IT en kwaliteitseisen ten behoeve van aan te sluiten testaanbieders

Informatiedocument
Versie 1.5 - 6 April 2021

Inhoudsopgave

Samenvatting

DIT DOCUMENT

Stichting Open Nederland (hierna: SON) heeft als doel het (doen) realiseren van COVID-19 testcapaciteit in een netwerk van teststraten verspreid over heel Nederland.

Dit document geeft inzicht in de **rollen en verantwoordelijkheden** van SON ten opzichte van meerdere aanbieders van teststraten op de volgende onderdelen; functioneel, interfaces en privacy & security.

VERANTWOORDELIJKHEDEN

Testaanbieders zijn verantwoordelijk voor:

- afspraakbevestiging naar de burger,
- het testen,
- de testuitslag verzenden naar de burger,
- aansluiting met VWS CoronaCheck app ten behoeve van het genereren van een testbewijs
- melding naar de GGD van positieve resultaten.

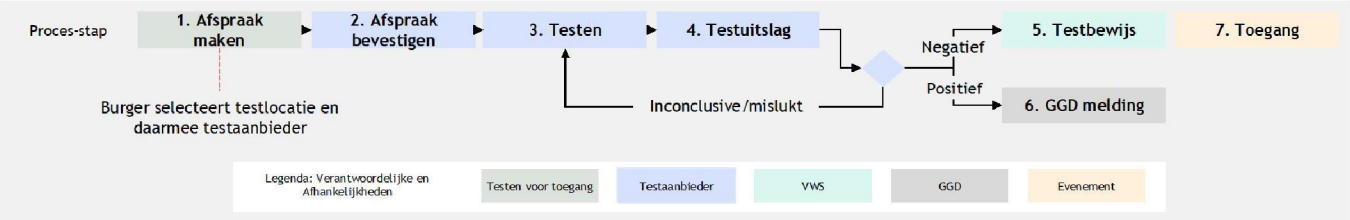
SON is verantwoordelijk voor :

- Use cases met betrekking tot landingspagina en afspraak maken.
- Coördinatie van contact van testaanbieders met VWS, GGD en overige partijen.

PRIVACY & SECURITY

SON heeft een *kaderstellende* en *controlerende* rol ten aanzien van privacy- en securitynormen

Testaanbieder dient te voldoen wet- en regelgeving, zoals de (beveiligings)eisen uit NEN7510/7512/7513, en wetgeving voor verwerking van medische persoonsgegevens.



1. Aanleiding & doel

1. Aanleiding en doel

DOEL

Stichting Open Nederland (hierna: SON) heeft als doel het (doen) realiseren van COVID-19 testcapaciteit in een netwerk van teststraten verspreid over heel Nederland.

SCOPE

Tot de scope behoort het (doen) realiseren van de IT voor het end-to-end proces, bestaande uit:

- Capaciteitsplanning (strategisch / tactisch)
- Beheren van het netwerk van teststraten (toevoegen, verwijderen)
- Inplannen van afspraken door de burger
- Ondersteuning van het testproces in de teststraat (inclusief koppeling met GGD)
- Koppeling aan de CoronaCheck app van VWS
- Leveren van managementinformatie over aantallen afspraken en uitgevoerde tests

AANLEIDING

- Het organiseren van operationele testcapaciteit en de daarvoor benodigde teststraten wordt verzorgd door externe partijen. SON wil verschillende aanbieders van teststraten de mogelijkheid geven om testcapaciteit aan te bieden.
- Daarbij wil SON het mogelijk maken voor aanbieders van teststraten om aan te sluiten op het afspraken portaal zoals dat door SON wordt aangeboden via Testenvoortoegang.nl.
- Aanbieders van teststraten kunnen daarbij in principe een eigen teststraatapplicatie gebruiken, welke voldoet aan de eisen van SON rondom technologie, security, privacy & confidentialiteit.

INHOUD

- De **rollen en verantwoordelijkheden** van SON ten opzichte van meerdere aanbieders van teststraten op de volgende onderdelen; functioneel, interfaces en privacy & security.
- Lifecycle procesflow teststraatapplicatie

2. Rollen en verantwoordelijkheden

2. Rol SON – Opdracht

PROJECTSTRUCTUUR

Het voorbereiden, opzetten en uitwerken van de projectstructuur: de projectstructuur bestaat onder meer uit het inrichten van afname- en testcapaciteit verdeeld over het land. Hierbij kunnen testbewijzen gegenereerd worden die gebruikt kunnen worden voor toegang tot activiteiten in spoor 2a;

END2END IT-PLATFORM

Het voorbereiden en ontwikkelen van een end2end IT-platform waarbij afspraken kunnen worden gemaakt, testuitslagen kunnen worden gegenereerd en vastgelegd, positieve testuitslagen kunnen worden doorgegeven aan onder andere Coron-IT, negatieve uitslagen worden omgezet in een al dan niet digitaal testbewijs, er wordt voldaan aan de NEN7504, alles privacy-proof wordt ingericht en indien dit wettelijk noodzakelijk is data kan worden bewaard conform de WGBO (waarbij indien wettelijk nodig een medisch dossier kan worden ingericht met minimale gegevens) waarbij Partijen als uitgangspunt hebben dat het gebruik van Coron-IT gebeurt onder de verantwoordelijkheid van de GGD-en;

TESTCAPACITEIT

Het (doen) realiseren van een testcapaciteit voor het doen uitvoeren van covid-19 tests in een netwerk van locaties verspreid over heel Nederland en de administratieve ondersteuning hiervan oplopend tot 400.000 tests per dag;

UITVOERINGSTOETSEN

Het organiseren van uitvoeringstoetsen al dan niet aan de hand van evenementen waar de uitgifte, (ver)werking en toepassing van een al dan niet Low-Tech testbewijs en de werking van het IT-platform kan worden getest.

2. Rol SON - Verantwoordelijkheden

1. KADER STELLEND

SON zal in lijn met de opdracht die zij van VWS heeft gekregen, kaders stellen aan teststraat aanbieders die zich bij SON willen aansluiten.

Daarbij zijn allereerst wet en regelgeving het uitgangspunt, maar zullen er door SON specifieke eisen gesteld worden aan technologie die wordt ingezet op de teststraten en de inrichting van systeem en proces controls ten aanzien van security, privacy & confidentiality.

2. CONTROLEREND

SON zal bij onboarding en periodiek, toetsen of teststraat aanbieders voldoen aan de onder 1. genoemde kaders.

3. UITVOEREND

SON zal zelf een platform beheren voor het beheren van capaciteit en het aansluiten van teststraten. Daarnaast zal SON het afsprakenportaal beheren.

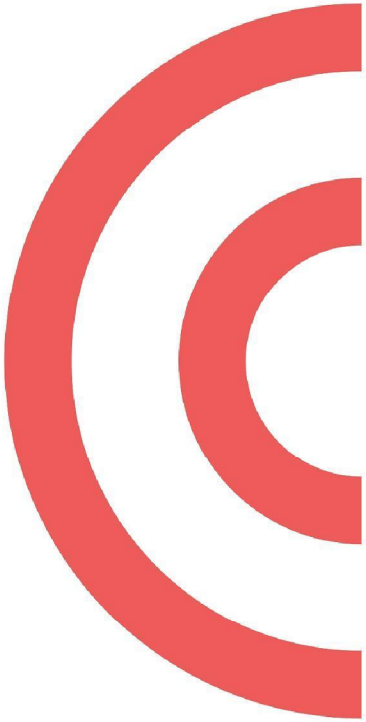
SON kan tot op zekere hoogte teststraat aanbieders ondersteunen om aan de onder 1. genoemde kaders te voldoen. Hierbij ligt de opdracht en het initiatief bij de testaanbieders.

