Gegevensbeschermingseffectbeoordeling (PIA)

VWS | Directie Informatiebeleid / CIO

PIA CoronaCheck / CoronaCheck scanner app

Den Haag, 26-03-2021 / Status: opvolging 5.1.2e – Ter akkoord 5.1.2e

Vaststelling verwerkersverantwoordelijke: 26-3-2021
Naam: 5.1.2e

Kennisgenomen 5.1.2e 26-3-2021
Acceptatie restrisico na genomen maatregelen: 26-3-2021

Datum: 26-3-2021
Handtekening:

5.1.2e 25-3-2021

Gegevensbeschermingseffectbeoordeling (PIA)

VWS | Directie Informatiebeleid / CIO

PIA CoronaCheck / CoronaCheck scanner app

Contact:

Ministerie van Volksgezondheid, Welzijn en Sport
Directie Informatiebeleid/CIO
Parnassusplein 5
2511 VX Den Haag

Versie: 1.0, 26 maart 2021

Inhoud

Inleiding

Deze PIA is opgesteld door het programma 'Realisatie Digitale Ondersteuning' binnen het Ministerie Volksgezondheid, Welzijn en Sport (hierna VWS) en geldt voor het 'Testbewijs'. Het Testbewijs is een middel waarin wordt aangegeven of iemand recent negatief is getest op Corona.

In deze PIA wordt beschreven welke privacy beschermende maatregelen zijn genomen om het testbewijs als middel te kunnen inzetten.

Deze PIA is geschreven voor de inzet van de apps CoronaCheck en CoronaCheck scanner tijdens pilots die vanaf 27 maart 2021 worden gehouden. Tijdens deze pilots wordt gebruik gemaakt van een versie van beide apps, die voorafgaat aan de versie zoals deze is beschreven aan het wetsvoorstel en bijbehorende Memorie van Toelichting, versie 8 maart 2021 die ter consultatie is aangeboden[1].

[1] https://www.internetconsultatie.nl/wetsvoorsteltestbewijzen

A. Beschrijving kenmerken gegevensverwerking

1. Voorstel

Nederland wordt, net als de rest van de wereld, geconfronteerd met de uitbraak van het SARS-CoV-2, een virus dat kan leiden tot de ziekte COVID-19. De verspreiding van SARS-CoV-2 wordt beteugeld door diverse maatregelen. Daar waar bewegingsvrijheid worden beperkt door een lockdown, ontstaat ook de behoefte om op een gecontroleerde manier de samenleving weer te openen.

Het testbewijs is een bewijs dat iemand negatief is getest en is tijdelijk geldig. Dit bewijs kan worden gebruikt om toegang te geven tot specifieke activiteiten en voorzieningen. Het testbewijs maakt het (in combinatie met andere risicobeperkende maatregelen) mogelijk om daar waar verlichting van de lockdown mogelijk is, dit ook te doen. De beheerders van activiteiten en voorzieningen waarvoor een testbewijs gevraagd wordt, dienen te controleren of de deelnemer of gebruiker een geldig testbewijs heeft en kunnen daarvoor de applicatie CoronaCheck Scanner te gebruiken.

Deelnemers aan de pilot en gebruikers van de voorzieningen moeten zich daarvoor laten testen en - samen met een legitimatiebewijs - het testbewijs tonen bij de betreffende activiteit of voorziening. Daarvoor kunnen zij de applicatie CoronaCheck gebruiken. De applicaties CoronaCheck en CoronaCheck Scanner worden onder verantwoordelijkheid van de Minister van VWS ontwikkeld. Dit document bevat een Privacy Impact Assessment, (hierna: PIA) van het gebruik van persoonsgegevens[2] voor het testbewijs en de applicaties, conform artikel 35 van de Algemene Verordening Gegevensbescherming (hierna: AVG).

Gebruikte afkortingen

AVG	Algemene Verordening Gegevensbescherming
Controleur	Iemand die de geldigheid van een testbewijs controleert
PIA	Privacy impact assessment
SON	Stichting Open Nederland
Testresultaat	Resultaat van een test dat door teststation wordt verstrekt aan persoon
Testbewijs	Deel van gegevens van testresultaat nodig is om bij toegang te tonen
Verstrekker	Teststation (GGD of anders) die een testresultaat verstrekt
VWS	Volksgezondheid, Welzijn en Sport
Wpg	Wet publieke gezondheid

Scope van de PIA

Een wetsvoorstel om testbewijzen op grote schaal in te kunnen gaan zetten bij het heropenen van de samenleving is ter consultatie[3] aangeboden. In dit voorstel wordt de Wet publieke gezondheid (Wpg) gewijzigd. Door preventief te testen en daarvan een testbewijs te verstrekken kunnen verschillende evenementen en activiteiten eerder veilig georganiseerd worden.

[2] Uitgangspunt van deze PIA is het voorgenomen gebruik van (persoons)gegevens zoals bekend op 22 maart 2021.
[3] https://www.internetconsultatie.nl/wetsvoorsteltestbewijzen

VWS is op zoek naar meerdere bouwstenen die bijdragen aan preventie en reductie van het risico van verspreiding van het Covid-19 virus. De ontwikkelde events zijn gericht op het vergaren van kennis en data rondom evenementen in tijden van Corona. Aan de hand van de onderzoeksresultaten wordt toegewerkt naar veilige en verantwoorde evenementen met een verhoogde bezoekerscapaciteit, zoals voorheen. VWS werkt hierbij samen met Stichting Open Nederland (SON) aan de uitbreiding van de testcapaciteit en met 'Fieldlabs' voor de organisatie van evenementen.

Totdat de voorgestelde wetswijziging is goedgekeurd, bestaat de behoefte om in diverse pilots en proefevenementen gebruik te maken van CoronaCheck app en Coronacheck Scanner app en ook op dit punt kennis en data te vergaren.

Binnen de scope van deze PIA valt:
- het ophalen van een (negatief) testresultaat bij een teststation (verstrekker);
- het genereren van een testbewijs (in CoronaCheck);
- de validatie van het testresultaat bij een toegangsdeur (door CoronaCheck Scanner).

Buiten scope van deze PIA valt de gegevensverwerking bij SON. In de plaatjes en beschrijvingen hierna wordt het proces wel in zijn volledigheid inzichtelijk gemaakt en wordt specifiek aangegeven wat wel en niet in scope is van het gebruik van (persoons)gegevens. Voor de gegevensverwerking van SON wordt verwezen naar de PIA van SON[4].

