# OSG PKI Transition

Impact on CMS

# Impact on End User

- After March 23 2013, DOEGrids CA will stop issuing or renewing certificates.
- If a user is entitled to get certificates from the CERN CA, we strongly recommend that the user should get CERN certificate
- Exceptions (get an OSG certificate):
  - Users who cannot for some reason obtain a CERN certificate
  - User who need to digitally sign their email (e.g. CMS Sponsors)
- Must register new certificate with:
  - CMS VOMRS (Required to get a VOMS proxy)
  - SiteDB (Required to run CMS jobs)
- May need to register new certificate with:
  - CERN SSO (Only if you are getting a non-CERN certificate)
  - REBUS
  - GGUS
  - OIM, MyOSG, OSG Ticketing System
  - Site local storage
- https://twiki.cern.ch/twiki/bin/view/CMSPublic/EndUsers

# Impact on Sys Admins

- If your proxy is used for PhEDEx, then make sure you update your mapping in GUMS for storage
- After March 2013, you should obtain host/service certificates from the OSG CA
- There is a web interface (through OIM) and a command line interface.
- All Tier-2 sites should have at least one administrator registered as a grid-admin
  - Much quicker turn around in receiving certificates
  - Self approve certificate requests automatically
- Tier-3 site admins can talk to Rob Snihur to determine if they want or need to become grid-admins
- [https://twiki.cern.ch/twiki/bin/view/CMSPublic/SysAdmins](https://twiki.cern.ch/twiki/bin/view/CMSPublic/SysAdmins)

# CMS Site Specific Impact

- No real impact on running a job
- Number of dedicated CMS Pool accounts goes up (if using pool accounts)
- However… Storage may be impacted
  - CMS allows storage on a per user basis
  - Need to ensure user is mapped to an account with rw privileges to their own files
  - Not an issue with sites using gridmap files
  - Not an issue with sites that do not use pool accounts
- Sites using GUMS will need to do a little work

# (Re)Map Users in GUMS

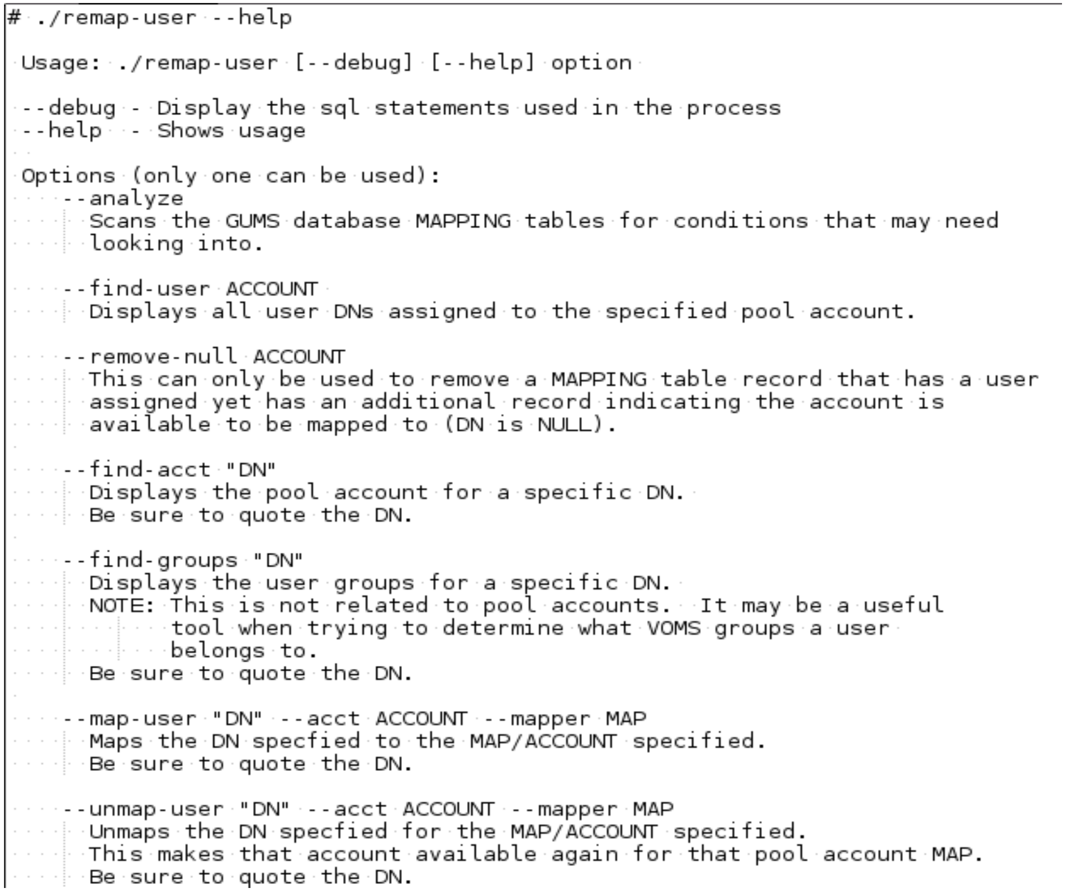
- Unfortunately, there is no automated way to update user mappings
  - Many users let their certs expire before requesting new certs
  - Many users create new registrations in VOMRS rather than associate their new cert with their existing VOMRS registration
  - As a consequence, we cannot automatically determine the DNs to associate with each other
  - Additionally, sites have different procedures on how to handle cert changes