ROLLEN

De rollen en verantwoordelijkheden zijn onder verdeeld in:

1. Functioneel beheer (slide 8)
2. Componenten en inrichting van interfaces (slide 15)
3. Privacy en security (slide 25)

2. Rollen en verantwoordelijkheden



2.1.1 High-level Procesflow

Per Use case is bepaald wie de verantwoordelijkheid draagt voor functioneel beheer. De testaanbieder dient er zelf voort te zorgen dat er een beheermogelijkheid is voor onderstaande use cases die niet onder SON vallen:

TESTAANBIEDERS

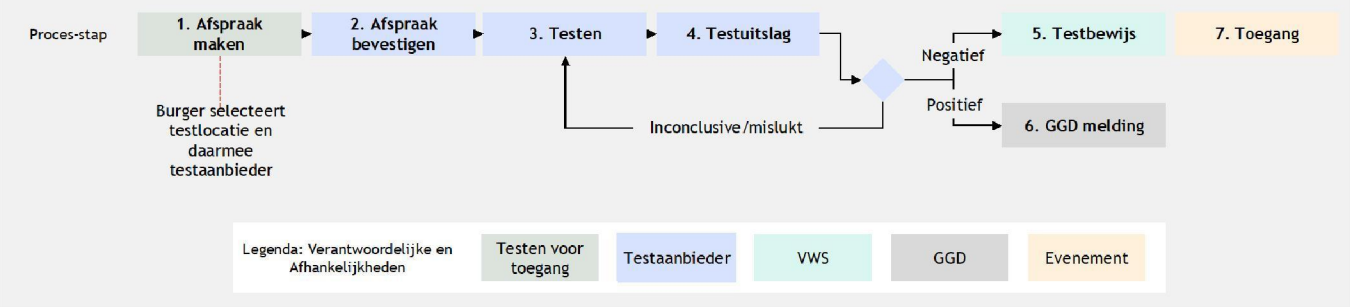
Testaanbieders zijn verantwoordelijk voor:

- afspraakbevestiging naar de burger,
- het testen,
- de testuitslag verzenden naar de burger,
- aansluiting met VWS CoronaCheck app ten behoeve van het genereren van een testbewijs
- melding naar de GGD van positieve resultaten.

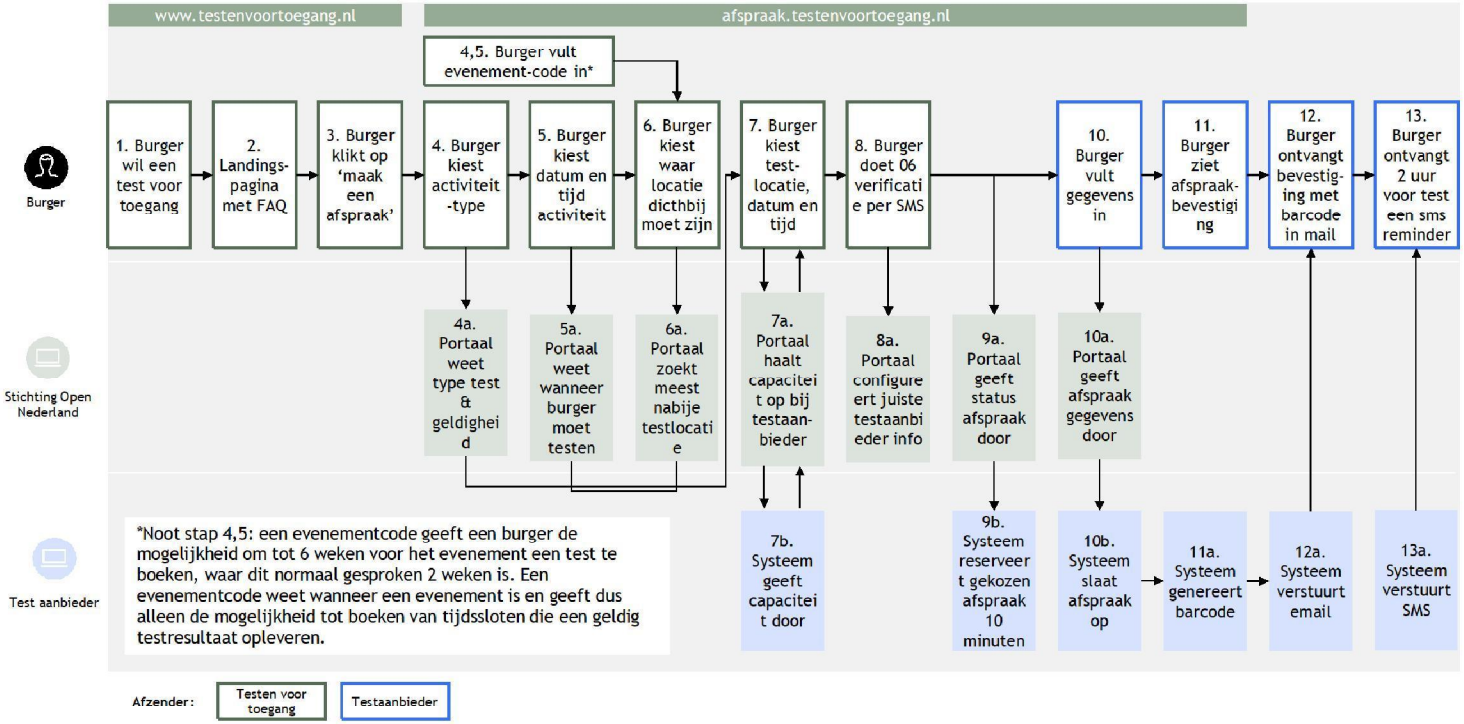
STICHTING OPEN NEDERLAND

SON is verantwoordelijk voor use cases met betrekking tot landingspagina en afspraak maken.

Coördinatie van contact van testaanbieders met VWS, GGD en overige partijen.



2.1.2 Procesflow I afspraak maken



2.1.3 Procesflow I afspraak maken toelichting

BEHEER

SON is verantwoordelijk voor het beheer van het afsprakenportaal en de business regels daarin, in afstemming met VWS.

De testaanbieder is verantwoordelijk voor het aanleveren van beschikbare capaciteit per locatie, per tijdslot en voor de afspraakbevestiging (per mail en sms) naar de burger.

PERSOONSGEGEVENS

De testaanbieder is verwerkings-verantwoordelijk voor de verwerking van (medische) persoonsgegevens in de zin van de AVG.

SON verwerkt in het afsprakenportaal persoonsgegevens ten behoeve van de testaanbieder. Vanaf stap 8 is de testaanbieder afzender van informatie naar de burger (in een blauw kader weergegeven).

