GEANT 5th Generation Trusted Certificate Service - NL eScience support

revision G5.01.2025-05-06/DLG

The GEANT Trusted Certificate Service (TCS) has been providing credentials for access to research and e-Infrastructure services in Europe for over 15 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. Just beware to choose the proper 'product': email certificates for signing mail, and authentication certificates to prove your identity.

As an end-user you can obtain personal certificates for authentication (proving your identity to services), for personal software agent certificates, and for signing email, 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:

- **GÉANT Personal Authentication** - provides secure client authentication, and allowed you to connect to e-Infrastructure services, or to your institutional account login services.
- **GÉANT Personal Automated Authentication** - 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 **GÉANT Personal Authentication**.
- **GÉANT Organisation Automated Authentication** - provides secure client authentication for teams and managed services (requires independent validation of the email address)
- **Email signing and encryption** - 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 - which require eSignatures, not part of the GÉANT contract).

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

> https://cm.harica.gr/

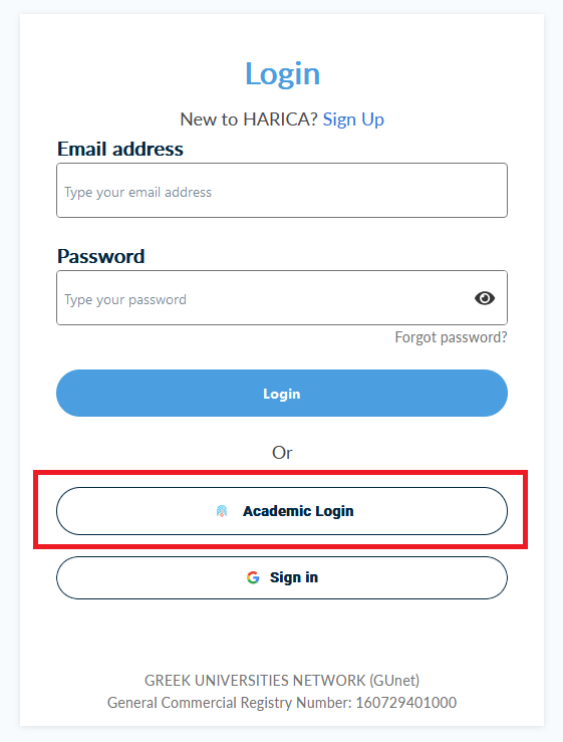
This guide will help you

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

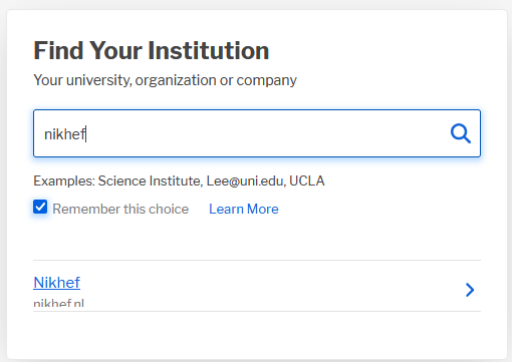
and point you to installation support for web browsers and email clients. In case of problems, please contact your institutional helpdesk for your organisation (scs-ra@*your-institution.nl*).
For issues specific to authentication for e-Science and migration from the legacy DutchGrid CA – send mail to *ca@dutchgrid.nl*. Other e-Infrastructure support questions should be directed through the regular e-Infra helpdesk (see https://servicedesk.surf.nl/wiki/x/kIAW) or to your coordinating site (SURF or Nikhef).

