3. Eisen en features	9
3.1 Wie mag coronabewijzen uitgeven, opslaan en controleren?	9
3.2 Wat zijn de eisen rondom privacy?	9
3.3 Wat zijn de eisen rondom schaalbaarheid?	9
3.4 Hoe verhouden deze eisen zich tot de eisen die VWS stelt?	9
4. Wat zijn de risico's?	11
4.1 Wat is het risico dat er toch iemand binnenkomt die besmettelijk is?	11
4.2 Wat is het risico dat iemand binnen kan komen zonder coronabewijs, of een vals of verouderd coronabewijs?	11
4.3 wat is het risico dat iemand binnenkomt met een coronabewijs dat over een ander persoon gaat?	11
4.4 Wat is het risico dat je gedwongen wordt om coronabewijzen te delen?	11
4.5 Wat is het risico op misbruik van persoonsgegevens?	11
4.6 Wat is het risico op gedonder/teleurstellingen dat een bepaald type test niet wordt geaccepteerd voor een evenement?	12
4.7 Wat is het risico dat iemand bij mijn gegevens kan als ik mijn QR-code of telefoon kwijt ben?	12
5. Conclusie.....	13
6. Referenties	14
Annex A: Checklist event apps	15
Samenvatting	15
Veiligheid 15	
Operationeel.....	15
Privacy – DPIA	16

Commented [BS(d1)]: Er gaat iets mis met nummertjes in secties. Hoe kan ik dit oplossen?

1. Probleemstelling en oplossingsrichting

Wat is het probleem?

Het startpunt is de wens om het sociaal leven (zoals evenementenbranche, horeca en toerisme) in Nederland weer op gang te brengen, terwijl het coronavirus nog rondwaart en nog niet alle Nederlanders beschermd zijn door een vaccinatie. Mensen willen graag weer toegang tot activiteiten, op een coronaveilige wijze. De Gezondheidsraad geeft ook aan dat winkels, bedrijven, horeca en andere organisaties bezoekers mogen vragen naar een vaccinatiebewijs, mits voldaan aan strikte criteria¹.

Wat is uNLock?

uNLock² biedt een digitale oplossing om op privacy-vriendelijke en fraudebestendige wijze coronaveilige toegang te verlenen tot locaties op basis van een recente negatieve testuitslag.

uNLock helpt "veilige" bubbels te creëren: gecontroleerde omgevingen waar de kans op een coronabesmetting erg klein is. Dat kan bereikt worden door maatregelen zoals afstand houden, handen wassen, slimme looproutes en goede ventilatie, maar ook doordat alle personen binnen een bubbel zeer recent negatief zijn getest. Een bezoeker van een evenement kan het digitale bewijs leveren dat hij/zij voldoet aan de toegangscriteria door het tonen van een QR-code danwel een app op zijn/haar telefoon. De toegangscontroleur kan op basis van interactie met die QR-code danwel met die app vaststellen dat de persoon in kwestie voldoet aan het corona-toelatingsbeleid.

Wat is de stichting uNLock?

De uNLock toepassing wordt ontwikkeld door de Stichting uNLock. Stichting uNLock is een initiatief van de Dutch Blockchain Coalition (DBC), Universiteit Leiden, Rabobank, TNO, Deloitte, Ledger Leopard, CMS en stichting RINIS.



Welke ideeën liggen ten grondslag aan uNLock?

Privacy, veiligheid en schaalbaarheid zijn essentiële onderdelen van een systeem met als doel op een gecontroleerde wijze de huidige beperkingen te relaxen.

Privacy is zeer belangrijk omdat de coronabewijzen gaan over persoonsgegevens, en in het bijzonder over medische gegevens. De privacy van gebruikers wordt beschermd door gebruik van de denkmogelijkheden van Self-Sovereign Identity (SSI)³ en Regie op Gegevens⁴. De coronabewijzen worden digitaal aan de burger verstrekt, en deze is zelf in controle waar en met wie hij deze gegevens toont of

¹ [Ethische en juridische afwegingen COVID-19-vaccinatie | Advies | Gezondheidsraad](#)

² <https://unlockapp.nl/>

³ <https://www.tno.nl/en/focus-areas/information-communication-technology/roadmaps/data-sharing/ssi/>

⁴ <https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/regie-op-gegevens/>

deelt. Met behulp van cryptografische protocollen zijn deze bewijzen ook niet te zien door partijen hier geen recht op hebben. Wanneer een bezoeker toegang wil tot een evenement, sportwedstrijd of horeca, kan deze aan een controleur laten zien of deze voldoet aan de criteria. Door middel van een check weet de controleur alleen of iemand aan deze criteria voldoet, maar ziet hij niet op welke data dit is gebaseerd (bijvoorbeeld of iemand een PCR test heeft ondergaan of is gevaccineerd). Bovendien kan de persoon ook zelf van tevoren al testen of hij aan de eisen voldoet, zodat hij zich de reis kan besparen als dat niet zo is, of maatregelen kan nemen om alsnog aan de eisen te gaan voldoen.