AFSPRAKENPORTAAL

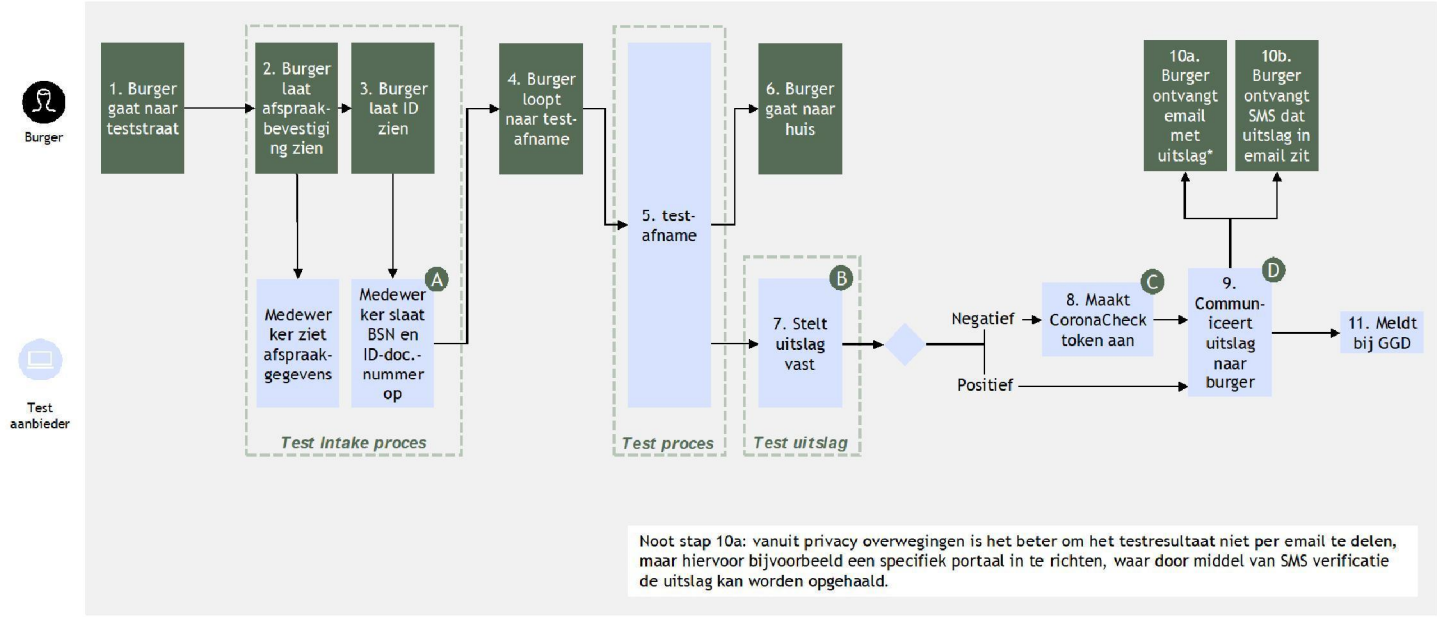
Vanaf stap 8 wordt automatisch geconfigureerd door het afsprakenportaal:

- het privacy statement van testaanbieder,
- logo van testaanbieder,
- de algemene voorwaarden testaanbieder (stap 10), SMS (stap 12) en
- email (stap 11) vanuit testaanbieder.

MAIL EN SMS

De testaanbieder dient een mailserver te hebben, waarmee noreply@[naam testaanbieder].nl emailberichten kunnen worden getriggerd. De emailberichten kennen een standaard layout welke wordt vastgesteld door SON, maar afzender is duidelijk de testaanbieder (logo, helpdesk gegevens testaanbieder etc.). Daarnaast zorgt de testaanbieder voor een SMS dienst, waarmee noreply SMS verzonden wordt (stap 13)

2.1.4 Procesflow I testen



2.1.5 Procesflow I testen toelichting

De testaanbieder is is end-to-end verantwoordelijk voor het testproces. SON schrijft niet voor hoe dit proces er exact uit moet zien. Best practice voorbeelden zijn beschikbaar op aanvraag. Er zijn wel een aantal requirements aan het proces, waar in de procesflow hieronder aandacht op gevestigd wordt:

A Als zorgaanbieder moet de testaanbieder op grond van de wet een medisch dossier aanleggen. Als de burger zich voor de eerste keer tot de testaanbieder wendt, moet de testaanbieder de identiteit controleren en het BSN en documentnummer van het identificatiebewijs vastleggen. Als een burger geen BSN heeft, moet postcode en huisnummer worden vastgelegd.

B De uitslag wordt op de teststraat vastgesteld. De testaanbieder is in alle gevallen verantwoordelijk om het resultaat te communiceren met de burger.

C Voor het aanmaken van het testbewijs is een token nodig van de CoronaCheck app. Dit token kan worden opgehaald door een API koppeling met CoronaCheck app van VWS. SON faciliteert testaanbieders in het veilig aansluiten op de infrastructuur met kennis en eventueel met dienstverlening op specifieke gebieden, zoals het aanvragen van een PKI certificaat.

D Uitslagenmail wordt verzonden door testaanbieder, met in acht naming van het gestandaardiseerd template, waarin uitdrukkelijk ruimte is voor eigen logo en invulling.

2.1.6 Functioneel Beheer

Per Use case is bepaald wie de verantwoordelijkheid draagt voor functioneel beheer. De testaanbieder dient zelf te zorgen dat beheermogelijkheid er is voor onderstaande use cases die niet onder SON vallen:

1. TESTAANBIEDER

- Support desk burgers vanaf afspraakbevestiging
- Identity management voor teststraatapplicatie (accounts, rollen en rechten)
    - Beheer
    - Teststraatmedewerker
    - Support desk teststraatmedewerkers
    - Support desk burgers vragen mbt testen
- Aanmaken / verwijderen locaties
- Configureren openingstijden en capaciteit (per tijdslot) van teststraatlocatie(s) - note: dit is input voor afsprakenportaal
- Afspraakbevestiging opnieuw versturen
- Uitslag email opnieuw verzenden
- GGD melding bij positieve uitslag
- Management rapportage naar SON conform document *Management rapportage-eisen Data & Informatie*

2. STICHTING OPEN NEDERLAND

- Support desk burgers tot afspraakbevestiging en doorverwijzen naar testaanbieder
- Toevoegen / Verwijderen aanbieders
- Aanmaken evenementcodes (geldig in alle teststraten van alle aanbieders)
- Toevoegen / inactiveren type tests en geldigheidsduur tests
- Toevoegen / inactiveren type activiteiten
- Afspraak plannen voor burgers
- Batch afspraken plannen voor grote evenementen
- Tickets aanmaken voor testaanbieder om afspraakbevestiging opnieuw te versturen
- Capaciteitsmanagement in afstemming met VWS
- Rapportage over bezettingscapaciteit aan Dienst Testen en VWS

2. Rollen en verantwoordelijkheden

2.2.1 Introductie op componenten en interfaces

INLEIDING

Deze sectie beschrijft de end-to-end IT keten (componenten en interfaces) voor het proces zoals dat hiervoor beschreven is. Het doel van deze sectie is om:

a) het overzicht te geven van de hele IT keten (high-level) als context voor (b) en (c)

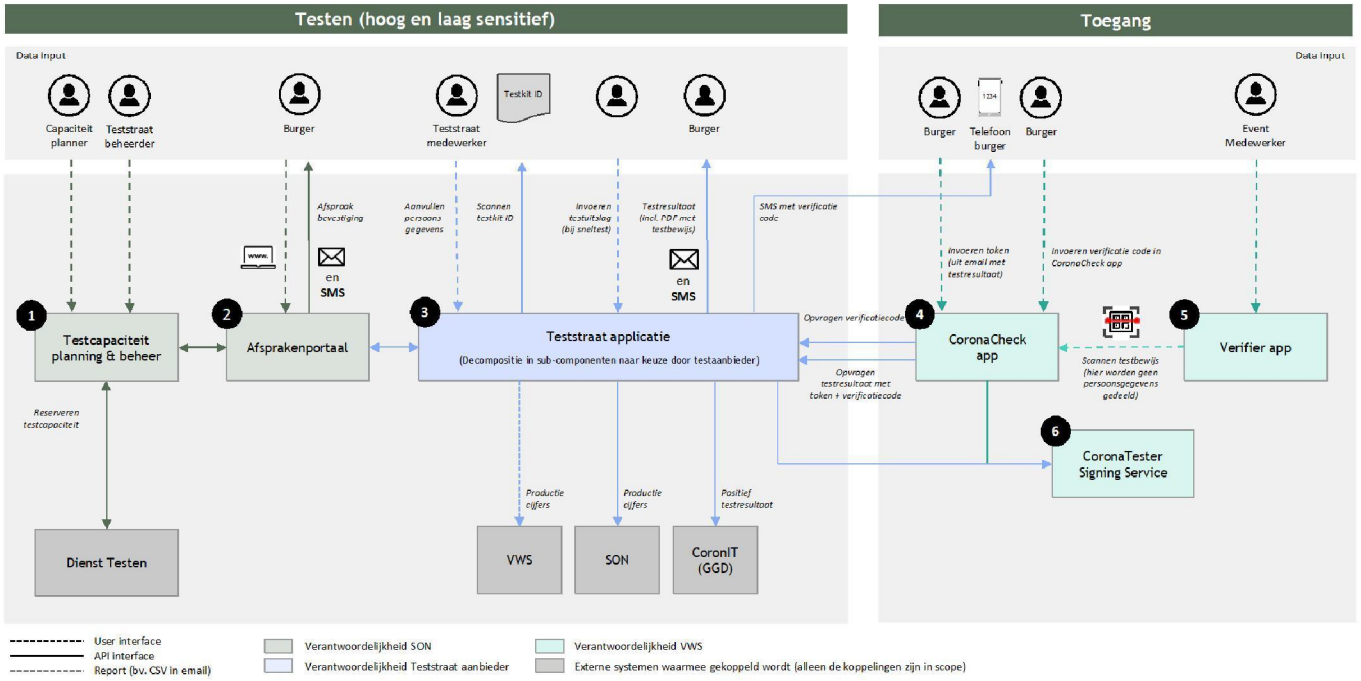
b) de scope af te bakenen van het deel van de IT keten dat door de testaanbieders wordt ingevuld

