Historical: SUNET TCS 2015-2020 FAQ for administrators

Note: this document is about the DigiCert service 2015-2020. For the new Sectigo service 2020-, please see SUNET TCS 2020- Information for administrators

Getting Help

How do we get help with DigiCert portal, validation and certificate issues?

Use the Live Chat function at https://www.digicert.com/. If you cannot get the issue solved that way, contact SUNET TCS.

How do we contact SUNET TCS to get help or to report problems?

Email tcs@sunet.se after making sure that this FAQ list does not contain the answer.

Getting Information

Where do we find the Certificate Practice Statements and related documents?

At https://www.terena.org/activities/tcs/repository-g3/

Where do we find the the SUNET TCS Server Subscriber Agreement (version 2015.1)?

At Historical: SUNET TCS Server Subscriber Agreement 2015.1. As you can see, it contains the required legalese mandated in the model TCS Subscriber Agreement at the GÉANT document repository above.

Where do we find the GÉANT Association home pages for the new TCS?

For the moment, at GÉANT wiki: Trusted Certificate Service (new TCS) Home. You will find information about the DigiCert portal there, as well as information learnt during the earlier testing phases.

What is the GÉANT Association?

It is the result of TERENA and DANTE joining forces. That also means that TCS now stands for Trusted Certificate Service, not TERENA Certificate Service. You may still see TERENA using in the certificate names, where it would hurt to change the names.

Where to we find information about SUNET TCS Personal?

FIXME! We used to link to SWAMID wiki: Generell information om TCS Personal

Starting to Use the New System

We were members of the Comodo generation of SUNET TCS Server. How do we get access to the new system?

Follow the same procedure as those who were not members earlier (see next question).

We were not members of the Comodo generation of SUNET TCS Server. How do we get access to the new system?

Download SUNET TCS Server Subscriber Registration Form (version 3.0). Fill it in and send it (all pages) to the address stated at the end.We will create a division for you in the DigiCert portal. As part of that, your chosen admin contact gets an email from DigiCert and will be able to set his/her password. He /she will become the first administrator for your division. Make sure that person is available to handle the email before you apply.

How do we get the rest of our administrators added?

Your initial administatror can add more administrators using the **Add User** button under **Account Users**. Do not forget to select the Administrator Role.

Getting Validated

How do we get our organization validated for use?

Use the **New Organization** button under **Certificates Organizations**. We recommend that you use your official Swedish name as Legal name. Do not fill in Assumed name. Use the most senior member of your TCS team as your Validation Contact.

You might want to check that the organization name you request is the one that is used for your organization in databases listing companies, government agencies etc (e.g. credit information sites like www.upplysning.se, ratsit.se, well-known search sites like www.eniro.se, www.hitta.se, etc.)

We recommend that you validate for all certificate types from start.You can read more at the GÉANT TCS Wiki page about Validation.

Can we have more than one organization validated?

Yes, you can. If your university is made up of several legal entities (companies, foundations etc) you might have to register more than one organization. However, you should not create organizations for departments, schools etc that are really part of the same legal entity as the university (or similar) as such.

How do we get our domains validated for use?

Use the **Add Domain** button under **Certificates Domains**. The domain will be registered as belonging to an Organization you already added. Make sure that the domain is registered to that legal entity in the public databases (check with https://www.iis.se/ first for .se domains).You can enter one or more domains for validation while the organization validation is still pending.

What happens during validation?

DigiCert will use public databases and may also make phone calls and send emails to verify the provided information. Make sure that you are available for that the during the day.

Domain validation emails will be sent to a list of addresses based on the domain name (e.g. {admin,administrator,hostmaster,postmaster,webmaster}@yourdomain.se) as well as addresses registered in WHOIS databases. All addresses are used simultaneously, but you only need to act on one of the emails.

Verify that you can receive email to at least one of the fixed addresses above *before* submitting the domain for validation. As of 2015-04-01, the automatic DigiCert emails are sent from support@digicert.com or admin@digicert.com. Before contacting DigiCert or SUNET about emails not received, please check your spam filters.

What if the validation stalls?

During the test phase, DigiCert has validated our organizations and domains quickly. We expect that to be the case during production too. If the validation stalls with no detectable progress for a couple of hours, use the DigiCert Live Chat (see above) and ask them about the status.

What if they validate the wrong thing?

During the test phase, we have seen instances of DigiCert being "helpful" and changing the organization name when they found something similar to what you asked for, for example validating "University of Whatever Holding AB" instead of "University of Whatever". If that happens to you, use the DigiCert Live Chat (see above) to explain that they have made an error and ask them to correct it at once.

We want grid (e-Science) certificates and have an organization name containing å, ä or ö. Do we need to do something special?

Yes. As name components in grid (e-Science) certificates are not allowed to contain non-ASCII characters, you need to validate an additional organization with a name not containing the non-ASCII characters. For example, if you normal organization is "Linköpings universitet", you should also get "Linkopings universitet".

You should then be able to add the domain or domains you want grid (e-Science) certificates for under the new special organization.

Can we validate more than one administrator for EV?

Yes! Go to **Certificates Organizations** and select the right organization. Then click **Submit for Validation**. In the popup, check "EV" and select the right adminstrator as "EV Verified User". Then click **Submit for Validation** again.

