Ministerie van Volksgezondheid,
Welzijn en Sport

Eisen informatiebeveiliging en privacybescherming voor aansluiting op CoronaCheck

Ministerie van Volksgezondheid, Welzijn en Sport

Versie 1.1 | 21 juni 2021

Disclaimer. Het Ministerie van VWS heeft de aansluitdocumentatie voor CoronaCheck met zorg samengesteld. Nieuwe inzichten en maatschappelijke ontwikkelingen kunnen aanleiding geven tot aanpassingen. Het Ministerie van VWS zal (aansluitende) testaanbieders hierover informeren.

Versiehistorie

Versie	Datum	Wijzigingen
0.8	21 april 2021	Eerste deelbare concept.
1.0	28 april 2021	Eerste versie van de eisen voor informatiebeveiliging en privacybescherming voor testaanbieders die willen aansluiten op CoronaCheck.
1.1	21 juni 2021	Eisen 2, 3, 7 en 9 aangescherpt op basis van eerste ervaringen.

Inhoudsopgave

Eis 1. Aanvraag door rechtsgeldig vertegenwoordiger

Een rechtsgeldig vertegenwoordiger van de organisatie doet de aanvraag voor aansluiting op CoronaCheck. Hiermee ontstaat een rechtsgeldige aanvraag, weet het Ministerie van VWS met wie zaken wordt gedaan en wie gezondheidsgegevens verstuurt.

Aan te leveren bewijsstuk 1. Testaanbieder vult rechtsgeldig vertegenwoordiger in op aanmeldformulier. Rechtsgeldig vertegenwoordiger tekent bij intakegesprek de aansluitvoorwaarden voor akkoord.

Eis 2. Voldoen aan NEN-7510/7512/7513

Testaanbieder voldoet aan de NEN-7510/7512/7513. De verplichting van deze normen vloeit voort uit de Regeling gebruik burgerservicenummer in de zorg. Indien een testaanbieder niet voldoet, dan betekent dit dat de testaanbieder onvoldoende technische en organisatorische maatregelen heeft genomen. Dit is een risico voor de burger die getest wordt bij testaanbieder.

Aan te leveren bewijsstuk 2. Testaanbieder levert (audit)certificaten van voldoen aan. Is dat niet mogelijk dan wordt een eigen verklaring ingevuld en aangeleverd voor alle onderdelen van de standaarden. Voor de onderdelen waaraan testaanbieder niet voldoet, volgt een uitleg en een plan om hieraan alsnog te voldoen. Bij een eigen verklaring geeft de testaanbieder aan wanneer een audit zal plaatsvinden. Testaanbieder levert ondersteunend bewijsmateriaal, waaronder een actuele directiebeoordeling en documentatie, waaruit blijkt dat de organisatie de resultaten van het monitoren en meten van de beheersmaatregelen vastlegt. Het sjabloon voor de eigen verklaring is op verzoek beschikbaar bij uw aansluitcoördinator.

Eis 3. Voldoen aan NTA-7516

De testaanbieder past voor ad-hoc-communicatie met de burger de NTA-7516 toe. Dit is de norm voor veilige ad-hoc-communicatie in de zorg. Vanwege de gevoelige aard van de gegevens wordt door de testaanbieder niet gewoon gemaild.

Aan te leveren bewijsstuk 3.
Indien er meerdere partijen gebruik maken van de dienstverlener van de mailoplossing, dan moet de leverancier NTA 7516 gecertificeerd zijn. Testaanbieder levert een geldig NTA-7516 certificaat op naam van de leverancier en Verklaring van Toepasselijkheid (VvT) aan.

Indien de partij enige gebruiker is van de niet-gecertificeerde NTA 7516 mailoplossing moet worden opgeleverd:

- een Verklaring van In– en Uitsluitingen NTA 7516;
- een toetsing van alle NTA 7516 normen conform NCS 7516;
- testresultaten waaruit blijkt dat testuitslagen en overige ad-hoc communicatie conform NTA 7516 worden uitgewisseld.

In alle gevallen levert testaanbieder een zelfverklaring aan. Hiervoor is het sjabloon “Zelfverklaring toepassing NTA-7516” beschikbaar.

