Getting your Extended Validation certificate from the Gen3 TCS "DigiCert" re-issued

As announced by DigiCert on July 7th in

https://knowledge.digicert.com/alerts/DigiCert-ICA-Replacement

all certificates issued by our "TERENA SSL High Assurance CA 3" CA, the one used for *all Extended Validation* certificates of the 3rd generation TCS, **will be revoked** on July 11th, i.e. **this week-end Saturday**. Extended Validation is the certificate profuct that gets you either a 'green address bar' or the name of your organisation immediately shown when the padlock is clicked in the browser.

If, by now, have ready access to the TCS Gen4 "Sectigo" service and can issue EV certificates there (because an EV anchor is already in place), that is the preferred route. And anyway, you should – as a backup plan – also get OV "GEANT OV Multi-domain" certificate replacements done.

But if you want EV and can complete this process, partially by hand, today or tomorrow, you can try 're-issuance'. As described by DigiCert, they offer (obviously free) replacements, that will be valid also after Saturday. These certificates

- Must be "re-issued"
- Will get a **new intermediate** CA "DigiCert EV RSA CA G2", so also the certificate chain file must be replaced
  for Nginx, this is thus *also* the *second* PEM blob in the certificate file
  for Apache httpd, this is content of the SSLCertificateChainFile
  for IIS and other products, please see your documentation
- You must have up to 30min of patience
  (and possibly longer if the EV validation for your organisation or your domains, has lapsed)
- You can re-use the same key pair (by using the same CSR)
- You can do this all also on behalf of any users and certificate owners in your organisation
- You must restart or reload services afterwards

Instructions from DigiCert

In a very concise way, DigiCert said it all:

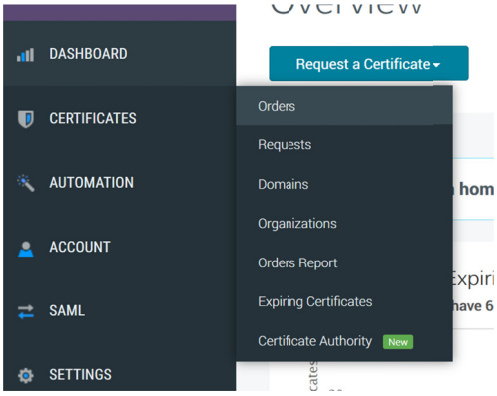
What Action is Required?

1. Sign in to your account and locate if your certificate(s) are affected.
2. **Reissue ("Replace" if you are still managing certificates on the MSSL/CWS portals) and re-install affected certificates before July 11.**

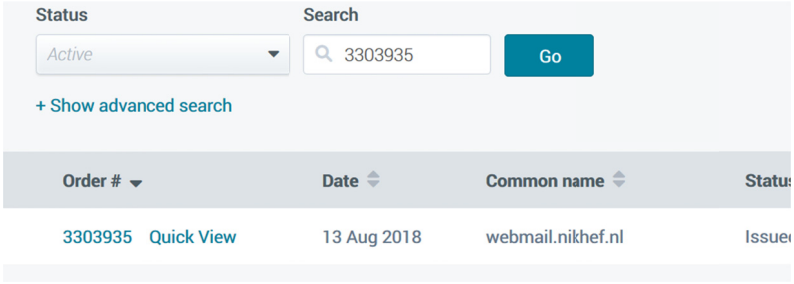
Step by step guide

1. Login, with an Administrator account from your organization – the same one you used before May 1st, at https://www.digicert.com/account/login.php

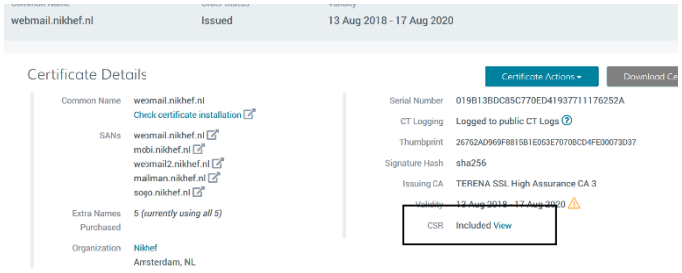
2. Go to “Certificates” -> “Orders”



