Trusted Certificate Service

Certificates for e-Science and clients (NL edition)

With the new GÉANT **Trusted Certificate Service TCS** more people in the Netherlands now have access to more services. Also if, before 2015, you could only get regular personal certificates from the TCS, now you can also get the 'e-Science' or "Grid" certificates in the same easy way.

The following products are available:

- **Grid Premium**
  Your personal certificate for almost all **authentication & e-Science** purposes. Contains a uniqueID and does not contain diacritics in the name for better interoperability.
- **Premium**
  Regular personal certificates **for e-mail signing**. These have a 'human-targeted' representation of your name in it (including any diacritics), but since it has no unique ID it is **not suitable** for authentication and e-Science.
- **Grid Robot Name**
  A special **machine-to-machine** authentication certificate that you are personally responsible for

No access to the TCS service in NL?

- Test first by going to www.digicert.com/sso and type (part of) the name of your institution
- No luck finding your organisation? Ask your institute help desk to request "that the AAI responsible person or SURFnet ICP requests a connection be made to DigiCert in the SURFcontext dashboard and to permit inclusion of the IdP in eduGAIN"
- You find your institution but cannot log in (it complains about missing attributes) but you are an employee? Ask your institute helpdesk to request "that the eduPersonEntitlement to access the TCS, `urn:mace:terena.org:tcs:personal-user`, is set by default for all employees, since they are eligible anyway because the organization keeps a copy of a photo-ID to fulfil the requirements of the 'Wet op de Loonbelasting'"
- Still getting stuck and does your institution need help? Tell them to contact the SURFnet product manager for TCS and request the "SURFcertificaten" service. Once connected, you can contact your own organisation by mail at scs-ra@*instelling.nl*

All these products are available from the same portal, to which you authenticate with your own institutional credentials:

https://www.digicert.com/sso

This guide will lead you through the request process. You can request certificates

1. Directly in your browser – and if needed later export them to files for use with command-line tools or your email client
2. Create a certificate on the command line, submit the request using your web browser – and if desired import them into any web browser or mobile client later

For questions regarding the Dutch TCS service, you can contact your institutional helpdesk.

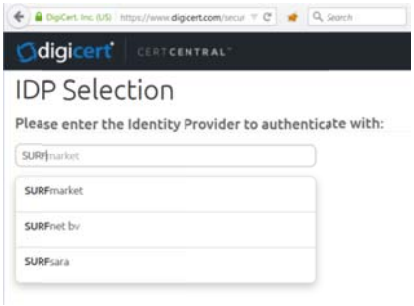
For issues specific to authentication for e-Science and migration from the legacy DutchGrid CA – send mail to ca@dutchgrid.nl. Other e-Infrastructure support questions should be directed through the regular e-Infra helpdesk (https://surfsara.nl/support/helpdesk) or to your coordinating site (SURFsara, Nikhef, or RUG-CIT).

Logging in to the TCS Portal with your institutional account

Whichever method you choose, you first have to login with the DigiCert TCS service

1. Go to the DIgiCert TCS sign-in portal **www.digicert.com/sso**:

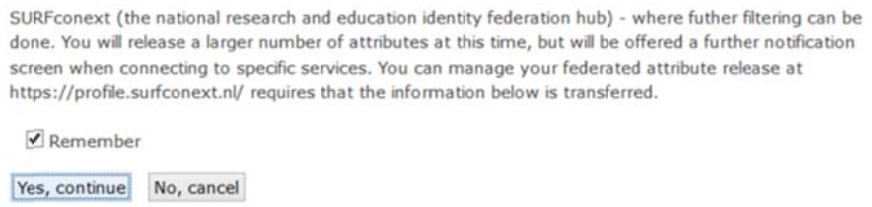
2. Select your institution from the list, by typing some of its name. *The box starts empty*, so type:



3. Select your institution from the list by clicking on it, and press “Start single sing-on”:

4. Authenticate to your institution in the usual way (username-password, one-time tokens, or PKI), e.g.

5. Permit the transfer of your personal data to SURFconext and TCS DigiCert:



and wait (max 30 seconds) to be redirected to the DigiCert portal.

Once the DigiCert product list appears, you are in. From here you can review, retrieve and revoke your existing certificates, request new ones in your web browser, or request new ones based on your own “Certificate Signing Request” (CSR).