Veiligheid valt uiteen in twee categorieën.

Veiligheid van gezondheid: deze wordt geborgd door het creëren van bubbels, waarbinnen het risico op besmetting tot een acceptabel niveau verkleind wordt. De coronabewijzen kunnen gebruikt worden om mensen toe te laten tot dergelijke bubbels. Een evenement, sportwedstrijd of horeca kan afspraken maken welke test en welke geldigheid zij acceptabel vinden voor toegang, in overleg met de *assurance community*⁵ waartoe zij behoren en altijd tenminste in lijn met richtlijnen van het bevoegd gezag.

Veiligheid van gegevens: Het systeem is zo ontworpen en uitgevoerd dat de kans op ongeoorloofde toegang zeer klein is, en dat bij incidenten de opgelopen schade minimaal is. Het gaat hierbij om risico's als het lekken van persoonsgegevens, maar ook bijvoorbeeld om aanvallen van hackers om het systeem plat te leggen voor wat voor reden dan ook.

Schaalbaarheid is noodzakelijk om grote groepen mensen binnen een kort tijdsbestek toegang te geven tot verschillende evenementen zoals festivals, concerten en sportwedstrijden. Het is hierbij belangrijk dat de oplossing voor iedereen te allen tijde bruikbaar is en dat er bijvoorbeeld geen opstoppen ontstaat bij grote evenementen, zeker ook als het risico bestaat dat zich in die groep besmette personen bevinden. Daarmee heeft schaalbaarheid ook effect op veiligheid.

Kan dit probleem ook worden opgelost met een andere aanpak?

Om deze vraag te beantwoorden worden drie alternatieve scenario's geschetst.

- **Het nulscenario:** handhaven van basis coronamaatregelen, maar verder niets. Het nulscenario is dat de evenementenbranche, de horeca en toerisme in Nederland op gang gebracht worden zonder gebruik van coronabewijzen. De coronaveiligheid blijft in dit scenario beperkt tot algemene basishygiëne coronamaatregelen: mondkapjes, handen ontsmetten, afstand houden, bij-klachten-blijf-thuis. Dit scenario is uiteraard zeer privacy-vriendelijk en schaalbaar: iedereen mag overal naar toe. Echter, de veiligheid van bezoekers kan niet gegarandeerd worden omdat ook mensen zonder klachten mogelijk een coronabesmetting kunnen overdragen naar andere bezoekers, of omdat bezoekers met klachten mogelijk ondanks waarschuwingen toch naar een evenement gaan om wat voor reden dan ook.
- **Een standaard centrale IT-oplossing:** gebruik van een centrale database. Alle communicatie tussen burger, testorganisatie en toegangsverlener verloopt via een centrale database. Hierbij wordt aangenomen dat privacy, veiligheid en schaalbaarheid zo goed mogelijk worden geïmplementeerd. Een dergelijk systeem kan risico's voor veiligheid van gezondheid van de burgers wellicht beperken. Echter, het gebruik van een centrale database kan problemen geven rondom privacy. In hoeverre kan een centrale partij alle uitwisselingen van gegevens zien? En hoe schaalbaar zijn dit soort IT-oplossingen? Omdat een dergelijk systeem nog van de grond af aan opgebouwd zou moeten worden, is dit een belangrijk punt.
- **Een papieren bewijs van een coronatest:** Alle communicatie tussen burger, testorganisatie en toegangsverlener verloopt via papier (post), telefoon of pdf's (email), en er is beperkte mogelijkheid tot automatisering. Echter, tegenwoordig zijn pdf's en brieven relatief makkelijk te vervalsen, waardoor bezoekers met een vals bewijs binnen zouden kunnen komen. Dit brengt de veiligheid van bezoekers mogelijk in gevaar. Ook voor schaalbaarheid is dit niet de beste oplossing. Wanneer een controleur veel stukken papier moet lezen voor een toegangscheck, kan dit niet snel gaan. De privacy wordt redelijk beschermd: wanneer de burger een papieren bewijs kan tonen, is niet zichtbaar voor de uitgever van dat bewijs waar het getoond wordt. Daarentegen is een dergelijk papier wel interessant voor misbruik van persoonsgegevens. Wanneer iemand een bewijs vindt,