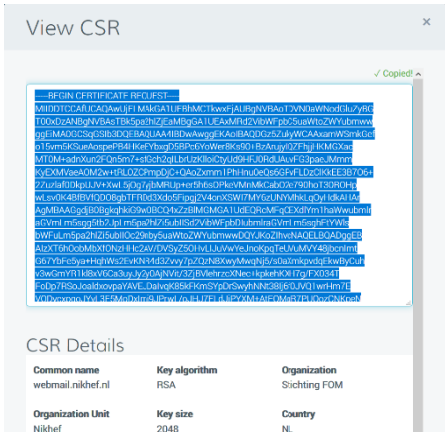
3. You can search for your certificate **by order ID**, and order IDs affected were sent to you by DigiCert (in the mail from Ruud-Maarten). Or look the hosts up by name.



4. You can re-use the same CSR. That CSR is helpfully given on the order page, so klik on the order number (**not** the Quick View), and find the CSR viewer:

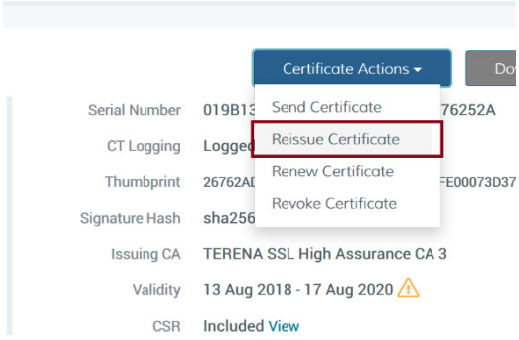


and click on “View” to see the CSR blob.

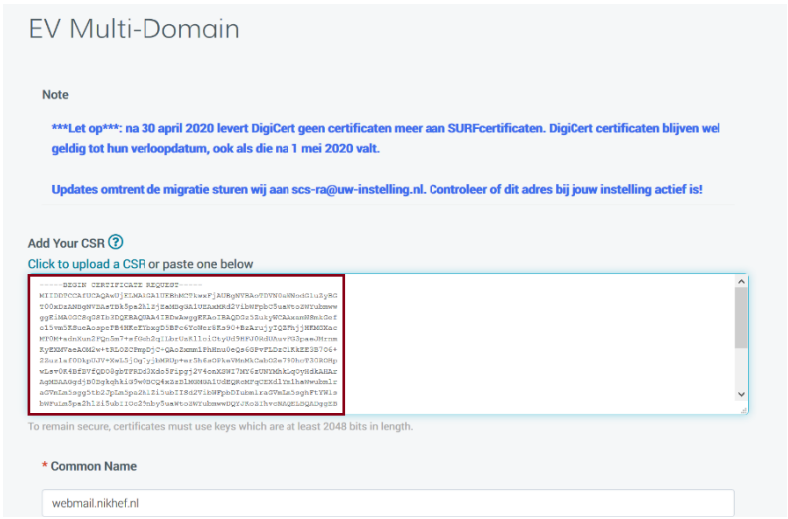


Copy that into your clipboard buffer, by clicking once inside the text. Make sure you select all (that’s the default anyway).