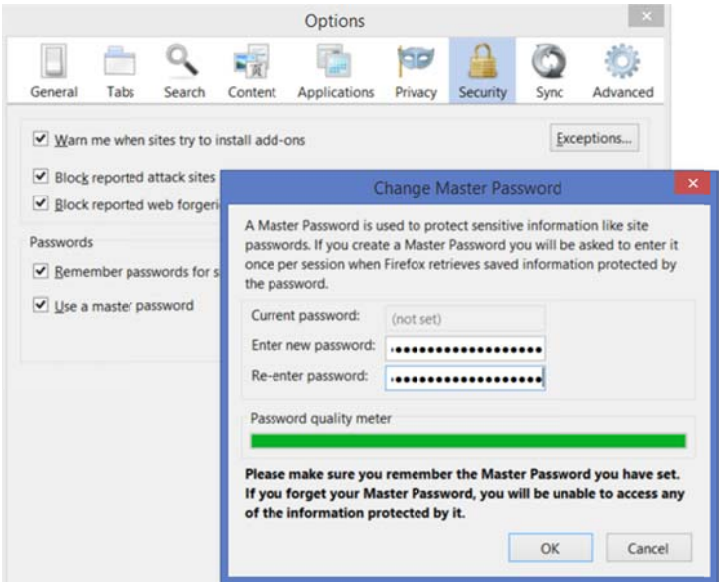
In order to manage your certificates, you will *always* have to explicitly log in (again). Having requested a certificate, you cannot immediately continue to manage existing ones. Visit https://www.digicert.com/sso again to manage your certs.

Setting a master password in your browser or mailer

To use the TCS server, you are required by policy to secure your certificates and other credential such as your institutional one. This is accomplished with a Master Password (Firefox, Thunderbird), or by setting the security level to “High” in your operating system key store (‘request my permission with a password’).

To set the master password in Firefox and Thunderbird, open the “Options” dialog, select “Security”, and follow the setup to set or change the Master Password.

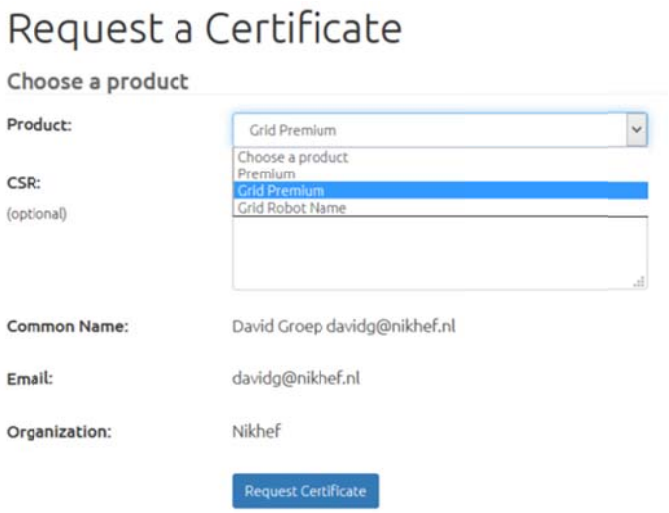
IMPORTANT: you MUST protect your private key with a strong passphrase, of at least 12 chars!



Request a certificate in your browser – *and how to export it afterwards*

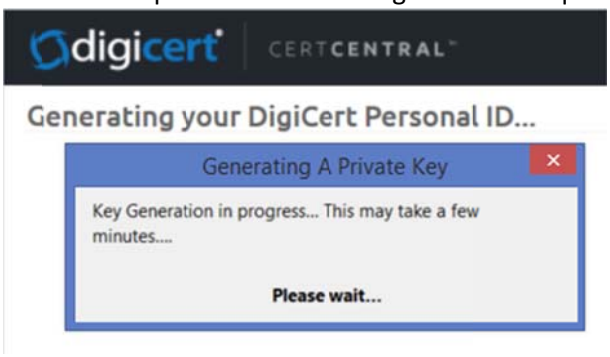
You will need to export and import if you want to use your certificate in your mail client (except for mailers that use the operating system key store). For Thunderbird, you need to export from Firefox and re-import in Thunderbird. Follow the instructions at the end of this section.