⁵ TNO is in de Trust-over-IP Foundation bezig met een uitwerking van het concept "SSI assurance community", welke voor een groep gelieerde organisaties de verificatie criteria vaststelt en beheert.

kan deze dit eenvoudig lezen. Bovendien bevat papier vaak meer gegevens dan strikt noodzakelijk. Het klassieke voorbeeld is het tonen van je hele paspoort bij een drankenhandel om te bewijzen dat je 18 bent, terwijl leeftijd en foto (of desnoods geboortedatum en foto) genoeg zouden zijn en de rest van de info op het paspoort afgeschermd zou moeten kunnen worden.

Het moge duidelijk zijn dat geen van deze drie scenario's voldoet aan de gestelde eisen rondom privacy, veiligheid en schaalbaarheid.

Hoe ver is uNLock?

Het uNLock consortium (actief sinds maart 2020) heeft een decentrale architectuur opgezet en daarbij diverse functionele bouwblokken technisch werkend gekregen. Deze bouwblokken zijn en worden beproefd via Fieldlab Evenementen, en continu doorontwikkeld.

2. Impact in de praktijk

In de voorgaande sectie is omschreven wat de achterliggende ideeën zijn van uNLock. Om te bepalen of een oplossing al dan niet geschikt is, is het ook belangrijk om te kijken hoe het in de praktijk werkt, en welke impact daarmee gecreëerd wordt.

2.1 Hoe werkt uNLock in de praktijk?

Er zijn drie stappen:

1. **Laat je testen.** Zoals nu ook gebruikelijk is, maak je een afspraak om je te laten testen en legitiemeer je je voor de COVID-19 test. De teststraat stuurt het testmateriaal naar het testlab, waar de uitslag vastgesteld wordt of, bij een sneltest, het testmateriaal wordt ter plekke geanalyseerd. Er wordt aan de burger teruggekoppeld dat er een uitslag is, en bij een positieve uitslag worden de juiste gegevens ook doorgegeven aan de juiste instanties voor bron- en contactonderzoek (dat is wettelijk verplicht).
2. **Haal de uitslag op.** Zodra de testresultaten beschikbaar zijn, kan de geteste persoon deze ophalen. Daarbij zijn twee routes. Personen die gebruik maken van de uNLock app⁶ op hun smartphone kunnen de uitslag direct ophalen in de veilige omgeving van hun app. Personen die geen smartphone willen of kunnen gebruiken kunnen een QR code krijgen. Die QR-code functioneert als een verwijzing naar een beveiligde opslagplek voor het coronabewijs. In dat coronabewijs staat het verifieerbare testresultaat en een pasfoto van de geteste persoon.
3. **Doe de toegangcheck.** Door het tonen van de QR-code, vanaf papier of vanuit de mobiele app, kan de testuitslag gedeeld worden met de controleur van de locatie. Deze controleur krijgt alleen de pasfoto te zien op het moment dat aan alle criteria is voldaan om toegang te krijgen tot de locatie. Op basis van die pasfoto kan de toegangscontroleur vaststellen of de persoon in kwestie ook hoort bij het bewijs van het voldoen aan de toegangscriteria. In geval van het niet voldoen aan de toegangscriteria om wat voor reden dan ook krijgt de toegangscontroleur ook geen pasfoto te zien, dat is immers niet nodig om iemand de toegang te weigeren.

2.2 Kan iedereen uNLock gebruiken?

Deze vraag kan tweeledig worden beantwoord:

- Ja, elk individu kan uNLock gebruiken om toegang te krijgen tot evenementen. Het is niet nodig om in bezit te zijn van een smartphone, de coronabewijzen kunnen ook via een QR-code op papier worden getoond.
- Nee, niet iedereen kan zomaar coronaverklaringen van anderen controleren. Dat kan alleen door partijen die zijn ingeschreven in een register van "betrouwbare controleurs", dat wordt bijgehouden door een of meerdere daartoe geëigende partijen. Welke partijen dat bepalen is nog niet duidelijk, dit zou kunnen gebeuren door een relevant *assurance community*. Uiteraard is het positief dat verificatie alleen maar kan na accreditatie.

2.3 Wat is de rol van uNLock voor het doen van coronatesten en verwerking van deze data?

uNLock is niet verantwoordelijk voor het afnemen van coronatesten. uNLock faciliteert het proces van uitgeven, beheren, tonen en verifiëren van coronabewijzen.

