TCS 2020 FAQ

- **INFOSHARE SLIDES**
  - Q: Where can I find documentation for Sectigo?
  - A: A quick start guide can be found at: https://support.sectigo.com/Com_KnowledgeDetailPage?Id=kA03l000000vFnd
  - 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=
  - Details on S/MIME Validation can be found in the attached slideset.

  - Q: Where can the Sectigo certificate chains be found?
  - Q: What Membership Category is my NREN?
  - Q: What are the Support Hours for Sectigo?
  - Q: I am an NREN MRAO, why does my organisation have to be validated?
  - Q: What is the difference between MRAO and RAO?
  - Q: Can Sectigo login to the MRAO accounts?
  - Q: How do I enable SAML?
    - To enable SAML for admin access to SCM:
    - To use SAML "self-enrollment" for server certificates (allows users outside of SCM admin to request server certificates):
    - To use SAML in order to allow users to order client certificates:
  - Q: What is needed to validate an organisation?
  - Q: Where can I find maintenance and status information for the service?
  - Q: What about the expiring certificates in the certificate chain?
  - Q: Do we really need all those certificates in the chain?
  - Q: Where can we check if our server sends the correct chain?
  - Q: Should I Use OV or Multi-domain OV?
  - Q: Are Document Signing Certificates available via Sectigo?
  - Q: Are eIDAs Certificates available via Sectigo?
  - Q: How Do I Order OV Code Signing Certificates?
  - Q: How Do I Order EV Code Signing Certificates?
  - Q: How do I create an EV Anchor?
  - Q: Where can I report abuse issues?
  - Q: My Code Signing request is stuck in applied status?
  - Q: How do GÉANT and Sectigo deal with GDPR / data protection?
  - Q: How can I make sure I get the location details right in my certificate?
  - Q: How do I deal with non-ASCII characters for IGTF certificates?
  - Q: How can I create a .csr file?
  - Q: Why is My order stuck in Applied?
  - Q: Why are there now also 'authentication' TCS certificates?
  - Q: What happened to the list of profiles in the 'clientgeant' (SAML) portal?
  - Q: I have relying parties using client authentication for services (web site access, IdP login, eduroam, ...). Do they need to act?
  - Q: does my organisation need to be re-validated to issue S/MIME certificates after August 28th, 2023?
  - Q: is GÉANT looking at the impact of the changing / volatile certificate market?
Q: Where can the Sectigo certificate chains be found?

- https://crt.sh/?CAName=%25GEANT+Vereniging%25
- TCS Trust Anchors and Intermediates

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 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
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:

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.
3. Step 3: check that all the needed attributes are correctly released at the following URL: http://cert-manager.com/customer/<YOURNREN>/ssocheck/.
4. 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):

1. go to Settings>Organizations>select organization.
2. Edit the organization and select the SSL certificates tab.
3. Select "self enrollment using SAML". This will provide you with a unique url that can be shared with users.
4. 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:

2. Configure your IdP correctly for Sectigo. See below.
3. 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.
4. 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 for Authentication certificates:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>urn: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 for Authentication certs.</td>
</tr>
<tr>
<td>cn</td>
<td>urn:oid:2.5.4.3</td>
<td>John Doe</td>
<td>fallback for CN for Authentication certs.</td>
</tr>
<tr>
<td>sn</td>
<td>urn:oid:2.5.4.4</td>
<td>Doe</td>
<td>fallback for CN for Authentication certs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>required for email signing certs (used for CN).</td>
</tr>
<tr>
<td>givenName</td>
<td>urn:oid:2.5.4.42</td>
<td>John</td>
<td>fallback for CN for Authentication certs.</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>required</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>required</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:tcs:personal-user</td>
<td>required</td>
</tr>
<tr>
<td>schacHomeOrganization</td>
<td></td>
<td></td>
<td>required</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;
A third party database that is periodically updated and considered a Reliable Data Source;
A site visit by the CA or a third party who is acting as an agent for the CA; or
An Attestation Letter.

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.

For S/MIME certificates, the CA/B forum requires:

1. Formal name of the Legal Entity;
2. A registered Assumed Name for the Legal Entity (if included in the Subject);
3. An organizational unit of the Legal Entity (if included in the Subject);
4. An address of the Legal Entity (if included in the Subject);
5. Jurisdiction of Incorporation or Registration of the Legal Entity; and
6. Unique identifier and type of identifier for the Legal Entity.

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

For Sectigo Cert Manager: https://sectigo.status.io/pages/5938a0dbef3e6af26b001921.