c) de componenten en interfaces binnen deze scope nader te detailleren (of te verwijzen naar andere documentatie waarin deze details zijn beschreven)

INHOUD

De volgende bladzijde geeft het overzicht van componenten en interfaces in de end-to-end IT keten. Aan het begin van de IT keten staan applicaties van de Stichting (Capaciteitsplanning en Afsprakenportaal). Het middengedeelte van de IT keten wordt ingevuld door de testaanbieders (Teststraat applicatie). Het laatste deel van de IT keten bestaat uit de apps van VWS (CoronaCheck app, Verifier app).

2.2.2 Componenten en Interfaces



2.2.3 High-level functionaliteit van componenten

1 Testcapaciteit planning & beheer

De testcapaciteit *planning* functionaliteit laat de planner 'what if' analyses uitvoeren, die de beleidsmakers ondersteunen bij het nemen van maatregelen die een balans opleveren tussen vraag naar testcapaciteit en aanbod van testcapaciteit. De testcapaciteit *beheer* functionaliteit wordt gebruikt door de medewerkers van SON voor:

- toevoegen / verwijderen teststraat aanbieders
- toevoegen / verwijderen teststraten (locaties)
- aanmaken van evenementcodes
- configureren van het soort test die nodig is voor bepaalde activiteit
- configureren van de geldigheidsduur van een test voor een soort activiteit

2 Afsprakenportaal

Een webapplicatie waarmee burgers een afspraak kunnen maken voor een test bij een door hen gekozen teststraat. Het afsprakenportaal vraagt om de datum/tijd van de activiteit waarvoor een negatief testbewijs nodig is, en laat de gebruiker een beschikbaar tijdslot kiezen voorafgaand aan de start van de activiteit (rekening houdend met de geldigheidsduur van de test). Gemaakte afspraken worden via een interface doorgegeven aan de Teststraatapplicatie.

Het systeem stuurt direct na het maken van de afspraak de reserveringsbevestiging per email naar de burger. Op de dag van de test stuurt het systeem per email/SMS een herinnering aan de burger.

3 Teststraatapplicatie

Een webapplicatie die gebruikt wordt door de medewerkers van de teststraat, en waarmee het hele proces in de teststraat wordt ondersteund. Het systeem laat de geautoriseerde medewerker een burger opzoeken op basis van naam. Na het identificeren van de burger via zijn legitimatiebewijs voert de medewerker de nog ontbrekende persoonsgegevens in en scant het ID van een testkit om daarmee de persoon te koppelen aan een testkit. Na het afnemen van de test en het bepalen van het resultaat worden de uitkomst van de test door de medewerker in het systeem ingevoerd.

Bij een negatieve test stuurt de teststraatapplicatie het testresultaat per email naar de burger inclusief een *token* (geanonimiseerde code) waarmee de burger via de CoronaCheck app het testresultaat kan inladen. Bij een positieve test wordt de burger gebeld en wordt het testresultaat doorgegeven aan CoronIT van de GGD.

De teststraat applicatie heeft een API interface dat wordt gebruikt door de CoronaCheck app van VWS om op basis van het token, en een verificatie van het telefoonnummer, het testresultaat in de CoronaCheck app in te laden.

4 CoronaCheck app

Een door VWS ontwikkelde app die gebruikt wordt door de burger om - op basis van een geanonimiseerd token en een extra verificatiecode - testresultaten te kunnen downloaden in de CoronaCheck app. Deze app zet het testresultaat om in een scanbaar testbewijs (QR-code) en toont dat testbewijs op het scherm van de CoronaCheck app. Het scanbare testresultaat is slechts kort houdbaar waardoor doorgeven of doorverkopen van negatieve testresultaten moeilijker wordt.

5 Verifier app

Een door VWS ontwikkelde app die gebruikt wordt door de medewerker van de locatie die de burger op basis van een negatief corona-testresultaat toegang wil verlenen. De app laat de medewerker het testbewijs scannen die de burger op het scherm van de CoronaCheck app toont. De Verifier app controleert of het getoonde testbewijs geldig is en toont de uitslag hiervan op het scherm van de Verifier app. Er worden geen gegevens in de Verifier app opgeslagen.

6 CoronaTester Signing Service

Een door VWS ontwikkelde service die de QR-code in het papieren testbewijs voorziet van een digitale handtekening.

2.2.4 Verantwoordelijkheden componenten

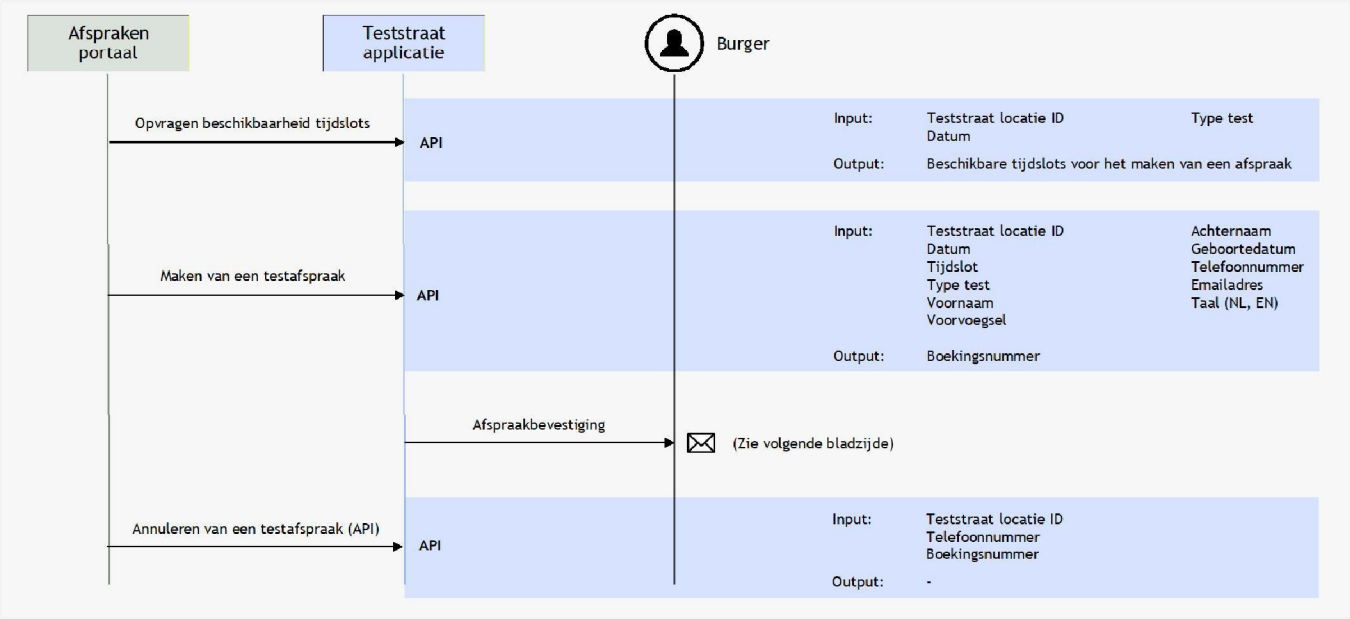
Component	SON	VWS	Testaanbieder
Capaciteit planning & beheer	Volledige verantwoordelijkheid (ontwerp, realisatie, operatie, beheer)		
Afsprakenportaal	Volledige verantwoordelijkheid (ontwerp, realisatie, operatie, beheer)		
Teststraat applicatie	Kaderstelling (proces, controls)		Testaanbieder: ontwerp, realisatie, operatie, beheer
CoronaCheck app		Volledige verantwoordelijkheid (ontwerp, realisatie, operatie, beheer)	
CoronaVerifier app		Volledige verantwoordelijkheid (ontwerp, realisatie, operatie, beheer)	
CoronaTester Signing Service		Volledige verantwoordelijkheid (ontwerp, realisatie, operatie, beheer)	