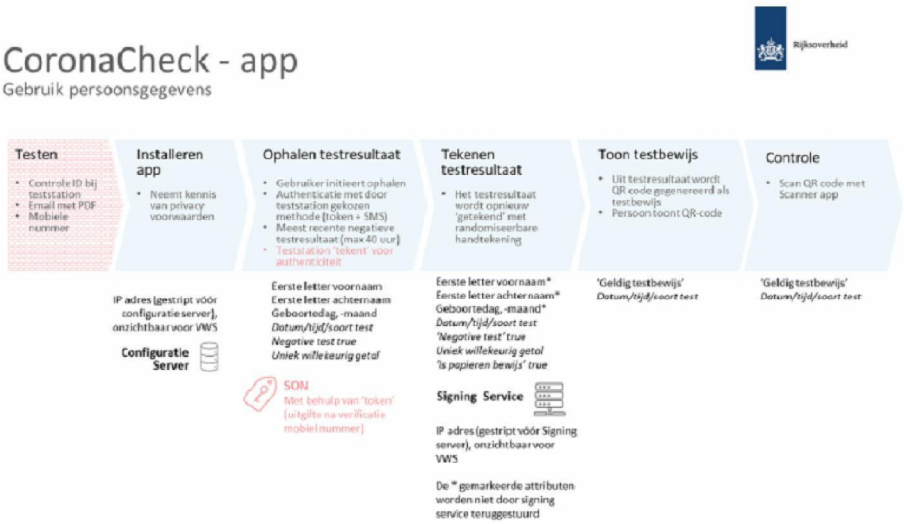
Grafisch ziet de scope er als volgt uit.

Het testbewijs kent zowel een digitale variant, waarbij het testbewijs via een smartphone wordt getoond, als een variant die op papier aan de deur kan worden getoond. Enkel de digitale variant is in scope van deze PIA. De fysieke variant wordt ter informatie wel genoemd en deels beschreven in deze PIA om de inzet van CoronaCheck in het gehele proces nader te duiden.

[4] IT-DPIA ten behoeve van de SON IT platform, versie concept 0.95, d.d. 22 maart 2021

Om de app te downloaden moeten gebruikers toegang hebben tot de Apple App Store of de Google Play Store. De gegevens die Apple en Google gebruiken voor toegang tot de Stores (zoals een emailadres) worden in het kader van CoronaCheck niet gebruikt. Als zodanig valt de verwerking daarvan door Apple en Google buiten het bereik van deze PIA.

Beschrijving van het gebruiksproces (digitaal testbewijs)
Een persoon ondergaat allereerst een corona test. Dit kan een PCR test zijn, of een andere goedgekeurde test. Hierna worden deze teststations ook 'verstrekker' genoemd. Bij de afname van de test is de verstrekker verplicht de identiteit van de persoon te controleren.



Bij het teststation vindt een controle plaats op het ID, om vast te stellen dat degene die de testafspraak heeft gemaakt, ook degene is die de test afneemt. Bij het teststation wordt ook het emailadres en mobiele nummer van de persoon gevraagd, dit is nodig om (op het moment dat het testresultaat beschikbaar is) het testresultaat met de persoon te kunnen delen. SON is de enige partij die beschikt over dit emailadres en mobiele nummer. Het gebruik van deze persoonsgegevens valt daarmee buiten scope van deze PIA en is herkenbaar aan de afwijkende kleur in het paatje.

De persoon installeert de CoronaCheck app op de smartphone via de Apple Store of de Google PlayStore. Na installatie van de app, zoekt de app contact met de Configuratie Server van VWS, om daar de meest recente instellingen en actueel sleutelmateriaal op te halen.

De persoon haalt via de CoronaCheck app op de smartphone[5] de testresultaten op bij SON en plaatst deze in de CoronaCheck app van de persoon. Zodra het testresultaat beschikbaar is ontvangt de persoon van SON een email met daarin een token (een unieke code). Vervolgens vult de persoon via de smartphone in de CoronaCheck app deze token in. De persoon krijgt ter controle een SMS op het mobiele telefoonnummer dat is opgegeven bij het teststation om het ophalen van het testresultaat te bevestigen. Vervolgens wordt het testresultaat van de persoon vanuit de de backend van SON op de smartphone in de CoronaCheck app geladen.

[5] Vanaf Android 6 en iOS 11.

SON tekent het testresultaat cryptografisch, waarmee CoronaCheck kan controleren dat het testresultaat ook daadwerkelijk van SON afkomstig is. De wijze van tekenen vindt plaats bij SON en is daarmee buiten scope van deze PIA.

Op basis van het testresultaat dat de persoon in CoronaCheck heeft opgehaald laat de persoon het testresultaat in de CoronaCheck app opnieuw tekenen door een signing service. Dit 'opnieuw tekenen' houdt in dat CoronaCheck het testresultaat voorziet van een randomiseerbare handtekening. Deze randomiseerbare handtekening zorgt dat het testbewijs steeds op een verschillende manier is getekend. Zo kan geen van de betrokken partijen (SON, VWS, controleur) volgen waar mensen dit testbewijs gebruiken. Ten slotte genereert CoronaCheck een testbewijs in de vorm van een QR code. Tijdens deze signing worden de eerste letter van de voornaam, de eerste letter van de achternaam, de geboortedag en geboortemaand niet meegetekend. Deze gegevens worden gestript van het testresultaat en worden dus opgenomen in het ondertekende testbewijs.

Aan de poort wordt het testbewijs gecontroleerd door een 'controleur'. De controleur maakt voor de controle op een geldig negatief testbewijs gebruik van de 'CoronaCheck Scanner app'.

Deze CoronaCheck Scanner app heeft als functionaliteit het interpreteren van de QR code en het op basis daarvan aangeven of deze persoon inderdaad beschikt over een geldig negatief testbewijs.

Beschrijving van het gebruiksproces (fysiek testbewijs) – buiten scope van deze PIA, ter illustratie
Iedere deelnemer aan de pilot die zich heeft laten testen krijgt het testresultaat en een testbewijs via de e-mail toegestuurd. Indien iemand CoronaCheck niet wil of kan gebruiken doordat zij/hij niet beschikt over een smartphone, kan dus het testbewijs die zij/hij heeft gekregen via de e-mail uitprinten en als fysiek testbewijs gebruiken. Daartoe is het nodig dat iemand kan beschikken over een computer met printer. Dit kan ook een computer / printer zijn bij buren of bij de bibliotheek.

In de QR-code op het fysieke (geprinte testbewijs staat hetzelfde als in de digitale QR code. Met deze print kan de persoon naar de poort, waar de controle plaatsvindt door de QR code te laten scannen door de CoronaCheck Scanner app. Het fysieke testbewijs valt onder de verantwoordelijkheid van SON en is buiten scope van deze PIA.