Logging in to the TCS HARICA portal

1. In a web browser, go to https://cm.harica.gr/ and select **Academic Login**:



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:



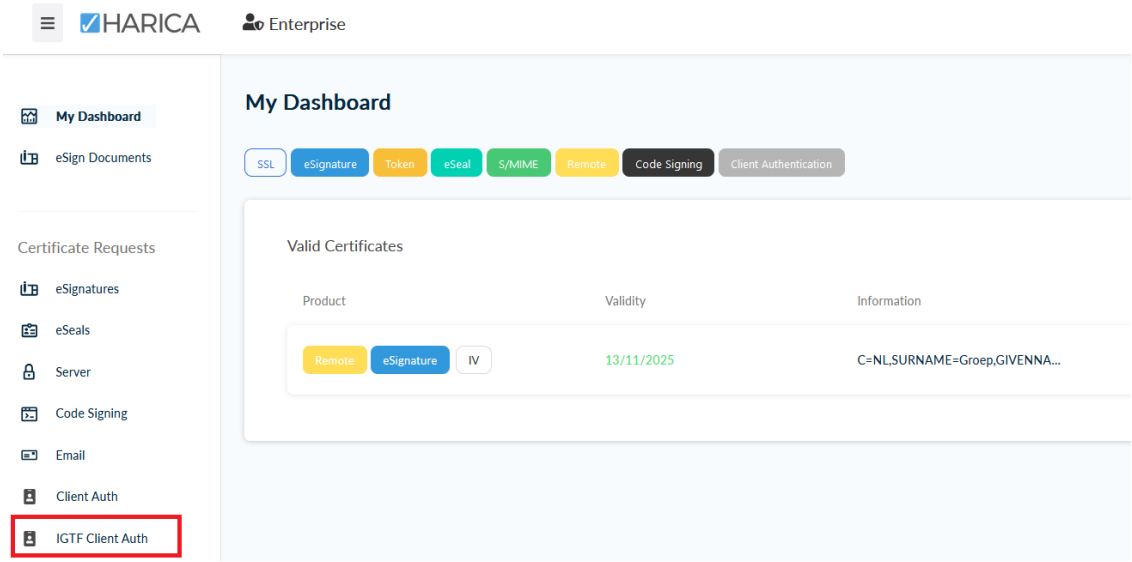
(the organisation name will auto-complete when you start typing)

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

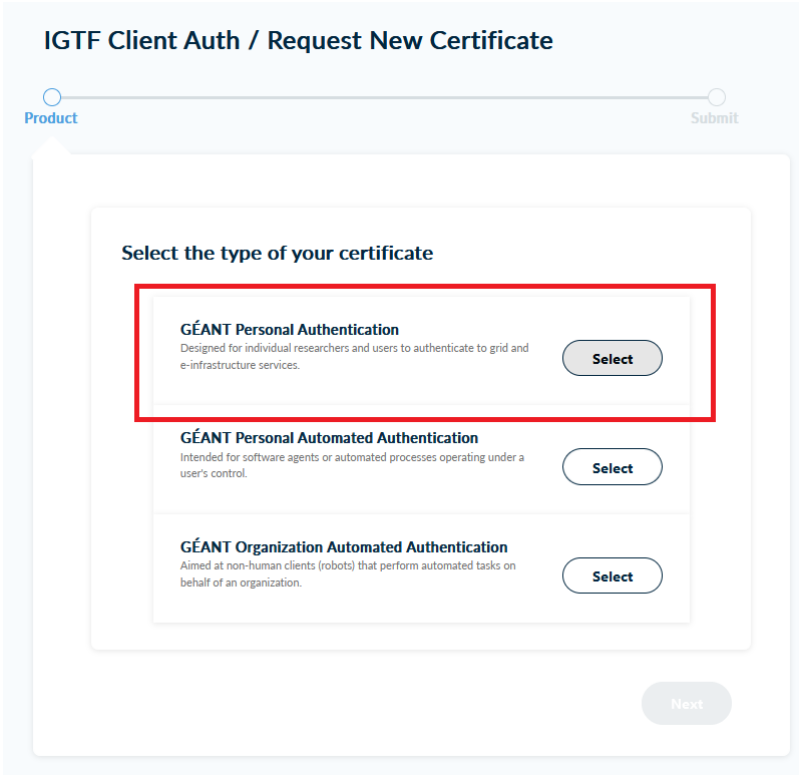
and proceed through any attribute information screens. This service, since it issues personal credentials, needs some personal data about you: your given name and family name (or "display name"), your email address, a persistent and unique identifier (called

"eduPersonPrincipalName" in most cases in the Netherlands), and a confirmation that you have the right to access the service (called eduPersonEntitlement).