5. From the “Certificate Actions” button, select “Reissue Certificate”

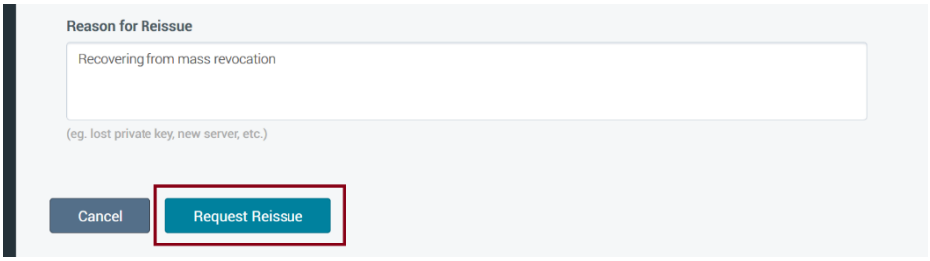


6. In the CSR text box, paste the CSR you copied in step #4:

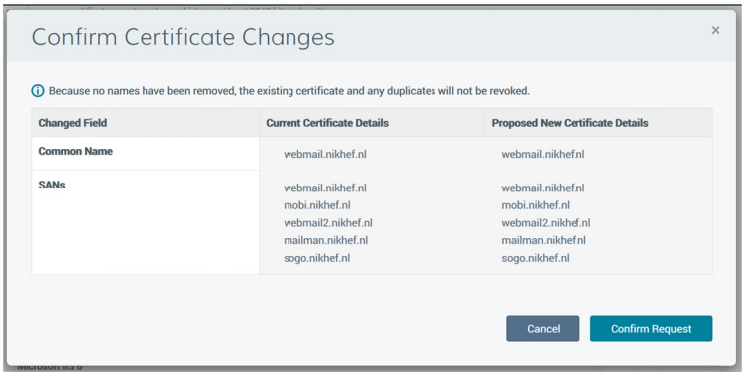


but do **not** change the other fields. Otherwise, important subject alternname names might be lost, and you have an operational problem later.

7. Scroll to the bottom of the page. You can even type a reason for re-issuance in case you want. Anyway, press “Request Reissue”

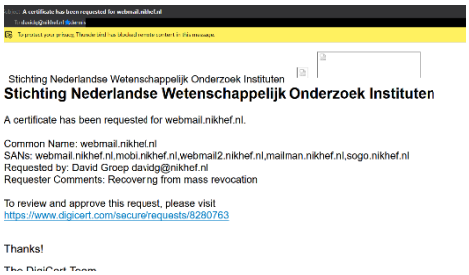


8. You get a dialog box to confirm the subjectAltName. Make **sure** that all names are there, no names are added, and no names are lost:



and the “Confirm Request”

9. (potentially, only in exceptional cases) At this point, a mail **may** be triggered to the organisation/domain owner. Whether this happens depends on the validation status of the org and domain. It might be automatic as well. Otherwise, catch the mail to the EV validation user, as shown below, and approve it. It should not happen, but may.



Stichting Nederlandse Wetenschappelijk Onderzoek Instituten

Stichting Nederlandse Wetenschappelijk Onderzoek Instituten

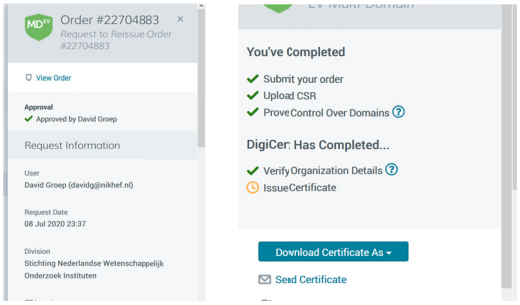
A certificate has been requested for webmail.nikhef.nl.

Common Name: webmail.nikhef.nl
SANs: webmail.nikhef.nl,mobi.nikhef.nl,webmail2.nikhef.nl,mailman.nikhef.nl,sogo.nikhef.nl
Requested by: David Groep davidg@nikhef.nl
Requester Comments: Recoverng from mass revocation

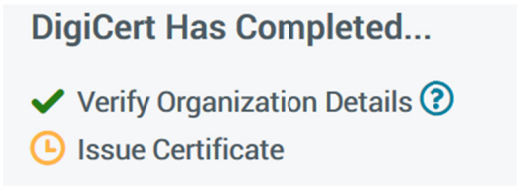
To review and approve this request, please visit
https://www.digicert.com/secure/requests/8280763

Thanks!