Componenten van CoronaCheck
CoronaCheck bestaat uit de volgende componenten:
- De CoronaCheck app – dit is de app die de persoon gebruikt om een testbewijs te presenteren.
- De CoronaCheck Scanner app – dit is de app die de controleur gebruikt om te controleren of iemand beschikt over een geldig negatief testbewijs.
- Een configuratie server en een Signing service.
-

Voor het beheer van beide apps is een configuratie server actief. Hiermee wordt de app beheerd. Zo wordt bij het opstarten van de app de configuratie opgehaald. Deze bevat deze configuratie server instellingen zoals de duur van de geldigheid van testbewijzen en sleutels die gebruikt worden voor de beveiliging. Ook bevat de configuratie server een mogelijkheid waarmee, de service om testbewijzen te valideren éénmalig of volledig beëindigd kan worden. Dit is bijvoorbeeld nuttig als de inzet van de app definitief niet meer wenselijk/proportioneel wordt geacht.

Met de Signing service wordt ieder testresultaat in de CoronaCheck app cryptografisch 'getekend'. Het resultaat hiervan is een geldig testbewijs die in de app als QR-code wordt getoond.

2. Verwerkingen van persoonsgegevens

De volgende gegevens worden gebruikt.

- In het **testresultaat** zijn de volgende gegevens opgenomen:
    - Geregistreerde datum en tijdstip van testen (t.b.v. geldigheidsduur testresultaat), afgerond op een heel uur.
    - Type test (t.b.v. eventueel te maken onderscheid in verschillende testsoorten in de toekomst).
    - Indicatie negatieve test ('true'). Hierbij betekent 'true' dat er een negatieve test is overlegd en iemand dus tijdens de test niet besmet was. Een positief testresultaat wordt niet via een aparte procedure teruggekoppeld aan de geteste persoon en is volledig buiten scope van deze PIA.
    - Geboortedag en geboortemaand van getest persoon, aangevuld met de eerste letter van de voornaam en de eerste letter van de achternaam. Deze attributen helpen de persoon om voor zichzelf vast te stellen of het testresultaat ook van henzelf is.
    - Digitale handtekening van Verstrekker (waarmee ze verantwoording dragen voor het juist uitgegeven negatieve testresultaat en waarmee kan worden gecontroleerd of de gegevens in het resultaat niet zijn aangepast nadat ze door de drager zijn ontvangen). De digitale handtekening bevat ook het exacte tijdstip dat die handtekening gezet is.

  Deze gegevens worden in de app op de smartphone van de persoon opgeslagen.

- In het **testbewijs** is opgenomen[6]:
    - Geregistreerde datum tijdstip van testen (t.b.v. geldigheidsduur testresultaat), afgerond naar het eerstvolgende hele uur
    - Type test (t.b.v. eventueel te maken onderscheid in de toekomst
    - Indicatie negatieve test (true)
    - Digitale handtekening van de Signing Service (waarmee kan worden gecontroleerd of de gegevens in het resultaat niet zijn aangepast nadat ze door de drager zijn ontvangen).

  Dit testbewijs wordt via de CoronaCheck app verwerkt en als QR code op de smartphone van de persoon gepresenteerd.

In het testresultaat en in het testbewijs is ook een uniek willekeurig getal (niet persoonsgebonden) opgenomen om dubbele uitgifte van bewijzen te kunnen voorkomen. Dit getal wordt als metadata meegelezen door de signing service.

Het omzetten van een testresultaat in een testbewijs gaat via een configuratie service en de signing service van VWS. Het testresultaat wordt hiervoor naar de server van VWS gestuurd. Inherent aan internetcommunicatie is dat hiervoor een IP-adres wordt gebruikt. Het IP adres van de drager van de persoon wordt binnen de beheeromgeving niet vastgelegd, deze wordt als het ware 'gestript'[7] voordat deze bij de signing service komt, zodat de signing service niet ziet welk testbewijs aan welk IP nummer is gekoppeld. VWS ziet dus niet de externe IP adressen, maar alleen het interne IP adres van de verwerker. Het strippen van het IP-adres gebeurt door Prolocation, dit is de verwerker van VWS. Het testresultaat zelf is versleuteld. Prolocation kan en mag de gegevens in het testresultaat niet zien. Op de servers van VWS wordt vervolgens de geboortedag en geboortemaand de eerste letter van de voornaam en de eerste letter van de achternaam van getest persoon verwijderd van het testresultaat. Vervolgens wordt de digitale handtekening van de Signing Service gezet en wordt

[6] 'Opgenomen' betekent in dit geval dat deze gegevens worden gerepresenteerd in een (voor mensen niet leesbare) QR code.

[7] Door een derde partij (Prolocation) worden deze (externe) IP adressen vervangen door een intern IP adres.

het testbewijs teruggestuurd naar de gebruiker. Dit testbewijs wordt in de app getoond in de vorm van een QR code.

- In de CoronaCheck Scanner app worden de volgende gegevens gepresenteerd:
    - Indicatie: 'Persoon beschikt over geldig negatief testbewijs' / 'Persoon beschikt niet over geldig negatief testbewijs'.

De scanner app van de controleur slaat van deze controles geen gegevens op, de app beperkt zich tot het tonen van de genoemde indicatie ('geldig negatief testbewijs'). De gegevens die verdwijnen van het scherm bij de eerstvolgende scan of anders uiterlijk na 180 seconden (dit is configureerbaar).

Bij de fysieke variant (buiten scope voor deze PIA) wordt in het testresultaat op dezelfde manier omgezet in het testbewijs. In het papieren testbewijs wordt bovendien een indicatie toegevoegd dat de QR code een papieren testbewijs is. Deze indicatie betreft een ja/nee indicatie of het een QR code is die als fysiek testbewijs dient. Dit is nodig omdat bij de digitale variant de QR code periodiek verandert om misbruik te voorkomen en bij de fysieke variant is dit niet mogelijk.

De scanner app wordt gebruikt voor zowel de digitale als fysieke testbewijzen.

3. Doeleinden van de beoogde gegevensverwerking

Het testbewijs is een nieuw middel in ontsluiten van de maatschappij uit een lockdown en kan samen met andere middelen worden ingezet (bijvoorbeeld afstand houden, dragen mondkapje). Een testbewijs laat zien dat iemand binnen de afgelopen periode negatief is getest. Doeleinde van CoronaCheck is dat een persoon bij toegang tot een bepaalde faciliteit aan de poort op digitale wijze kan laten zien dat hij of zij beschikt over een negatief testbewijs dat niet ouder is dan vastgestelde termijn van 40 uur.

4. Betrokken partijen

Bij de bespreking van de betrokken partijen in het onderstaande, wordt ingegaan op de verwerkingen die plaatsvinden binnen CoronaCheck. Andere verwerkingen die plaatsvinden door – bijvoorbeeld – de verstrekkers blijven buiten beschouwing. Zo zijn de artsen van de verstrekkers altijd wettelijk verplicht om testgegevens aan GGD te verstrekken als iemand positief test.