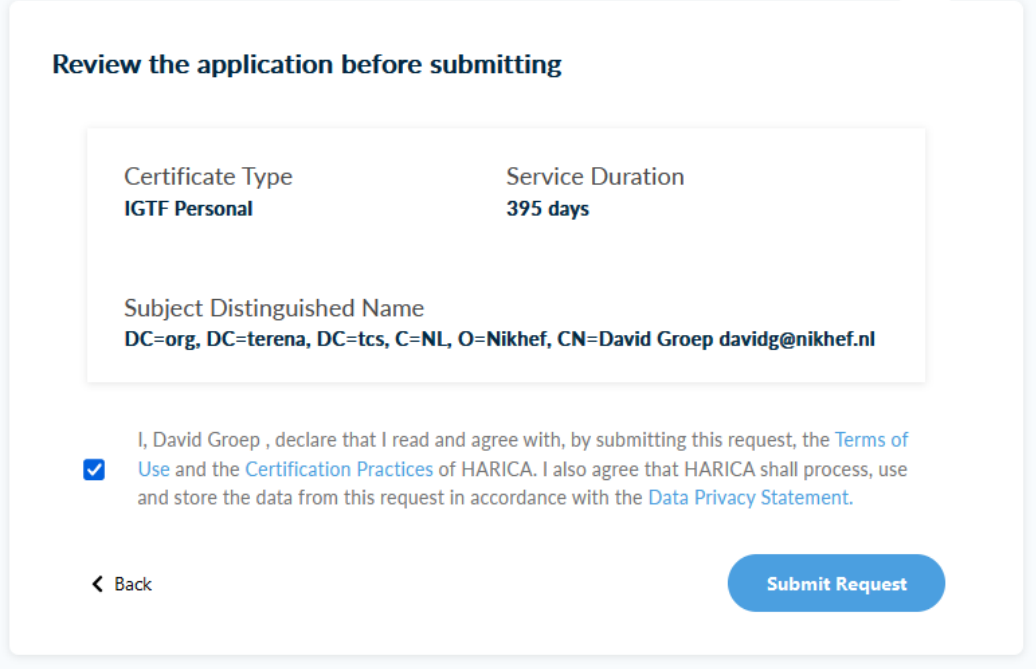
4. You will see your HARICA dashboard. You will start off empty, but it may soon be populated with personal (and also server, if you are also a systems admin) certificates:



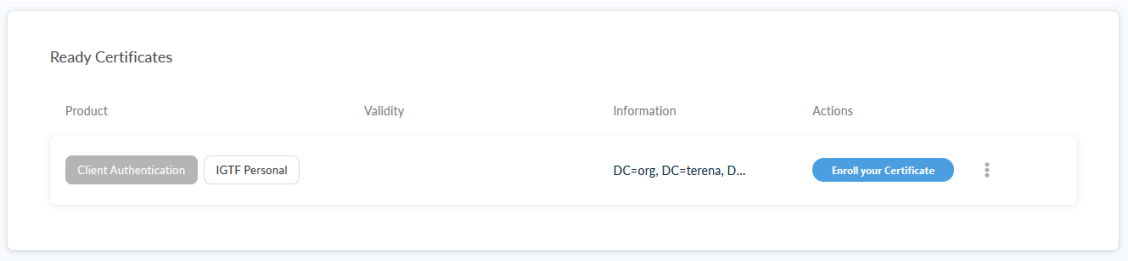
5. From the product selection page, you will most likely want **Personal Authentication**:



6. Accept the conditions on the application review page (and check your configuration):



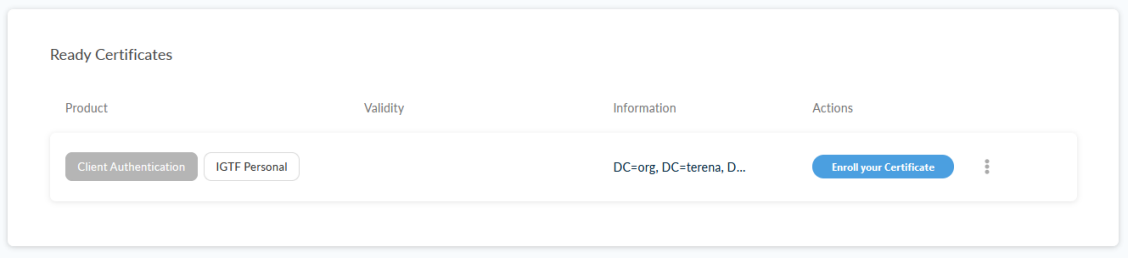
7. Submit the application, and return to the dashboard (top-left menu item).
8. In the dashboard, you should now see the Digital Certificate Enrollment form:



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

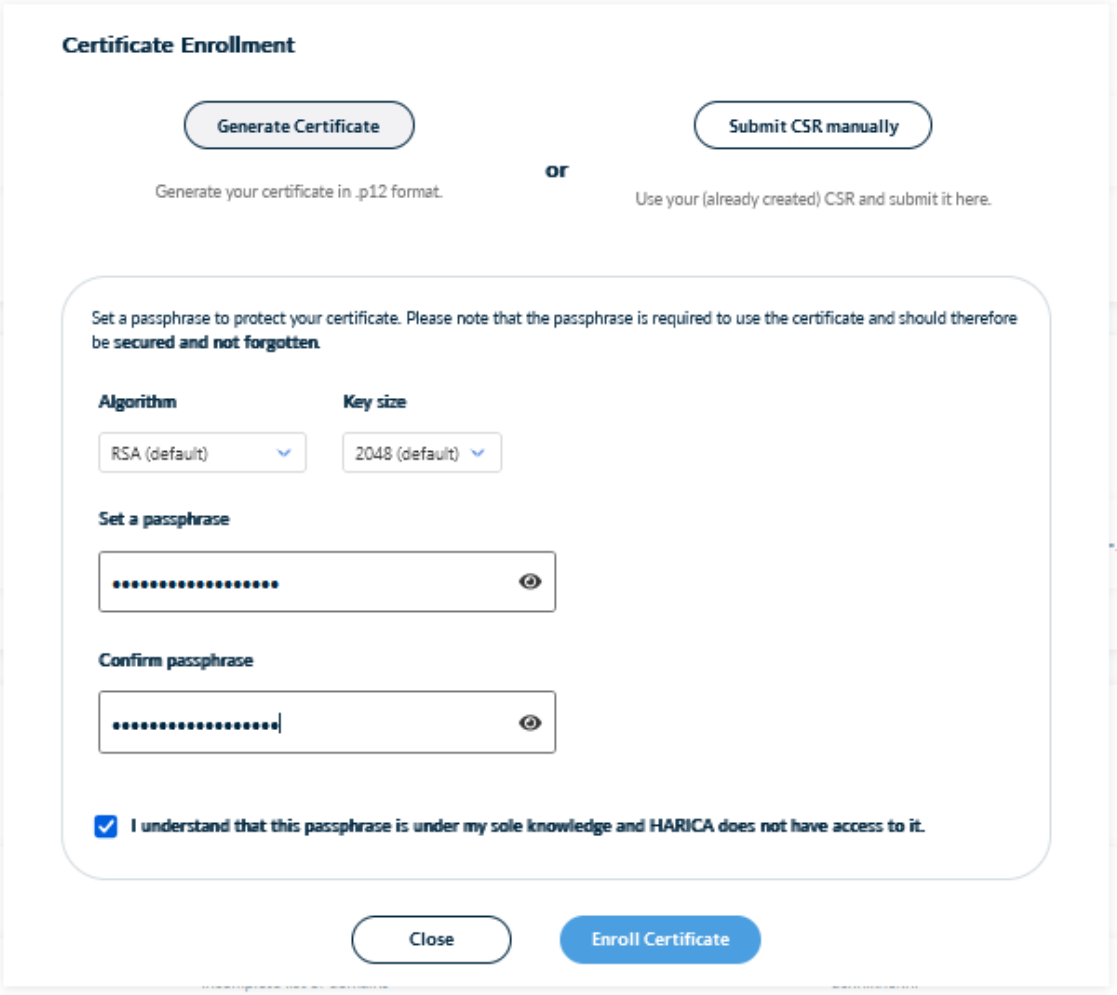
Generating a personal certificate

7. You have now successfully entered the HARICA certificate enrolment portal and authenticated yourself, and you can start generating your certificate:



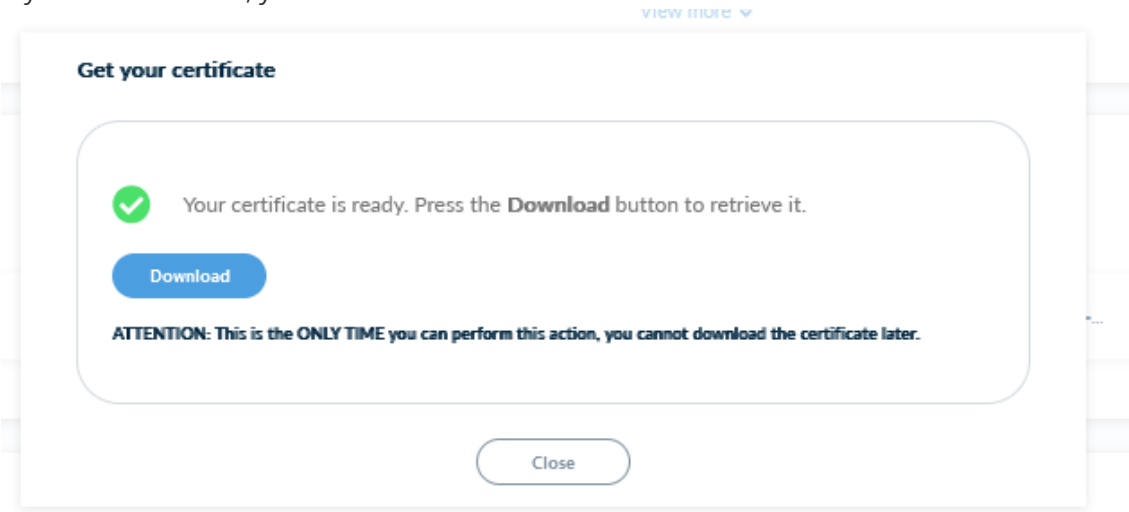
where you click on "Enrol your Certificate"

8. Unless you are an expert, we strongly recommend to select "Generate Certificate" and select "**Key Type RSA**" option under "Algorithm". You may upgrade your security by selecting 4096 bit key length:



9. Povide a strong passphrase, twice. **This passphrase is important** and you must not loose it. If you loose it, contact your institutions help desk to have your certificate revoked.
   Other requirements of the passphrase:
   - it should be strong, and long (at least 16 characters). Use a password manager to generate a strong password and to keep it safe. There are many options here, such as KeePass, LastPass, BitWarden, &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.
   - You must type it twice here (the same password)
10. Check the box "I understand ..." and click
11. Now, you can hit "Enroll Certificate"!

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, thats "chmod go-rwx *name*"):

Making your certificate suitable for eScience use

14. Open a terminal window to turn the "PKCS#12" blob from HARICA 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/tcs/#p12install. You should see:

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

15. Download the script `tcsg4-install-credential.sh` (yes, the TCS G4 version will still work!)

```
   curl -o tcsg4-install-credential.sh https://ca.dutchgrid.nl/tcs/tcsg4-
install-credential.sh
   chmod +x tcsg4-install-credential.sh
```

16. 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 HARICA portal.

