Programma RDO

Ministerie van Volksgezondheid, Welzijn en Sport

Design – Certificate Pinning van SSL en CMSvoor test providers

Corona Check Project, MinVWS

– 1.08– 25 mei 2021–

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.
1.05	2021-02-026	Drop deel eis PKI-O op private test stations TLS
1.06	2021-02-026	Correctie datum & volledige naam private root
1.07	2021-02-026	Verduidelijking commerciële handtekening test resultaat
1.08	2021-02-026	Verduidelijking print portaal, typo in table. Versie test providers.

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 volgens het volgende schema:

Wat	(met) Wie	Hoe	CA	CN check	whitelist	wildcards
Connectie	test provider	TLS	PKI-O (all)/EV (all)	ja	ja	ja
	test provider	CMS	PKI-O (all)	nee	ja	*n/a*
Printportaal	test provider	TLS	PKI-O (EV/Server 2020)	ja	ja	ja

Waarbij TLS de bescherming is van de connectie en CMS de bescherming is van de '*payload*' (zoals een testbewijs of configuratie bestand).

Dit document[1] getailleerd dit ontwerp en de gedachtes erachter in

[1] Zie ook het uitgebreidere algemene document:"Design – Certificate Pinning van SSL en CMS", version 1.08, Corona Check Project, MinVWS

Uitgangspunten

De Holder app heeft hier ten behoeve van het ophalen van test resultaten contact met de server van de test provider (direct, of unomi/events). Ook hierbij is het van belang dat de app *'zeker'* weet dat het met een legitieme test provider te maken heeft[2]. Daarnaast kan het zijn dat de burger het testportaal moet benaderen.

1.1 Risico afweging / Contigency

Omdat een probleem inzake deze een Kritiek[3] 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 waar mogelijk.
2. Het toestaan van een gecontroleerde set certificaten (van PKI Overheid) om integratie door derden makkelijk te maken inzake de signature *'waar integriteit belangrijk is'* – bij het test resultaat, terwijl er nog wel goede (Nederlandse) controle is.
3. Het toestaan van een zeer brede reeks van (commerciële) certificaten (PKI Overheid of CAB-Forum EV certified) inzake de TLS connectie naar test providers - maar, ter compensatie, dit gecombineerd met whitelisting op leaf level.
4. Daar waar geen whitelisting mogelijk is (bijvoorbeeld omdat de connectie vanuit de webbrowser geïnitieerd wordt) enkel een PKI Overheid certificaat toestaan - zodat er goede (Nederlandse) controle is (de meeste CAB-Forum certificaten vallen onder buitelandsrecht).

[2] Daarnaast neemt het monitoring backend op gezette tijden ook contact op met de test provider om de verbindingsinstellingen te controleren.

[3] Treft alle gebruikers, reële kans op politieke verantwoording, reputatie schade landelijke media

1.2 Ontwerp - Connecties (commerciële test) providers

Daarnaast zal de Holder app met diverse providers contact moeten opnemen. Hiervoor gelden eisen inzake de TLS connectie en eisen inzake de data(testuitslag) zelf.

1.2.1 Eisen TLS connectie met derden

Hiervoor geldt dat:

1. voor de TLS connectie controleerd zal worden dat:
   (a) Een PKI overheid certificaat uit een specifieke, hardcoded lijst, deel uit maakt van de trust-chain betreft. In dat geval zal de pinning zal plaatsvinden op:
      i. Staat der Nederlanden Root CA - G3
      ii. Stamcertificaat Staat der Nederlanden EV Root CA
      iii. Staat der Nederlanden Private Root CA

      –Of–

   (b) dat het een Extended Validation Certificate (EV) betreft welke voldoet aan de eisen gesteld in versie 1.7.4 (of nieuwer mits door Ballot bevestigd) van de richtlijnen van het CA/Browser Forum "'*Guidelines For The Issuance And Management Of Extended Validation Certificates*"[4].
   (c) Er is geen beperking qua diepte.
2. Dat het fqdn en Subject Key Identifier (2.5.29.14) paar op de lijst voorkomen van geaccepteerde providers.
3. Dat het certificaat gewhitelist is.
4. Gecontroleerd worden dat de fqdn van de server waarmee contact opgenomen wordt overeenkomt met de CN of SubjectAlterNative name[5]. Hierbij zijn wildcards toegestaan (normale CAB forum matching rules).
5. HTTP-Redirects zijn *niet* toegestaan.

1.2.2 Eisen CMS signature payload derden (testuitslag)

Daarnaast zal bij het ophalen van de data via de API ook gecheckt worden dat deze (testuitslag) 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) Staat der Nederlanden Root CA - G3
   (b) Stamcertificaat Staat der Nederlanden EV Root CA
   (c) Staat der Nederlanden Private Root CA
2. Dat het certificaat gewhitelist is.
3. Er is geen beperking qua diepte.

[4] `https://cabforum.org/extended-validation/`
[5] Dit staat dus los van andere aspecten, zoals DNS Sec

1.2.3 Eisen TLS connectie Printportaal, serverzijde

Aangezien het online printportaal van CoronaCheck[6] vanuit de browser van de burger direct een TLS-verbinding legt met de test provider - dient het certificaat er één te zijn die op de trustlist van de browser staat. Daarnaast dient zij te zijn uitgegeven door de Staat der Nederlanden.

Dus voor dit TLS certificaat geldt dat bij connectie met de webserver er:

1. gecontroleerd zal worden dat:
   (a) Staat der Nederlanden Root CA - G3
   (b) Stamcertificaat Staat der Nederlanden EV Root CA
2. Dat het certificaat voorzien van de juiste CN and Subject Alternative Name (als per CA/Browser forum (cab regelgeving). Dus gecontroleerd worden dat de fqdn van de server waarmee contact opgenomen wordt overeenkomt met de CN of SubjectAlterNative name[7]. Hierbij zijn wildcards toegestaan (normale CAB forum matching rules).
3. HTTP-Redirects zijn *niet* toegestaan.

[6] `https://coronacheck.nl/nl/print/`
[7] Dit staat dus los van andere aspecten, zoals DNS Sec

Bijlage A

Key IDs

De huidige keys (peildatum 25 mei 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 – G1 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.