Partijen die testresultaten aanleveren ('verstrekkers') zijn eveneens betrokken partijen. CoronaCheck haalt op verzoek van de persoon bij hen de negatieve testresultaten op. Verstrekkers zijn de partijen die testen uitvoeren. Voor het gebruik van persoonsgegevens die zij vragen voor het uitvoeren van testen en het verstrekken van testresultaten (denk aan emailadres en/of nummer van smartphone) zijn zij zelfstandig verwerkingsverantwoordelijk. Op dit moment voorzien we de volgende betrokken partijen:

- Testcapaciteit die door SON wordt ingericht – deze Stichting zorgt (in nauwe samenwerking met Project Amsterdam, EZK, OCW) voor een versnelde uitrol van testcapaciteit naar een capaciteit

[8] Zie ook https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2021Z03637&did=2021D08036

[9] IT-DPIA ten behoeve van de SON IT platform, versie concept 0.95, d.d. 22 maart 2021

van 400.000 testen per dag in mei[8]. SON vervult de rol van verwerker[9], waarbij zij de rol van verwerkersverantwoordelijke ziet bij de verstrekker, de teststations.
- Fieldlabs als organisator van evenementen. Met Fieldlabs worden geen (persoons)gegevens uitgewisseld.

De CoronaCheck app is ontwikkeld door het ministerie van VWS. De Minister van VWS is verantwoordelijk voor de regie op de wijze waarop we uit de lockdown komen en de wijze waarop CoronaCheck daarvoor wordt ingezet. De Minister is daarmee opdrachtgever voor de ontwikkeling van de CoronaCheck en de CoronaCheck Scanner app

De minister van VWS is de verwerkingsverantwoordelijke voor de verwerkingen van persoonsgegevens die bij CoronaCheck worden gebruikt. Deze verantwoordelijkheid geldt voor de CoronaCheck app en de CoronaCheck Scanner app, de werking van de configuratie server en de Signing service. VWS stelt verder eisen aan de wijze waarop de testresultaten door de verstrekkers worden aangeleverd.

Controleurs – Iedereen met de CoronaCheck Scanner app kan het testbewijs controleren.

Personen – Op de smartphone van personen worden testresultaten en testbewijs opgeslagen.

5. Ontvangers

CoronaCheck toont alleen gegevens aan de geteste persoon: de persoon ontvangt via CoronaCheck testresultaten van de verstrekker. Dit resultaat wordt door de CoronaCheck app omgezet in een testbewijs.

De controleur scant met de CoronaCheck Scanner app de QR code in CoronaCheck. De controleur krijgt daarbij te zien of de persoon beschikt over een geldig negatief testbewijs door middel van een groen of een rood scherm in de scanner app. Groen betekent dat de persoon beschikt over een geldig negatief testbewijs. Rood betekent dat de persoon niet beschikt over een geldig negatief testbewijs.

6. Belangen bij de gegevensverwerking

De persoon is degene met het grootste belang bij het gebruik van CoronaCheck – deze kan kiezen of hij of zij een testbewijs wil gebruiken om toegang te krijgen tot een gekozen voorziening.

De controleur heeft een verplichting om enkel personen toe te laten tot het evenement die beschikken over een negatief testbewijs en hebben uit hoofde van die verplichting belang bij het doel waarvoor CoronaCheck wordt ontwikkeld.

VWS heeft een belang bij het gebruik van CoronaCheck. Dit belang betreft een maatschappelijk belang: dat CoronaCheck een effectief middel is om gecontroleerd uit de lockdown te komen.

[8] Zie ook https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2021Z03637&did=2021D08036

[9] IT-DPIA ten behoeve van de SON IT platform, versie concept 0.95, d.d. 22 maart 2021

7. Verwerkingslocaties

De middelen die nodig zijn voor het beheer van de CoronaCheck app (de configuratieserver en de Signing service) staan in Nederland bij leverancier Prolocation.

Alle andere activiteiten vinden plaats op de smartphone van de gebruiker. De controle van het testbewijs vindt plaats op de smartphone van de controleur.

8. Techniek en methode van gegevensverwerking

CoronaCheck ontvangt de testresultaten op basis van gestandaardiseerde interface / api, wat inhoudt dat het format van de gegevens die door de verstrekker moeten worden aangeleverd juist is. De verantwoordelijkheid voor de juistheid en actualiteit van de gegevens ligt bij de Verstrekker.

De conversie van testresultaat naar testbewijs vindt geautomatiseerd plaats waarbij het testresultaat wordt geconverteerd naar een QR code. Deze QR code is het testbewijs.

De controleur controleert met de CoronaCheck Scanner app het testbewijs. De controleur ziet of iemand beschikt over een geldig negatief testbewijs. Hier is alleen sprake van visuele raadpleging van de geldigheid van het testbewijs ('wel geldig testbewijs' / 'geen geldig testbewijs') Dit is een geautomatiseerde gegevensverwerking waarmee de QR-code wordt opgezet in een visueel leesbare indicatie van de geldigheid van het negatieve testbewijs.

Er is geen sprake van geautomatiseerde besluitvorming, als bedoeld in artikel 22, eerste lid, AVG omdat het besluit over al dan niet toelaten door een controleur wordt genomen.

9. Beveiliging

Bij het ontwerp van de infrastructurele beveiligingsmaatregelen voor de configuratieserver en de signing service van CoronaCheck is uitgegaan van niveau BBN2+ met de maatregelen uit het VIRBI. Daarnaast zijn aanvullende maatregelen getroffen om de beveiliging op te trekken naar het niveau van bescherming tegen het niveau Statelijke Actor, bijvoorbeeld bij de keuze van de toegepaste cryptografie.

In deze PIA wordt (in Bijlage D) volstaan met een korte beschrijving van de beveiligingsmaatregelen in CoronaCheck. Een meer gedetailleerde beschrijving is als losse bijlage beschikbaar.

10. Juridisch en beleidsmatig kader

In het proces van inladen van het testresultaat in CoronaCheck tot aan het lezen van het testbewijs door de controleur worden persoonsgegevens verwekt. Daarbij inbegrepen persoonsgegevens over de gezondheid van een persoon zoals bedoeld in de zin van artikel 9 AVG.

Een testbewijs valt onder gegevens over gezondheid, hetgeen in artikel 4, onderdeel 15, AVG is gedefinieerd als persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven.

Op grond van artikel 9, tweede lid, onderdeel a, AVG vormt de uitdrukkelijke toestemming van de betrokkene een doorbrekingsgrond van het verwerkingsverbod uit artikel 9, eerste lid, AVG. Deze grondslag is passend omdat de persoon bij de installatie van de app expliciet wordt gevraagd

kennis te nemen van de privacy voorwaarden en toestemming te geven voor de verwerking van deze gegevens.

11. Bewaartermijnen

Uitgangspunt is dat gegevens zo kort mogelijk worden bewaard. Er gelden verschillende bewaartermijnen voor de gegevens die worden gebruikt binnen CoronaCheck.

