INFOSHARE SLIDES

Q: Will we still have access to the DigiCert portal after 30th April 2020?
A: Based on the contract between GÉANT and DigiCert, "upon termination, DigiCert shall provide entities operating under the GÉANT Association Account with a Transition Period during which DigiCert shall continue to support the GÉANT Association Account, the NREN Accounts, and each Participant’s account, including continued use of DigiCert’s Certificate revocation services. However, Participants and NRENs may not order any new Certificates during the Transition Period. DigiCert shall continue to provide revocation services for the Certificates until all Certificates issued under this Agreement expire." You and your members will be able to order DigiCert certificates until 30 April and they will remain valid until their expiration date, will have access to the portal to see your existing certificates and receive notifications, but will not be able to order new certificates.

Q: Where can I find documentation for Sectigo?
A quick start guide can be found at: https://support.sectigo.com/Com_KnowledgeDetailPage?id=kA03I000000vFnd

MRao guide: https://support.sectigo.com/Com_KnowledgeDetailPage?id=kA01N000000bvJA

Full admin guides (including API documents) can be found at: https://support.sectigo.com/Com_KnowledgeProductPage?c=Admin_Guides&k=&lang=

Q: When will the new certificate chains for the Sectigo supplier be available?

The certificates can be found at: https://crt.sh/?CAName=%25GEANT+Vereniging%25.

Q: What Membership Category is my NREN?

<table>
<thead>
<tr>
<th>Membership category</th>
<th>NRENS in category</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IS, BG, LV, MT, ME, MK, MD, AM</td>
</tr>
<tr>
<td>2</td>
<td>BY, LU, LT, EE, RS, AL, LB, CY, GE</td>
</tr>
<tr>
<td>3</td>
<td>SI, HR, MA, OM, SK, AZ</td>
</tr>
<tr>
<td>4</td>
<td>CZ, HU, RO, IE</td>
</tr>
<tr>
<td>5</td>
<td>DK, GR, FI, PT, IL</td>
</tr>
<tr>
<td>6</td>
<td>NL, CH, BE, SE, TR, AT, PL, NO</td>
</tr>
<tr>
<td>7</td>
<td>ES</td>
</tr>
<tr>
<td>8</td>
<td>DE, UK, FR, IT</td>
</tr>
</tbody>
</table>

Q: What is the last day we can use the DigiCert platform?

NRENs will be able to use the DigiCert platform and issue certificates up to and including the 30th April 2020. After this date, it will be possible to revoke certificates but not add new organisations or issue certificates.

Q: Will it be possible to migrate data to Sectigo?

Yes, you can either:

- Use the “csv” option in the DigiCert interface to pull out organisational data and we can share this with Sectigo.
- Use the DigiCert API to pull out data.

Q: Is State mandatory for Sectigo?

For now, State is mandatory and the European users are advised to out the city as the state and the validation team will correct anything that is wrong.

However, Sectigo is working on implementing the change per your concerns (to make State field not mandatory). No ETA at this time, but they have it as a High priority in their backlog.

Q: What are the Support Hours for Sectigo?

Sectigo staffs and operates 4 support centres globally in North America (Ottawa, Canada and Salt Lake City, Utah), United Kingdom (Manchester) and India (Chennai) respectively. **Ticketing, telephone and chat service is available 365x7x24 in the English language**, with multiple language capability available from our North American facility (Ottawa, Canada).

Once all the NREN’S have been fully on-boarded onto SCM platform and are ok with how to use platform we will then begin the **Premier Support Handoff**. As of right now all NREN “MRAO” admins can only contact support via the following below. After the on-boarding to Premier Support all NREN’s will then need to utilize contacting their respected SAM/TAM “Premier Support Rep” for any concerns they have.

Support Contact Info: https://support.sectigo.com/Com_KnowledgeMainPage

Submitting a Ticket: https://sectigo.com/support-ticket

Q: I am an NREN MRAO, why does my organisation have to be validated?