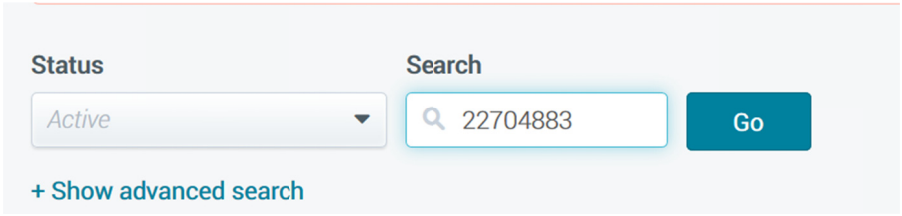
10. You get the confirmation dialog that issuance is pending. Click on “View Order” to get the sidebar status:



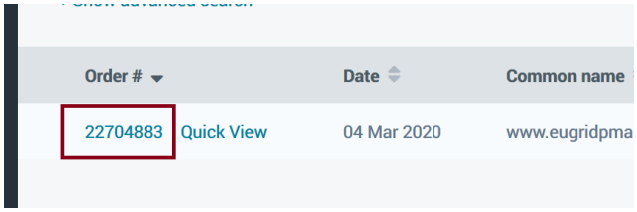
It will be in “Issue Certificate” pending status:



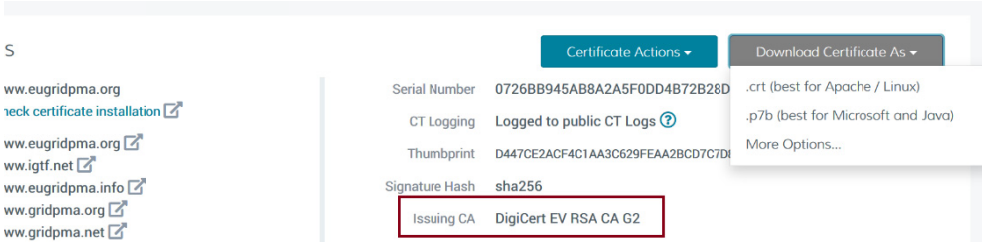
11. Please proceed to the full order page, by entering the order ID in the search box and “Go”ing



12. Click on the order number, **not** on the “Quick View”:



13. Wait until it *actually re-issues*, which you can see by refreshing and looking for



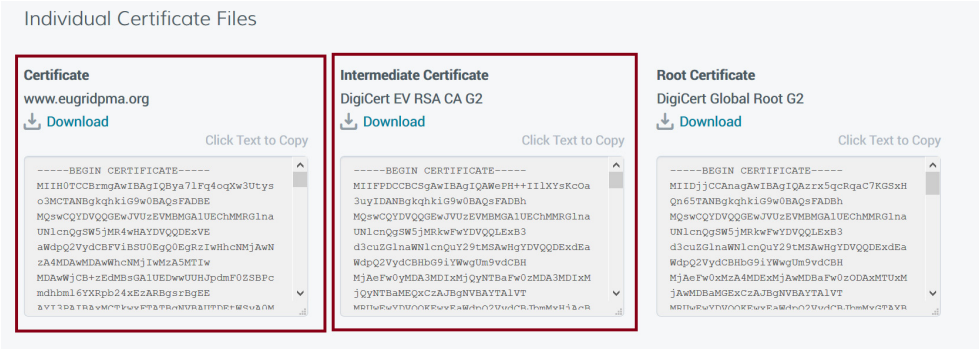
Once re-issued, you and/or the original certificate requester *also* get the email with the canonical ZIP file.

PLEASE wait until you actually see “DigiCert EV RSA CA G2” here.

This may take up to ~30 minutes, but could be as quick as 5 seconds.

If you continue before re-issuance is done, you get the old cert back. So, really …

14. At this point, make sure you get both the new certificate **as well as** the new intermediary:



15. Install both of these in your favourite server software
    you can in this case leave the **key file unchanged**, since the re-issued cert is based off the same keypair.

And now go for the next certificate you need to replace.

You can do this also via the API – but no ready tool is available at this moment (if you build one, please share it!)

What should go where?