Requesting Certificates

Can anybody enter a certificate request into the system?

No. You need a user in the system to be able to request a certificate. As an administrator, use the **Add User** button under **Account Users**. Select the User Role, not Administrator, for this kind of user. The user will get an email and gets to set his/her password.

How do we request a certificate?

After logging in at http://www.digicert.com/account/, got to **Certificates** and press the **Request a Certificate** button. Select the right type of certificate, press **Order Now**, fill in the form and use **Submit Certificate Request**

What SSL Certificate types should we use?

This is for server certificates outside of the grid (e-Science) world. Use

- **Multi-Domain SSL** for normal, OV certificates. They can contain subject alternative names if you want (up to 150 names). There should be no reason to use the more limited SSL Plus version.
- **EV Multi-Domain** for EV (Extended Validation) certificates. They can contain subject alternative names if you want. There should be no reason to use the more limited EV SSL Plus version.
- **WildCard Plus** if you need a wildcard subject name (CN).

What Grid Certificate types should we use?

For server and robot certificates in the grid (e-Science) world.Use

- **Grid Host Multi-Domain SSL** for server certificates (there should be no need to use the more limited Grid Host SSL type).
- Read the GÉANT Wiki page about Grid Certificates for information about **robot certificates**.

Do not request client/personal grid certificates using this portal. Use the DigiCert personal certificate portal.

What Client Certificate types should we use?

Do not request client/personal certificates using this portal. Use the DigiCert personal certificate portal.

What Code Signing types should we use?

See the GÉANT Wiki page about Code Signing certificates.

What Document Signing types should we use?

See the GÉANT Wiki page about Document Signing certificates.

How do we approve requested certificates?

Logged in as an administrator, go to **Certificates Requests**, select the pending request, and FIXME!

Managing Certificates

How do we manage existing certificates?

Logged in as an administrator, use **Certificates Orders** and select the certificate. You will find buttons for downloading, reissuing and revoking the certificate.

Personal certficates

Can we isue personal certficates to our users?

The TCS eScience Personal Certificate Policy requires conformance with the Euro GRID PMA policy. SWAMID Identity Assurance Profile 2 fulfills the requirements to request personal certificates. Both the organisation and the user needs to fulfill the requirements for SWAMID AL2. If you want to check if your organisation is approved for SWAMID AL2 please check on the SWAMID members page. For more information the rquirements see Historical: Personal certificates requirements in Sunet TCS.

How do we configure our SAML WebSSO Identity Provider to work with the DigiCert Portal?

SWAMID has published one Wiki page in Swedish with information on how to configure Shibbooleth IdP for SAML-konfiguration Sunet TCS. If you use ADFS or another Identity Provider software you could use that wiki page as an template.

How do we enable our users to login to the personal certficate portal?

The user that sets up the configuration for your organisation Identity Provider login need to be an administrator for you organization.

In the administrative console for DigiCert choose the menu option SAML Organization Mapping and click the button "+ New Mapping". In the form that opens up choose you home organization Identity Provider, your correlalting home organization name and write the domain name that your Identity Provider sends in the attribute schacHomeOrganization, normaly your top DNS.name, e.g. uu.se for Uppsala University. To save click the button "Add Organization" and now everything should work. Go to the DigiCert SAML portal choose your Identity Provider and test to login. Please note that you have configure your Identity Provider correctly and your user must have the right entitlement before you login.

Customizing

Can we limit the certificate types our users can order?

Yes! Logged in as an administrator, use **Settings Limit Products**. Then enable **Use My Own Setttings** and **Use this setting for my division and any subdivisions**, and disable **Allow subdivisions to override this setting**.

Enable **Restrict the products that users with different roles can order** and disable all the product types you want to remove under the **Administrator** h eading. Then click on the **User** heading and do the same there. Finally, use **Save Settings**.

Certificate Chaining

How do we get the certificate chain?

It is included together with the certificate and instructions in the email the requester gets (and that you can download via **Certificates Orders** as discussed above).

Are the chain and root certificates the same as for the Comodo generation of the service?

No, they are different. Do not reuse your saved files from the Comodo system.

How do we check if the server sends a good certificate chain?

You could use openssl s_client -connect nim.nsc.liu.se:443 (replacing nim.nsc.liu.se with your address). You then have to check the lines following "Certificate chain" in the output to see that it contains more than the server certificate. The following is an OK example for an EV certificate:

```
Certificate chain
 0 s:/businessCategory=Private Organization/1.3.6.1.4.1.311.60.2.1.3=SE/serialNumber=1970/street=M\xC3\xA4ster
Mattias V\xC3\xA4g/postalCode=583 30/C=SE/ST=\xC3\x96sterg\xC3\xB6tland/L=Link\xC3\xB6ping/O=Link\xC3\xB6pings
University/OU=NSC/CN=nim.nsc.liu.se
   i:/C=NL/ST=Noord-Holland/L=Amsterdam/O=TERENA/CN=TERENA SSL High Assurance CA 3
 1 s:/C=NL/ST=Noord-Holland/L=Amsterdam/O=TERENA/CN=TERENA SSL High Assurance CA 3
   i:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert High Assurance EV Root CA
```