Digicert EV certificaten vervangen door Sectigo OV certificaten

Velen van jullie ontvangen deze dagen een mail met als subject “ACTION REQUIRED: You must replace your certificate(s) before July 11”.

Er is naar aanleiding van een audit een probleem bij Digicert waardoor EV certificaten worden ingetrokken. Zie https://knowledge.digicert.com/alerts/DigiCert-ICA-Replacement

Omdat EV certificaten uitgegeven door intermediate "TERENA SSL High Assurance CA 3" (https://crt.sh/?id=5797998) hier onder vallen is er een probleem ontstaan.

Advies is om de getroffen certificaten te vervangen door OV certificaten uitgegeven door Sectigo.

Voor grote aantallen is dit te automatiseren (zie hieronder).

Zie ook de Frequently Asked Questions omtrent ingetrokken Digicert EV Certificaten.

Automatiseren

Via de APIs van Digicert en Sectigo is het opnieuw aanvragen van certificaten te automatiseren. Hieronder een stappenplan

- Log in bij Digicert en maak een API key aan via https://www.digicert.com/secure/automation/api-keys/ zodat we orders kunnen opvragen via de order-info API.
- Log in bij Sectigo SCM en maak een API account aan. Zie REST API
- Installeer software: openssl, jq, curl (versie 7.55 +).
- De mail van Digicert bevat de order nummers van getroffen certificaten. Als je die niet hebt: mail scs-ra@surfnet.nl voor een overzicht.
- Clone deze repository: https://github.com/joostd/digicert2sectigo (of download de zip file: https://github.com/joostd/digicert2sectigo/archive/master.zip)

De repo bevat een script om een certificaat bij Sectigo aan te vragen op basis van de CSR die oorspronkelijk naar Digicert is gestuurd.

Maak de volgende aanpassingen in de files uit te repo:

- plaats de Digicert API key in de file digicert-headers
- plaats de Sectigo API key in de file sectigo-headers
- vul jouw orgId en certType in, in de file enroll-template.jq (zie REST API)

Vraag het certificaat aan voor Digicert order# 12345 en requester jdoe@example.edu met:

```
./replace.sh 12345 jdoe@example.edu
```

Opmerkingen

- De werkelijke uitdaging is om het certificaat vervolgens geïnstalleerd te krijgen op de server. Schakel mensen tijdig in.
- ~~In principe werkt dit ook met Sectigo EV certificaten (pas het certType aan). Doe dit alleen als je een EV anchor hebt, en dit snel genoeg gaat~~. Als je al een EV anchor hebt zou je kunnen proberen om EV in plaats van OV certificaten aan te vragen. Dat gaat echter fout indien de subject DN in de CSR zoals gebruikt bij Digicert niet overeenkomt met datgene wat bij Sectigo in het EV anchor staat. De veiligste optie is om voor OV certificaten te gaan en EV te bewaren voor een later tijdstip.
- Vergeet niet te checken of de domeinen in de requests al gevalideerd zijn door Sectigo
- Vergeet niet te checken of je CAA records al hebt aangepast voor Sectigo
- Merk op dat meerdere ordernummers op de lijst van Digicert voor certificaten voor dezelfde server kunnen zijn. Let op dat je in dat geval het juiste certificaat vervangt.

Alternatief: reissue door Digicert

GEANT laat 9 juli weten:

- DigiCert have been sending out offers to replace certificates with DCV and asking organisations to sign up for a new account at CertCentral to do this. WE STRONGLY ADVISE YOU NOT TO ACCEPT THIS OFFER. The DCV certs offered are not of a standard we would expect in the community, and if an organisation sets up these new separate accounts with DigiCert we will have no way of tracking any future issues centrally at GÉANT. It will also confuse organisations that will then inevitably be offered to buy renewals further down the road via the commercial DigiCert system.
- It seems it is possible to renew certificates via https://www.digicert.com using the existing credentials organisations should have to manage their remaining certificates with DigiCert. David Groep has kindly prepared a guide here: https://www.nikhef.nl/pdp/tcsg3/Getting-your-Extended-Validation-certificate-reissued-from-the-Gen3-TCS.pdf. We have so far tested this in NL only but it does seem to work. My personal advice would still be to take this opportunity to replace DigiCert with Sectigo given the sheer number of mass revocations

we've seen over the last 18 months with DigiCert, but this might be a good back-up plan for some organisations, especially if they are not far along their migration path with Sectigo as yet.

- Obviously here at GÉANT we are also affected with our own certificates needing replacement. We managed to successfully reissue ours with Sectigo last night using the script Dick has shared. If anyone has any questions about how this works or the process we used, please feel free to reach out.