- Uitgeven: uNLock registreert de gevalideerde testlabs, welke de coronabewijzen mogen uitgeven.
- Beheren: uNLock beheert de infrastructuur waarover de data met de relevante partijen gedeeld kunnen worden. uNLock beheert deze data zelf niet.

⁶ In SSI-termen wordt een dergelijke app ook wel een *Wallet* genoemd. De bewijzen die erin komen te staan, worden typisch aangeduid met de term *Verifiable Credential*.

- Tonen: door middel van QR-codes is het mogelijk om de beveiligd opgeslagen coronabewijzen te tonen.
- Verifiëren: uNLock registreert verifiërende partijen, en staat hen toe om de echtheid van de coronabewijzen te verifiëren.

Let wel: niet elk lab is zomaar een gevalideerd testlab en niet iedereen is een verifiërende partij. Echter, uNLock bepaalt zelf niet welk testlab gevalideerd is, dit doet het Ministerie van VWS. Ook wie een verifiërende partij is, bepaald uNLock niet, dit is een taak voor de eerder genoemde *assurance communities*. Verder bepaalt uNLock niet of een burger zijn coronabewijzen toont of deelt met een locatie om toegang te krijgen, hiervoor moet de burger zelf toestemming geven.

2.4 Welke pilots zijn er al geweest?

In december 2020 is een eerste pilot uitgevoerd met Fieldlab Evenementen, waar alle aspecten (identificatie, toegang, ...) op locatie met proefpersonen zijn getest. De pilot wordt als geslaagd beschouwd. Zie https://youtu.be/zsE0LokH_M8 vanaf 1'.14" voor een kort filmverslag van deze pilot.

3. Eisen en features

Zoals eerder genoemd, liggen privacy, veiligheid en schaalbaarheid ten grondslag voor de oplossing zoals uNLock presenteert. Andere aspecten die ook meegenomen worden zijn: *governance*, logistiek, technologie, kwaliteit, juridische en ethische aspecten.

3.1 Wie mag coronabewijzen uitgeven, opslaan en controleren?

- Testlabs moeten verifieerbare test bewijzen kunnen uitgeven. Alleen testlabs die daartoe gecertificeerd zijn door het Ministerie van VWS komen hiervoor in aanmerking.
- Burgers moeten verifieerbare testbewijzen kunnen ontvangen, opslaan en tonen. Een coronabewijs wordt alleen naar hen uitgegeven als ze een negatief testresultaat hebben.
- Controleurs moeten verifieerbare testbewijzen kunnen opvragen en verifiëren. Een individu mag alleen namens een bepaalde organisatie controleren als de *SSI assurance community* deze organisatie daarvoor accrediteert.

3.2 Wat zijn de eisen rondom privacy?

- Verifieerbare testbewijzen kunnen alleen gecontroleerd worden door een verifiërende partij. De relevante SSI-assurance community bepaalt of een partij toegestaan is om te mogen verifiëren.
- Geminimaliseerde bewijzen bevatten alleen de noodzakelijke gegevens, zoals het corona testresultaat, het type test, of het testbewijs binnen een bepaalde tijd is uitgegeven, en een pasfoto.
- Positieve testresultaten worden niet verwerkt tot een QR-code of opgeslagen in de app. Dit zorgt ervoor dat een positief testresultaat hetzelfde behandeld wordt als geen testresultaat, om discriminatie te voorkomen richting positief geteste personen.
- Burgers moeten in regie zijn van hun eigen testbewijs. Hun coronabewijs zal niet gedeeld worden zonder dat ze daar zelf toestemming toe gegeven hebben.

3.3 Wat zijn de eisen rondom schaalbaarheid?

- De oplossing moet schaalbaar zijn en grote hoeveelheden data kunnen verwerken. Dit gaat niet alleen over het registreren van coronabewijzen, maar ook over het controleren. Ook moet het mogelijk zijn om een groot aantal apps te beheren.
- De oplossing moet door een groot deel van de Nederlandse bevolking te gebruiken zijn. Het is hiervoor belangrijk om een intuïtieve app aan te bieden, welke voor iedereen te begrijpen is.
- Burgers moeten de keuze hebben om ook een niet-digitale optie te hebben om deze test bewijzen te gebruiken. Daarom is het ook mogelijk om een coronabewijs te tonen via een uitgeprinte QR-code.