2.2.5 Verantwoordelijkheden interfaces

Interface	SON	Testaanbieder	GGD	VWS
Afspraken portaal	Specificatie van API's die de Teststraat applicatie moet aanbieden aan het Afsprakenportaal	Realisatie van de API's in teststraat applicatie		
SON	Specificatie van aan te leveren informatie en wijze van aanlevering	Realisatie van gegevensaanlevering		
GGD CoronIT	Coördinerende rol	Realisatie interface aan Teststraat applicatie kant	Specificatie interface, realisatie interface aan GGD kant[1]	
Corona-Check app	Coördinerende rol	Realisatie API's in Teststraatapplicatie		Specificatie interface (API's in de Teststraat applicatie die aangeroepen worden door CoronaCheck app)[2]
Burger	Specificatie inhoud email aan de burger (inclusief papieren testbewijs met QR-code)	Realisatie email aan de burger (inclusief papieren testbewijs met QR-code)		

Noot 1: Benodigd aparte documentatie van de GGD
Noot 2: Benodigd aparte documentatie van VWS

2.2.6 Interfaces – Afspraak maken (1/2)



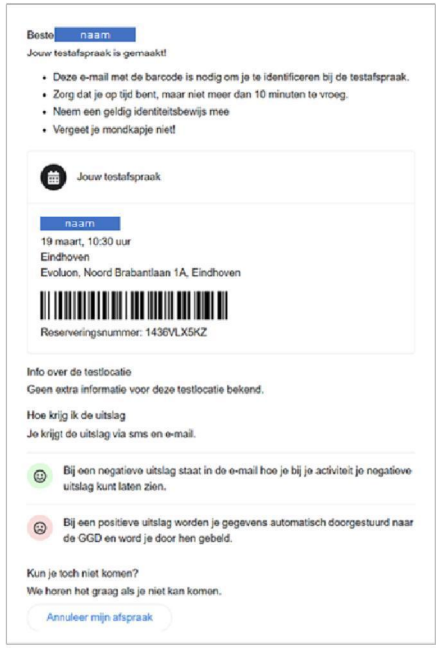
2.2.7 Interfaces – Afspraak maken (2/2)

BEVESTIGINGSMAIL

De email met de bevestiging van de afspraak wordt door de Teststraatapplicatie naar de burger gestuurd. Deze bevestiging bevat:

- Naam
- Datum en tijd van de afspraak
- Locatie / adres van de afspraak
- Reserveringsnummer

Een voorbeeld van de inhoud en layout van de afspraakbevestiging is hiernaast weergegeven. De testaanbieder kan de layout van de email opmaken in de eigen huisstijl.


Beste naam

Jouw testafspraak is gemaakt!

- Deze e-mail met de barcode is nodig om je te identificeren bij de testafspraak.
- Zorg dat je op tijd bent, maar niet meer dan 10 minuten te vroeg.
- Neem een geldig identiteitsbewijs mee
- Vergeet je mondkapje niet!

Jouw testafspraak

naam
19 maart, 10:30 uur
Eindhoven
Evoluon, Noord Brabantlaan 1A, Eindhoven

Reserveringsnummer: 1436VLX5KZ

Info over de testlocatie
Geen extra informatie voor deze testlocatie bekend.

Hoe krijg ik de uitslag
Je krijgt de uitslag via sms en e-mail.

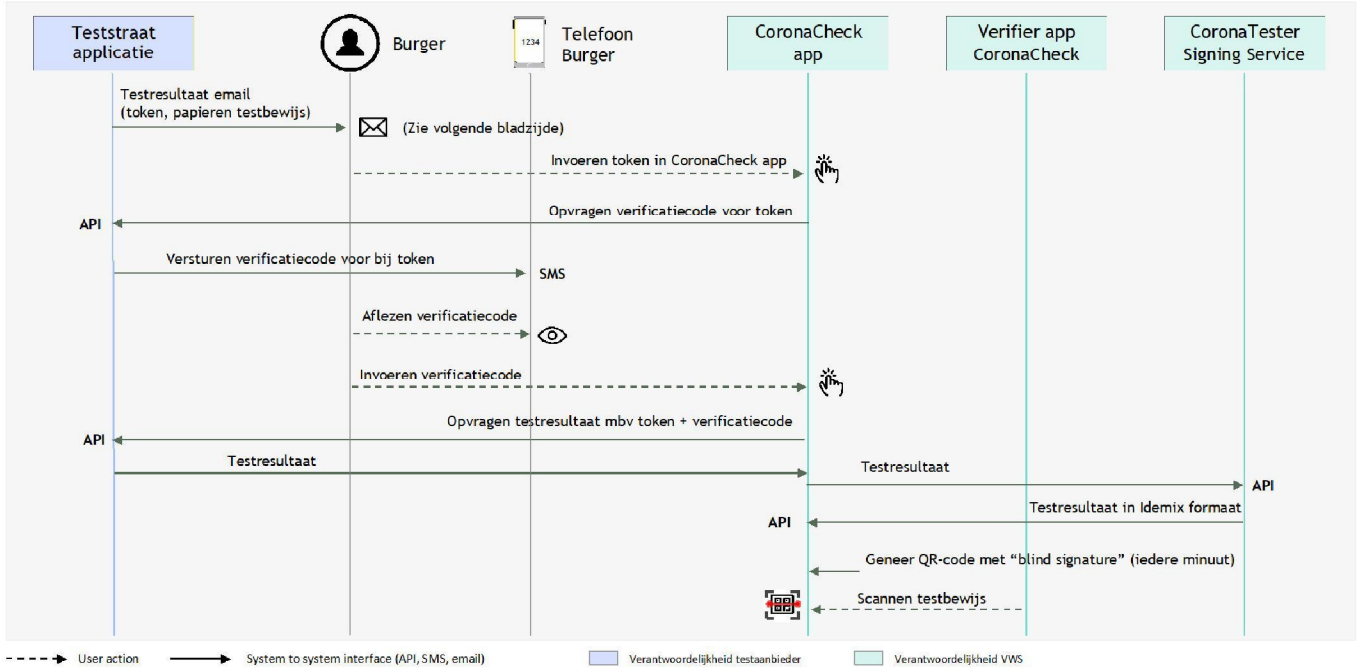
Bij een negatieve uitslag staat in de e-mail hoe je bij je activiteit je negatieve uitslag kunt laten zien.

