

New Certificates from the cern.ch/gridca certificate authority

If you get a certificate from the new (early 2014) cern.ch/gridca certificate authority (CA), it will be of a new "type", following the SHA-2 standard. Your previous certificate from the cern.ch/ca authority follow the older SHA-1 standard.

The VOMS machinery sees these two certificate authorities as separate entities, while you will get your certificate with the same DN (as it comes from the same organisation). Unfortunately, when you are asked to re-sign for your VO certificate, the VOMS machinery will look only at the combination of "your DN" AND "Certificate Authority", so it will think you are a "newcomer" when you use your new certificate when going to the web page. If you then simply follow the procedure, it will later complain that the DN is already in use (and, yes, it is: in combination with the "old" certificate authority).

As this change of the certificate standard has caused some confusion, we have written a short description how to avoid the most obvious problems.

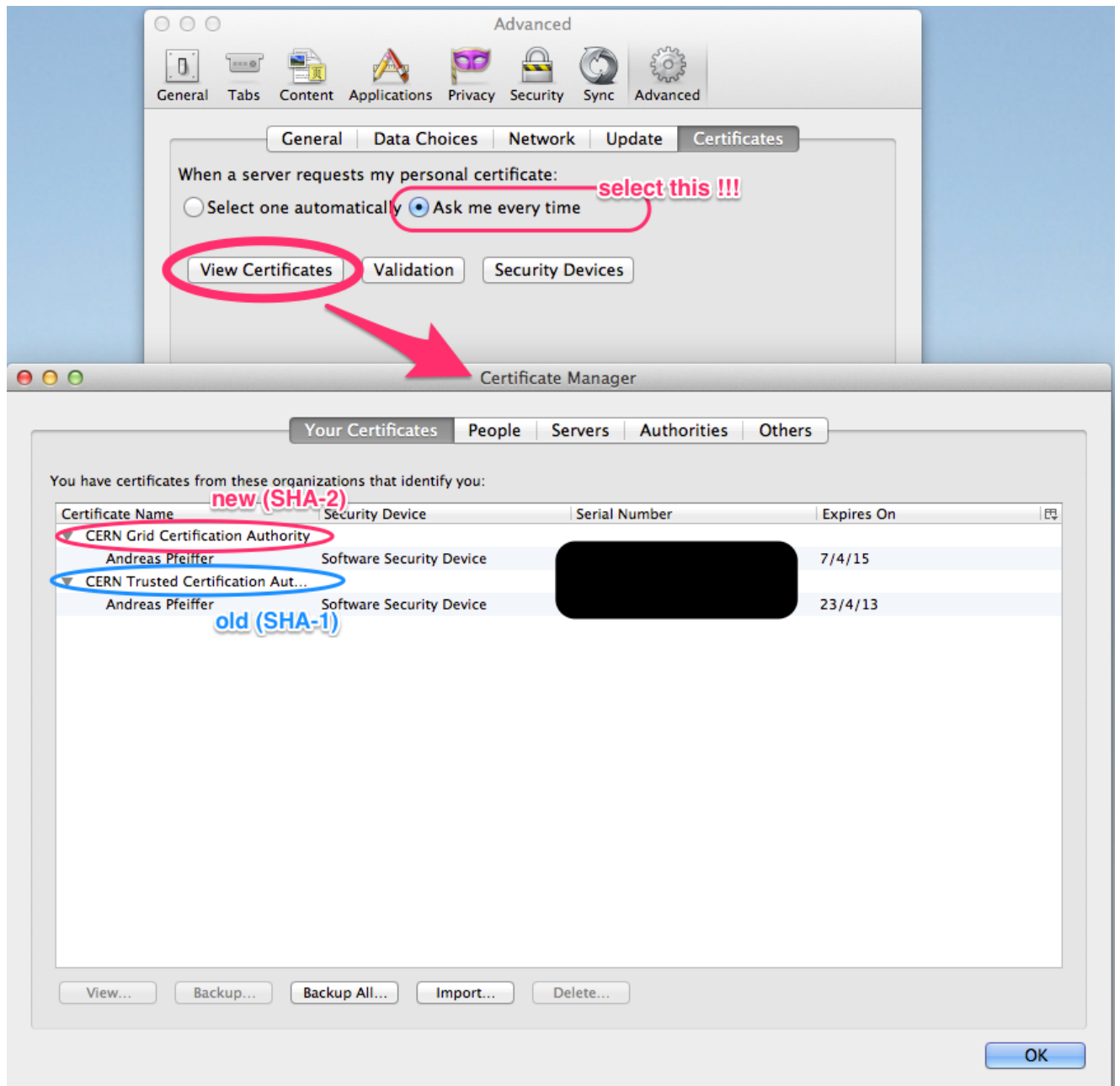
If your (old) certificate is still valid

1. You need a SHA-1 -type certificate (old).

In the example below it is from the old CERN CA: <https://ca.cern.ch/ca/>, but it could be from another CA

2. You need a SHA-2 -type certificate (new).

In the example below it is from the new CERN Grid CA: <https://gridca.cern.ch/gridca/>, but it could be from another CA You can verify which certificates you have: from the generic part of the Firefox follow the chain: Firefox -> Preferences -> Advanced -> Encryption -> View certificates -> "Your Certificates" The "SHA-1" is from "CERN Trusted Certification Authority" and "SHA-2" is from "CERN Grid Certification Authority" see:



As you have to choose which certificate is used at each of the following steps, you must tick-mark the choice "ask every time" from the Firefox "Certificates" page (View certificates, see the picture above).

3. Add the new certificate into CMS-VOMRS:

<https://lcg-voms.cern.ch:8443/vo/cms/vomrs?path=/RootNode/MemberAction/MemberDNs/AddDN&action=execute>

To get there, you must use the (old) SHA-1 certificate. A detailed example on how to add a new certificate to you CMS-VOMRS account is here:

<https://twiki.cern.ch/twiki/bin/view/CMSPublic/VoRegForExistingMember>

4. Set the new certificate as the primary one in CMS-VOMRS:

<https://lcg-voms.cern.ch:8443/vo/cms/vomrs?path=/RootNode/MemberAction/MemberDNs/ChangeDN&action=execute>

To get there, you must again use the (old) SHA-1 certificate.

5. Now you can forget the existence of your (old) SHA-1 certificate, but you might as well keep it - just in case.

6. If you want, you can now un-tick the "ask every time" from your Firefox, so it does not prompt you every time.

If your (old) certificate is still valid

If your (old) certificate is no longer valid

1. Get a new SHA-2 type certificate for example from <https://gridca.cern.ch/gridca/>
2. Ask your representative to erase your old data (DN) from the CMS-VOMRS by emailing to <mailto:project-lcg-vo-cms-admin@cernNOSPAMPLEASE.ch> please note that this might take a day or two.
3. Register yourself into CMS-VOMRS the same way as a new member (newcomer):
<https://lcg-voms.cern.ch:8443/vo/cms/vomrs?path=/rootnode> or
<https://lcg-voms.cern.ch:8443/vo/cms/vomrs?path=/RootNode/MemberAction/MemberRegistration&action=execute>
following the documentation in <https://twiki.cern.ch/twiki/bin/view/CMSPublic/WorkBookStartingGrid>

-- AndreasPfeiffer - 10 Apr 2014

This topic: CMSPublic > CERNGridCertificateIssues

Topic revision: r3 - 2014-04-29 - AndreasPfeiffer



Copyright &© 2008-2020 by the contributing authors. All material on this collaboration platform is the property of the contributing authors.

or Ideas, requests, problems regarding TWiki? use Discourse or Send feedback