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

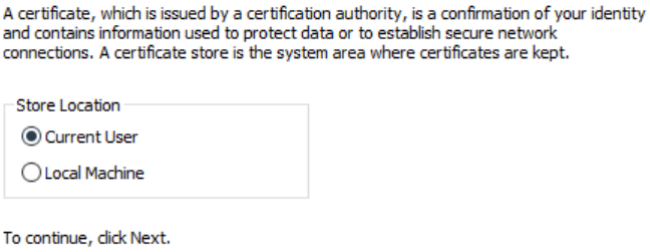
17. The session should look like this:

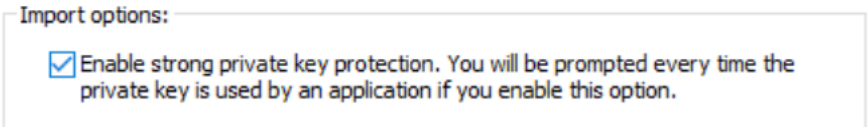
```
davidg@x13davidg /m/security/HARICA/tcsg5-GPA-David_Groep-davidg_nikhef_nl-
2025.06.06
$ tcsg4-install-credential.sh -R Certificate.p12
Passphrase (existing) for your secret key:
Processing EEC certificate: David Groep davidg@nikhef.nl
  (friendly name: David Groep davidg@nikhef.nl issued 6 May 2025)
Processing CA  certificate: GEANT TCS Authentication RSA CA 5
Processing EEC secret key
Repackaging David Groep davidg@nikhef.nl issued 6 May 2025 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

$ 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 eInfrastructure use. Commands such as `voms-proxy-init` should work, using the same passphrase you used on the HARICA site.

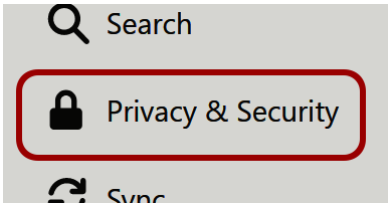
Import in browsers, for VOMS and other purposes

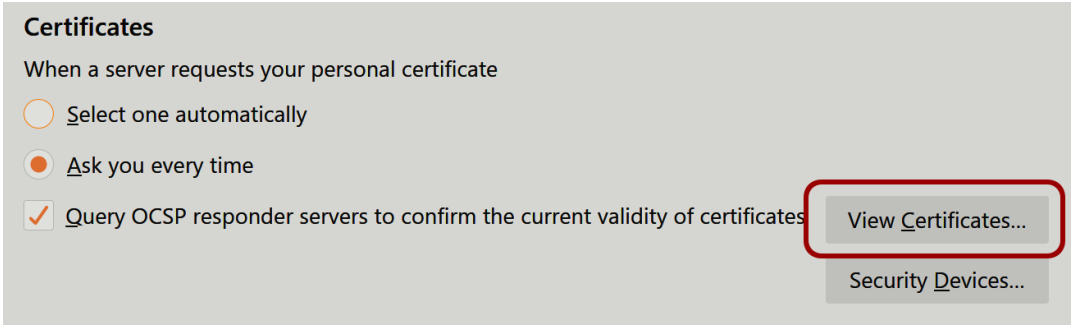
19. In the target directory used above (e.g. `$HOME/.globus`) there is a "PKCS#12" (.p12) file that you can use with your browser, email client, and operating system keychain.
20. Chrome, Safari, Internet Explorer, and Edge all use certificate management provided by the operating system (Windows or MacOS):
    - You can usually double-click on the .p12 file (`package-Your_Name_yourmail_domain_tld.p12`), starting a Certificate Import Wizard:

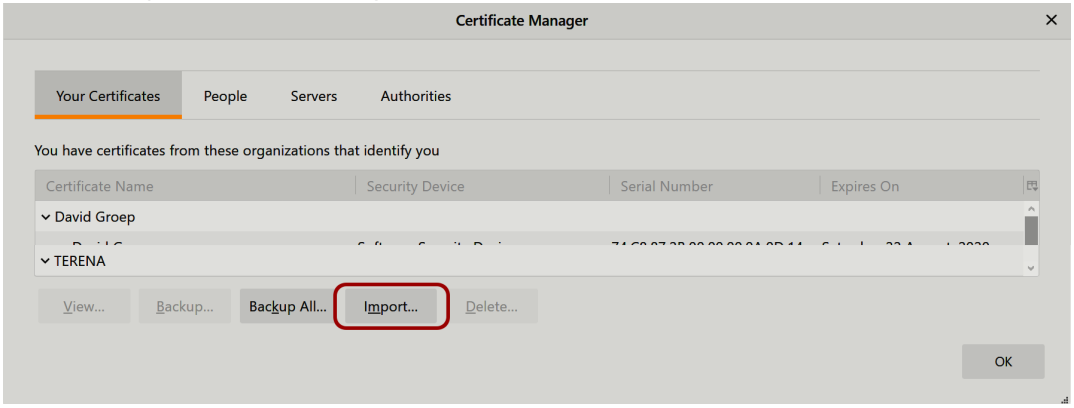


- Import it into the keychain or certificate store for you, the current user
- you will be prompted for a passphrase - this is the same passphrase you used on the HARICA portal and during the conversion script.
  If you are given a choice to '*enable strong private key protection*' you **must do so**:
  

