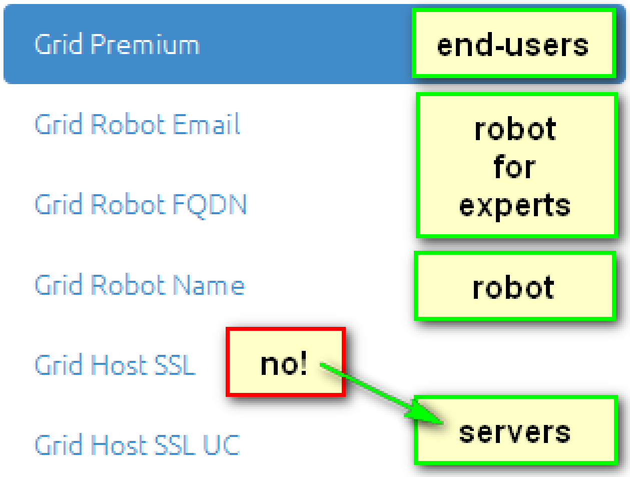
Request Grid Certificates



- There are six types of Grid certificates

  a. **end-users** should get **Grid Premium**
  b. **Grid Host Multi-Domain SSL** is the proper eScience SSL **server** certificate; Grid Host SSL (without Multi-Domain SSL) is useless.
     In 2015 Grid Host Multi-Domain SSL was called Grid Host SSL UC; in early 2016 the name changed. Only the name; not the certificate profile.
  c. end users asking for a robot by default should get **Grid Robot Name**
  d. **Grid Robot Email** is for collaborative operations teams with a security incident response capability (at least they have to react to inquiries within one business day)
  e. **Grid Robot FQDN** is for OV vetted servers, administred by forks who can react in one working day

- In eScience Grid Certificates, long term stability of names is very important as ownership of data sets is coupled to the exact content of Distinguished Names. This is a subject that will be repeated in the wiki page on Validation of Organisations. David Groep himself explains the following.

- In the transition from Comodo to DigiCert, there are a few things that will ease the transition for the subscribers, and in particular for the end-users of the eScience *Personal* certificates. Some of these merit specific attention by the subscriber, i.e. the university, research organisation or more generally the customer organisation itself. In the DigiCert testing phase we tweaked the service long enough that the migration can - in most cases - be completely transparent for end-users (i.e. the humans inside a subscriber organisation).

- The name of an organisation is (pre) validated by DigiCert before you can get certificates for it. The name is based on data provided by the administrator. It is specifically important that the **NAME** of the organisation is **EXACTLY the SAME** as the name that was set in the Comodo service in the Confusa eScience Personal portal(s) - including the same capitalisation.

schacHomeOrg	O=
surfnet.nl	SURFnet BV
lumc.nl	Leids Universitair Medisch Centrum
amc.nl	Academisch Medisch Centrum Universiteit van Amsterdam
wur.nl	Wageningen Universiteit en Research
nikhef.nl	Nikhef
maastrichtuniversity.nl	Universiteit Maastricht
sara.nl	Stichting Academisch Rekencentrum Amsterdam
vu.nl	Vrije Universiteit Amsterdam
tudelft.nl	Technische Universiteit Delft
rug.nl	Rijksuniversiteit Groningen
eur.nl	Erasmus Universiteit Rotterdam
tue.nl	Technische Universiteit Eindhoven

uva.nl	Universiteit van Amsterdam
amolf.nl	FOM-instituut AMOLF
terena.org	TERENA

- I used to have in my eScience Personal certificate as issued by Comodo:
/DC=org/DC=terena/DC=tcs/C=NL/O=Nikhef/CN=David Groep davidg@nikhef.nl
and from DigiCert I now have
/DC=org/DC=terena/DC=tcs/C=NL/O=Nikhef/CN=David Groep davidg@nikhef.nl
which is the Right Thing.

- End-users need to get the same subject name as they had before. This name is habitually used as the 'owner name' in long-term data archives, and for defining community membership.
    - if the name were to change, end-users will likely loose ownership of some data and have to go through a more involved process to retain community memberships automatically.
    - the structure of the DigiCert client certs was specifically tuned so that the transition could be fully transparent to end-users, so it's a 'sales benefit' as well.
    - if your institution(s) choose a service-targeted identifier ('ePTID') as the unique key for eScience Personal certs, users unfortunately still have to re-enrol and take special actions. For the (majority) of the institutions that used 'eduPersonPrincipalName' as the unique identifier, it is all fine and well.

- If your preferred organisation name contains non-ASCII characters, please **also** enrol the corresponding ASCII-fied organisation name next to the original name - with the same caveat as above - so that client-certificate end-users and administrators can select that one for use with the distributed computing infrastructures.

- The certification and (identity) vetting requirements for regular and eScience ("Grid") Personal certificates are exactly the same; there is no reason not to offer eScience (Grid) certificates if you already support regular (Digital Signature Plus or Premium) Personal certificates for the same class of end-users.

- For eScience SSL, in **SERVER ONLY** certs, the name will change: for compliance with public trust requirements ("CABforum BR"), the ST and L fields will be added. So a server that using the Comodo service looked like
/DC=org/DC=terena/DC=tcs/C=NL/O=Nikhef/CN=hooimijt.nikhef.nl
now looks like
/DC=org/DC=terena/DC=tcs/C=NL/L=Amsterdam/ST=Noord-Holland/O=Nikhef/CN=hooimijt.nikhef.nl
Since the certificates have to be publicly trusted, this is unavoidable. But then server SSL certs are not usually the ones 'owning' data, and not usually have community membership themselves. And this change is essentially 'reverting' the DCV change that was imposed on us by Comodo in February 2013.

- The TCS service now also offers "Robot" certificates often used with science gateway portals and such.

- There are special 'by-passes' (in policy and technically) to issue low-volume eScience Personal certs directly from the DigiCert portal; of course after appropriate vetting and validation of the applicant, and by adding what would have been the uniqueID (like ePPN) by hand to the Recipient's Name. Higher volume eScience Personal certificates come from an infrastructure that couples Identity Providers via SAML to a special server.