Bij een positieve uitslag worden je gegevens automatisch doorgestuurd naar de GGD en word je door hen gebeld.

Kun je toch niet komen?
We horen het graag als je niet kan komen.

Annuleer mijn afspraak

2.2.8 Interfaces - Koppeling met CoronaCheck app (1/2)



2.2.9 Interfaces – Koppeling met CoronaCheck app (2/2)

Papieren testbewijs

De email met het testresultaat die door de Teststraatapplicatie naar de burger gestuurd wordt bevat (naast de tekstuele weergave van het testresultaat:

- Het unieke **token** dat nodig is voor het gebruik van de CoronaCheck app
- De PDF met de QR-code die het **papieren testbewijs** vormt

Een voorbeeld van de inhoud en layout van de PDF met het papieren testbewijs is hiernaast weergegeven. De variabele gegevens bestaan uit:

- Testdatum en -tijd
- Geldig tot datum en -tijd
- Initialen
- Geboortedag
- QR-code, deze bevat:
  - Testdatum en -tijd
  - Initialen
  - Geboortedag
  - Type test
  - Digitale handtekening

Functionaliteit en code

De functionaliteit om uit de input parameters de PDF met het papieren testbewijs te maken moet door de testaanbieder gerealiseerd worden. SON stelt C# code beschikbaar waarin deze functionaliteit is geprogrammeerd.
Testaanbieders hebben de keuze om deze C# code te gebruiken, of zelf de functionaliteit te realiseren in een andere programmeertaal.


Instructies

1. Print dit **testbewijs**.
2. Neem een geldig **legitimatiebewijs** mee naar de activiteit.
3. Toon dit testbewijs bij de toegang van je activiteit en eventueel je **toegangskaartje**.

Wil jij liever jouw testbewijs op je telefoon laten zien? Gebruik dan de CoronaCheck app met de unieke code uit de e-mail.

Je testbewijs

Initialen: **M.B.**
Geboortedag: **20 juli**

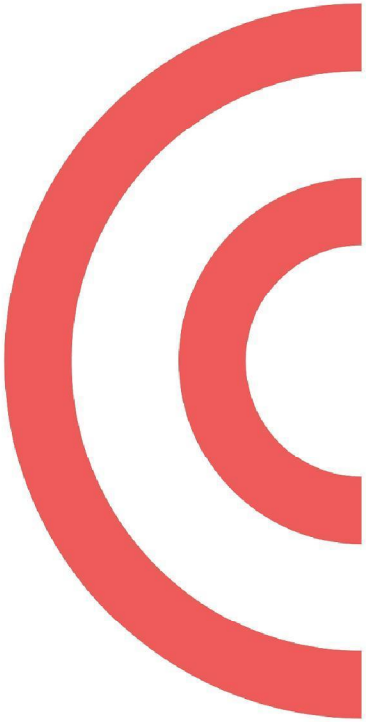
Getest op: 11-03-2021, 14.33u
Geldig tot: 11-03-2021, 14.33u

JOUW JE BEWIJS

Let op: Dit testbewijs is géén toegangsticket voor je evenement

Vragen? Neem contact met op met de klantenservice van Lead Covid.
Tel.: 073-12345678 | E-mail: info@test.nl

2. Rollen en verantwoordelijkheden



2.3 Rol Stichting Open Nederland

VERANTWOORDELIJKHEDEN STICHTING OPEN NEDERLAND:

1. Het **stellen van de privacy- en securitykaders** voor een veilige verwerking van gegevens.
2. Het **uitvoeren van controle en houden van toezicht** op de naleving van de kaders.
3. Het **coördineren van testaanbiederoverstijgende zaken**, zoals het veilig verzorgen van afspraken en ondersteunen in het afhandelen van (beveiligings)incidenten met een impact op meerdere testaanbieders.
4. Het **faciliteren van testaanbieders** in het veilig aansluiten op de infrastructuur met kennis en eventueel met dienstverlening op specifieke gebieden.

VERANTWOORDELIJKHEDEN TESTAANBIEDERS:

1. Het **voldoen aan de kaders** voor een veilige verwerking van gegevens, en het **dragen van verantwoordelijkheid** voor deze veilige verwerking.
2. Het **aanleveren van informatie en het meewerken aan controles** op naleving van de kaders.
3. Het **informeren van SON over (mogelijk) testaanbiederoverstijgende zaken**, zoals (beveiligings)incidenten, en het **meewerken aan afhandeling** hiervan.

2.3 Activiteiten Stichting Open Nederland

1. PRIVACY- EN SECURITYKADERS STELLEN

SON levert een Privacy- en securitykader op (zie bijlagen), o.a. gebaseerd op:

- NEN7510, 7512, 7513;
- Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg;
- Besluit elektronische gegevensverwerking door zorgaanbieders;
- Wet publieke gezondheid;
- Wet op de geneeskundige behandelingsovereenkomst;
- Algemene Verordening Gegevensbescherming.

Dit kader bevat geprioriteerde privacy- en securityeisen voor de teststraatapplicatie en context (gebruikslocaties, hosting, etc.), met:

1. Organisatorische eisen (beleid en processen)

2. Technische eisen (systeem)

3. Rapportage-eisen op het gebied van privacy & security, waaronder logging en monitoring en testaanbiederoverstijgende issues / incidenten

2. CONTROLE UITVOEREN EN TOEZICHT HOUDEN

SON beoordeelt de documentatie bij de aanvragen tot toelating in eerste instantie op volledigheid ('wordt voldaan aan de gestelde eisenlijst?'), daarna op inhoud ('is de juiste invulling aan de eis gegeven?') met inachtneming van de prioritering van de eisen. Hierbij geldt het Comply or Explain-principe, rekening houdend met eventuele restrisico's en de voorgestelde mitigatie.

Wanneer er afgeweken wordt van een eis, moet dit expliciet met inzicht in het te nemen risico, met daarbij ook voor wiens rekening het risico is, gebeuren. SON beoordeelt of dit voldoende is. Na toelating voert SON controles uit op de daadwerkelijke implementatie van de eisen, en geeft een go/no go op operatie voor de teststraat.

3. COÖRDINEREN TESTAAN-BIEDEROVERSTIJGENDE ZAKEN

SON zorgt voor een veilig koppelvlak aan de afspraakzijde. Vanaf dat koppelvlak is het de verantwoordelijkheid van de teststraat dat er veilige communicatie kan plaatsvinden.

Daarnaast ondersteunt SON bij het afhandelen van (beveiligings)incidenten die een mogelijke impact op meerdere testaanbieders heeft, of waar andere testaanbieders lering uit kunnen trekken. Hiervoor is het noodzakelijk dat de testaanbieders alerts van een vastgesteld niveau delen met SON, die vervolgens coördineert met de andere teststraten.

Het is nadrukkelijk de verantwoordelijkheid van de teststraten om hun eigen incidenten af te handelen. Daarnaast voert SON risicogebaseerd threat hunting uit (d.w.z. zoeken naar abnormaliteiten in de logs) binnen de applicaties van de diverse testaanbieders. Dit als aanvulling op de real-time monitoring die de testaanbieders zelf zullen uitvoeren in overeenstemming met de privacy- en securityeisen (conform NEN7510/7512).

4. FACILITEREN TESTAAN-BIEDERS BIJ AANSLUITEN INFRA

SON ondersteunt met advies over de eisen voor het veilig aansluiten op de infrastructuur. Testaanbieders kunnen twee keer per week in gezamenlijke calls hun issues voorleggen aan een 'helpdeskfunctie' die ondersteuning biedt bij het maken van keuzes.