For the Seamless Access SAML discovery service: 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 which tests this and a lot of other useful things (most of them related to you 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. These can be ordered here: https://www sectigo.com/ssl-certificates-tls/document-signing-certificates. Participants can use the following discount code which will only charge you for the token and not the certificate itself: QQY1XB49V9.

Q: Are eIDAs Certificates available via Sectigo?

eIDAS certificates can be ordered via: https://sectigo.com/ssl-certificates-tls/eidas-signing-certificates-for-citizens. There is a charge for these certificates.

Q: How Do I Order OV Code Signing Certificates?
From 8th May 2023 it will only be possible to order code signing certificates that comply with specific HSM standards OR that are supplied directly on a token by Sectigo. More information is available here: https://sectigo.com/knowledge-base/detail/Changes-to-Sectigo-Code-Signing-Offerings /kA03l000000BoIs. Currently supported devices are:

- Thales/Safenet Luna and nethSM devices
- Yubico FIPS Yubikeys (for ECC keys only)

If you have a specific device you want to use that is not currently supported, please let the TCS Service Owner know and we can raise with Sectigo. We STRONGLY recommend that you purchase your own device rather than ordering one from Sectigo as the delivery times cannot be guaranteed and you may be charged additional international shipping / customs charges which are outside of our control.

More information about using your own Yubikey to order a certificate can be found at: https://www.sectigo.com/knowledge-base/detail/Key-Generation-and-Attestation-with-YubiKey/kA03l000000roEV.


To order an OV Code Signing certificate on your own device, please order via Cert Manager.

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. These can be ordered here: https://www.sectigo.com/ssl-certificates-tls/code-signing using discount code: 3G5YPN6T8.

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: 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 different 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-ASCII characters for IGTF certificates?

IGTF certificates must not contain non-ASCII 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. GEANT 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.

Q: Why is My order stuck in Applied?

Applied generally means that the request has been sent for manual review. Checking the following may help:

1. CAA records of all FQDNs & domains contained in the certificate request
2. Umlauts, diacritics etc in the org name or province/state etc - at some time that caused a manual review of the first request which included these characters by Sectigo
3. org names that are exactly 64 "bytes" and beware that single UTF-8 characters might count as 2 bytes
4. block-listed words in the requested domains like "test", "demo" etc
5. some very special encoding of ECC keys caused stalled applied cert requests
6. reasons given by the Sectigo Order Checker https://secure.trust-provider.com/products/ORDERSTATUSCHECKER

If a certificate has been in applied for more than a few hours, please contact support: https://sectigo.com/support-ticket/

Q: Why are there now also 'authentication' TCS certificates?

The CA/Browser forum industry standard body in 2023 introduced an assurance baseline as well as specific technical profiles for S/MIME certificates that affect the way we have deployed a joint-trust S/MIME and authentication client certificate profile for the 4th generation GEANT TCS. While the trust and assurance levels defined in these S/MIME Baseline Requirements are currently already met (or exceeded) by the GEANT TCS Personal CAs Certification practices, the technical profiles envisioned for S/MIME BR make it impossible to continue to use a single Issuing CA and publicly-trusted Root CA for both email-signing and client authentication personal certificates.

We have concluded that separating the email S/MIME use cases and the client authentication use cases is the best way forward. Client authentication will be serviced by an independent, community specific trust model (i.e., a private CA), and we will keep the publicly-trusted S/MIME CA service available for email signing and encryption use cases, which are also ubiquitous in the TCS community.

Both a public-trust service as well as a private-CA service will be operated in parallel, and both will be available to the entire TCS constituency based on the current assurance practices.

The details for the transition as well as additional background can be found in the "GEANT TCS Gen4 private CA extension" specification of July 12th, 2023.

Q: What happened to the list of profiles in the 'clientgeant' (SAML) portal?

As soon as practical, the 'clientgeant' SAML portal will add the two new profiles in addition to the current ones. So "GEANT Personal Authentication" (private trust individual client authentication) and "GEANT Personal Automated Authentication" (private trust agent authentication for personally-controlled agents) will be added to the list.

After August 28th, the old "GEANT IGTK MICS Personal" and "GEANT IGTK MICS Personal Robot" will be removed from the SAML portal. At the same time, the "GEANT Personal" profile (which will be renamed to "email signing and encryption") will become a public-trust S/MIME only email signing and encryption profile. This public S/MIME will use the sponsor-validated profile to insert the givenName and surname of the applicant alongside the organisation name.

