Programma RDO

Ministerie van Volksgezondheid, Welzijn en Sport

Design – Certificate Pinning van SSL en CMS voor test providers

CoronaCheck, MinVWS

– 1.08– 27 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 CoronaCheck-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.

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

Uitgangspunten

De CoronaCheck-app heeft, ten behoeve van het ophalen van test resultaten, contact met de server van de test provider (direct, of unomi/events). 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 printportaal moet benaderen.

1.1 Risico afweging / Contigency

Omdat een probleem inzake de veiligheid en vertrouwelijkheid van de medische informatie van de burger (of de betrouwbaarheid van een uitgeven verklaring) 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 gebruik van een gecontroleerde, maar relatief toegankelijke, set van certificaten (verstrekt PKI Overheid). Dit om integratie door derden makkelijk te maken met een digitale signature '*waar integriteit belangrijk is*'. Zoals het geval is bij een test resultaat. Maar er voor zorgdragen dat er wel een goede (en in het Nederlands recht systeem verankerde) 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 buitenlands recht).

1.2 Ontwerp - Connecties (commerciële test) providers

Voor de resultaten zal de CoronaCheck-app met diverse test providers contact op moeten opnemen. Hiervoor gelden eisen inzake de TLS connectie en eisen inzake de data (testuitslag) zelf.

Het gaat hier om 3 soorten certificaten; waarvan de eerste twee gecombineerd kunnen worden:

1. Eén voor de TLS connectie naar de server van de test provider waar de app van de burger het resultaat op haalt,
2. Eén voor de TLS connectie die de burger haar webbrowser maakt naar de server van de test provider om een papieren testbewijs aan te maken.

   Deze kan gecombineerd worden met eerste TLS certificaat.
3. Eén ten behoeve van het digitaal ondertekenen van de test uitslag.

1.2.1 Eisen TLS connectie met derden ten behoeve resultaat

Dit is de TLS connectie die de app (client) maakt met de (web)server van de test provider. Hiervoor geldt dat:

[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. 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 (*Niet toegestaan indien gecombineerd met het printportaal – zie de uitzondering in sectie 1.2.3*).

   –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].

   (*Niet toegestaan indien gecombineerd met het printportaal – zie de uitzondering in sectie 1.2.3*).

   (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 wordt 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 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 is van de juiste CN and Subject Alternative Name (als per CA/Browser forum (cab regelgeving). Dus gecontroleerd wordt 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.

[4] `https://cabforum.org/extended-validation/`

[5] Dit staat dus los van andere aspecten, zoals DNS Sec, toegankelijkheidseisen (`https://www.digitoegankelijk.nl/wetgeving/wat-verplicht`, waar van toepassing richtlijnen als ?? en met name de pas-toe-of-leg uit lijst.

[6] `https://coronacheck.nl/nl/print/`

[7] Dit staat dus los van andere aspecten, zoals DNS Sec

1.2.3 Combineren TLS certificaten in één

Indien organisatorisch mogelijk kan voor het printportaal (technisch) hetzelfde certificaat als dat uit sectie 1.2.1 gebruik worden. Bijvoorbeeld indien de partij die deze dienst levert -en- de service één en dezelfde is. In dat geval gelden er twee extra beperkingen.

Ten eerste kan men in dat geval niet de Private Root gebruiken (optie 1(a)iii in sectie 1.2.1). Want voor het printportaal is het het certificaat in de CAB Forum lijst van de browsers van de burger staat. En dat is niet het geval bij de "Staat der Nederlanden Private Root CA". Deze staat niet op de internationale CA lijst die in de browsers van de burgers zit.

Ten tweede is het van belang dat de controle over de connectie (naar het printportaal) onder Nederlandse controle blijft vallen - dus de tweede optie - het gebruik van een 'Extended Validation Certificate (EV)' van een CAB partij (optie 1b in sectie 1.2.1) valt ook af.

Het certificaat moet dus van een van de volgende twee types zijn:

1. Staat der Nederlanden Root CA - G3
2. Stamcertificaat Staat der Nederlanden EV Root CA

1.2.4 Eisen CMS signature payload derden (testuitslag)

Tot slot 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.

Bijlage A

Key IDs

De huidige keys (peildatum 27 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.