

SUNET TCS 2020- Information for administrators

This is for administrators at SUNET TCS members for the 2020- "Sectigo generation" of the SUNET TCS service.

If you are a user of SUNET TCS but not an administrator, please see SUNET TCS documentation at your organization.

Note about the change of SCM web UI on 2021-11-20

The web interface changed on 2021-11-20. We have updated this document to reflect changes introduced by that, but we may have missed things. Please remind us if that is the case.

You can watch a video from Sectigo that presents what has changed:

Our SUNET instance of SCM

Our SUNET instance of the Sectigo Certificate Manager is at <https://cert-manager.com/customer/sunet>

To access it, you need to have your organization and your admin user(s) set up. See below under "Getting access to the system".

Getting help

Check Sectigo Status Page

First, check at <https://sectigo.status.io/> if there are known issues with the service for the moment. You may also want to use the **Subscribe** function to get email (or notifications via webhook or RSS) about updates to that page.

Join the TCS network at SUNET Forum

Consider joining the TCS network at <https://forum.sunet.se/s/tcs/> to get information and to be able to discuss the service with SUNET TCS and other users. Important news will also be shared, as before, using the SUNET-TCS-MEMBERS mailing list (where one function address per organization is present since your organization joined the service), but information about minor issues may be shared here, as well as tentative information before we know enough to raise it to the SUNET-TCS-MEMBERS level.

Help from SUNET TCS

Email tcs@sunet.se after making sure that this document does not contain the answer to your question or a solution to your problem. Do not email Kent's personal email address.

Help from Sectigo Support

If instructed by SUNET TCS or this document, or if you are waiting for a certificate stuck in Applied, contact Sectigo Support:

- Go to <https://sectigo.com/support-ticket>
- Use type "Validation Support" and reason "Certificate Validation" for issues related to certificates (delays, problems with the contents, etc).
 - Use case type "Technical Support" and case reason "Sectigo Certificate Manager (SCM)" for issues with SCM not related to certificates per se
- Include the certificate order number in the specific field for that.
 - If the ticket is about more than one certificate, include one order number (the most important one?) in that field, and include all of the order numbers in the description.
- In the description, include a line at the top saying "We are a SUNET member of the GEANT TCS service, using the <https://cert-manager.com/customer/sunet> SCM instance."
- Describe the problem, for example "The following certificates are stuck in Applied instead of being issued. Please issue them or tell us what we need to do."

If you need urgent support, contact tcs@sunet.se for help with escalation. Tell us the support case number. Also tell us other information we need to know (for example order numbers and CNs in the case of delayed certificates).

Sectigo Documentation

Sectigo documentation can be found at https://support.sectigo.com/Com_KnowledgeProductPage?c=Sectigo_Certificate_Manager_SCM

Some highlights:

- "SCM - Sectigo® Certificate Manager Quick Start Guide" is a short introduction to the SCM system

- "SCM - Sectigo Certificate Manager Administrator's Guide" is the very much longer description
- "SCM - Sectigo Certificate Manager REST API" describes the REST API

Differences from the DigiCert generation 2015-2020

New vendor, new web interface

Sectigo is the new vendor for TCS instead of DigiCert. We are using their Sectigo Certificate Manager (SCM) instead of DigiCert CertCentral. The rest of this section describes the most important changes you need to understand.

No "division" objects in the new system

There is no concept of divisions in SCM as there was in DigiCert CertCentral.

- SUNET TCS has an instance of SCM at <https://cert-manager.com/customer/sunet> which is used by all SUNET TCS administrators (at your level and at the SUNET "superuser" level) but not by GEANT TCS members from other countries.
- At the SUNET level, we cannot just create a division for a SUNET TCS member and ask you to create an organization object yourselves with all relevant information, as you did in CertCentral. We have to create an Organization in the system to be able to add you. See below for more practical information on how you join.
- If you need to validate another organization (due to the need to have something different in the O= field of the certificates), that new organization will be "at the same level" as your original organization and there is no division that contains them. You will have access to both organization due to the fact that we/you will add the same admins for both organizations.