Some NRENs are not legal entities and therefore cannot be validated, but the MRAO is representing the NREN (and not the University, which is a legal entity).
The NREN Accounts must be tied to an Organization that can be validated if they want to be able to order certificates. If not, Sectigo can add them however, the NREN MRAO Admin will not be able to place orders for SSL or Code Signing Certificates. They can still play with the platform just not order certificates.

For those Universities that will be added by the NREN MRAO admins and will be managed by the Organization admin not an NREN MRAO then they will be a RAO admin Only. If the NREN MRAO Admin is going to be placing order they do not need to be an RAO and those Organisations must be validated before ordering can be done.

Q: What is the difference between MRAO and RAO?

**NREN MRAO Admins Managing Includes:**

- Adding New Organizations
- Validating New Organization “Triggering OV Anchor”
- Creating the first RAO Admin for New Organizations > If an RAO “the main rao” admin leaves the “NREN” is then responsible for creating the next RAO responsible for managing that org if one does not exist already
- Training of RAO Admins on how to use SCM platform
- Handling any Q&A directed to them about how to use SCM
- Responsible for Premier Support Contact as no RAO/DRAO admins are allowed to contact Premier Support or obtain Premier Support information.

**RAO Admin Managing includes:**

- Adding/delegating/dcv domains
- Adding/delegating admins “RAO or DRAO”
- Department Creation “If Needed”
- Notification Creation
- Discovery Creation
- Placing orders “SSL/Client Authentication ‘s/mime’ Code Signing Certificates”
- Reports
- Contacting Support/Validation: If an issue arises the RAO/DRAO can contact Level 2 support/validation for assistance during normal business hours Monday – Friday 4am – 8pm EST. *If an issue occurs after normal business hours they can reach out to the NREN “MRAO” admins to raise a concern with Premier support.

Q: Can Sectigo login to the MRAO accounts?

Support along with the Onboarding Team Members have the access to login as any MRAO in the system. The process is only used to support a MRAO who has questions regarding SCM or Support/Validation Related issues. In the process any of Sectigo staff needing to login as a MRAO they will notify the MRAO who asked for support or if we deem something is wrong they may just login as prior to responding.

Q: How do I enable SAML?

You MUST be a member of eduGAIN to use SAML for the Sectigo Certificate Manager.

**To enable SAML for admin access to SCM:**

- Step 1: If you do not see the "your institution" button on the home page, please set up an IdP Template: under "admin" in cert-manager please select “add template” and then tick the RAO Admin - SSL and the organisation box below that.
- Step 2: make sure that the Sectigo SP is imported in your federation: the entityId is https://cert-manager.com/shibboleth, you can also check https://met.refeds.org/met/search_service/?entityid=cert-manager.com.
- Step 3: check that all the needed attributes are correctly released at the following URL: http://cert-manager.com/customer/<YOURNREN>/ssocheck/
- Step 4: in the SCM enter the ePPN of the admin you want enable in the "IdP Person ID" field.

**To use SAML "self-enrollment" for server certificates (allows users outside of SCM admin to request server certificates):**

- Step 1: go to Settings>Organizations>select organization.
- Edit the organization and select the SSL certificates tab.
- Select "self enrollment using SAML”. This will provide you with a unique url that can be shared with users.
- The token string used in the url can be changed by administrators if issues occur.

**To use SAML in order to allow users to order client certificates:**

- Configure your IdP correctly for Sectigo. See below.
- Edit your organization in SCM (Settings>Organizations>select) and set "Academic code (SCHAC Home Organization)” to the same value as your IdP sends for schacHomeOrganization. It will typically be your main domain, but confirm this with your IdP admins.
- Edit your organization object and set "Secondary Organization Name" to the name used in grid certificates (ASCII). Please check existing certificates. As grid certificate subjects are used as "usernames" in systems, it is vital that the whole subject string is kept as it was before for your users.
IdP must release the following information:

<table>
<thead>
<tr>
<th>Type</th>
<th>OID</th>
<th>Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>displayName</td>
<td>urn:oid:2.16.840.1.113730.3.1.241</td>
<td>Johnny Doe</td>
<td>USED for CN.</td>
</tr>
<tr>
<td>cn</td>
<td>urn:oid:2.5.4.3</td>
<td>John Doe</td>
<td>fallback for CN.</td>
</tr>
<tr>
<td>sn</td>
<td>urn:oid:2.5.4.4</td>
<td>Doe</td>
<td>fallback for CN.</td>
</tr>
<tr>
<td>givenName</td>
<td>urn:oid:2.5.4.42</td>
<td>John</td>
<td>fallback for CN.</td>
</tr>
<tr>
<td>mail</td>
<td>urn:oid:0.9.2342.19200300.100.1.3</td>
<td><a href="mailto:johndoe@example.edu">johndoe@example.edu</a></td>
<td>yes</td>
</tr>
<tr>
<td>eduPersonPrincipalName</td>
<td>urn:oid:1.3.6.1.4.1.5923.1.1.1.6</td>
<td><a href="mailto:jd@example.edu">jd@example.edu</a></td>
<td>yes</td>
</tr>
<tr>
<td>eduPersonEntitlement</td>
<td>urn:oid:1.3.6.1.4.1.5923.1.1.1.7</td>
<td>urn:mace:terena.org:terena:personal-user</td>
<td>yes</td>
</tr>
<tr>
<td>schacHomeOrganization</td>
<td>urn:oid:1.3.6.1.4.1.25178.1.2.9</td>
<td>example.edu</td>
<td>yes</td>
</tr>
</tbody>
</table>

Q: What is needed to validate an organisation?

The rules for validation are set by the CA/B Forum. The rules are as follows:

*If the Subject Identity Information is to include the name or address of an organization, the CA SHALL verify the identity and address of the organization and that the address is the Applicant’s address of existence or operation. The CA SHALL verify the identity and address of the Applicant using documentation provided by, or through communication with, at least one of the following:

1. A government agency in the jurisdiction of the Applicant’s legal creation, existence, or recognition;
2. A third party database that is periodically updated and considered a Reliable Data Source;
3. A site visit by the CA or a third party who is acting as an agent for the CA; or

The CA MAY use the same documentation or communication described in 1 through 4 above to verify both the Applicant’s identity and address. Alternatively, the CA MAY verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable.

Q: Where can I find maintenance and status information for the service?

For Sectigo Cert Manager: [https://sectigo.status.io/pages/5938a0dbef3e6af26b001921](https://sectigo.status.io/pages/5938a0dbef3e6af26b001921).

For the Seamless Access SAML discovery service: [https://status.seamlessaccess.org/](https://status.seamlessaccess.org/).

Q: What about the expiring certificates in the certificate chain?

Some of you may have noticed that the chain certificates we get from Sectigo contains a certificate at the top with CN = AddTrust External CA Root and an expiration on 2020-05-30. For an explanation of why this should not cause problems for you, please see "Sectigo AddTrust External CA Root Expiring May 30, 2020" on the Sectigo site.

You may also notice that the next level down in the chain is CN = USERTrust RSA Certification Authority which also expires on 2020-05-30, and that is the certificate that has signed the CN = GEANT OV RSA CA 4 certificate that in turn has signed the SSL certificate for your server. That also seems bad, doesn’t it? It turns out that certificate is there to support the CN = AddTrust External CA Root "feature" and that there is another version of CN = AddTrust External CA Root present in the root store of the browsers (using the same key) which is valid until 2038-01-18, and that is the one that matters and makes the browser trust the GEANT-branded CA certificate and therefore your server certificate.

The conclusion is that things will work after 2020-05-30 too.

Do we really need all those certificates in the chain?

No. You should be fine with only the GEANT-branded sub-CA certificate (CN = GEANT OV RSA CA 4 or similar) configured as chain certificate in your server.

Where can we check if our server sends the correct chain?

We recommend [Qualys SSL Server Test](https://www.qualys.com/products/ssl-server-test/) which tests this and a lot of other useful things (most of them related to your server configuration, not the certificates as such). For the chain specifically, look at the "Chain issues" heading where you want to see "None" (if you have trimmed the unnecessary certificates from the chain) or "Contains anchor" (if you have kept the full set).