- De persoon kan via CoronaCheck een testbewijs genereren. Het testbewijs is maximaal 40[10] uur geldig (dit tijdstip van testen wordt door de verstrekker meegeleverd). Nadat het testbewijs zijn geldigheid heeft verloren, is deze automatisch onbruikbaar en wordt deze verwijderd. Mocht de persoon de app op dat met moment van vervallen van geldigheid moment niet aan hebben staan, dan wordt het testbewijs verwijderd, zodra de app wordt geopend.
- Een testbewijs is een afgeleide van het testresultaat. Het testresultaat wordt verwijderd uit CoronaCheck zodra het om wordt gezet in een testbewijs. Het testrultaat wordt ook direct verwijderd van de server van VWS nadat het is omgezet in een testbewijs.
- In de CoronaCheck Scanner app worden geen gegevens blijvend opgeslagen. De gegevens die worden getoond bij de controle (indicatie geldigheid testbewijs, eerste letter voornaam, eerste letter achternaam, geboortedag en geboortemaand) verdwijnen van het scherm bij de eerstvolgende scan of anders uiterlijk na 180 seconden (dit is configureerbaar).
- Het IP adres dat in de communicatie van en naar Configuratie Server en de Signing Service wordt gebruikt, wordt door de beheerder 7 dagen bewaard om bij incidenten deze te kunnen onderzoeken. Na deze 7 dagen worden deze automatisch verwijderd. VWS heeft geen toegang tot de Ip-adressen.

Het bewaren van de gegevens bij de verstrekker en bij SON is buiten scope van deze PIA.

[10] Maximale geldigheidsduur kan worden geconfigureerd.

B. Beoordeling rechtmatigheid gegevensverwerkingen

12. Rechtsgrond / Gebruik van bijzondere persoonsgegevens

De informatie die in het testresultaat, het testbewijs en door middel van de QR-code wordt getoond betreft persoonsgegevens in de zin van artikel 4, onderdeel 1, AVG. Daarbij geldt dat het ook bijzondere persoonsgegevens betreft, als bedoeld in art. 4, onderdeel 15 resp. art. 9, eerste lid, AVG. De informatie die door middel van de QR-code wordt getoond omvat de melding dat een persoon negatief getest is, en tot wanneer de betreffende testuitslag geldig is. Het gaat dan ook om gegevens over verleende gezondheidsdiensten waarmee informatie over de gezondheidstoestand wordt gegeven.

Het proces waarbij een QR-code wordt gegenereerd kwalificeert als een verwerking in de zin van artikel 4, onderdeel 2, AVG. Dit omdat, bij dit proces testresultaten worden verwerkt. Ook het uitlezen van de QR-code met behulp van de controle app kwalificeert als verwerking zoals bedoeld in de AVG.

Bij het uitlezen van de QR-code is sprake van een geautomatiseerde verwerking van (bijzondere) persoonsgegevens in de zin van artikel 4, onderdeel 2, AVG. Immers, het is de app die zorgt voor een vertaling van de QR-code naar een groen of rood scherm.

Wat betreft het aflezen van het groene of rode scherm door de controleur, kan naar analogie van het (huidige) standpunt van de AP betreffende het temperaturen van werknemers[11], worden beargumenteerd dat daarbij geen sprake is van een verwerking[12].

Op grond van artikel 9, tweede lid, onderdeel a, AVG vormt de uitdrukkelijke toestemming van de betrokkene een doorbrekingsgrond van het verwerkingsverbod uit artikel 9, eerste lid, AVG. Deze grondslag is passend omdat de persoon bij de installatie van de app expliciet wordt gevraagd kennis te nemen van de privacy voorwaarden en toestemming te geven voor de verwerking van deze gegevens. Hier wordt ook de nadruk gelegd op het vrijwillige gebruik van de app en de uitdrukkelijke toestemming als grondslag voor de verwerking.

13. Doelbinding

De gegevensverzameling binnen CoronaCheck is minimaal en bevat primair die gegevens ('drager is negatief getest' en 'geldigheidsinformatie') die nodig zijn om datgene te doen dat van CoronaCheck wordt verwacht: het mogelijk maken dat de gebruiker op digitale wijze negatief testbewijs kan tonen.
Daarmee biedt het middel een basisfunctionaliteit die kan worden ingezet op het moment dat er beleidsdoelstellingen bij zijn die de inzet van dit middel legitimeren.

De geboortedag en -maand, eerste letter voornaam en eerste letter achternaam worden gebruikt om de persoon te laten zien dat het testresultaat dat is opgehaald ook daadwerkelijk het eigen testresultaat is.

[11] Zie: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/corona/temperaturen-tijdens-corona
[12] Wel moet worden opgemerkt dat AP verschillende keren haar standpunten over het opnemen van de temperatuur heeft aangepast. In zoverre past wat dat betreft vooralsnog een voorbehoud.

14. Noodzaak en evenredigheid

Het ministerie van VWS werkt er hard aan de samenleving verantwoord te openen. Toegangstesten is daar een onderdeel van. Met toegangstesten kunnen sociale, culturele en sportieve locaties in tijden van corona sneller verantwoord open. Met een negatief testresultaat krijgen bezoekers van deze locaties toegang. Met CoronaCheck kunnen bezoekers digitaal hun negatieve testbewijs tonen om toegang te krijgen tot locaties..

Bij het ontwerp van CoronaCheck is het uitgangspunt geweest dat het gebruik van persoonsgegevens tot een minimum moest worden verwerkt. Het testbewijs zelf geeft de minimaal benodigde informatie 'de drager hiervan beschikt over een geldig negatief testbewijs'. Hoewel de app vrij te downloaden is in de appstores kunnen enkel personen die deelnemen aan de pilots hun testbewijs inladen in de app. Andere testaanbieders zijn nog niet aangesloten.

Het gebruik van de eerste letters van voornaam en achternaam en de geboortedag en – maand van persoon zorgt er bijvoorbeeld voor dat een persoon kan controleren dat het juiste testresultaat wordt opgeslagen op de eigen smartphone. Deze gegevens worden niet opgenomen in het testbewijs en kunnen daardoor ook niet uitgelezen worden met gebruik van de CoronaCheck Scanner app.
Op deze wijze is het gegevensgebruik minimaal en toegespits op het doel van de verwerking. Door CoronaCheck nu naast het fysieke traject in te zetten kan in een gecontroleerde omgeving getoetst worden. In CoronaCheck zijn bovendien extra securitymaatregelen toegepast die op papier niet mogelijk zijn. Bijvoorbeeld het automatisch verwijderen van de gegevens zodra die niet meer noodzakelijk zijn of zodra het testbewijs zijn geldigheid verliest.

15. Rechten van betrokkene

Het testresultaat / het testbewijs staan op de smartphone van de persoon. Niemand, behalve de persoon zelf, weet dat hij of zij over een testbewijs beschikt.

De gegevensstroom is zodanig ontworpen dat VWS niet weet wie er op welk moment over een geldig negatief testbewijs beschikt.

