

Trusted Certificate Service - NL eScience support

revision G4.03.2021-06-08/DLG

The GEANT Trusted Certificate Service (TCS) has been providing credentials for access to research and e-Infrastructure services in Europe for over 10 years. Your TCS certificates are recognised for national, European, and global services that deploy the IGTF assurance trust anchors, and are recognised by all major browsers, email clients, and operating systems.

As an end-user you can obtain personal certificates, and personal software agent certificates, from this service directly. Organisational ICT staff and service operators can also get server certificates for combined public web trust and e-Infrastructure use by contacting their local Registration Authority Officer (RAO) in their own IT department (ask scs-ra@yourdomain.nl).

There are three product to choose from, each with a different purpose:

- **GEANT Personal Certificate** - provides secure email services, and enables you to encrypt and digitally sign email communications, as well as sign and protect some types of document (but not sign PDF documents).
- **GEANT IGTF-MICS Personal** - provides secure email services and client authentication, enables you to encrypt and digitally sign email communications, and to authenticate you to e-Infrastructure services.
- **GEANT IGTF-MICS-Robot Personal** - provides secure client authentication for software agents and processes running under your control, and authenticate these to e-Infrastructure services. For access to research services (such as the DNI - the Dutch National e-Infrastructure coordinated by SURF, GinA, NDPF, EGI, PRACE, WLCG, WeNMR, ELIXIR) select **GEANT IGTF-MICS Personal**.

All products are available from a common end-user request portal ¹ :

<https://cert-manager.com/customer/surfnet/idp/clientgeant>

This guide will help you

- access the portal via your browser
- create the certificate and download it on your own computer
- install this certificate for e-Infrastructure use

and point you to installation support for web browsers and email clients. In case of problems, please contact your institutional helpdesk or the RAO for your organisation (scs-ra@your-institution.nl).

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 Sectigo portal

1. In a web browser, do to <https://cert-manager.com/customer/surfnet/idp/clientgeant>
2. In the Organisation Discovery service, select your organisation by typing (part of) its name. If you have used a SeamlessAccess service before, it may be pre-selected



- The organisation name will auto-complete

Find Your Institution

Your university, organization or company

Examples: Science Institute, Lee@uni.edu, UCLA

[SURF-bureau](#)
[surf.nl](#)

- In your institutional login page, enter your usual (federated) credentials



Authenticate yourself with your Nikhef credentials.

Username	<input type="text" value="davidg"/>
Password	<input type="password" value="....."/>
One-time code	<input type="text" value="666666"/> <input type="button" value="x"/>

and proceed through any attribute information screens. This service, since it issues personal credentials, needs some personal data about you: your givenname and family name (or "display name"), your email address, a persistent and unique identifier (called "eduPersonPrincipalName" in most cases in the Netherlands), and a confirmation that you have the right to access the service (called eduPersonEntitlement).

- You should now see the Digital Certificate Enrollment form

Digital Certificate Enrollment

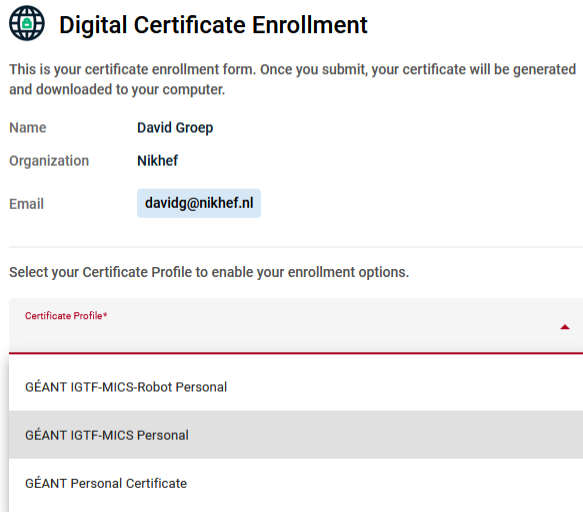
You have been authorized to enroll for a digital certificate. Please validate that your name and email addresses are correct.

