



Programma RDO
*Ministerie van Volksgezondheid,
Welzijn en Sport*

Design – Certificate Pinning van SSL en CMS

Corona Check Project, MinVWS

Document geschiedenis

Versie	Datum	Veranderingen
1.00	2021-02-017	Concept.
1.01	2021-02-017	Comments IJ verwerkt – detail counterfeit data.
1.02	2021-02-017	Comments HV verwerkt – redirect niet toegestaan
1.03	2021-02-018	Verzoek HV tot opname keyids verwerkt.
1.04	2021-02-018	Verzoek RB tot opname URL met certs.

Hoofdstuk 1

Executive Summary

De veiligheid van Corona Check App berust, onder andere, op de betrouwbaarheid van de connecties naar het backend systeem en dat van (commerciële en publieke) test providers.

Een aspect hiervan is het hebben van een hoge mate van zekerheid dat de app praat met het 'echte' backend of systeem waar het mee denkt te praten. En niet met een totaal ander systeem of een 'man in the middle'.

Om deze reden wordt onder andere Certificaat Pinning toegepast op de Certificaat Autoriteit (in deze PKI Overheid) en de vertrouwensketen (chain) alsmede een controle lijst en verificatie van bepaalde velden.

Dit document getailleerd dit ontwerp en de gedachtes erachter.

Uitgangspunten

De Verifier en Holder app moeten op gezette tijden contact opnemen met een aantal backend services van de overheid. Daarnaast moet de Holder app tijdens het laden van het test resultaat contact opnemen met de server van de publieke (e.g. GGD) of private (e.g. commerciële) test provider.

Specifiek gaat het om:

1. Connectie Verifier/Holder app ten behoeve van het ophalen van de basis configuratie¹.
2. Connectie Verifier/Holder app met de backend API - bijvoorbeeld voor het 'inwisselen' van een test resultaat voor een C.L. getekende code.
3. Connectie Holder app ten behoeve van het test certificaat.

1.1 Risico afweging / Contingency

Omdat een probleem inzake deze een Kritiek² incident oplevert zijn er de volgende mitigaties meegenomen in het ontwerp:

1. Gebruik van de PKI overheids infrastructuur welke onder Nederlandse controle is (geen afhankelijkheid van (buitenlandse) derden.
2. Geen 'harde' pinning op het leaf certificaat - zodat in samenwerking met PKI Overheid vervangende sleutels in de door hun gecontroleerde infrastructuur gemaakt kunnen worden.
3. Het toestaan van een (relatief onbetrouwbaar) Content Delivery Network (cdn) om de distributie van het configuratie zeer robuust te maken.
4. Het toestaan van een brede reeks certificaten (van PKI Overheid) om integratie door derden makkelijk te maken (maar gecompenseerd door een striktere CN validatie).

1.2 Ontwerp - API

Deze connecties zullen beschermd worden met Certificaat Pinning. Hierbij zal:

1. Gecontroleerd worden een PKI overheid certificaat uit een specifieke, hardcoded lijst, deel uit maakt van de trust-chain.
De pinning zal plaatsvinden op:
 - (a) Staat der Nederlanden Domein Server CA 2020 CA (zie appendix A op pagina 7 voor de keyIDs).
 - (b) Er is geen beperking qua diepte.
2. Gecontroleerd worden dat de Fully Qualified Domain Hostname (fqdn) van de server waarmee contact opgenomen wordt overeenkomt met de CN of SubjectAltNative name³. Hierbij zijn geen wildcards toegestaan.
3. Dat de fqdn eindigd op coronacheck.nl (case insensitive).
4. HTTP-Redirects zijn *niet* toegestaan.

Deze laatste optie is strict genomen niet nodig (het betreft hier fqdn welke hardcoded zijn c.q. uit de configuratie komen) – maar is toegevoegd als 'backstopper' bij een partial backend compromise.