No "User level users"

In DigiCert CertCentral, there were two basic kind of users: "Administrators", who could order/approve certificates, change settings and do other admin level stuff, and "Users" who could only request certificates (but who were nevertheless authenticated by logging into CertCentral just like the Administrators).

In the SCM, there are basically only Administrator level users. In fact, the SCM does not talk about users, it talks about admins. That means that you cannot have users logging in to the SCM who can only request certificates. See below under "SSL certificates" for solutions to this.

Departments

The SCM lets you create Departments under Organizations. ~~Just like the Organization name is what goes into the O= of a certificate, the Department name is what goes into the OU= of a certificate.~~ You can use Departments in two ways:

- Just as a tool to sort certificates ~~and get the correct OU= set~~, but it will still be the Organization's admins doing the approval.
- To delegate approval of certificates to department admins for their department. In most(?) cases that would be combined with registering a subdomain (or a completely different domain) and restrict the department to that.

Since the summer of 2022, OU is no longer present in the certificates due to decisions within the CA/B forum.

MRAO, RAO, DRAO!

There are three levels of admins in the SCM, all called something with RAO (Registration Authority Officer) in the name:

- MRAO: the "superuser level" for SUNET people that can work with all organizations, departments, domain, certificates, admins, etc.
- RAO: the admin level for working with an organization and the departments, domains, certificates, admins etc that belong to that organization.
- DRAO: the admin level for working with a department, and the domains, certificates, admins etc that belong to that department.

It is a bit more complicated than that: a RAO is connected to one or more organizations, and a DRAO to one or more departments, and there is also the possibility to only have the right for SSL certificates, client certificates and/or code signing certificates. Thus, an admin could be "RAO - SSL Certificates" and "RAO - client certificates" for Organization A, while also being "DRAO - SSL Certificates" for a department belonging to another organization.

The first admin you will get when joining with your organization will be RAO for all certificate types and for your organization.

Getting access to the system

Members of the "Digicert generation" 2015-2020 service

To get access to the new system, email tcs@sunet.se with a subject line like "TCS2020: *organization name*" and tell us:

- First name, last name, email and preferred user name for the first admin (RAO) of your organization. That person should be a current Administrator in the DigiCert CertCentral system.
- Organization name, address line, postal code, city and county (*län*).

We know that Sectigo uses at least <https://www.infobel.com/en/sweden> and <https://proff.se/> to check address and postal code, so please try to find a record there for your organization and use that address line and postal code if it is not obviously wrong (it's not likely that people will rely on the address information in your OV certificates to send you paper mail...). Also, they seem to prefer the visiting address (*besöksadress*) over the mailing address (*postadress*) so please use the former.

If you try to use other address/postal code information you risk having your organization validation delayed. You are encouraged to include a direct link to the matching infobel/proff record in your email.

New members (not in the "DigiCert generation" 2015-2022 service)

If you have not been a member of the 2015-2020 "DigiCert generation" of the service, you are still welcome to join. SUNET TCS is available to all SUNET customers without extra charge. Contact tcs@sunet.se about membership in the service. Do not send any paper documents before that.

Please note that during the spring of 2020 we are prioritizing bringing the current members over to the new service.

Validation

Domains

You must validate one or more domains before you can have certificates issued. You validate your "top domain", not internal subdomains or the name of individual servers (i.e. *example.org*, not *www.example.org* etc)

There are multiple steps in this process. This is how you add the domain *example.org*:

1. Make sure that you are not having CAA records in your DNS zone that forbids Sectigo from issuing certificates for the domain. If that is the case, domain validation will fail too. Having no CAA records is OK, as is having CAA records mentioning "sectigo.com" as approved.
2. Go to **Domains** and press the **+** button. Fill in the domain name (*example.org*) and the optional description. Select the type of certificates (SSL, client, CS) that should be enabled for this domain. For your main domain you would typically enable all of them, but for most additional domains you would only enable SSL certificates. If you have set up Departments and this domain should be delegated to the DRAOs of that department, expand the selection line and enable the domain for the right department and the appropriate types too.
3. Use **+** again, and redo exactly the same step for the domain name with "." prepended to it (**.example.org* in our example). If you do not do this step, you will only be able to issue certificates for the domain name itself (*example.org*) but not for names below it (such as *www.example.org*).
4. Wait for a SUNET MRAO to approve your domain delegations. When this is done, the delegation status will be approved and you can proceed to the next step.
5. Go to **Domains** and select the domain. Use the **Validate** button on the Domain Control Validation card to the right to initiate DCV. Select method:
 - **Email** means that you select one of the five allowed addresses for the domain, and then receive and handle an email sent to that address. For our example, it would be one of "admin@example.org", "administrator@example.org", "hostmaster@example.org", "postmaster@example.org" or "webmaster@example.org".
 - **CNAME** means that you will be instructed to put a CNAME record with a hash value name in your DNS zone, pointing to another hash value. The system will tell you the values. Please verify using an external resolver that the CNAME record is in place and externally visible.
 - **Do not use HTTP/HTTPS**. This method means that you will be instructed to put certain contents in a file with a certain name on the web server for your domain name. As of November 2021, this method is not enough to cover names below the validated name itself. See [Sectigo notification about this](#).
6. Follow the instructions for the method you selected.
7. When the validation is OK, you will see Validation Status as Validated in the Domain Control Validation card.
8. You are now ready to use this domain and its subdomains for certificate requests.

Revalidation of Domains

The domain validation (DCV) is valid for one year. Domains have to be revalidated to continue to issue certificates for them. To revalidate a domain, follow the same steps as above from item 5.

Note: if a domain has validation status Validated but does not show a Expires date, it needs to be validated again. Follow the same steps as above from item 5.

See below under **Notifications** about adding that for DCV Expiration.

Deleting Domains

There is no way for a RAO or DRAO to delete a domain from the system. If this is needed, contact tcs@sunet.se for help.

Additional organizations

If you need additional organization names (values for the O= part of a certificate), that will have to be added by a SUNET MRAO for you. Follow the same steps as for your first organization (see above under "Getting access to the system"), but instead of providing information about a "first admin", tell us the usernames for the administrators of your "main organization" that should also be RAOs for the new organization.

Note: you will not add an extra organization ("Smorgasboda Högskola" in addition to "Smörgåsboda Högskola") for a name without non-ASCII characters for grid certificates, as that will be handled differently. We will update this document when Sectigo has provided the details.

Departments

To add a department:

- Go to **Organizations** and click on the organization line to check it, then use the **Add Departments** button in the card shown for the Organization.
- Fill in the desired department name in the Department Name field. The rest of the name components will be as for your organization. Do **not** fill in the Secondary Organization Name or Academic code.
- On the second page, select Client Certificates and disable "Allow Key Recovery by Master Administrators" and "Allow Key Recovery by Department Administrators", respectively). It will already be disabled for Organization Administrators as that was part of the organization setup done by SUNET.
- Do not fret over other options on the various tabs, as they can be changed later. Do not enable or change things you do not understand. Finish using the **Save** button.

Admins connected to the department

You can now go on to create admins (see below) that are DRAOs connected to just this department instead of being RAOs for the whole organization.


Domains connected to the department

If you add department admins (DRAOs) that can approve certificates for their department, you will most likely want to limit them to their own domain (*department-example.com*) or a subdomain of your main domain (*department.example.org*) if we imagine that your main domain is *example.org*.

In the first case with a completely new domain for the department, follow the normal domain validation procedure above to add *department-example.com* (and **.department-example.com* if needed for wildcards) with delegation to the department and initiate DCV as you did for your main domain.

In the second case with a subdomain of your already validated main domain, you will still add *department.example.org* (and **.departement.example.org* if needed for wildcards) with delegation to the department but you will **not** have to initiate DCV again, as the SCM is smart enough to know that *example.org* is already validated.

Admins

You create additional admins (RAOs for your whole organization or DRAOs for departments you have created) under the **Settings Admins** tab with the  button. You can also edit existing admins by clicking on the line to check them and then using the **Edit** button.