Name	David Groep
Email	<input type="text" value="davidg@nikhef.nl"/>
Organization	Nikhef

if you *do not see this screen* or see an explicit red box, ask your administrator (see below)

Generating a personal certificate

7. You have now successfully entered the Sectigo certificate enrolment portal. You should now select the proper product. For eScience use, select "GÉANT IGTF-MICS Personal", for email signing, or signing Office documents, use "GÉANT Personal Certificate":



Digital Certificate Enrollment

This is your certificate enrollment form. Once you submit, your certificate will be generated and downloaded to your computer.

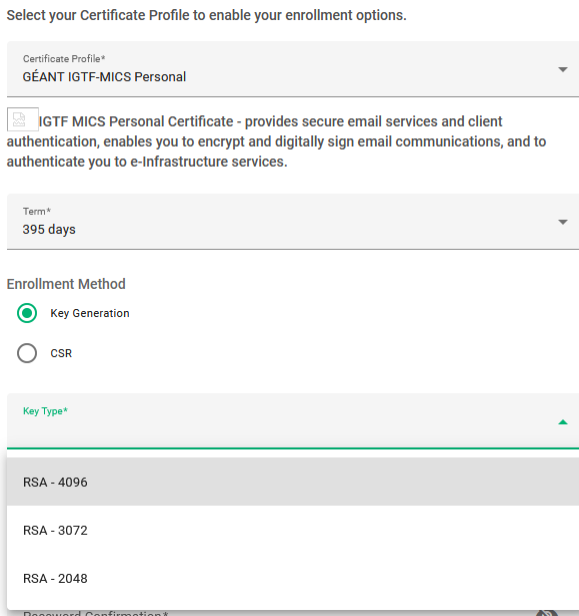
Name: David Groep
Organization: Nikhef
Email: davidg@nikhef.nl

Select your Certificate Profile to enable your enrollment options.

Certificate Profile*

- GÉANT IGTF-MICS-Robot Personal
- GÉANT IGTF-MICS Personal**
- GÉANT Personal Certificate

8. Unless you are an expert, we strongly recommend to select "Key Generation" and select "Key Type RSA" option under "Enrolment method". Really! And RSA-4096 is a pretty good choice in terms of security:



Select your Certificate Profile to enable your enrollment options.

Certificate Profile*
GÉANT IGTF-MICS Personal

IGTF MICS Personal Certificate - provides secure email services and client authentication, enables you to encrypt and digitally sign email communications, and to authenticate you to e-Infrastructure services.

Term*
395 days

Enrollment Method

Key Generation
 CSR

Key Type*

- RSA - 4096**
- RSA - 3072
- RSA - 2048

Password Confirmation*

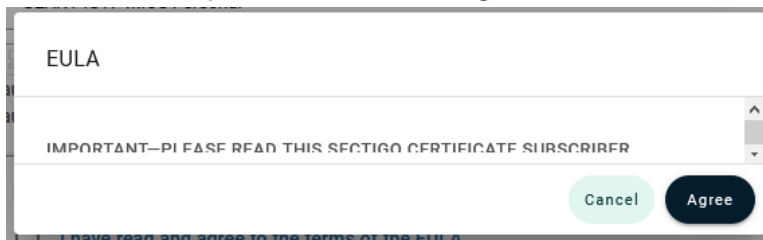
9. Now, provide a strong passphrase, twice. **This passphrase is important** and you must not lose it. If you lose it twice within the year, you have to contact your organisational helpdesk to perform a reset on your certificates. Other requirements of the passphrase:
- it should be strong, and longish (at least 12 characters). Use a password manager to generate a strong password and to keep it safe. There are many options here, such as KeePass, LastPass, &c.
 - You will need this passphrase to import the certificate into your browser, email clients, and for eScience use (such as the Grid Community Toolkit's \$HOME/.globus directory) later.