3.4 Hoe verhouden deze eisen zich tot de eisen die VWS stelt?

Recent zijn eisen van VWS aan een digitaal coronapaspoort openbaar geworden⁷. Deze eisen lijken uit te gaan van een keuze voor een digitaal coronabewijs. Hieronder wordt aangegeven in hoeverre de al ontwikkelde uNLock oplossing voldoet aan die eisen die wij ontvingen van VWS in een document genoemd "[ICT opdracht \(003\).docx](#)". Het is ook aan te raden dat VWS de eisen zoals geformuleerd in 3.1 Wie mag coronabewijzen uitgeven, opslaan en controleren?, 3.2 Wat zijn de eisen rondom privacy?, en 3.3 Wat zijn de eisen rondom schaalbaarheid? meeneemt voor een digitaal coronapaspoort.

Systeem:

⁷ [nl-COVID19-coronatester-app-coordination/Solution Architecture VTR.md at main · minvws/nl-COVID19-coronatester-app-coordination · GitHub](#) en document "ICT opdracht (003).docx"

1. **Triage:** het is mogelijk om de testresultaten door te zetten naar GGD, zodat triage kan plaatsvinden. De GGD kan dan het bron- en contactonderzoek uitvoeren.
2. **Toegang tot afsprakenportaal:** via het uNLock systeem is het niet mogelijk om testafspraken te maken. Het is wel mogelijk om de resultaten van de testen te verwerken in uNLock. Hiervoor dient andere software gebruikt te worden.
3. **Registratie:** zoals eerder beschreven, is het mogelijk om een negatief testresultaat te registreren met behulp van het uNLock systeem. Een positief testresultaat wordt niet opgeslagen in uNLock.
4. **Koppeling CoronIT:** dit is een generieke eis. Het is mogelijk om het uNLock systeem aan te sluiten op CoronIT. Op dit moment worden hiermee geen problemen voorzien.
5. **Terugkoppeling naar burger:**
 - a. De testuitslag wordt direct teruggekoppeld met de burger. In geval van een negatief testresultaat, wordt de testuitslag ook opgeslagen.
 - b. Voor gebruiksgemak is het mogelijk om het testbewijs op verschillende manieren te verkrijgen. Voor degenen die een coronabewijs graag digitaal ontvangen, is het mogelijk om deze op te slaan in een app op een smartphone. Voor degenen die het coronabewijs liever op papier ontvangen, is dat ook mogelijk in de vorm van een QR-code. Hierdoor wordt het testbewijs van alle gemakken voorzien.
6. **Ondersteuning testmethoden:** het uNLock systeem is dusdanig flexibel, dat het mogelijk is om alle huidige testresultaten te ondersteunen, zoals PCR, -LAMP, antigeen coronatesten, en later mogelijk ook vaccinatiebewijzen en/of immuniteitsbewijzen. Er is een register van betrouwbare testpartijen die met dat type test mogen werken. Dit register wordt opgesteld door het Ministerie van VWS. Aan de kant van de controleur wordt in een policy bijgehouden hoe verschillende testen verschillend behandeld worden. Bijvoorbeeld: voor een bepaald sportevenement wordt bepaald dat toegang met een negatieve PCR-test van maximaal 72 uur oud, of een antigenetest van maximaal 48 uur oud. In geen enkel geval kan een controleur nagaan of een bezoeker een negatief testresultaat heeft, een immuniteitsbewijs of een vaccinatiebewijs.

Randvoorwaarden:

1. **Dataopslag:** uNLock is een decentraal systeem. De coronabewijzen worden alleen opgeslagen waar de eigenaar van de bewijzen bij kan. Er is geen mogelijkheid tot een centrale toegang. Voor de papieren QR-code wordt alleen een pasfoto en negatief testresultaat opgeslagen in de zogenaamde kluisjesmuur. Het is alleen mogelijk om de QR-code te scannen gedurende de geldigheid van het coronabewijs. Gebruikt een bezoeker een app, dan wordt de pasfoto en negatief testresultaat opgeslagen in deze app. Wanneer dit coronabewijs niet meer geldig is, kan de eigenaar van de app ervoor kiezen om dit bewijs te verwijderen. Indien gewenst kan de app ook zo ingesteld worden dat de coronabewijzen automatisch verwijderd worden wanneer ze niet meer geldig zijn. Dit kan een keuze zijn van de app aanbieder, een optie die de gebruiker al dan niet activeert of een eis die de overheid stelt aan het ontwerp van een dergelijke app.
2. **Privacy en security:** diverse partijen uit het uNLock consortium zijn NEN 7510 gecertificeerd. De plekken waar persoonsgegevens verwerkt worden, zullen dan ook gehost worden bij deze partijen. Componenten waar geen persoonsgegevens benodigd zijn, zoals het register van geverifieerde testlabs, kunnen wel bij andere partijen gehost worden die deze certificering niet hebben, omdat die certificering dan niet relevant is. Het uNLock consortium heeft een DPIA opgesteld waarin dit verder omschreven is.
3. **DOTT:** een afgevaardigde van het uNLock consortium zal graag aansluiten aan deze regiegroep.