The following profiles should be available:

- **GÉANT Personal email signing and encryption**
  - this is a public certificate and thus follows the new issuance/validation rules
  - issued via SAML Self-Enrollment
  - since the Subject CN contains a person's name, this must be based on the new Public S/MIME Sponsored Validation Multipurpose certificate template
  - since this template is of new sub-type Public Sponsored Validated, "it can only be issued to person's with a validation type of High". This will block issuance of this profile to brand new persons created during the enrollment flow. New persons start with a validation type of Standard.
- **GÉANT Organisation email signing**
  - this is a public certificate and thus follows the new issuance/validation rule
  - issued via Invite
  - since the Subject does not contain any person information it should be based on the new Public S/MIME Organization Validation Multipurpose certificate template
  - it can be issued to newly created persons with validation type of Standard
- **GÉANT Personal Authentication – RSA**
- **GÉANT Personal Authentication – ECC**
  - two profiles needed that show as one option in the self enrollment service – there are two private CAs and thus two certificate templates
  - this is a private certificate
  - issued via SAML Self-Enrollment
  - same as old IGTK Personal
- **GÉANT Personal Automated Authentication – RSA**
- **GÉANT Personal Automated Authentication – ECC**
  - two profiles needed that show as one option in the self enrollment service – there are two private CAs and thus two certificate templates
  - this is a private certificate
  - issued via SAML Self-Enrollment
  - same as old IGTK Personal Robot
- **GÉANT Organisation Automated Authentication - RSA**
Q: I have relying parties using client authentication for services (web site access, IdP login, eduroam, ...). Do they need to act?

Yes, relying parties using TCS Personal and eScience Personal certificates must act before August 28, 2023. There are a few scenarios:

- the service uses GEANT eScience Personal (uniquely-named) client certificates: install the new “Research and Education Trust” certificates, and depending on the client application - also the "GEANT TCS Authentication RSA/ECC CA 4B". These can be found in the TCS Repository. All relevant certificates are also distributed by the IGTF in distribution versions 1.122 and above (ECC variants in version 1.123). The subject naming of the end-users will remain the same.
- After August 28th, applicants will no longer be able to request eScience Personal certificates from the joint-trust eScience Personal (ECC) CA 4. This option will be removed from the clientgeant portal. Already issued certificates will remain valid for their entire stated period.
- the service uses GEANT Personal (common-name only) client certificates: review your use case carefully. If authentication relies on the subject name in the certificate, note that - even today! - this name is not guaranteed to be unique. There may be multiple users that end up getting the same subject name! You are urgently encouraged to change to the new "Research and Education Trust" and the "GEANT TCS Authentication RSA/ECC CA 4B".
- Even if you decide to stay with the current GEANT Personal CA 4 S/MIME email certificates, beware that the subject name format will change: it may no longer contain a commonName, will include givenName and sn attributes, and may include other RDN components not currently present in the name format.
- the service uses GEANT eScience Personal Robots for role-based authentication (e.g. monitoring agents, data movement agents, &c): install the new "Research and Education Trust" certificates, and depending on the client application - also the "GEANT TCS Authentication RSA/ECC CA 4B". Through the SCM invite process, you will request a "GEANT Organisation Automated Authentication" certificate for these subscribers.
- the service uses GEANT eScience Personal Robots for sending emails (re-signing mail list servers, automated mailing by roles such as security teams sending user notices, &c): for these applications you need public S/MIME trust. This means continuing to use the GEANT Personal CA 4, but in SCM request "GEANT Organisation email signing"

Note that the "GEANT IGTF Robot Email" profile is thus split by purpose: there are two new profiles, one private trust for authentication, one public trust for organisation-validated S/MIME!

Q: does my organisation need to be re-validated to issue S/MIME certificates after August 28th, 2023?

Yes, due to slight differences in the industry requirements the set of ‘authentic information sources’ that Sectigo has to use for organisation validation is different. Whereas for SSL validation an independent information source may be used, for S/MIME only government agency sources and Legal Entity Identifier (LEI) data references are allowed. This means Sectigo has to do re-Validation. This is not triggered automatically - it needs to be requested by an MRAO. We strongly recommend that you DO NOT SELECT TO REVALIDATE AN ORGANISATION as this will block the ability to issue SSL certificates as well. Instead, choose to edit an organisation and enter an organisational identifier in the new relevant field...this is typically a VAT number or equivalent. If you do not have this, enter FIXME in the field and the validation team will attempt to find the correct number.

Q: is GÉANT looking at the impact of the changing / volatile certificate market?

Yes, we have prepared a briefing paper for NRENs and will be undertaking a series of information gathering and discussion workshops in 2024.