- o You must type it twice here (the same password):

The screenshot shows a form with a dropdown menu set to "RSA - 4096". Below it, a message states: "Password is required to unlock the certificate file download to protect private key." There are two password input fields, both filled with dots. Below the password fields is a checkbox labeled "I have read and agree to the terms of the [EULA](#)". At the bottom of the form is a "Submit" button.

10. Check the box "I have read..." and click through the EULA, but do keep in mind to take proper care of your certificate, so not share it with anyone else, keep the passphrase secure, and inform your institutions helpdesk immediately in case you lose it or if your system is compromised by malware or viruses.

If you leave the organisation, you must request your certificate to be revoked as well. So check the box, and click away the End-User License Agreement:

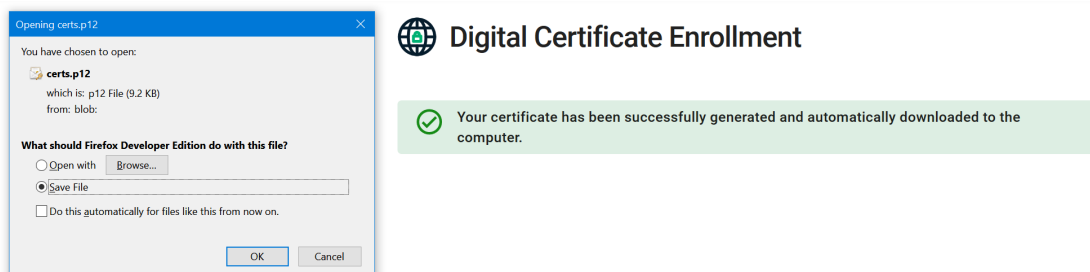


11. Now, you can hit "Submit"!

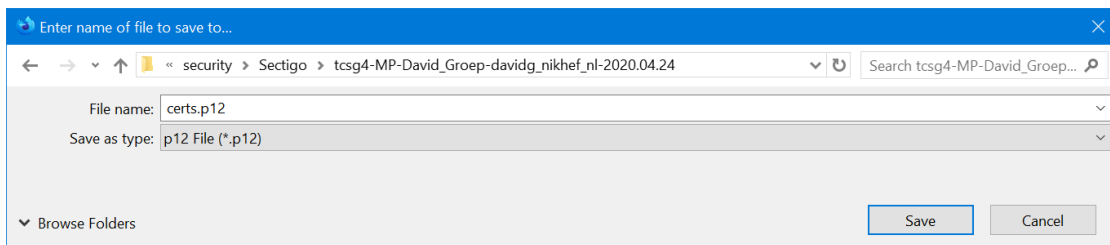
The screenshot shows the same form as in step 10, but now the checkbox "I have read and agree to the terms of the [EULA](#)" is checked with a green checkmark. The "Submit" button is now highlighted in a dark blue color.

Note: If you subsequently see "Sectigo Certificate Manager enrollment request failed. Please contact your security administrator." you may already have a certificate, see below.

13. If you are successful, you will see



14. Save the file in a secure, local directory. Please make sure that the permissions do not allow reading by others (on unix-like systems such as Linux, MacOS, and on Cygwin, that's "chmod go-rwx name "):



Making your certificate suitable for eScience use

- Open a terminal window to turn the blob from Sectigo into a format you need for use in e-Infrastructures and for clean import in your browser or email client, and follow guidance on <https://ca.dutchgrid.nl/tcsG4/#p12install>. You should see:

```
$ ls -l
total 10
-rw-r--r-- 1 davidg None 9377 Apr 24 11:23 certs.p12
```

- Download the conversion script `tcsG4-install-credential.sh`

```
curl -o tcsG4-install-credential.sh https://ca.dutchgrid.nl/tcsG4/tcsG4-
install-credential.sh
chmod +x tcsG4-install-credential.sh
```