VWS kan de betrokkene niet identificeren. De techniek die wordt gebruikt voor de cryptografische handtekening is dusdanig dat er geen 1:1 relatie te leggen is met een gescande QR, ook niet met een kopie van (alle) data uit haar signing service.

De source code en alle technische informatie openbaar beschikbaar via Github.

De personen worden geïnformeerd over de veiligheid en betrouwbaarheid van CoronaCheck. Deze informatie wordt verstrekt in de vorm van een privacy statement dat de persoon bij het installeren van de app leest. De persoon wordt nadrukkelijk gevraagd kennis te nemen van het privacy statement en dit te bevestigen.

C. Beschrijving en beoordeling risico's voor de betrokkenen

16. Generieke risico's inzet van testbewijs

In een PIA is het noodzakelijk om stil te staan bij de risico's van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen. Het is hierbij noodzakelijk om daarbij in ieder geval in te gaan op:

- de negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen;
- de oorsprong van deze gevolgen;
- de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;
- de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.

17. Specifieke risico's CoronaCheck

In deze PIA worden de specifieke risico's beschrijven die van toepassing zijn op CoronaCheck als middel. Deze risico's zijn opgenomen in de bijlage.

D. Beschrijving voorgenomen maatregelen

In onderdeel D wordt bezien welke maatregelen kunnen worden getroffen om de in onderdeel C erkende risico's te voorkomen of te verminderen. Welke maatregelen in redelijkheid worden getroffen is een belangenafweging van de wetgever of verwerkingsverantwoordelijke. Voor dit onderdeel van de PIA is, als het gaat om beveiligingsmaatregelen, expertise over informatiebeveiliging belangrijk. In deze bijlage wordt ***op hoofdlijnen*** beschreven hoe de cruciale gegevens binnen CoronaCheck zijn beveiligd.

18. Wat gebeurt bij 'omzetting' van testresultaat naar testbewijs, hoe werkt de cryptografie

Nadat de persoon een coronatest heeft gedaan bij de aangewezen verstrekker, kan hij of zij een ondertekend testresultaat op te halen en in de app laden. Dit resultaat is ondertekend met een private tekensleutel van de verstrekker.

Voor het ondertekenen van het testresultaat vanuit de signing service wordt gebruik gemaakt van een bestaande implementatie van anoniem ondertekende gegevens volgens het Idemix-protocol. Dit protocol maakt gebruik van een Camenisch-Lysyanskaya (CL) handtekening in combinatie met Zero Knowledge Proofs (ZKP).

Deze CL handtekening wordt elke keer dat een testbewijs gegenereerd wordt gerandomiseerd om ervoor te zorgen dat de handtekening niet naar een individu herleidbaar is. Met andere woorden: de handtekening wordt gerandomiseerd, ofwel "door elkaar gehusseld". Door een Zero Knowledge Proofs (ZKP) toe te voegen, kan de app zien dat de gerandomiseerde handtekening geldig blijft.

In de ZKPs wordt ook de huidige tijd opgenomen, zodat het testbewijs beperkt geldig is.

19. Wat gebeurt bij het scannen van de QR door de controleur en wat ziet deze?

De controleur scant het testbewijs (de QR-code) van een persoon. De ondertekening van de QR-codewordt gecontroleerd door de sleutel die in de CoronaCheck Scanner app aanwezig is. Vervolgens wordt berekend of de handtekening en de ZKPs geldig zijn met behulp van de publieke tekensleutel van VWS. Ook wordt gecontroleerd of het tijdstip dat in de ZKPs is opgenomen, overeenkomst met de huidige tijd met een marge van ongeveer 45 seconden (omdat het handtekening elke anderhalve minuut ververst wordt).

De controleur ziet dus: 'geldig negatief testresultaat' (groen scherm in de scanner app), of 'niet geldig negatief testresultaat' (rood scherm in de scanner app). In het laatste geval worden daarbij de mogelijke oorzaken genoemd, vooral om te voorkomen dat de controleur er niet automatisch van uitgaat dat de persoon Corona heeft. De controleur kan de persoon niet herkennen aan de uniekheid van de handtekening, omdat deze steeds gerandomiseerd wordt.

20. Welke maatregelen nemen we om fraude/misbruik te voorkomen?

We nemen natuurlijk tal van maatregelen om fraude te voorkomen. Een paar voorbeelden:

- De QR-code maar beperkt geldig is; na een aantal minuten 'rouleert' deze.
- In de app worden (bewegende) echtheidskenmerken opgenomen die handmatig en eventueel automatisch gecontroleerd kunnen worden. Deze kenmerken zijn na te maken, maar het maakt het onmogelijk om bijvoorbeeld een screenshot door te sturen of een real-time video verbinding van het ene scherm naar het andere te gebruiken. Daarmee verhoogt het de barrière voor fraude.

21. Hoe wordt de communicatie van en naar CoronaCheck beveiligd

CoronaCheck maakt gebruik van transport encryptie (TLS) voor alle verbindingen in combinatie met certificaten van de Nederlandse Public Key Infrastructure (PKI) Overheid en pinning. Dit laatste betekent dat de app alleen contact maakt met servers welke certificaten hebben die uitgegeven zijn door de PKI Overheid.

Daarnaast worden belangrijke configuratie bestanden (waarin bijvoorbeeld de werking van de app beïnvloed kan worden) digitaal getekend. Ook hiervoor worden (alleen) certificaten gebruikt (en geaccepteerd) die onder auspiciën van de Nederlandse haar PKI Overheid uitgegeven zijn met een aantal additionele verificaties. Dit mechanisme wordt zowel gebruikt voor de connecties van de app, alsmede voor de uitslag berichten van de GGD en commerciële partijen. Deze laatsten dienen op een expliciete lijst te staan alvorens geaccepteerd te worden.