4. Wat zijn de risico's?

4.1 Wat is het risico dat er toch iemand binnenkomt die besmettelijk is?

Helaas bestaat 100% veilig niet. Dit heeft een aantal redenen:

1. Negatief geteste personen blijken toch besmettelijk te zijn
 - a. Omdat de test hun besmetting (nog) niet kon vaststellen; of
 - b. Omdat ze pas na de test besmet zijn geraakt en besmettelijk zijn geworden.
2. Positief geteste of niet geteste personen komen toch binnen (en kunnen misschien besmettelijk zijn) omdat de toegangscontroleur hen toch binnenlaat door misidentificatie of vervalste coronabewijzen.

Voor het eerste punt biedt gebruik van uNLock geen waterdichte oplossing. Er zijn wel mogelijkheden om het risico te beperken, zoals een beperkte geldigheid van een coronabewijs. Uiteraard kunnen specialisten advies geven over deze geldigheid. Voor het tweede punt biedt uNLock mogelijkheden om risico te beperken, bijvoorbeeld door gebruik van een pasfoto en cryptografische protocollen, zie 4.2

Wat is het risico dat iemand binnen kan komen zonder coronabewijs, of een vals of verouderd coronabewijs?.

4.2 Wat is het risico dat iemand binnen kan komen zonder coronabewijs, of een vals of verouderd coronabewijs?

Wanneer de verifiërende partij een QR-code scant van een bezoeker, wordt er een check gedaan of de bezoeker aan alle criteria voldoet. Hierbij wordt ook de echtheid en geldigheid van het coronabewijs gecontroleerd door middel van cryptografische protocollen. Een nep of een verouderd coronabewijs zal dan niet goedgekeurd worden.

4.3 wat is het risico dat iemand binnenkomt met een coronabewijs dat over een ander persoon gaat?

Een van de criteria waar een bezoeker moet voldoen, is het tonen van een pasfoto. Deze kan de controleur dan verifiëren. Hier is een beperkt risico dat je kunt binnenkomen met pasfoto en coronabewijs van een ander persoon, bijvoorbeeld bij een tweeling. Echter, dit is hetzelfde risico dat iemand zich zou kunnen legitimeren met een identiteitsbewijs van een ander persoon.

4.4 Wat is het risico dat je gedwongen wordt om coronabewijzen te delen?

In principe kunnen alleen bepaalde partijen aangewezen worden als verifiërende partij voor coronabewijzen. Een bezorgde werkgever die zijn personeel om testbewijzen vraagt, zou dan geen toegang moeten krijgen tot coronabewijzen van zijn personeel. Vanwege de gezagsverhoudingen tussen werkgever en personeel gelden andere juridisch eisen dan bij een vrijwillig bezoek aan een evenement. uNLock heeft daarom de keuze gemaakt om alleen bepaalde SSI-assurance communities te accepteren welke verifiërende partijen kunnen accrediteren.

4.5 Wat is het risico op misbruik van persoonsgegevens?

Hackers, datalekken, meekijkers en toegangsverleners die opzettelijk data lekken, zijn mogelijkheden waardoor misbruik gemaakt kan worden van persoonsgegevens. Dit leidt tot negatieve gevolgen voor burgers wiens data is gelekt, of die op een niet-afgesproken manier zijn gebruikt. Echter, het risico op hackers en datalekken wordt gemanaged doordat de informatie alleen decentraal staat opgeslagen. Elke individuele app op een smartphone zal dan gehackt moeten worden. Ook in de kluisjesmuur moet elk afzonderlijk kluisje geopend worden. Het risico op meekijkers of toegangsverleners die data lekken is ook beperkt, omdat alleen de pasfoto wordt getoond wanneer een bezoeker voldoet aan de criteria. Ook deze pasfoto wordt niet opgeslagen.

Daarnaast wordt de privacy van de controleurs geborgd. Omdat de controleur namens de locatie verifieert, zal deze zelf niet aansprakelijk worden, en ook zijn persoonsgegevens worden niet gedeeld. De controleur krijgt persoonsgegevens van de bezoekers niet in te zien, waardoor het risico op verkeerd gebruik een stuk minder wordt.