- Convert the file into a useful format. Change your working directory to the place where you saved your file, e.g. in `$HOME/Downloads` or on your desktop (e.g. `C:\Users\myuser\Desktop\`)
 - if you will be using the Grid Community Toolkit GCT or other 'grid' tools, install in your `.globus` directory

```
cd $HOME/Downloads
./tcsG4-install-credential.sh -R certs.p12
```

- if you will be installing it in browsers or email clients only, you can leave it in any safe directory. If you picked a safe directory to begin with, you can use that same directory

```
./tcsG4-install-credential.sh -R -d . certs.p12
```

and you have to provide your passphrase once. This is *the same passphrase* you entered in the Sectigo portal.

(if you are an advanced user and want to re-use the keypair later, add a `--csr` option to the script above)

- The session should look like this:

```
davidg@x13davidg /m/security/Sectigo/tcsG4-MP-David_Groep-davidg_nikhef_nl-
2020.04.24
$ tcsG4-install-credential.sh -R certs.p12
Passphrase (existing) for your secret key:
Processing EEC certificate: David Groep davidg@nikhef.nl
(friendly name: David Groep davidg@nikhef.nl issued 24 Apr 2020)
Processing CA certificate: GEANT eScience Personal CA 4
Processing EEC secret key
Repackaging David Groep davidg@nikhef.nl issued 24 Apr 2020 as PKCS12
The following files have been created for you:
```

```

-rw-r--r-- 1 davidg None 2224 Apr 24 11:41 /home/davidg/.globus/cert-
David_Groep_davidg_nikhef_nl_issued_24_Apr_2020.pem
-rw-r--r-- 1 davidg None 2469 Apr 24 11:41 /home/davidg/.globus/chain-
David_Groep_davidg_nikhef_nl_issued_24_Apr_2020.pem
-rw----- 1 davidg None 1834 Apr 24 11:41 /home/davidg/.globus/key-
David_Groep_davidg_nikhef_nl_issued_24_Apr_2020.pem
-rw----- 1 davidg None 5253 Apr 24 11:41 /home/davidg/.globus/package-
David_Groep_davidg_nikhef_nl_issued_24_Apr_2020.p12
Making Grid Community Toolkit compatible link in /home/davidg/.globus
userkey.pem
usercert.pem

davidg@x13davidg /m/security/Sectigo/tcsg4-MP-David_Groep-davidg_nikhef_nl-
2020.04.24
$ ls -l $HOME/.globus/
total 22
-rw-r--r-- 1 davidg None 2224 Apr 24 11:41 cert-
David_Groep_davidg_nikhef_nl_issued_24_Apr_2020.pem
-rw-r--r-- 1 davidg None 2469 Apr 24 11:41 chain-
David_Groep_davidg_nikhef_nl_issued_24_Apr_2020.pem
-rw----- 1 davidg None 1834 Apr 24 11:41 key-
David_Groep_davidg_nikhef_nl_issued_24_Apr_2020.pem
-rw----- 1 davidg None 5253 Apr 24 11:41 package-
David_Groep_davidg_nikhef_nl_issued_24_Apr_2020.p12
lrwxrwxrwx 1 davidg None 56 Apr 24 11:41 usercert.pem -> cert-
David_Groep_davidg_nikhef_nl_issued_24_Apr_2020.pem
lrwxrwxrwx 1 davidg None 55 Apr 24 11:41 userkey.pem -> key-
David_Groep_davidg_nikhef_nl_issued_24_Apr_2020.pem

```

18. Your system is now ready for elnrastructure use. Commands such as `voms-proxy-init` should work, using the same passphrase you used on the Sectigo site.