Eis 4. Veilig datatransport

Testaanbieder voldoet aan de volgende eisen voor datatransport:

1. Het datatransport is versleuteld met HTTPS TLS 1.3 met de juiste ciphers en PFS (of iets vergelijkbaars, zodat een key compromise op dag 10 niet leidt tot verlies van vertrouwelijkheid op dag 1-9).
2. Als testaanbieder uit oogpunt van gebruikersacceptatie oudere OS-versies moet ondersteunen, gebruikt testaanbieder daarvoor een TLS-versie niet lager dan TLS 1.2 voor. (Android < versie 6, iOS < 12.2).
3. Op de test van Qualys SSL Lab haalt testaanbieder een A+.
4. SSL pinning: Testaanbieder past CA (PKIoverheid EV) en leaf-node pinning toe om zeker te stellen dat er alleen met vertrouwde uitgegeven certificaten wordt omgegaan. Dit is bedoeld om onder andere Machine In The Middle aanvallen tegen te gaan.

Met deze eisen voldoet de testaanbieder aan de wettelijke vereisten voor technische en organisatorische maatregelen vanuit de AVG en de plekken in de wet waar expliciet versleuteling wordt genoemd.

Aan te leveren bewijsstuk 4. Geen aparte bewijsstukken. Voor een werkende setup is dit noodzakelijk.

Eis 5. Moderne versleutelingscijfers

Testaanbieder maakt gebruik van moderne versleutelingscijfers. Verouderde ciphers leveren onnodige risico's op. Voor het gebruik van TLS zijn alleen de volgende ciphers toegestaan:

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- ECDHE-RSA-AES128-GCM- SHA256
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384

Aan te leveren bewijsstuk 5. Geen aparte bewijsstukken. Voor een werkende setup is dit noodzakelijk.

Eis 6. PKIoverheid-certificaten

Testaanbieder gebruikt voor de aansluiting op de productieomgeving van CoronaCheck twee PKIoverheid-certificaten. Dit zorgt voor goede versleuteling en borging van de aanvrager en maakt helder met wie zaken wordt gedaan (digitaal getekend en geborgd door de overheid).

Testaanbieder levert de testuitslag bij CoronaCheck op de volgende wijze aan: PKCS#7/CMS signature op basis van een PKIoverheid-certificaat met minimaal een SHA256 hash en RSA-PSS padding.

Voor aansluiting op de test- en acceptatieomgeving moet de testaanbieder andere certificaten gebruiken, dit mogen niet-PKIoverheid certificaten zijn.

Aan te leveren bewijsstuk 6.
Testaanbieder deelt publieke sleutel van PKIoverheid-certificaten in aanmeldproces met het Ministerie van VWS. De certificaten worden gebruikt voor een werkende aansluiting.

Eis 7. DPIA

Testaanbieder levert voor de werking van de systemen die worden toegepast in het kader van CoronaCheck een DPIA aan. Deze DPIA moet minstens aan onderstaande eisen voldoen:

- de DPIA moet voldoen aan de wettelijke eisen vanuit de AVG en voldoen aan de DPIA Richtsnoeren van de EDPB;
- de DPIA moet expliciet zien op het proces van testaanbieder tot aansluiting op CoronaCheck;
- de DPIA moet blijk geven van de bewustzijn van het gevoelige karakter rond de aard, context en doel van de gegevensverwerking en de eisen vanuit de WGBO.
- doel beschreven;
- noodzaak en proportionaliteit beschreven;
- analyse risico's voor de betrokkenen;
- risico's uit preambule 75 geanalyseerd;
- technische en organisatorische maatregelen benoemd;
- informatie met betrekking tot de door Aanbieder geïmplementeerde procedurele maatregelen ten aanzien van door Aanbieder ingeschakelde medewerkers en facilitaire diensten;
- autorisatiematrix voor toegang tot de teststraatapplicatie en lokale IT-omgeving;
- beschrijving van fysiek testkit proces en koppeling met teststraatapplicatie;
- beschrijving proces koppeling testkit aan identiteit van burger, uitgifte van testkit, uitvoering van de test en het transport van de test naar de ruimte waar de test verder wordt verwerkt;

- overige verwerkingen (als die er zijn) benoemd.

Daarnaast moeten partijen een FG hebben aangesteld, wat blijkt uit het FG-advies op de DPIA.

Aan te leveren bewijsstuk 7. Testaanbieder levert DPIA aan, inclusief een FG-advies op de DPIA.

Eis 8. Websites conform standaarden W3C

Indien testaanbieder een website/websites aanbiedt in het kader van CoronaCheck, dan zijn deze conform W3C-standaarden. Hiermee beperkt de testaanbieder uitsluiting van mensen.

Aan te leveren bewijsstuk 8. Testaanbieder levert eigen verklaring met overzicht van websites en emailadressen aan die gebruikt worden in het kader van CoronaCheck. Zie sjabloon "Zelfverklaring gebruik websites en emailadressen".

Eis 9 Pentest op systemen in de keten voor CoronaCheck

Testaanbieder voert pentest uit op alle systemen die een rol spelen in de keten voor CoronaCheck. Doel hiervan is het voorkomen van datalekken en serieuze kwetsbaarheden.

