SWITCHpki long lived grid user certificates

PKI meeting in Bern

SWITCH

Serving Swiss Universities

Alessandro Usai
alessandro.usai@switch.ch

Bern, 15 June 2010

Trust Link Interface

- Long lived grid user certificates are now handled by the QuoVadis Trust Link interface (the same system which is used for SSL certificates). Why?
  1. **More stable platform**, compatible with different architectures.
  2. **Certs are easier to manage**, better control (no secret url etc).
  3. **One unique system** for all the certificates.

- The legacy system (webrao) will be discontinued and the existing grid user certificates holders “migrated” to Trust Link by **issuing new certificates**.

Migration plan to Trust Link

- The new system already live and the new **user** documentation available.
- From now until September **we will reissue new grid user certificates** for all the existing users “within the webrao interface” (apologies for this!).
- We will coordinate it directly with the users, so as to minimize the hassle! (I will eventually talk to you on the phone ☺
- The webrao certificates will be revoked in parallel and the webrao system discontinued after September (**you don’t need to know about this**).

Overall Procedure in a nutshell 1/3

- The user is identity vetted by his/her RA: **no change**

Note: please make sure you see the original document, not a copy.

- Id vetting docs are sent to SWITCH RA: **no change**
- SWITCH RA creates in TLSSL an invitation for the user to login into the system, with as user name the user e-mail address, and as password the first 6 character of the user id-document number. Notice: All the necessary checks on the user details are done by the SWITCH RA.

Overall Procedure in a nutshell 2/3

- The user receives an e-mail with a “logging link”, accesses the system (with the password “from his/her id document”), chooses yet another certificate pickup password and submits the CSR. The private key is generated within his/her browser. **No change**
- The certificate is automatically issued and the user notified via e-mail, which contains a logging link.
- The user accesses the system with as user name the user e-mail address, and as password the certificate pickup password, and retrieves the certificates (the CA certificate can also be downloaded): **no change**

Overall Procedure in a nutshell 3/3

Certificate renewal/replacement:

- A warning e-mail will be sent 1 month before the cert expires.
- The user sends an e-mail to SWITCH RA requesting a new certificate: **no change**
- SWITCH RA checks the request: **no change**
- If all ok an invitation is sent, if not the user is asked to be identity vetted again: **no change**
- The old still valid grid user certificate will be revoked after 7 days from the invitation: **no major change**

How are you affected?

- SWITCHpki RAs: **no change**
- All the grid user certificates will still be handled directly by the SWITCH RA: **no change**
- From the user point of view the change is also minimal+ benefits:
  1. **Triggered e-mail from QuoVadis**, instead of template e-mail from SWITCH.
  2. **Better access control**, thanks to predefined password access (the user's passport details are used).
  3. **A procedure to renew/replace certificates** will be available (see previous slide about the warning e-mail).

Future possible improvements

User portal, where to automatically renew one's certificate:

It requires the storing of the User's details and the date of the identity vetting: this is essential to reduce the overhead from the RA side.

Possibility for other Organization to handle long lived grid user certs: only meaningful if the number of certs increases, and in parallel QuoVadis delivers the needed extra functionalities for the automatic update.

General comments

- Long lived grid user certificates are not free.
- You should only request one if you need to “grid-enable” your browser.
- Long lived grid user certificates still handled directly by the SWICTH RA for the time being: **your feedback on this?**
- **SWITCH recommends to also use SLCS certificates (check with us grid@switch.ch in case you have doubts).**

SLCS enrollment procedure change

Based on the SLCS self audit with EUGridPMA we decided to modify the organization enrollment for SLCS i.e.

- Organizations acknowledge the IdP best practice guidelines.

- Organizations agree to report to SWITCH should they not be able to comply with the guidelines, in which case they might be asked by SWITCH to present a self-audit.