- Fill in a suitable username, email, forename and surname. We advice you to leave the rest of the contact information empty, as it is not needed. Save this.
- Under the Authentication tab, select "Your Institution" as SAML IDP and provide the users EPPN ("federated identity") in the EPPN field. You can also set a password for the new admin. The first time they login they will have to change it.
- Select the desired privileges under **Role & Privileges**. Do not check "WS API Use Only" (will be explained later).
- Select the desired role (RAO for the organization or DRAO for a department) in the **Roles** dropdown. Select the certificate types the admin will be able to manage and use the pencil icon to select organization and/or departments.
- Save when done.
- You have to communicate the selected password to the new admin (it is not emailed by the system).

We **strongly** recommend that you create personal admin users (not shared ones), to be able to see who has done what in the system.

It was earlier the case that some privileges (management of peer admins, Allow DCV) could not be assigned by one RAO to another. This is no longer the case - if you can create/edit peer admin users, you can delegate your privileges too.

Note: the **Automatically approve certificate requests** privilege seems to be a bit misnamed after recent changes. Without it, the admin does not get the manual Approve button either. Thus, you need to set this privilege for admins that should be able to request and approve certificates.

Locked Account

You can get locked if you fail to login a number of times. You will then get an "Incorrect login details, account is locked, password has expired or your source IP is blocked." message when you try to login, even if you use the correct password. It will be the case even if your password have been changed by another admin who can do that for you. This requires the lock to be reset and that can only be done by an MRAO, so you need to contact tcs@sunet.se.

SSL Certificates

Applying for and approving certificates in the SCM as an admin

Go to **Certificates SSL Certificates** and press  to request a certificate.

- Select the **Using a Certificate Signing Request (CSR)** mode

- Select organization/Department as needed, and the correct Certificate Profile. You can also add Comments and provide the email address of the external requester.
- On the next page, provide a CSR by pasting it into the text area or upload it as a file using the upload icon.
- On the next page, add any additional Subject Alternative Names, one at a time, using the +-button after each entry.
- On the next page, accept or decline auto-renewal and finish with **OK**.

If your admin has the "Allow SSL auto approve" privilege selected, the certificate will be automatically approved (which makes sense, because why would you have entered all the information above if you did not want to approve the certificate?) and will show up as "Applied".

If your admin does not have that privilege selected, the certificate will show up as "Requested" and you will have to approve it by selecting it and using the **Approve** button.

When the certificate has been issued, its status will be shown as "Issued" and you will get an email about it.

If needed, you can also download the certificate by clicking on the line to check it and using the **View** button, then the download icon (arrow pointing down at a line).

Notes on specific certificate types

GÉANT OV SSL

Currently (2020-04-08), if you use the GÉANT OV SSL type and request a certificate for `mail.test.example.org`, you will get that name put in a DNS Subject Alternative Name, but you will also get a DNS Subject Alternative Name for `www.mail.test.example.org`. We recommend that you use GÉANT OV Multi-Domain instead if you do not want this, as no extra www-prepended name is added for that type. *This has been reported to GÉANT.*

EV Certificates

As of the autumn of 2021, SUNET TCS recommends that you do not use EV certificates. The benefits are limited and the procedure for requesting them is more complicated and prone to complications than for OV certificates.

Please do not order EV certificates or EV anchor certificates without talking to tcs@sunet.se first, as the procedure will not be to just to request an individual EV certificate, and you may be locked out of ordering normal OV certificates while EV validation takes place.

IGTF (Grid) Certificates

If you are not currently using IGTF (grid) certificates, talk to tcs@sunet.se first before starting to request them.

Allowing non-admins to request certificates

This has changed. Contact us if you need this functionality.

~~You can allow persons who are not admins in the SCM to request certificates ("enroll" in Sectigo speak). To do that, go to **Organizations** and select your organization and select **Edit**. (Or, if this should apply only to a department, after selecting the organization, use the **Departments** button, select the department, and use **Edit** on that instead).~~