Import in browsers, for VOMS and other purposes

19. In the target directory used above (e.g. `$HOME/.globus`) there is a "PKCS#12" (.p12) file that you can use with ayour browser, email client, and operating system keychain.
20. Chrome, Safari, Internet Explorer, and Edge all use certificate management provided by the operating system (Windows or MacOS):

- o You can usually double-click on the .p12 file (`package-Your_Name_yourmail_domain_tld.p12`), starting a Certificate Import Wizard:

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

Current User

Local Machine

To continue, click Next.

- o Import it into the keychain or certificate store for you, the current user
- o you will be prompted for a passphrase - this is the same passphrase you used on the Sectigo portal and during the conversion script.

If you are given a choice to 'enable strong private key protection' you **must do so**:

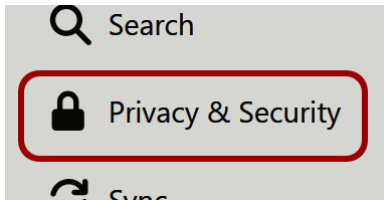
Import options:

- Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

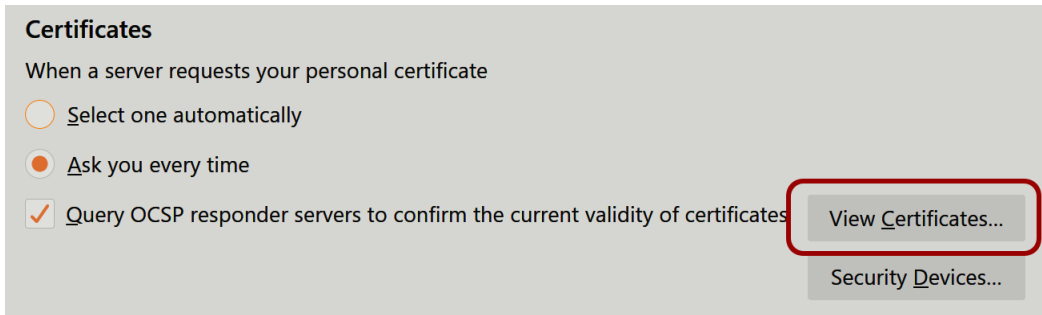
- o The certificate should be installed in the personal certificate store (usually automatically selected based on the type of the certificate)
- o Finish the import. On Windows, allow the import application to create a "Protected Item", clicking "OK".

21. In Firefox and Thunderbird, enable the Master Password, and import the certificate by

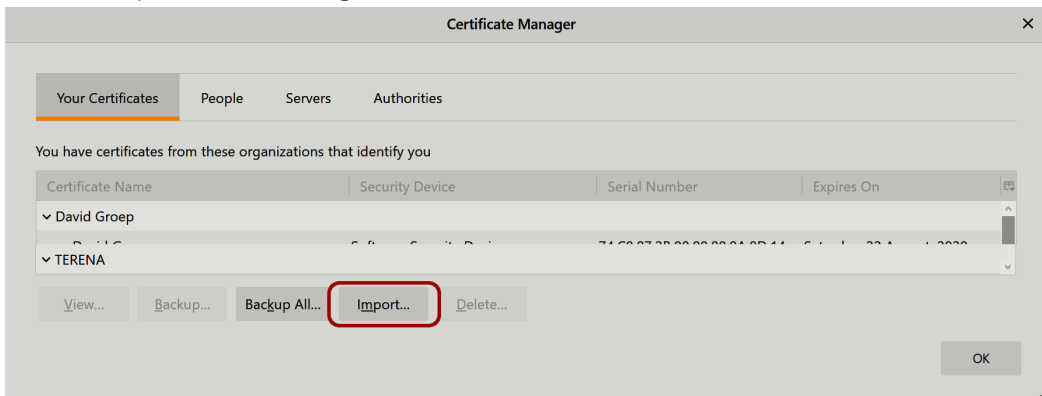
- o opening the "Options" window (e.g. by typing `about:preferences` in the Firefox address bar), and select the "Privacy and Security" options:



- o scroll to the bottom of the page, and click on "View Certificates" in the Certificate section:



- o Click on "Import..." in the dialog box



- o Select the file from the file-chooser dialog, click OK
- o enter the passphrase you used on the Sectigo page and in the tool above

For IGTF eScience certificates, you can verify the successful import by visiting the informational URL

<https://www.eugridpma.org/your-identity/>

Welcome to Your Identity

You have successfully connected to the *YourIdentity* service of the IGTF. You have provided the following information about yourself:

Your subject DN	/DC=org/DC=terena/DC=tcs/C=NL/O=Nikhef/CN=David Groep davidg@nikhef.nl
Your CA issuer DN	/C=NL/O=GEANT Vereniging/CN=GEANT eScience Personal CA 4 (hash: 5e9e302b)
Your serial number	0x69107c4949c208d8785289bf74d11657
Your cert will expire	in 395 days (now it is 10:12:46 UTC on Friday, 24 April 2020)
Issued by	GEANTeSciencePersonalCA4, an accredited:mics IGTF CA emergency email: tcs-pma@lists.geant.org a subordinate of <i>USERTrustRSACertificationAuthority</i> operating under policy https://wiki.geant.org/display/TCSNT/TCS+Repository

Are you Elliptic? Or an Expert?

The ClientGeant TCS interface also allows you to generate your own key pair locally and have a certificate generated using a key that only you have ever held. For that, you can upload your own "Certificate Signing Request" (CSR) to the web portal by selecting "CSR" as the Enrolment Method. Here, you can also upload Elliptic Curve signing requests for the two NIST curves:

The screenshot shows a web form for certificate enrollment. Under the heading "Enrollment Method", there are two radio buttons: "Key Generation" (unselected) and "CSR" (selected). Below this, under "Allowed Key Types", there are five buttons: "RSA - 4096", "RSA - 3072", "RSA - 2048", "EC - P-384", and "EC - P-256". A file upload area contains a "Choose file" button and the text "No file chosen". Below this, it says "OR paste below" and there is a large text input field labeled "CSR*" with a small icon in the bottom right corner.

This option is really for experts, so unless you know what a P-256 curve is, or if you really would have preferred '25519' and you now realise that you cannot get it ... this method might be to your liking!

In case of errors

If you see the following error messages

- **Organization with schacHomeOrganization nikhef.nl was not found on Sectigo Certificate Manager. Please contact your security administrator**
either you have started with the wrong URL (wrong NREN, correct the starting URL in this case), or your organisation has not yet configured SAML self-enrolment. Your security administrator (RAO) must:
 1. Login to the Sectigo SCM system <https://cert-manager.com/customer/surfnet>
 2. Under "Settings" > "Organisations", click on the organisation name and use the "Edit" button to bring up the configuration dialog
 3. Add the organisation domain name in the "Academic code (SCHAC Home Organization)" field and click "OK"

also, your identity provider must release the schacHomeOrganization attribute with this value to Sectigo

- **Your are not entitled to use this service** (or similar)
you have not been given the proper entitlements to use the service. If you are an employee of your organisation, or have had your identity checked at some point (e.g. through student services), this is most likely incorrect. Ask your identity provider service (probably through your local help desk) to also enable sending "urn:mace:terena.org:tcs:personal-user" as your eduPersonEntitlement.
- **Sectigo Certificate Manager enrollment request failed. Please contact your security administrator. or You cannot generate more certificates**
for each of the certificate products, you can have at most two (2) valid certificates at any one time. If you already have two of one product, the portal will not allow you to generate a third. Ask your RAO (via the helpdesk) to revoke your existing certificates of this product type. Then, you can start again.

1. this URL is specific to the Netherlands. There is a URL for each country, named after your national research networking organisation. For example, in France it is <https://cert-manager.com/customer/renater/idp/clientgeant> , in the Czech Republic it is <https://cert-manager.com/customer/cesnet/idp/clientgeant> , in Greece it's <https://cert-manager.com/customer/grnet/> , &c. ↩