1. Select the “Grid Premium” (authentication) or Premium (email-only) product after logging in

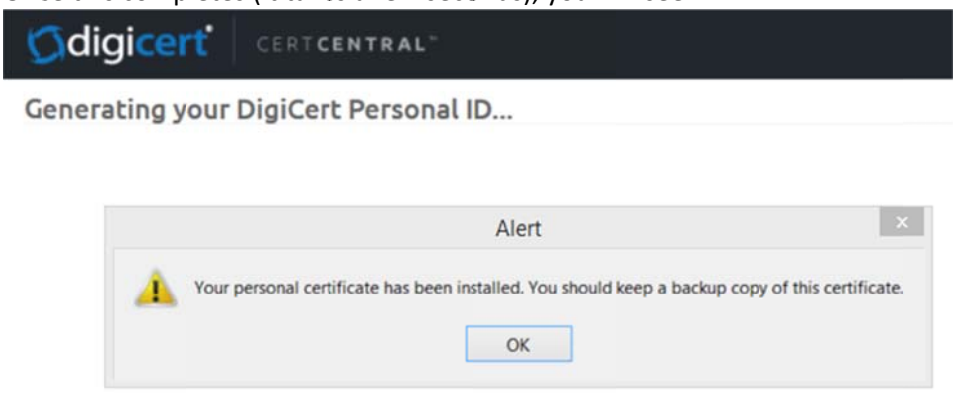


2. Make sure your name and the “uniqueID” (the magic token e*PPN@instelling.nl*) are correct for authentication certificates.

3. Click on “Request Certificate” to generate a request in your browser:



4. Once this completes (it takes a few seconds), you will see:

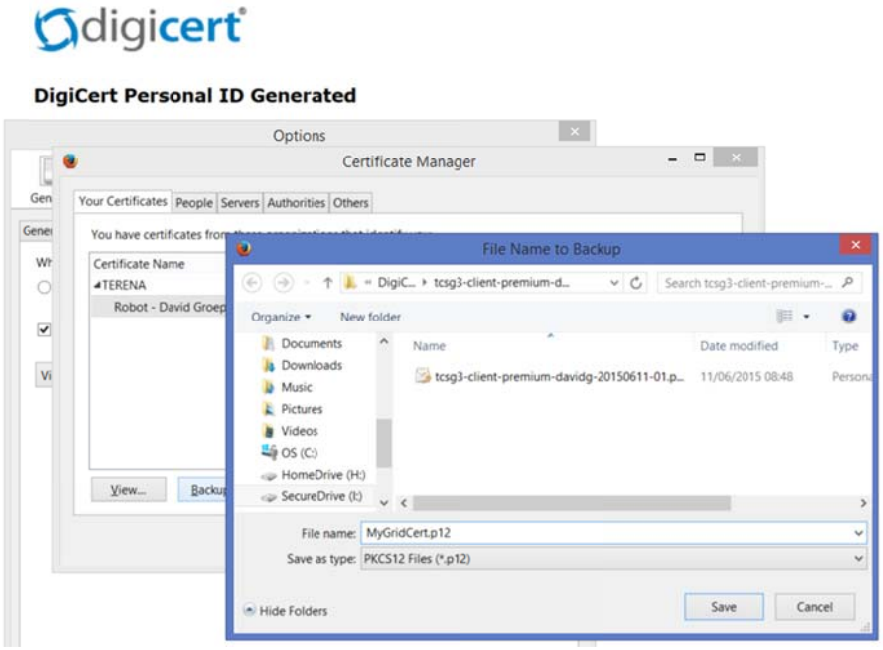


5. Click on OK and the dialog box will disappear.
Congratulations: your certificate is now **ready for use** in your web browser. You can for example authenticate to web sites, and to community portal to enrol for your membership.

6. You can also export your certificate for use with command-line clients:

by opening your browser preferences (the example above is for Firefox), or Internet Connection Settings (look for “Tools” -> “Internet Options” and under the “Content” tab click on “Certificates”).

7. Locate your certificate in your Personal certificate store (“Your Certificates”) under the “TERENA” list :



8. Save the certificate with private key, protected with a strong passphrase, to local secure storage (e.g. your own laptop, or an encrypted disk partition:

9. For authentication and e-Science use: To convert the "PKCS#12" file, with the .p12 extension, to a set of files that you can use for commandline tools (such as 'grid-proxy-init'), you can use the OpenSSL command tool. This is available in all standard Unix distributions (package name "openssl"), for MacOS, and for MS Windows (see https://www.openssl.org/related/binaries.html):

```
chmod 0600 cert.p12
openssl pkcs12 -nocerts -in cert.p12 -out $HOME/.globus/userkey.pem
openssl pkcs12 -clcerts -nokeys -in cert.p12 -out $HOME/.globus/usercert.pem
chmod 0600 $HOME/.globus/userkey.pem
chmod 0644 $HOME/.globus/usercert.pem
```

10. For email use in Thunderbird, open your mail client, select "Tools -> Options", and in the Security/Certificates dialog (like the one above) select "Import" again. Also secure your mailer with a master password!