Q: Should I Use OV or Multi-domain OV?

When a TCS member orders a GEANT OV SSL certificate in Cert Manager for a name, such as mail.sample.example.org, in the Subject Alternative Names, they get a correct entry for DNS: mail.sample.example.org but they also get DNS: www.mail.sample.example.org. I have confirmed this by looking at issued certificates in our SCM instance. We recommend ordering GEANT OV Multi-Domain for the time being instead of GEANT OV SSL. This issue has been raised with the supplier.
Q: Are Document Signing Certificates available via Sectigo?

It is currently possible to order Document Signing Certificates on a preconfigured USB token from Sectigo. More information on this process is available in this GUIDE.

Q: How Do I Order EV Code Signing Certificates

Similarly to document signing certificates, EV Code Signing Certificates need to be provided on a preconfigured USB token from Sectigo. More information on this process is available in this GUIDE.

Q: How do I create an EV Anchor?

After the NREN MRAO validates all domains, organisations themselves have to set EV anchors and then order EV certificates. A draft of the EV Anchor guide is AVAILABLE.

Q: Where can I report abuse issues?

These can be reported following the information at: https://sectigo.com/support/report-abuse.

Q: What are the names of the grid certificates in Sectigo?

For the grid products, the mapping is:
- Grid Host SSL -> GEANT IGTF Multi Domain
- Grid Premium -> GEANT IGTF-MICS Personal RSA
- Grid Robot Email -> GEANT IGTF-Classic Robot Email RSA
- Grid Robot Name -> GEANT IGTF-MICS Robot Personal RSA

Q: My Code Signing request is stuck in applied status?

Login in to the Portal > goto Settings>Certificate Profiles Filter Certificate Type Code Signing> Select Sectigo Public CA> click edit> Where Term is click the select button remove the multiple selected years and select only the one term form now (to three years only). This will temporarily fix the stuck in requested state.

Q: How do GÉANT and Sectigo deal with GDPR / data protection?

Sectigo has a detailed Privacy Notice available for all users. As part of the procurement process, data protection and security measures at Sectigo were evaluated according to the standard GÉANT process for service procurement. The GÉANT GDPR team has prepared a document showing their overall review of the privacy position for Sectigo.

Q: How can I make sure I get the location details right in my certificate?

In order to meet the CA/B guidelines, it is essential that all location information is correctly entered in certificate fields. We recommend ONLY completing the Locality and Country information where possible - the more information entered, the more likelihood there is that something will go wrong. Certificates may be revoked for something as small as the difference between Noord Holland and Noord-Holland in the State field. https://en.wikipedia.org/wiki/ISO_3166-2 is generally used a guide to the correct way to add information, but may not be completely consistent with official local sources given the nature of wikipedia. The most common problem is with incorrect use of State - we recommend not filling this in wherever possible. If this field is populated, please make sure it matches the ISO guidelines as described in the ”sub-divisions” column in the cited wikipedia page. Do not abbreviate names (N-Holland is not allowed), or add excess data.

Q: How do I deal with non-ACII characters for IGTF certificates?

IGTF certificates must not contain non-ACII characters. There are several ways to manage this:

- If your organisation name contains non-ASCII characters, please enter an ASCII version in the ”Secondary Organization Name” box under Settings. E.g. GÉANT Vereniging becomes GEANT Vereniging.
- Try to limit the fields that you complete for the certificate - it is only necessary to complete Locality and Country.
- Sectigo are happy to change fields to include ASCII characters once validation has occurred. Please contact the helpdesk for this.
- If you would prefer to keep non-ASCII characters within your normal certificates, you can create a second organisation with the same data but with non-ASCII characters completed. We recommend alerting the helpdesk that this is your intention.

Q: How can I create a .csr file?

There’s a simple tool to create OpenSSL .csr files here: https://www.digicert.com/easy-csr/openssl.htm

Sectigo provide a guide on the creation of .csr files here: https://support.sectigo.com/Com_KnowledgeDetailPage?Id=kA01N000000zFIo