- ~~• On the **Certificate Settings - SSL Certificates** tab, enable **Self Enrollment** and put a shared secret value in **Access Code** and copy the URL present below that field. You can now hand out this URL to persons who can use it with the access code to access the Certificate enrollment page for non-admins. As you can see when you test using it, it contains approximately the same fields as the "Add Certificate" pages in the SCM itself. *Be aware that the email address is not checked (more than for having the right domain) so you need an out of band method of authenticating the requester.*~~
- ~~• If you have SAML attribute release working towards Sectigo (see "SAML Configuration" below), you can also enable "Self Enrollment via SAML", keep the Access Code secret and hand out the URL below the Token field to users. They will then have to authenticate using SAML before getting to the same kind of enrollment form as above. *As the email address will now come from your IdP via SAML you can be more confident that it is correct, but it is up to you to decide if it is good enough, or you still will require additional conformation out of band before approving.*~~
- ~~• **Do not** enable "Automatically Approve Self Enrollment Requests". At least, you will want to manually approve certificate requests arriving via this route!~~
- ~~• You might also want to customize the SSL Types for the Enrollment Form (on the right hand side), to stop users from selecting certificate types you do not want them to. You can still keep the ability to select them in the SCM (the left hand Admin UI selection). *2020-08-18: This does not work like this after the certificate profile changes earlier this summer. We will update this later.*~~

Revoking SSL Certificates

Certificates issued on 2021-06-07 and later: You should be able to revoke them in SCM under **Certificates SSL Certificates**, using the **Revoke** button with the certificate selected.

Certificates issued before 2021-06-07: You cannot revoke them in SCM. If there is a security-related reason for revoking (for example, you suspect the private key has been leaked), use the revocation portal linked below. Otherwise, we suggest that you do not revoke the certificate. You can stop notifications for a certificate in the **Details** dialog box, using the **Suspend Notifications** checkbox at the bottom.

You can use the [Sectigo Certificate Revocation Portal](#) to revoke certificates outside of the SCM, using other methods to authenticate the request.

Client Certificates

Self-service portal via SAML

Configuring your IdP and the SCM to enable the portal

The self-service portal is located at <https://cert-manager.com/customer/sunet/idp/>

For it to work for your users, you need to

- Have your IdP configured correctly for Sectigo. See below under "SAML Configuration".
- Edit your organization object (use the pencil icon when the Organization card is shown) 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. If you cannot edit this yourselves, contact tcs@sunet.se and tell us what to enter.

For it to work for your users who need IGTF/grid certificates, you also need to:

- Edit your organization object (use the pencil icon when the Organization card is shown) and set "Secondary Organization Name" to the name used in grid certificates (with åäö transcribed correctly to ASCII if needed, and with the same upper/lowercase conventions that you have used before with DigiCert). Please check existing certificates if you are unsure or as a last resort, ask us at SUNET TCS to help you check. 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.*
- Email tcs@sunet.se about this so that we can ask for a validation of the secondary name as you cannot perform this step yourself.

Configuring your relying servers (for grid/IGTF)

For the "normal" client certificates, you should not need to configure anything.

For the grid/IGTF certificates, make sure that your servers have an up-to-date IGTF Trust Anchor Distribution that includes trust for "/C=NL/O=GEANT Vereniging/CN=GEANT eScience Personal CA 4" (for example found in the `ca_GEANTeSciencePersonalCA4-1.105-1.noarch.rpm` or newer RPM package). From September 2023, you also need "C=NL, O=GEANT Vereniging, CN=GEANT TCS Authentication RSA CA 4B" (and the corresponding ECC version) and its root "O=Research and Education Trust, CN=Research and Education Trust RSA Root CA" (and its corresponding ECC version).

Revalidating your organisation

After the change at the beginning of September 2023, your organisation needs to be revalidated to be able to issue "GÉANT Personal email signing and encryption" certificates. Send an email to tcs@sunet.se with the subject "Validering" followed by your organization name so we can take care of this for you. If you try to do it yourselves you may accidentally lose the ability to issue server certificates while the validation is ongoing.

Using the portal

The instructions here are geared towards certificate-aware RAOs. You may need to expand on this when providing instructions for your end users, for example by showing them where to import certificates in your supported web browsers, etc.