Bijlage

Risico: Misbruik van testbewijzen

Het is voor mensen aantrekkelijk om te kunnen beschikken over een negatief testbewijs. Dit kan het aantrekkelijk maken om misbruik te willen maken van een onecht testbewijs of andermans testbewijs.
Impact: groot, als mensen het testbewijs niet vertrouwen, wordt de app minder gebruikt, wat ten laste gaat van het doel **Kans:** groot, mensen zullen proberen hoe makkelijk misbruik mogelijk is. Journalisten en hackers kunnen ook de uitdaging zien om de grenzen van het gebruik te verkennen **Risico:** hoog
Maatregelen: Het testbewijs is zodanig ontworpen dat misbruik wordt ontmoedigd. Zo kunnen testbewijzen niet zomaar worden gekopieerd of doorgestuurd. Zo zijn maatregelen genomen om grootschalig misbruik door het kopiëren of delen van QR codes met anderen te bemoeilijken of onmogelijk te maken, bijvoorbeeld door het toevoegen va een bewegende animatie. CoronaCheck is niet ontworpen om alle scenario's onmogelijk te maken waarbij mensen samenspannen om elkaars testbewijs te gebruiken. In de versie waar deze PIA betrekking op heeft, is nog geen sprake van een beperkte set aan identificerende gegevens (eerste letter voornaam en achternaam, geboortedag en – maand) waartegen bij de controle aan de deur de identiteit kan worden gecontroleerd. Het is in het belang van de persoon en van de organisator van een activiteit of voorziening om te zorgen dat het testbewijs zorgvuldig wordt gebruikt. Immers: als een gecontroleerde opheffing van de lockdown alsnog leidt tot een oplaaiende besmetting, zal de lockdown opnieuw worden verzwaard. Het frauderisico kan nog verder worden beperkt door maatregelen die los staan van CoronaCheck en waarbij het gebruik van gegevens van de persoon niet nodig is. Denk daarbij aan het monitoren van de besmettingsgraad na bezoek. Ook een zorgvuldige communicatie helpt, door mensen op hun eigen verantwoordelijkheid te wijzen dat in dit stadium de experimenten worden verstoord als niet op een passende manier gebruik wordt gemaakt van CoronaCheck.
Beperking / uitdaging: In het gebruik bestaat een afhankelijkheid van 2 actoren: de persoon zelf en de controleur. Als beide CoronaCheck verantwoord gebruiken, is het frauderisico beperkt.
Impact na maatregelen: Midden, de eenvoud om te frauderen kan ten laste gaan van de geloofwaardigheid van CoronaCheck. **Kans na maatregelen**: Kans op incidenteel misbruik is hoog. Er zullen zeker mensen zijn die dit toch willen uitproberen. **Risico na maatregelen**: Hoog.

Risico: Overheid of private partij kan gedrag van persoon volgen

Het digitale testbewijs wordt aangeboden via een app die door Ministerie VWS wordt gemaakt, op basis van een testresultaat die een teststation wordt gemaakt en een scan van

het testbewijs die aan de poort wordt bekeken. Dit kan leiden tot de vrees dat deze partijen kunnen volgen wie er een negatief testbewijs heeft ontvangen en waar iemand is geweest.
Impact: groot, als mensen het CoronaCheck niet vertrouwen, wordt de app minder gebruikt, wat ten laste gaat van het doel **Kans:** groot, een deel van de bevolking vertrouwt niet bij voorbaat alle middelen die de overheid aanbiedt **Risico:** hoog
Maatregelen: CoronaCheck is zodanig ontworpen dat dit niet het geval is en dat mensen niet worden gevolgd. Zo weet: • het teststation wel aan wie zij het testresultaat moet geven, maar niet of het testresultaat wordt gebruikt voor een testbewijs en of dit daarna wordt gebruikt om toegang te krijgen tot een evenement of locatie; • het ministerie van VWS niet wie een testbewijs heeft gegenereerd, of waar dit voor wordt gebruikt; • de controleur niet wie er allemaal toegang heeft gekregen. Tijdens het signing proces waarbij het test resultaat omgewisseld wordt voor het testbewijs 'ziet' VWS eenmalig de (zeer beperkte) informatie in het testresultaat. De inhoud van wat wordt getekend wordt echter niet vastgelegd. Het digitale testbewijs wordt daarbij gerandomiseerd om ervoor te zorgen dat de handtekening niet naar een individu herleidbaar is, door de handtekening te randomiseren, ofwel "door elkaar te husselen".
Beperking / uitdaging: Bij de fysieke variant is dit randomiseren technisch niet mogelijk omdat papier statisch is. Als VWS en de controleur de handtekening zouden bijhouden, dan zouden ze bij een tweede keer dat de handtekening wordt gebruikt, kunnen herkennen dat het testbewijs dat met deze handtekening is getekend, hetzelfde is. In de praktijk geldt dat VWS de testbewijzen of handtekeningen niet bewaart en dat voor Controleurs een verbod geldt om kopieën van testbewijzen of handtekeningen te bewaren.
Impact na maatregelen: Hoog. De maatregelen hebben vooral tot doel om de kans te minimaliseren. **Kans na maatregelen:** Kans is bij het digitale testbewijs laag. Bij het fysieke testbewijs is de kans nog steeds laag, maar zijn er scenario's denkbaar waarbij kan worden gevolgd waar iemand het testbewijs heeft gebruikt. **Risico na maatregelen:** Laag

Risico: CoronaCheck houdt bij wie een negatieve test heeft en wie niet

Alle testresultaten en testbewijzen moeten straks bij gebruikers in de CoronaCheck app worden opgeslagen. Kan de overheid dan bijhouden wie negatief is getest en wie niet
Impact: groot, als mensen het testbewijs niet vertrouwen, wordt de app minder gebruikt, wat ten laste gaat van het doel **Kans:** groot, een deel van de bevolking vertrouwt niet bij voorbaat alle middelen die de overheid aanbiedt **Risico:** hoog
Maatregelen: Het negatieve testresultaat wordt verstrekt door de partij die heeft getest (SON).

CoronaCheck bewaart alleen het negatieve testbewijs, voor zolang als dit geldig is. Als de geldigheidstermijn is verstreken, dan wordt het negatieve testbewijs verwijderd. Een testresultaat blijft altijd alleen op de drager van de persoon. Daarmee is dit risico niet van toepassing. Er is geen sprake van centrale opslag van testresultaten of testbewijzen. De source code van CoronaCheck is openbaar en er wordt transparant gecommuniceerd over CoronaCheck. Zo kan iedereen zelf zien dat er geen sprake is van centrale opslag en dat de overheid niet bijhoudt wie negatief is getest en wie niet.
Beperking / uitdaging: Geen
Impact na maatregelen: Laag. **Kans na maatregelen:** Laag. Er is geen sprake van centrale opslag van testresultaten of testbewijzen en VWS kan niet zien wie er beschikt over een negatief testbewijs. **Risico na maatregelen:** Laag

Risico: Een controleur misbruikt de gegevens uit mijn digitale testbewijs

Een controleur die bij een poort testbewijzen controleer ziet van een groot aantal mensen het testbewijs en dus veel gegevens
Impact: laag, de controleur ziet geen gegevens en weet enkel dat degene die de QR code presenteert beschikt over een geldig negatief testbewijs **Kans:** laag. Het leeuwendeel van de controleurs is betrouwbaar, maar een deel kan in de verleiding komen **Risico: laag**
Maatregelen: CoronaCheck geeft alleen aan dat iemand beschikt over een geldig negatief testbewijs. De controleur weet met de controle app dus alleen of de drager ervan (degene die het testbewijs op de smartphone presenteert) beschikt over een geldig negatief testbewijs. De controle app die de controleur heeft, slaat ook geen gegevens op. CoronaCheck vertelt de controleur niet wie een persoon is. De gegevens verdwijnen vanaf de scanner app van de controleur nadat een volgend bewijs is gescand of uiterlijk na 180 seconden.
Beperking / uitdaging: Niet van toepassing
Impact na maatregelen: Laag **Kans na maatregelen:** Laag **Risico na maatregelen:** Laag

Risico: Verlies van smartphone

Als de persoon zijn of haar smartphone verliest op het moment dat het testresultaat al is gedownload, dan kan deze persoon niet meer het testresultaat gebruiken om een testbewijs te maken en te presenteren.