Deze advisering vindt gescheiden plaats van de controle en toezicht binnen SON. Het is nadrukkelijk de verantwoordelijkheid van de testaanbieders dit advies te interpreteren en om daadwerkelijk keuzes te maken in de inrichting.

In overleg kan SON ervoor kiezen bepaalde brede dienstverlening aan de teststraten aan te bieden. Op dit moment is hier geen sprake van.

2.3 Activiteiten Testaanbieders

1. VOLDOEN AAN KADERS VOOR VEILIGE VERWERKING

Teststraten dragen de medische verantwoordelijkheid voor het testproces en zijn daarmee ook verantwoordelijke voor de gegevensverwerking in de zin van de Algemene Verordening Gegevensbescherming.

Dit betekent dat de testaanbieders de juiste beveiligingsmaatregelen moeten inrichten en uitvoeren. De kaders hiervoor zijn gebaseerd op de relevante wet- en regelgeving en de NEN7510-norm (en afgeleiden NEN7512 en NEN7513) voor verwerking van medische persoonsgegevens. De kaders zijn verder gespecificeerd door SON in de bijlage.

Hier kan gemotiveerd van worden afgeweken, waarbij SON inspraak heeft op de aanvullende mitigatie. Testaanbieders doen zelf aan real-time logging en monitoring, zoals vereist in de NEN7510 en NEN7513. Hieronder valt ook de communicatie met de CoronaCheck app en het bijbehorend certificaatbeheer*.

2. MEEWERKEN AAN CONTROLES OP NALEVING VAN KADERS

Testaanbieders leveren op verzoek tijdig informatie over de mate van naleving van de kaders bij de Stichting. Dit gaat zowel over de beschrijving van maatregelen ('opzet') als de uitvoering ('bestaan') en effectiviteit ('werking') van de maatregelen.

Vóór toelating moeten testaanbieders aan de hand van de privacy- en securitykaders aangeven in welke mate ze voldoen.

Op basis van deze maatregelen, in combinatie met gemaakte afspraken over onder meer beveiliging, controleert SON een gelijke mate van informatiebeveiliging bij de aanbieders.

De Stichting kan op verzoek ook aanvullende controles doen wanneer daar aanleiding toe is, en kan bij afwijking van de kaders (bijvoorbeeld, maar niet uitsluitend bij incidenten) actie ondernemen. Een belangrijk onderdeel hiervan is dat de testaanbieders door SON gespecificeerde logbestanden regulier kunnen aanleveren, zodat de Stichting hierop *threat hunting* / QA kan uitvoeren.

3. DE STICHTING INFORMEREN OVER TESTAANBIEDEROVERSTIJGENDE ZAKEN

Testaanbieders zijn verantwoordelijk voor (beveiligings)incidenten binnen hun teststraatomgeving en de afhandeling hiervan.

De Stichting onderzoekt testaanbiederoverstijgende zaken, zoals (beveiligings)incidenten en dreigingen, en houdt testaanbieders hiervan op de hoogte waar nodig. Om dit mogelijk te maken, informeren testaanbieders de Stichting over incidenten en alerts uit de monitoring van een afgesproken ernst. SON onderzoekt deze, en deelt informatie met de testaanbieders die het beveiligingsniveau verder kan verbeteren.

Vanwege het brede belang van het initiatief is het van groot belang dat testaanbieders meewerken aan het informeren van SON en meewerken aan de centrale afhandeling van incidenten, in overeenstemming met de overeengekomen service levels.

** Let op: conform de CoronaCheck-specificatie is een PKIoverheidcertificaat nodig. Het kan enige tijd duren voordat dit is aangevraagd, en het aanvraagproces bestaat uit verschillende stadia. Het is de verantwoordelijkheid van de teststraat tijdig over de juiste certificaten te beschikken. SON kan hierbij ondersteunen, maar heeft geen invloed op tijdlijnen.*

2.3 Privacy- en securitykader

UITGANGSPUNT

- Testaanbieder dient te voldoen wet- en regelgeving, zoals de (beveiligings)eisen uit NEN7510/7512/7513, en wetgeving voor verwerking van medische persoonsgegevens. Gecertificeerde partijen hebben de voorkeur. Een Gegevensverwerkingseffect-beoordeling (DPIA) conform de AVG met daarin een risicoanalyse en penetratietest zijn ook onderdeel van de eisenset.
- NEN7510 is gebaseerd op ISO 27001. Wanneer externe partijen, zoals hosting- en/of cloudaanbieders, de IT-omgeving ondersteunen, dienen zij aan ISO 27001 te voldoen, met een voorkeur voor gecertificeerde partijen.
- Wanneer gebruik gemaakt wordt van een cloudoplossing voor het verwerken van medische gegevens is ook het 'Advies Opslag Medische Data in de Cloud'[1] van toepassing.

ZIE OOK

Het is mogelijk voor testaanbieders zonder NEN7510-certificatie om zich in te schrijven. In dat geval worden de security & privacy controls risicogebaseerd getoetst door SON. Deze controls staan benoemd in de bijlage Privacy- en securitykader. Ook in het geval van NEN7510-gecertificeerde partijen zal SON de controls overigens toetsen tegen het kader, en worden ook certificeringsscope en risicobeslissingen specifiek meegenomen.

ONDERWERPEN

- Veilig personeel
- Beheer van bedrijfsmiddelen, waaronder het verwerken (persoonsgegevens) in overeenstemming met de AVG
- Toegangsbeveiliging, waaronder wachtwoordbeleid en Multi Factor Authentication (MFA) voor toegang tot medische gegevens
- Cryptografie
- Fysieke beveiliging en beveiliging van de omgeving
- Beveiliging bedrijfsvoering
- Communicatiebeveiliging
- Acquisitie, ontwikkeling en onderhoud van informatiesystemen
- Leveranciersmanagement
- Beheer van informatiebeveiligingsincidenten
- Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer
- Naleving

De volledige omgeving is gepentest, waarvan resultaten worden gedeeld met SON (zie ook de eisen aan pentesten in de privacy- & securitykaders)

Bron 1: https://www.rijksoverheid.nl/documenten/rapporten/2019/10/08/advies-opslag-medische-data-in-de-cloud

3. Lifecycle & on-boarding

3.1 Lifecycle testaanbieder

In de gehele lifecycle voor een testaanbieder zien wij verschillende fases, terug te brengen tot de on-boarding, de operatie en de off-boarding. Per fase zijn worden er op het gebied van IT en security & privacy verschillende onderdelen verwacht, van zowel SON als de testaanbieder. De volgende slide beschrijft een schematisch overzicht van deze activiteiten per fase.