This is how you get a certificate:

- Go to <https://cert-manager.com/customer/sunet/idp/clientgeant>, select your organization's IdP and login there.
- Select the right certificate profile:
 - Use "GÉANT Personal email signing and encryption" for normal client certificate for email signing etc outside of the grid/IGTF world (this used to be "GÉANT Personal Certificate")
 - Use "GÉANT Personal Authentication" for a grid/IGTF personal (client) certificate for normal use (this used to be "GÉANT IGTF-MICS Personal")
 - Use "GÉANT Personal Automated Authentication" for a grid/IGTD robot personal certificate (seldom used, this used to be "GÉANT IGTF-MICS-Robot Personal")
- Select the number of days the certificate should be valid.
- Select if you want the key generated on the server side or locally. While the former is more convenient, there may be policy reasons or technical reasons for not using that:
 - Use "Key Generation" as Enrollment Method if you want a certificate with the key generated on the server side.
 - Use "CSR" as Enrollment Method if you do not want the key generated on the server side. You will have to provide the CSR file via file upload or by pasting it into the text box.
- If you choose to provide the CSR, you must first have created your key and CSR locally, using whatever software you use for that. With OpenSSL, that could be:

```
openssl req -new -newkey rsa:2048 -out usercert_request.pem -keyout userkey.pem -subj '/CN=Mitt Namn'
chmod go= userkey.pem
cat usercert_request.pem
```

- If you choose to generate the certificate on the server side, you must provide:
 - The requested type and key size. Choose RSA-2048 if do not need a longer key and have tested that it works. Contact SUNET TCS if you need elliptic curve client certificates or RSA-8192).

- The password used to encrypt the PKCS#12 file that will be generated.
- 2023-06-12: It seems the default key protection algorithm "Secure AES256-SHA256" does not work on MacOS for importing into the Keychain, while it does work for direct import in Firefox). Select the non-default key protection algorithm "Compatible TripleDES-SHA1" instead.
- Click "Submit" and accept the click-through license.
- After a short while, you will get to download your certificate. The format depends on your choice above:
 - With "Key Generation", you will get a PKCS#12 file called certs.p12 containing key and certificate. You can import that in your browser using "Import Certificate" or similar.
 - With "CSR", you will get a PEM-formatted certs.pem containing just the certificate. If you need it in your web browser, you need to create a PKCS#12 file yourself. With OpenSSL as above, that could be:

```
openssl pkcs12 -export -inkey userkey.pem -in certs.pem -out certs.p12
```

- If you get the error message "Sectigo Certificate Manager enrollment request failed. Please contact your security administrator." when you have clicked the submit button and accepted the click-through license, it may be because you have hit the limit of two valid certificates per identity and certificate profile. You need to revoke at least one of the two certificate before another one can be issued. 2020-04-27: This behaviour will be reported as a bug to Sectigo to ask them to handle this in a smoother way.

Revoking client certificates

End users cannot revoke certificates themselves in the self-service portal. Instruct them to contact you if revocation is needed. You as RAOs can revoke certificates by going to **Certificates Client Certificates**, selecting the right certificate and clicking **Revoke**.

Issuing client certificates using the SCM

Note: this is a backup solution. The main way to issue client certificates is via the self-service portal discussed above. With that understood, this is how you can issue personal certificates using the SCM.

This has changed. Contact us if you need to use this.

- As a RAO, go to ~~Certificates Client Certificates~~ and use the ~~Add~~ button. Select the appropriate Organization, Department and Domain. Fill in the Email Address and the Common Name. Fill in the separate name fields. Leave Secret ID blank and Validation Type Standard.
- You have now added the person, rather than a certificate. Click the person to check the line and use the ~~Certificates~~ button. There, use ~~Send invitation~~ to send an invitation email to the user, containing a nonce that authorized that user to create a client certificate.
- The user will have to provide a **Password** (that will be used to encrypt the generated PKCS#12 file) and a **Passphrase** (that can be used to revoke the certificate without your assistance), as well as accept a click-through license.
- The user will then receive a PKCS#12 file containing the key, certificate and chain ready for importing in web browsers etc.

Things worth noting:

- Yes, the key is always generated on the server side when you use this method. There is no option of uploading a CSR to keep use a key generated on the client side. This may not be acceptable for users due to policy (not allowed to have the key generated on the server side) or technical reasons (key not exportable from hardware device). You can upload a CSR when you use the self-service portal.
- There is also the option of enabling a AccessCode, which is a shared secret between you and all users than enable them to get a client certificate as long as they have access to their email. *We advise you not to use that.*
- There is also the possibility to enter a SecretID per user, to enable them to get a client certificate by entering that together with their email address. *For occasional client certificates, we do not see the upside of this as compared to the invitation method above, and for bulk issuing we will rely on the self-service portal via SAML as soon as that is ready.*

Code Signing Certificates

Since spring 2023, both kinds of code signing certificates (OV and EV) needs to have the key generated on and confined to a hardware token (before this, "soft" OV code signing certificates were possible, were you generated the key on a normal computer).