Impact: Klein, het gaat om individuele gevallen **Kans:** Redelijk **Risico:** Klein
Maatregelen: Als de persoon met een nieuwe smartphone zich bij de verstrekker authenticeert en een testresultaat ophaalt, kan men in de CoronaCheck app alsnog een testbewijs genereren.
Beperking / uitdaging: Als men niet tijdig over een nieuwe telefoon beschikt en/of zich niet bij de verstrekker kan authenticeren met CoronaCheck. De persoon heeft tijdens de pilots altijd nog de mogelijkheid om gebruik te maken van het fysieke testbewijs.
Impact na maatregelen: Midden, misbruik kan ten laste gaan van de maatschappelijke acceptatie van het testbewijs. **Kans na maatregelen:** Kans op structureel misbruik is laag. **Risico na maatregelen:** Laag

Risico: VWS heeft inzicht in testresultaten en testbewijzen

VWS tekent wel de testbewijzen door de signing service, maar geeft aan geen inzicht in de inhoud van testresultaten of testbewijzen. Hoe weet ik dat zeker
Impact: Groot **Kans:** Redelijk **Risico:** Redelijk
Maatregelen: In de Signing service is geen opslagcapaciteit / database beschikbaar om de getekende bewijzen te kunnen opslaan of inzien. Ook op basis van de code (github) kan worden vastgesteld dat VWS hier niets mee doet.
Beperking / uitdaging: Dit risico treedt alleen op als VWS bewust de code aanpast en het principe van transparantie laat varen.
Impact na maatregelen: Laag **Kans na maatregelen:** Laag **Risico na maatregelen:** Laag

Incident: Door de telefoon door te geven is kleinschalige fraude mogelijk.
Kans: Medium.
Impact: Laag. In een enkel geval heeft dat weinig impact op de verwerking van persoonsgegevens
Risico: Laag.

Incident: Het live doorstreamen van het telefoonscherm
Kans: Low.
Impact: Hoog. Deze aanval is schaalbaar
Risico: Medium.
Mitigatie: De QR-code bevat zoveel data dat het niet goed te streamen is zonder speciale voorbereidingen.

Incident: Er wordt een foutief testresultaat verklaring aan VWS aangeleverd ter ondertekening.
Kans: Laag.
Impact: Laag.
Risico: Laag

Mitigatie: Geen. VWS test zelf geen mensen maar zet enkel het aangeleverde testresultaat van een gecontroleerde testaanbieder onder verantwoordelijkheid van SON om in een testbewijs.

Incident: Testresultaat verklaring VWS is valselijk ondertekend
Kans: Laag. Cryptografische borging in de verificatie app maakt dit zeer complex om uit te voeren.
Impact: Hoog. Als dit lukt dan zou een aanval schaalbaar zijn.
Risico: Medium.
Mitigatie: Intensieve controle op systemen en de processen bij de testbedrijven.

Incident: Gebruiker heeft testresultaat verklaring VWS aangepast
Kans: Hoog, dit zal men willen gaan uitproberen
Impact: Laag/Geen
Risico: Laag/Geen
Mitigatie: Wijzigingen worden gedetecteerd door het niet kunnen valideren van de VWS ondertekening. De gebruiker heeft geen toegang tot de private key om een nieuwe valide signature te produceren over de gewijzigde testresultaat-data. De nieuwe QRcode zal afgewezen worden door de Corona Scanner app

Incident: QR-code is niet te scannen (valse foute qrcode in slechte resolutie b.v.)
Kans: Medium
Impact: Laag
Risico: Laag
Mitigatie: Een onjuiste QRcode of niet-scanbare QRcode wordt altijd afgewezen, persoon zou geweigerd moeten worden door controleur

Incident: Incorrecte controle procedure
Kans: Medium, 5.1.2i Toelichting
5.1.2i Toelichting
Impact: Medium, wanneer er controleurs zijn die per abuis of doelbewust personen toegang geven zonder geldig testbewijs, bestaat de kans dat een potentiële virusdrager in aanraking komt met een grote groep mensen
Risico: Laag, onbewust foutieve handelingen zullen snel gedetecteerd worden door escalatie van gebruiker en/of sociale controle. Bewust misbruik bijvoorbeeld door omkoping zal vooral kleinschalig zijn door de pakkans en dat men deze mogelijkheid niet aan de grote klok zal hangen
Mitigatie: Heldere instructies en infographics voor controleurs, eenvoudig te gebruiken Corona Scanner app. Misbruik of onjuist gebruik strafbaar stellen. Goede communicatie over de noodzaak van correct en integer handelen

Incident: Gebruiker heeft verkeerde app gedownload
Kans: Medium, zoeken op “Coronacheck” toont niet altijd direct de officiële Rijksoverheid app als eerste zoekresultaat
Impact: Laag
Risico: Laag
Mitigatie: Op te lossen door helpdesk, vooraf goede herkenbaarheid door branding van de app en communicatie/reclame daarover (PR en promo)

Incident: Er worden screenshots van de app gestreamed vanaf een ander toestel
Kans: Laag. Technisch goed mogelijk, maar voor veel mensen niet eenvoudig toepasbaar.
Impact: Laag. Je kunt hier niet een grote groep mensen mee bedienen. Waarschijnlijker dat er een of twee mensen mee worden bediend.
Risico: Laag.

Mitigatie: Op lossen door persoonsgegevens in de QR-code op te nemen.

Incident: Iemand stuurt een screenshot met QR door, waardoor meerdere kopieën van dezelfde test worden misbruikt.
Kans: Hoog. Het is kinderlijk eenvoudig te executeren. Het is ook mogelijk dezelfde QR-code aan meerdere mensen te verstrekken.
Impact: Medium. Er kunnen kwaadwillenden daarmee ongetest naar het evenement. De verwachting is niet dat dit zeer massaal gebeurt.
Risico: Medium.
Mitigatie: Op lossen door persoonsgegevens in de QR-code op te nemen.

Incident: Er komt een website om QR-codes uit te wisselen of deze te bestellen.
Kans: Medium. Het opzetten kost tijd en inspanning. Daarnaast zal er marketing moeten worden gedaan.
Impact: Medium. Mensen die dit doen lopen een relatief hoge pakkans. Er kunnen kwaadwillenden daarmee ongetest naar het evenement. De verwachting is niet dat dit zeer massaal gebeurt.
Risico: Medium.
Mitigatie: Op lossen door persoonsgegevens in de QR-code op te nemen.