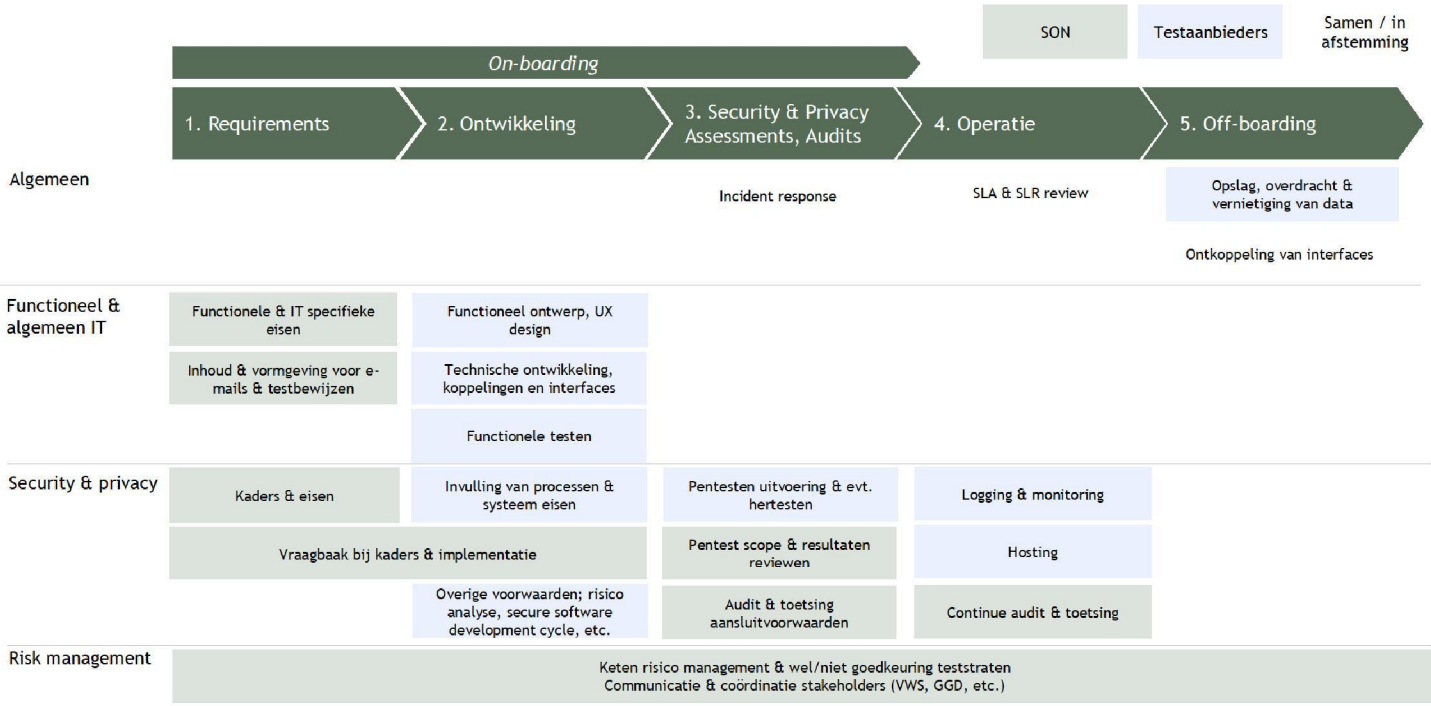
SON stelt de kaders vast waarbinnen de testaanbieder moet voldoen. Dit zijn o.a. functionele, security en privacy vereisten, waaraan voldaan moet worden, of templates die gebruikt moeten worden bij de ontwikkeling (bijvoorbeeld template & vormgeven voor testbewijzen). Op basis van deze kaders toont de testaanbieder aan op welke wijze de testaanbieder voldoet aan de gestelde kaders. Een lijst van verstrekte en verwachte documentatie is opgenomen in de Appendix [6.1 en 6.2]. Op basis van deze documentatie wordt door SON gecontroleerd of aan de eisen en voorwaarden is voldaan om te mogen starten met de operatie. Tijdens de operatie levert de testaanbieder verschillende rapportages aan, en voert SON ook actief controles uit op de processen en operatie van de testaanbieder, in lijn met de gestelde kaders.

ONDERSTEUNING

Zowel tijdens de on-boarding, operatie en off-boarding biedt SON ondersteuning aan dit proces via verschillende mogelijkheden, o.a.

- 2x 2 uur per week telefonisch contact t.b.v. uitleg kaders & eisen
- 2x 2 uur per week telefonisch contact t.b.v. specifieke development vraagstukken
- Meer ondersteuning naar behoefte en in afstemming
- Facilitering van communicatie met koppelpartijen zoals GGD en VWS (niet de daadwerkelijke koppeling of implementatie

3.2 Procesflow lifecycle testaanbieder



3.3 Procesflow lifecycle testaanbieder toelichting

1. REQUIREMENTS

- **Functionele & IT specifieke eisen** - Eisen qua koppelingen & evt. extra IT eisen zoals opgenomen in dit document.
- **Inhoud en vormgeving voor e-mails & testbewijzen** - Branding dient uniform te zijn over meerdere teststraten en wordt bepaald door SON.
- **Kaders & eisen** - Kaders en eisen gebaseerd op de geldende normen, met voorstellen tot implementatie.
- **Vraagbaak bij kaders & implementatie** - Volgens een specifieke cadans kan toelichting worden gegeven over deze kaders en eisen.

2. ONTWIKKELING

- **Functioneel ontwerp, UX design**
- **Technische ontwikkeling, koppelingen en interfaces**
- **Functionele testen**
- **Invulling van processen & systeem eisen**
- **Overige voorwaarden; risico analyse, secure software development cycle, etc.** - Eventuele aspecten uit de kaders en eisen die niet specifiek in de processen en systeem eisen naar voren komen dienen ook ingevuld en uitgevoerd te worden.

3. SECURITY & PRIVACY ASSESSMENTS, AUDITS

- **Pentesten uitvoering & evt. hertesten** - De uitvoer van pentesten die geregeld te worden door de teststraat aanbieder volgens industrie best practices en verder gespecificeerd in de kaders.
- **Pentest scope & resultaten reviewen** - De scope en resultaten worden door SON beoordeeld.
- **Audit & toetsing aansluitvoorwaarden** - Invulling van security kaders & eisen kan worden getoetst door SON.

4. OPERATIE

- **Incident response** - Incident response op (security) incidenten dient door de teststraat aanbieder zelf te worden opgepakt. SON dient wel geïnformeerd en betrokken te worden, vanwege overkoepelende impact en communicatie.
- **SLA & SLR review** - De testaanbieder rapporteert met een vastgestelde periodiciteit over de vastgestelde aandachtsgebieden.
- **Logging & monitoring** - Volledige logging & monitoring dient door de testraat uitgevoerd te worden conform kaders & eisen. SON wil graag meldingen/alerts krijgen vanuit teststraten zodat teststraat overstijgende zaken opgepakt kunnen worden. Logging dient beschikbaar te worden gesteld aan SON t.b.v. evt. proactieve analyse.
- **Hosting** - Hosting voor teststraat applicaties dient volledige door de teststraat aanbieder verzorgd te worden.
- **Continue audit & toetsing** - SON zal periodiek toetsen of de operatie van de testaanbieder in lijn is met de gestelde kaders & eisen.

5. OFF BOARDING

- **Opslag, overdracht & vernietiging van data** - Data dient over overdragen te worden aan SON, of bewaard volgens de gelden normen en wet & regelgeving, of vernietigd.
- **Ontkoppeling van interfaces** - Koppelingen met externe interfaces dienen te worden stopgezet, dit gebeurd in overleg tussen de partijen.

4. Appendix

4.1 Beschikbare documentatie

Documentatie	Referentie
Sample code voor generatie van QR code in papieren testbewijs (in C#)	
Instructies voor aanmaken materiaal t.b.v. PKI-O certificaat	
Templates voor e-mails en testbewijzen	
Interface specificatie communicatie CoronaCheckApp	In afstemming met VWS
Interface specificatie communicatie positieve resultaten GGD	In afstemming met GGD
Privacy- & securitykader (technische eisen)	
Privacy- & securitykader (organisatie-eisen)	
Operationele rapportage-eisen privacy & security	
Management rapportage-eisen Data & Informatie	

4.2 Testaanbieder documentatie

Documentatie	Referentie
Invulling eisen privacy- & securitykaders testaanbieder, inclusief Gegevensbeschermingeffectbeoordeling (DPIA) / risicoanalyse voor toetsing vooraf	
Penetratietesten conform privacy- & securitykader	
Operationele invulling eisen privacy- & securitykader testaanbieder voor bepaling voortgang en risico's	
Logbestanden applicaties met medische gegevens voor threat hunting	
Testaanbiederoverstijgende alerts en incidenten	