See the Code Signing parts in [GEANT FAQ](#) for general information. From the array of options described there, we think most Sunet TCS members would choose:

- Buying a Yubico FIPS Yubikey yourselves (not from Sectigo) and using it to generate a key (which stays on the device) and a CSR + key attestation (which proves to Sectigo that the key was generated by the device) that is used in the SCM interface to order the certificate at no extra charge. This gives you an OV code signing certificate (which is fine if that is what you need, but if you need EV code signing, it will not suffice) using an ECC key (which is fine if that works for your application, but not if you need RSA).
- Buying an EV code signing certificate on a hardware token from Sectigo using the URL and discount code provided in the GEANT FAQ above. You will not be using SCM for this (you order from Sectigo's "normal" webstore; TCS just provides the discount code) so the extended validation will be done specifically for this purchase. Sunet TCS members using this option have received certificates based on RSA keys.

Notifications

Under **Settings Email Notifications** you can add and edit what notifications the system will send you when certain conditions are met. Use the **Add** button to have a look at the various Notification Types that are available.

- You should add at least a notification for **SSL Expiration** to make sure you get expiration emails matching the ones you got from the earlier systems. Also **DCV Expiration** should be added for the same reason.

- If you have made it possible for non-admins to request certificates (see above), you may also want to get **SSL Awaiting Approval** to be aware that there is a request to approve.
- Please do not enable "Notify MRAO Admin(s)" as that would send email to the SUNET level "superusers" too.

If you have a need to change the text in the emails sent from the system, you can do that under **Settings Email Templates**. *If you do, please report your experience with that feature (good or bad) to tcs@sunet.se.*

SAML Configuration

Configure your IdP to work with Sectigo

SAML login is activated for the SUNET instance of SCM but you need configure the attribute manually in your Identity Provider due to that the SCM entity in metadata has no defined entity category. The reason behind this is that Sectigo has registered their Service Provider in inCommon and they can't issue the European only entity category .GÉANT Data Protection Code of Conduct.

The following single valued attributes should be released to the entityId <https://cert-manager.com/shibboleth>:

- eduPersonPrincipalName (urn:oid:1.3.6.1.4.1.5923.1.1.1.6)
- mail (urn:oid:0.9.2342.19200300.100.1.3)
- displayName (urn:oid:2.16.840.1.113730.3.1.241)
- givenName (urn:oid:2.5.4.42)
- sn (urn:oid:2.5.4.4)
- schacHomeOrganization (urn:oid:1.3.6.1.4.1.25178.1.2.9)
- eduPersonEntitlement (urn:oid:1.3.6.1.4.1.5923.1.1.1.7) with the value urn:mace:terena.org:tcs:personal-user
Please note that this entitlement value must only be released for those users that fulfils the requirements for requesting personal certificates, within Sweden the requirement is SWAMID Assurance Level 2 Profile (SWAMID AL2), or higher.

SWAMID has added instruction for both Shibboleth IdP and ADFS at the page Konfigur [SAML-konfiguration Sunet TCS](#).

Test that your IdP is correctly configured

After your Identity Provider administrators has configured the attribute release you should test it at <https://cert-manager.com/customer/sunet/ssocheck>. In this test only eduPersonPrincipalName and mail is required but for the upcoming personal certificates givenName, sn, displayName, schacHomeOrganization and eduPersonEntitlement (not displayed in the test right now) will be required. To further dig down and test you can look at <https://cert-manager.com/Shibboleth.sso/Session> after a login to see what attributes was released from your Identity Provider and recognised by Sectigo.