¹ Welke extra gevoelig is - omdat hier zaken als geldigheid en een onomkeerbare 'killswitch' in zitten

² Treft alle gebruikers, reële kans op politieke verantwoording, reputatie schade landelijke media

³ Dit staat dus los van andere aspecten, zoals DNS Sec

1.3 Ontwerp - ophalen config bestand

Daarnaast zal bij het ophalen van de configuratie ook gecheckt worden dat deze ondertekend is met een geldige CMS handtekening waarvan:

1. Gecontroleerd worden dat een PKI overheid certificaat, uit een specifieke, hardcoded lijst, deel uit maakt van de trust-chain.

De pinning zal plaatsvinden op:

- (a) Stamcertificaat Staat der Nederlanden EV Root CA
 - (b) Er is geen beperking qua diepte.
2. Dat de commonName van het distinguishedName veld het woord 'coronacheck' (case insensitive) bevat.

De reden voor deze extra laag van beveiliging is 1) dat dit bestand via een CDN gedistribueerd zal worden en dat 2) de configuratie een aantal extra gevoelige zaken bevat (en lang gecached kan worden) - zoals de 'killswitch'⁴

1.4 Ontwerp - ophalen andere data

Het is mogelijk dat er op basis van het configuratie bestand additionele data opgehaald moet worden (bijvoorbeeld voor de dagelijkse echtheidskenmerken).

Hiervoor geldt dat data welke via het CDN opgehaald wordt *altijd* getekend dient te zijn - gelijk aan het configuratie bestand (sectie §1.3).

En dat data welke direct, bij de eigen API servers opgehaald wordt, voldoet aan de eisen uit sectie §1.2 – en dus niet getekend hoeft te worden.

De reden voor dit verschil is dat de controle over het SSL certificaat in dit laatste geval geheel bij het Ministerie van VWS ligt op infrastructuur met additionele lagen van isolatie en beveiliging. Terwijl de CDN data via een gedeeld platform loopt waarbij de SSL certificaten hun private keys minder 'defence in depth' hebben.

⁴Welke aan het eind van de covid-19 risis de app volledig, onomkeerbaar, uitschakeld.

1.5 Ontwerp - Connecties providers

Daarnaast zal de Holder app met diverse providers contact moeten opnemen. Hiervoor geldt dat:

1. Gecontroleerd worden een PKI overheid certificaat uit een specifieke, hardcoded lijst, deel uit maakt van de trust-chain. De pinning zal plaatsvinden op:
 - (a) Staat der Nederlanden Root CA - G3
 - (b) Stamcertificaat Staat der Nederlanden EV Root CA
 - (c) Staat der Nederlanden Private Root CA
2. Er is geen beperking qua diepte.
3. Dat het fqdn en Subject Key Identifier (2.5.29.14) paar op de lijst van geaccepteerde providers.
4. Gecontroleerd worden dat de fqdn van de server waarmee contact opgenomen wordt overeenkomt met de CN of SubjectAltName⁵. Hierbij zijn geen wildcards toegestaan.
5. HTTP-Redirects zijn *niet* toegestaan.

⁵Dit staat dus los van andere aspecten, zoals DNS Sec

Bijlage A

Key IDs

De huidige keys (peildatum 18 februari 2021) zijn:

Stamcertificaat Staat der Nederlanden EV Root CA Vervaldatum: December 2022

FE AB 00 90 98 9E 24 FC A9 CC 1A 8A FB 27 B8 BF 30 6E A8 3B

Staat der Nederlanden Root CA - G3 Vervaldatum: 3 November 2028

54 AD FA C7 92 57 AE CA 35 9C 2E 12 FB E4 BA 5D 20 DC 94 57

Staat der Nederlanden Private Root CA Vervaldatum: 14 November 2028

2A FD B9 2B 1E FA C3 84 87 06 DB 81 FF 86 97 75 0D EB 01 8B

Zie <https://cert.pkioverheid.nl/cert-pkioverheid-nl.htm> voor de certificaten zelf in diverse formaten.