4.6 Wat is het risico op gedonder/teleurstellingen dat een bepaald type test niet wordt geaccepteerd voor een evenement?

Voor een bezoeker kan het heel vervelend zijn als hij zich voorafgaand aan een evenement heeft laten testen, maar ter plaatse blijkt dat ofwel de verkeerde test is afgenomen, of de test niet meer geldig is. Dit zou zelfs onveilige situaties kunnen opleveren voor de controleur. Om dit te voorkomen, is het mogelijk om als (potentiële) bezoeker van tevoren te controleren of er voldaan wordt aan alle criteria. Dit zou vanuit huis kunnen. Dit werkt alleen voor de appversie, niet de QR-code versie.

4.7 Wat is het risico dat iemand bij mijn gegevens kan als ik mijn QR-code of telefoon kwijt ben?

- QR-code: hierbij zijn twee gevallen te onderscheiden:
 - De vinder is geen geregistreerd controleur: in dit geval krijgt de vinder geen toegang tot de digitale kluis van de eigenaar van de QR-code.
 - De vinder is een geregistreerd controleur: als de QR-code nog geldig is, dan ziet de vinder de pasfoto van de eigenaar, indien voldaan is aan de criteria van de controlerende partij. Als niet aan deze criteria is voldaan, dan krijgt de vinder geen toegang tot de digitale kluis.
- App op smartphone: hier is alleen een risico als de vinder toegang krijgt tot de telefoon. Wanneer de vinder geen toegang krijgt tot de telefoon, kan deze ook geen toegang krijgen tot de app.

5. Conclusie

Op basis van bovenstaande kunnen we concluderen dat uNLock voldoet aan de privacy en veiligheidscriteria, zoals die door ons zijn opgesteld. Het is onze verwachting dat uNLock – mits juist geïmplementeerd – ook voldoende schaalbaar is om aan een grote vraag te voldoen. De uiteindelijke schaalbaarheid wordt bepaald door de lokale implementatie en de organisatie/governance daarachter. In de aankomende pilots met Fieldlab Evenementen zal ook die organisatie en lokale implementatie voldoende moeten worden getest en bijgesteld.

uNLock lijkt ook – behalve enkele kleine details - te voldoen aan de criteria zoals door VWS lijken te worden gesteld. TNO heeft nog vraagtekens bij een aantal criteria, namelijk:

- Triage: het uNLock systeem is niet bedoeld voor de GGD om contact op te nemen met positief geteste mensen voor bron- en contactonderzoek. De vraag is ook of dit nodig is. Het is natuurlijk wel mogelijk voor mensen om hun coronabewijs aan de GGD te tonen wanneer zij daarvoor bevoegd zijn.
- Toegang tot het afsprakenportal: het uNLock systeem is niet bedoeld om te gebruiken als afsprakenportaal. Het is natuurlijk wel mogelijk om de testresultaten in de vorm van een coronabewijs te verwerken met behulp van uNLock.

uNLock heeft zichzelf ook nog extra eisen opgelegd, welke ook aan te raden zijn voor VWS om mee te nemen in hun lijst:

- Schaalbaarheid is noodzakelijk om grote groepen mensen binnen een kort tijdsbestek toegang te geven.
- Niet zomaar iedereen zou coronabewijzen mogen uitgeven, en niet iedereen mag deze zomaar controleren. Zowel testlabs, als controleurs moeten hiervoor dan geaccrediteerd worden. Hiervoor heeft uNLock een oplossing gevonden in de vorm van *assurance communities*.
- Iedereen moet zelf kunnen besluiten of hij het coronabewijs dat over hem gaat, wil tonen. Hierbij moet geen sprake zijn van dwang.
- Er moet een manier zijn om discriminatie tegen positief of niet geteste personen tegen te gaan. Een middel hiervoor is het niet toekennen van een testbewijs als deze test positief is.
- ...

Commented [BS(d2)]: Check: vergeet ik niets?

6. Referenties

- [1] uNLock, <https://unlockapp.nl/>
- [2] Oskar van Deventer et al, "Self-sovereign identity - the good, the bad and the ugly", <https://blockchain.tno.nl/blog/self-sovereign-identity-the-good-the-bad-and-the-ugly/>, TNO, May 2019
- [3] Rieks Joosten et al, "Self-sovereign identities: it is going to happen!", <https://blockchain.tno.nl/blog/self-sovereign-identities-it-is-going-to-happen/>, TNO, May 2018
- [4] Sterre den Breeijen et al, "Four lessons on guardianship with self-sovereign identity", <https://blockchain.tno.nl/blog/four-lessons-on-guardianship-with-self-sovereign-identity/>, TNO, March 2020
- [5] Oskar van Deventer et al, "Verify the verifier - anti-coercion by design", <https://blockchain.tno.nl/blog/verify-the-verifier-anti-coercion-by-design/>, TNO, October 2020
- [6] W3C, "Verifiable Credentials Data Model 1.0", <https://www.w3.org/TR/vc-data-model/>, November 2019
- [7] Hyperledger Indy, "Providing digital identities rooted on blockchains", <https://www.hyperledger.org/use/hyperledger-indy>

Annex A: Checklist event apps

Oskar van Deventer, TNO, 3 Februari 2021

Samenvatting

Dit document is een checklist waarmee coronabubbel-oplossingen voor events ("event apps") beschouwd kunnen worden.