Configure SCM

When you have verified that your IdP is correctly configured, you can go on to configure use of SAML authentication:

- To use federated login in the SCM portal you need to go into all your current RAO and DRAO admin accounts (in **Settings Admins**) and in the **Authentication** tab change the field **SAML IdP** to "Your institution" and the field **EPPN** the ePPN (eduPersonPrincipalName) of the admin. If you don't do this manual mapping of eduPersonPrincipalName to the admin account then a much more insecure automatic mapping by mail address will be done at first SAML login. *Right now there is a annoying known bug when using the SAML integration. The SAML integration picks up the name from the SAML assertion but don't handle character encoding correct.*
- See above under "Allowing non-admins to request certificates" for information about "Self Enrollment via SAML" for SSL certificates.

Using the REST API

Sectigo REST API documentation can be found at https://support.sectigo.com/Com_KnowledgeProductPage?c=Sectigo_Certificate_Manager_SCM in the "SCM - Sectigo Certificate Manager REST API" document.

Authentication is via login name and password for a RAO or DRAO admin. The `customerUri` is "sunet".

For semiautomatic API use, for example scripts run by a person on the command line, it is fine to use the normal admin user for that person.

For fully automated API use, we recommend that you create separate RAO or DRAO admins to use with the API instead of reusing the same admins as for web UI work. To create an API-only admin:

- Use your RAO to create the new admin as you would create a "normal web UI admin", including setting a temporary password. You will not be able to use the API with this temporary password.
- Login to the new admin in the SCM and perform the mandatory initial password change for it.
- Back with your original RAO, select the new admin and use the Change Type button to change this user to an API user.

More gotchas we have discovered, so you do not have to discover them too:

- You may need to enable API calls for your Organization or Department. Select it in the admin interface, use the Certificate Settings button in the information card at the right, Select SSL Certificates in the dialog, enable "Enable Web / Rest API" and save.
- Be aware that the `"serverType": -1` in their certificate enroll example refers to the "other" Server Software type, so if you have removed that when cleaning up useless Server Software types, that example will not work.

As inspiration for API use, Fredrik Domeij at LADOK has provided bash scripts to request and retrieve certificates. You find them as [ladok-sectigo-bash-2024-02-09.zip](#).

ACME support

There is support for ACME and some of the test members have started to try that. We will update this section as we get feedback.

Miscellaneous Questions

What about the expiring certificates in the certificate chain?

Some of you may have noticed that the chain certificates we got from Sectigo until the beginning of May 2020 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 = USERTrust RSA Certification Authority 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.

2020-06-02: There are reports from other NRENs that some TLS-inspecting software/boxes take exception to the expired certificates present in this chain. There is also reports of non-browser clients not working. To get an idea of what may break, you can have a look at [documentation from Carnegie Mellon University](#) on what has been affected (as they use Sectigo via InCommon).

If this affects you, update the chain to only include the GEANT CA certificate as described below.

What if we see "AAA Certificate Services" instead of "AddTrust External CA Root"?

Starting at the beginning of May 2020, the chain we get from Sectigo instead contains the root certificate with CN = AAA Certificate Services expiring at the end of 2028, and the next level is CN = USERTrust RSA Certification Authority with the same expiry date.

This is their new workaround for legacy environments. It *should* not cause problems for modern browsers/operating systems, but we have got reports where including this caused problems for some users. If you do not need the compatibility with old legacy systems provided by this chain, send only the GEANT-branded sub-CA certificate (see below).

Do we really need all those certificates in the chain?

No. Your webserver or similar should be fine with only sending the GEANT-branded sub-CA certificate (CN = GEANT OV RSA CA 4 or similar) as a chain certificate together with the server certificate. The GEANT sub-CA certificate is signed by a version of CN= USERTrust RSA Certification Authority that is present in modern browser/OS trust stores (this version is self-signed, and does not rely on CN = AAA Certificate Services).

If you need the good version of CN= USERTrust RSA Certification Authority to import in some software (for example newer versions of VMware that does not like the CN = AAA Certificate Services root), you can find it via the link on Sectigo's documentation page [Sectigo Chain Hierarchy and Intermediate Roots](#)

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).

Where can we check if there is a scheduled or emergency maintenance at this time?

You can check at <https://sectigo.status.io/> and there is also a Subscribe button there that you can use to get updates via email, webhook or RSS.