Now you're all done. If you want to share the subject name of this certificate, so that e.g. web site or Wiki managers can add you to their access lists, use the OpenSSL PKCS12 command with "`-clcerts -nokeys`" to find it under the name "subject=".

Requesting a certificate from a command-line tool – *and how to import it*

Many command-line tools (such as compute services or file management) use a file-based certificate, typically called "usercert.pem" and "userkey.pem" in a ".globus" subdirectory of your home folder. You can use the TCS service with this kind of set-up by submitting the corresponding "userrequest.pem" file as a "Certificate Signing Request" (CSR) into the DigiCert portal.

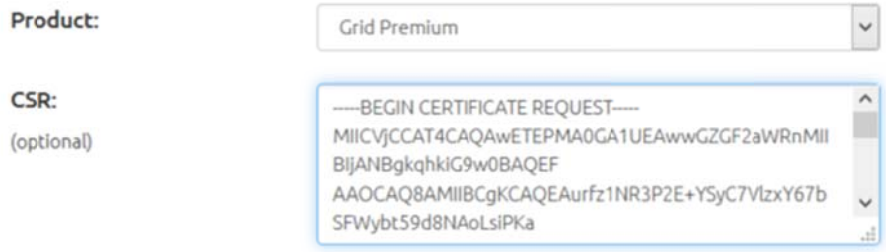
1. Install the OpenSSL command-line tools (see above, available for Unix/Linux, MacOS, and MS Windows).
2. To generate the certificate request files with OpenSSL:

   ```
   mkdir $HOME/.globus
   openssl req –new –newkey rsa:2048 -subj "/CN=Pietje Puk 42" -out
   $HOME/.globus/userrequest.pem -keyout $HOME/.globus/userkey.pem
   ```

   the actual name in the request does not matter: it will be replaced with the TCS provided name.

   IMPORTANT: you MUST protect your private key with a strong passphrase, of at least 12 chars.

3. Login to the DigiCert portal (see above), select the proper product (such as "Grid Premium" for authentication certificates), and paste the contents of the "userrequest.pem" file into the dialog window, like here:

4. Once you press the "Request Certificate" button, a certificate based on the your request is generated instantly.
   The resulting certificate is sent to you by email – to the email address provided by your institution!

5. No certificate is presented to you in the browser - it will just say "thank you". This is the intended behaviour.
   If you want to retrieve your new certificate via the web browser, log in *again* by visiting https://www.digicert.com/sso (note: you have to authenticate to your institution again).

6. In your mailbox, you will find a mail from DigiCert, containing a ZIP file with:
   a. Your own certificate (the name of which depends on your own name)
   b. The certificate of the TERENA (eScience) Personal CA 3
   c. A "readme" file with instructions

   The email also contains a "P7B" (PKCS#7 bundle) file with certificates for import in mail clients. We will use the ZIP file for now.

7. Take the ".crt" file with your own name from the ZIP file (use a file browser or extract with the "unzip" command) and copy it from "givenname_surname_uniqueid.crt" to "$HOME/.globus./usercert.pem"

Your authentication credential is now ready to be used with command-line tools like 'grid-proxy-init'.

If you want to also use this certificate in a browser (e.g. to register in a community management portal), you can convert the separate key and certificate files into a "PKCS#12" (.p12) file for browser import:

8. Run the OpenSSL pkcs12 command-line tool:

```
openssl pkcs12 -in $HOME/.globus/usercert.pem -inkey $HOME/.globus/userkey.pem
  -export -name "My DigiCert Premium Certificate 2015-01" -out $HOME/mycert.p12
chmod 0600 $HOME/mycert.p12
```

   IMPORTANT: you MUST protect your private key with a strong passphrase, of at least 12 chars, which may be the same as your private key password (it protects the same data).

9. Open your browser, go to "Tools -> Options" (Firefox) or "Tools -> Internet Options" (MS Windows via Internet Explorer), and open the Security/certificates tab.

10. Make sure your browser and/or operating system key store is protected with a master password

11. Select "Import" from the certificate management panel, and select the "mycert.p12" file you just created.

12. Import the certificate into your *Personal* key store (this is usually selected automatically).

13. In MS Windows, please *ensure you select the high protection level* for this certificate and key pair.

You can now proceed to web sites that request certificate authentication.