- The certificate should be installed in the personal certificate store (usually automatically selected based on the type of the certificate)
- 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
    - opening the "Options" window (e.g. by typing `about:preferences` in the Firefox address bar), and select the "Privacy and Security" options:
      

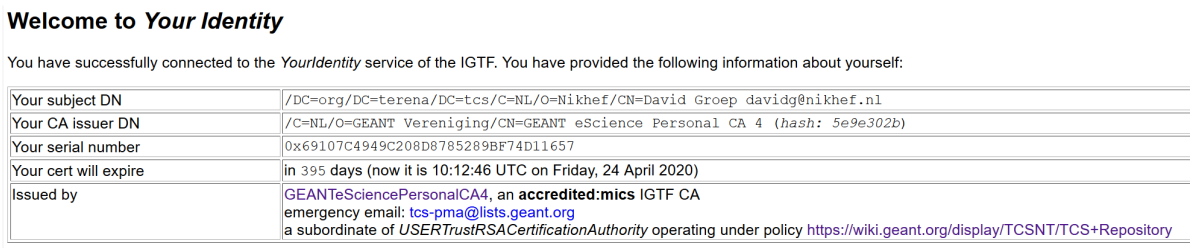
    - scroll to the bottom of the page, and click on "View Certificates" in the Certificate section:
      

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

    - Select the file from the file-chooser dialog, click OK
    - enter the passphrase you used on the HARICA 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 *USERTrustRSACertificationAuthority* operating under policy https://wiki.geant.org/display/TCSNT/TCS+Repository

Are you Elliptic? Or an Expert?

The HARICA 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 either select ECDSA, or upload your own "Certificate Signing Request" (CSR) to the web portal by selecting "CSR" as the Enrolment Method. Only the NIST curves are available.

In case of errors

If you see the following error messages

- **Organization harderwijk.nl was not found in Seamless Access**
  either you have started with the wrong URL, or your organisation has not yet joined eduGAIN. Your security adminstrator must contact SURF to appear in eduGAIN, and also:

  1. Login to the CM system https://cm.harica.gr/
  2. Under "Enterprise" > "Admin", click on the organsation name and use the "Tag" button (top right in the dialog box) and enable "#IGTF-org".

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

- **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. though 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. You can see what you have at https://cm.harica.gr/loginsaml/test.php