Contribution ID: **122** Type: **not specified**

Tweaking the Certificate Lifecycle for the UK eScience CA

Friday, 30 March 2012 11:00 (25 minutes)

Description of the Work

We describe two changes to our CertWizard software to reduce the need to re-apply and also an alternative to the currently required face to face meeting for such "technical renewals". Users will now therefore be able to renew recently expired certificates, amend their certificate's email address and avoid unnecessary face to face meetings when on secondment.

When a certificates is initially requested from the UK e-Science CA the user must have a face-to-face meeting with his Registration Authority (RA) to check and photocopy the user's PhotoID. Annual renewals require the RA Operator to confirm the user's entitlement to a certificate; no face to face is required.

One change we can make to our CertWizard tool(which is used to request and renew UK e-Science Certificates) is to support a grace period after certificate expiry within which a user may renew his certificate providing it hasn't been revoked. Ordinarily, once a certificate has expired he can do nothing with it, but it is often in the first few days after expiry that a user realises that it has expired. A second change would be to provide an interface to enable the user to change his certificate's email address without the need to revoke and then re-apply.

For the case of a user's certificate which has been expired for a longer period, or for when it is no longer in his possession, then renewal isn't possible. It usually won't be a problem for the user to request a new certificate, but if the user is not sited close to his RA (seconded to CERN for instance) then this isn't practical. Since the user has already had his ID checked and if the RA Operator still has a legible photocopy of his ID then we will permit a video meeting between the user and the RA Operator who will confirm that the user possesses a PhotoID that matches his copy. Note that this will not be permitted for an initial application, only for such re-applications.

Conclusions

Using this combined approach of changes to both software and policy we can reduce the number of renewals which require any RA Operator's involvement. It will also provide a less painful certificate experience for the user, especially those who would have no convenient way of of obtaining a replacement certificate.

A large percentage of tickets we receive on the NGS helpdesk are related to the issues described above, whether advising users or RA Operators, so reduced ticket numbers will be an additional benefit.

Impact

Many of our users have had email address changes in the past. For instance users at RAL now have both a legacy .rl.ac.uk one as well as their new stfc.ac.uk one. This change will allow them to change to their new ones seamlessly without the involvement of their RA Operator.

Renewing a recently expired certificate will only now require the RA Operator to check the user is still entitled to a UK e-Science Certificate. The time taken for both of them to participate in (and travel to) their face to face meeting is saved.

Users who are no longer in possession of a valid certificate (because of, for instance certificate revocation, certificate loss, hardware crash or operating system re-installation) and are unable to conveniently attend a face to face meeting, now have the possibility to use Video Conference or Access Grid rather which will save on travel time and costs.

URL

http://www.ngs.ac.uk/tools/certwizard

https://ca.grid-support.ac.uk

Overview (For the conference guide)

The UK e-Science Certification Authority (CA) is the 2nd largest IGTF-accredited Grid CA. This paper considers changes to its normal certificate lifecycle (New, Renew, ..., Expire/Revoke) to provide users with simpler ways to re-apply for the e-Science certificates it issues.

If a user's email address changes, or his certificate has expired or is lost, he needs to re-apply to the UK e-Science Certification Authority for a new certificate rather than renew it (if the old certificate hasn't expired it will also need revoking). This requires another face to face visit with the local Registration Authority (RA) Operator for photoID checking and might not be convenient if the user is at a different location.

It is this process of Re-applying that we want to simplify, reducing involvement of the RA Operator and attempting to eliminate the need for face to face meetings beyond the initial one.

Primary author: KEWLEY, John (STFC)

Co-authors: MEREDITH, David (STFC); JENSEN, Jens (STFC)

Presenter: KEWLEY, John (STFC)

Session Classification: Security