Het uitgangspunt is dat aan event deelnemers voldoende coronaveiligheid geboden kan worden door de gebruikelijke maatregelen (afstand, ontsmettingsgel, mondkapje) te combineren met betrouwbare coronatestuitslagen.

De checkvragen zijn opgesteld op basis van een klein jaar ervaring met dit soort coronaoplossingen vanuit het internationale COVID-19 Credentials Initiative en uit de uNLock samenwerking, aangevuld met een uitgebreide achtergrondkennis op identiteitsoplossingen, self-sovereign identity en attribute-based credentials. De checkvragen zijn in een aantal categorieën ingedeeld.

Veiligheid

- Hoe makkelijk of moeilijk is het voor een kwaadwillende om een nep-coronatest te produceren, waarmee deelnemers onterecht naar binnen gelaten kunnen worden? Waar zitten de risicoplekken in de van-test-tot-verificatie keten, en hoe worden deze gemitigeerd?
- Hoe makkelijk of moeilijk is het voor een deelnemer om met een coronatest van iemand anders naar binnen te komen? Waar zitten de risicoplekken in de identificatieketen, en hoe worden deze beveiligd?
- Hoe makkelijk of moeilijk is het voor een kwaadwillende om als nep-toegangsverlener toegang te krijgen tot het systeem? Hoe wordt de toegangsverlener (persoon) geïdentificeerd en wie is daarvoor verantwoordelijk?
- Hoe wordt gewaarborgd dat alleen coronatests van erkende testlabs door de oplossing geaccepteerd worden? Hoe loopt dat erkenningsproces?
- Hoe wordt gewaarborgd dat alleen een erkende toegangsverlener passerende deelnemers kan controleren op het voldoen aan de toegangseisen? Hoe loopt dat erkenningsproces?
- Hoe wordt gewaarborgd dat de toegangsverlener alleen ten tijde van het event passerende deelnemers kan controleren op het voldoen aan de toegangseisen?
- Hoe kan een toegangsverlener controle doen, is daar een speciale device voor nodig, een app op een smartphone van de locatie, of kan dit een persoonlijke smartphone zijn?

Operationeel

- Hoe snel werkt de oplossing in termen van doorstroom van deelnemers per poortje per minuut, en deelnemers-per-minuut voor het gehele systeem?
- Hoe vindt de identificatie van de deelnemer plaats in de teststraat? Wat is de level-of-assurance daarbij?
- Hoe vindt de identificatie van een deelnemer plaats bij de ingang van het event? Wat is de level-of-assurance daarbij?
- Hoe bruikbaar is de oplossing voor deelnemers zonder smartphone?
- Hoeveel van de oplossing bestaat al als implementatie? Welke inzichten kwamen uit eerste praktijktesten?

- Hoe flexibel is de oplossing, als een deelnemer op basis van een enkele coronatest kort op elkaar naar meerdere events wil gaan?
- Hoe flexibel is de oplossing, als er een aanpassing van de toegangscriteria aan de orde is? Bijvoorbeeld toevoeging van meerdere soorten coronatesten, verschillende tijden tussen test en toegang, of nieuwe inzichten over vaccinatie of immuniteit?
- Hoe flexibel is de oplossing, als een controleur op de ene dag op een bepaald evenement staat, en de andere dag op een ander evenement staat, waar mogelijk andere criteria zijn voor toegang?

Privacy – DPIA

- Welke informatie komt de toegangsverlener (persoon) te weten van de passerende deelnemer?
- Welke informatie over de deelnemer komt de elektronica van de toegangsverlener ("toegangspoortje") te weten van de passerende deelnemer?
- Welke persoonsinformatie over een deelnemer (identiteit, coronatest, ...) wordt op welke plekken en op welke wijze opgeslagen? Hoe is deze beveiligd? Wie heeft welke toegang tot deze informatie? Hoe lang wordt deze bewaard?
- Hoe wordt gewaarborgd dat een deelnemer niet gedwongen kan worden om een coronatest met een onbevoegde derde te delen?