Er zijn standaarden om te bepalen wat er getest moet worden. In deze standaarden staan de benodigde tests/verificaties beschreven. Deze worden allen uitgevoerd. Waar dat niet mogelijk is, wordt dat uitgebreid gemotiveerd.

Voor de volgende onderdelen zijn er standaarden beschikbaar:

- Infrastructuur: Penetration Testing Execution Standard (PTES): standaard ten behoeve van het pentesten van de infrastructuur.
- Voor een webapplicatie zijn er twee standaarden:
    - OWASP Top 10: de 10 meest kritische kwetsbaarheden van webapplicaties
    - OWASP WSTG: standaard ten behoeve van het pentesten van webapplicaties
- Voor een API: OWASP API Security Top 10: de 10 meest kritische kwetsbaarheden van API's.

- Voor mobiele applicaties (apps): OWASP MSTG: standaard ten behoeve van mobiele applicatie pentesten.

Aan te leveren bewijsstuk 9. Testaanbieder levert pentest-rapportage aan. De rapportage bevat geen openstaande bevindingen met een CVSS-score van 4,0 of hoger. Voor de rapportage gelden de volgende eisen:

- Het onderzoek moet, net als bij andere onderzoeken, zo worden beschreven dat het reproduceerbaar is voor contraexpertise.
- De rapportage wordt geschreven op basis van de fasen, zoals deze binnen de PTES worden gehanteerd. Deze stappen zijn als volgt:
    - Fase 1: Intelligence Gathering
    - Fase 2: Threat Modeling
    - Fase 3: Vulnerability Analysis
    - Fase 4: Exploitation
    - Fase 5: Post-Exploitation
    - Fase 6: Reporting
    - Fase 7: Re-audit
- Scopebeschrijving dient volgende onderdelen te bevatten:
    - Hostnames
    - IP-adressen
    - Andere scopeobjecten
- Verloop van de penetratietest, moet minimaal het volgende bevatten:
    - Tijdsslot van uitgevoerde acties
    - Beschrijving van taken per tijdsslot
- Rapportage van kwetsbaarheden
    - Lijst van getroffen scopeobjecten per kwetsbaarheid
    - Gebruik van de Common Vulnerability Scoring System (CVSSv3) voor classificeren van kwetsbaarheden. Daarbij is de Environmental Score bepalend. Hiervoor:
        - Wordt de CVSS-vector string (keuzes in het CVSS- model) in de rapportage opgenomen.

        - Wordt een risicoinschatting gemaakt voor bevindingen die geen kwetsbaarheid zijn. Deze scoren een waarde van 0.0 volgens CVSS, maar worden wel ingeschaald conform de risicoinschattingsmethodiek van testaanbieder. Deze levert daarvoor de informatie aan.
    - Gedetailleerde beschrijving van de kwetsbaarheid of het risico
    - Gedetailleerde reproductiestappen van de kwetsbaarheid
    - Gedetailleerde impactbeschrijving van de kwetsbaarheid of het risico
    - Gedetailleerde oplossingsrichting van de kwetsbaarheid of te nemen mitigerende maatregelen bij het risico
- Bijlagen bij het rapport
    - Scanresultaten per uitgevoerde scan, opgemaakt in leesbaar formaat
    - Overzicht van ontvangen documenten inclusief hashwaardes
    - Overzicht van verstrekte accounts die gebruikt zijn bij de penetratietest
    - In aanvulling op de uitgebreide beschrijving een checklist per gebruikte standaard (OWASP, PTES), afgevinkt op basis van keuzemogelijkheden:
        - Getest, kwetsbaarheid gevonden
        - Getest, geen kwetsbaarheid gevonden
        - Niet van toepassing met toelichting

Eis 10. Kwalificatie Internet.nl voor websites en emailadressen

Voor een in het kader van CoronaCheck toegepaste website scoort testaanbieder 100% op Internet.nl (enige uitzondering mag zijn als er nog geen IPv6-adres is). Voor een in het kader van CoronaCheck toegepast e-mailadres scoort testaanbieder een 90+% op Internet.nl. Testaanbieder voorkomt met deze scores de toepassing van verouderde en/of onveilige protocollen en het niet voldoen aan standaarden.

Aan te leveren bewijsstuk 10. Testaanbieder levert eigen verklaring met overzicht van websites en emailadressen aan die gebruikt worden in het kader van CoronaCheck. Zie sjabloon “Zelfverklaring gebruik websites en emailadressen”. Dit is hetzelfde bewijsstuk als voor eis 8.