In the SSLCertificateChain file, you should have the following content for the DigiCert EV RSA CA G2

```
-----BEGIN CERTIFICATE-----
MIIFPDCCBCSgAwIBAgIQAWePH++IIlXYsKcOa3uyIDANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBH
MjAeFw0yMDA3MDIxMjQyNTBaFw0zMDA3MDIxMjQyNTBaMEQxCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxHjAcBgNVBAMTFURpZ2lDZXJ0IEVWIFJT
QSBDQSBHMjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAK0eZsx/neTr
f4MXJz0R2fJTIDfN8AwUAu7hy4gI0vp7O8LAAHx2h3bbf8wl+pGMSxaJK9ffDDCD
63FqqFBqE9eTmo3RkgQhlu55a04LsXRLcK6crkBOO0djdonybmhrfGrtBqYvbRat
xenkv0Sg4frhRl4wYh4dnW0LOVRGhbt1G5Q19zm9CqMlq7LlUdAE+6d3a5++ppfG
cnWLmbEVEcLHPAnbl+/iKauQpQlU1Mi+wEBnjE5tK8Q778naXnF+DsedQJ7NEi+b
QoonTHEz9ryeEcUHuQTv7nApa/zCqes5lXn1pMs4LZJ3SVgbkTLj+RbBov/uiwTX
tkBEWawvZH8CAwEAAaOCAgswggIHMB0GA1UdDgQWBBRqTlC/mGidW3sgddRZAXlI
ZpIyBjAfBgNVHSMEGDAWgBROIlQgGJXm427mD/r6uRLtBhePOTAOBgNVHQ8BAf8E
BAMCAYYwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMBIGA1UdEwEB/wQI
MAYBAf8CAQAwNAYIKwYBBQUHAQEEKDAmMCQGCCsGAQUFBzABhhhodHRwOi8vb2Nz
cC5kaWdpY2VydC5jb20wewYDVR0fBHQwcjA3oDWgM4YxaHR0cDovL2NybDMuZGln
aWNlcnQuY29tL0RpZ2lDZXJ0R2xvYmFsUm9vdEcyLmNybDA3oDWgM4YxaHR0cDov
L2NybDQuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0R2xvYmFsUm9vdEcyLmNybDCBzgYD
VR0gBIHGMIHDMIHABgRVHSAAMIG3MCgGCCsGAQUFBwIBFhxodHRwczovL3d3dy5k
aWdpY2VydC5jb20vQ1BTMIGKBggrBgEFBQcCAjB+DHxBbnkgdXNlIG9mIHRoaXMg
Q2VydGlmaWNhdGUgY29uc3RpdHV0ZXMgYWNjZXB0YW5jZSBvZiB0aGUgUmVseWlu
ZyBQYXJ0eSBBZ3JlZW1lbnQgbG9jYXRlZCBhdCBodHRwczovL3d3dy5kaWdpY2Vy
dC5jb20vcnBhLXVhMA0GCSqGSIb3DQEBCwUAA4IBAQBSMgrCdY2+O9spnYNvwHiG
+9lCJbyELR0UsoLwpzGpSdkHD7pVDDFJm3//B8Es+17T1o5Hat+HRDsvRr7d3MEy
o9iXkkxLhKEgApA2Ft2eZfPrTolc95PwSWnn3FZ8BhdGO4brTA4+zkPSKoMXi/X+
WLBNN29Z/nbCS7H/qLGt7gViEvTIdU8x+H4l/XigZMUDaVmJ+B5d7cwSK7yOoQdf
oIBGmA5Mp4LhMzo52rf//kXPfE3wYIZVHqVuxxlnTkFYmffCX9/Lon7SWaGdg6Rc
k4RHhHLWtmz2lTZ5CEo2ljDsGzCFGJP7oT4q6Q8oFC38irvdKIJ95cUxYzj4tnOI
-----END CERTIFICATE-----
```

This is done:

- for Apache httpd usually configured in ssl.conf, under

```
SSLCertificateFile /etc/pki/tls/tcsg3/cert-igtf.net.pem
SSLCertificateKeyFile /etc/pki/tls/tcsg3/key-igtf.net.pem
SSLCertificateChainFile  /etc/pki/tls/tcsg3/chain-igtf.net.pem
```

with the re-issued certificate (“hostname.crt” in the zip file) going under the SSLCertificateFile
This same structure also holds for e.g. postfix, and for cyrus imapd (where the intermediate is in “tls_ca_file”)

- for nginx, concatenate the ‘*hostname*.crt’ and **the new** DigiCertCA.crt file in this order together as your new certificate for nginx
- The same concatenation holds for OpenVPN servers
- In some cases, the intermediate is in another place – see your software documentation.