# (Re)Map Users in GUMS

- John Weigand wrote a tool that helps you analyze your current GUMS situation and take steps to fix problems and re-map users appropriately
- **http://home.fnal.gov/~tiradani/downloads/remap-user**
- Must be run as root
  - Reads GUMS database info from the GUMS config
- Very useful for GUMS "archaeology" as well as remapping users

# (Re)Map Tool

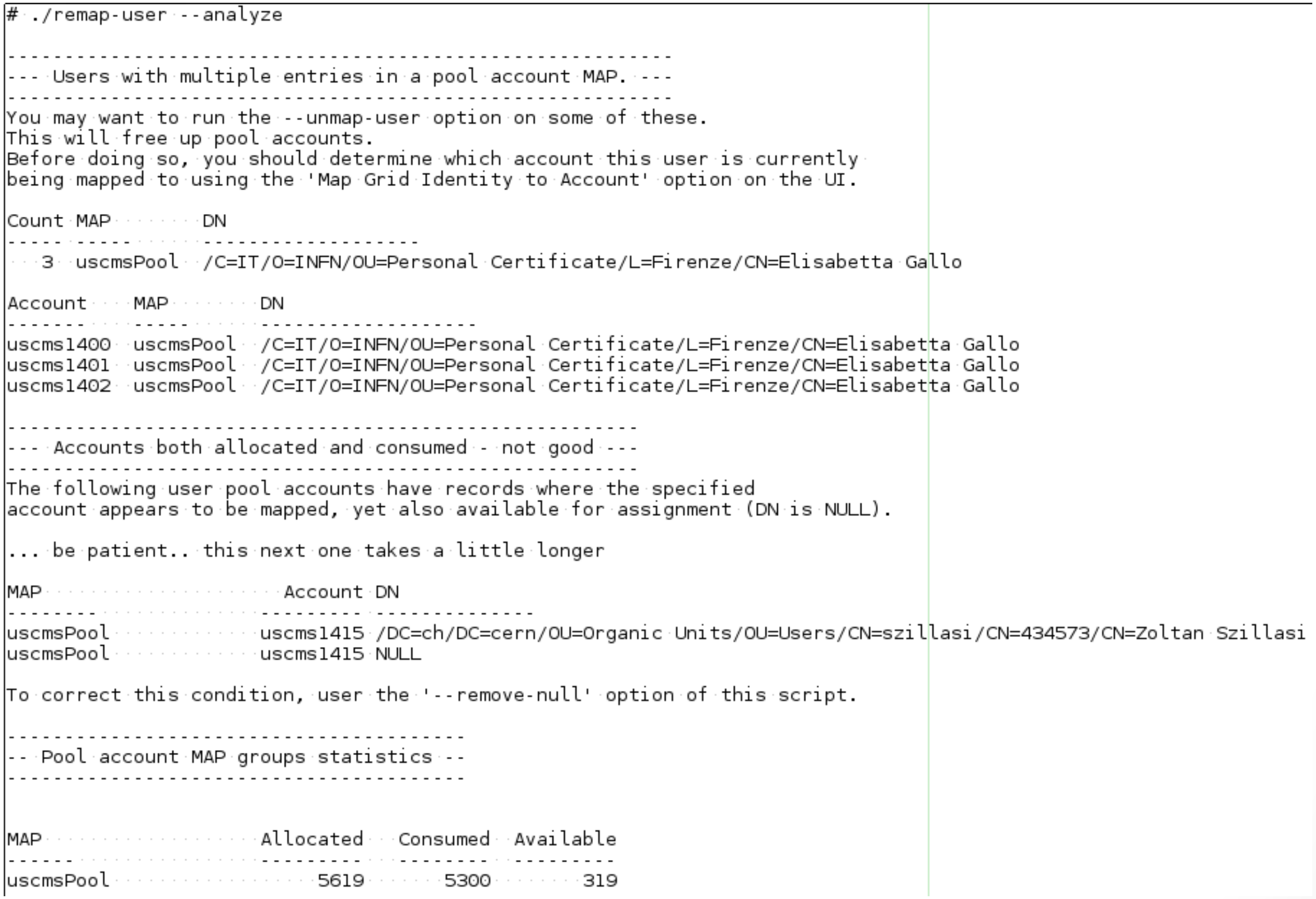
- GUMS archaeology: --find-user, --find-groups, --find-acct, --analyze
- GUMS Mod: --remove-null, --map-user, --unmap-user



```
# ./remap-user --help

 Usage: ./remap-user [--debug] [--help] option

 --debug - Display the sql statements used in the process
 --help  - Shows usage

 Options (only one can be used):
    --analyze
      Scans the GUMS database MAPPING tables for conditions that may need
      looking into.

    --find-user ACCOUNT
      Displays all user DNs assigned to the specified pool account.

    --remove-null ACCOUNT
      This can only be used to remove a MAPPING table record that has a user
      assigned yet has an additional record indicating the account is
      available to be mapped to (DN is NULL).

    --find-acct "DN"
      Displays the pool account for a specific DN.
      Be sure to quote the DN.

    --find-groups "DN"
      Displays the user groups for a specific DN.
      NOTE: This is not related to pool accounts.  It may be a useful
            tool when trying to determine what VOMS groups a user
            belongs to.
      Be sure to quote the DN.

    --map-user "DN" --acct ACCOUNT --mapper MAP
      Maps the DN specfied to the MAP/ACCOUNT specified.
      Be sure to quote the DN.

    --unmap-user "DN" --acct ACCOUNT --mapper MAP
      Unmaps the DN specfied for the MAP/ACCOUNT specified.
      This makes that account available again for that pool account MAP.
      Be sure to quote the DN.
```

# (Re)Map Tool

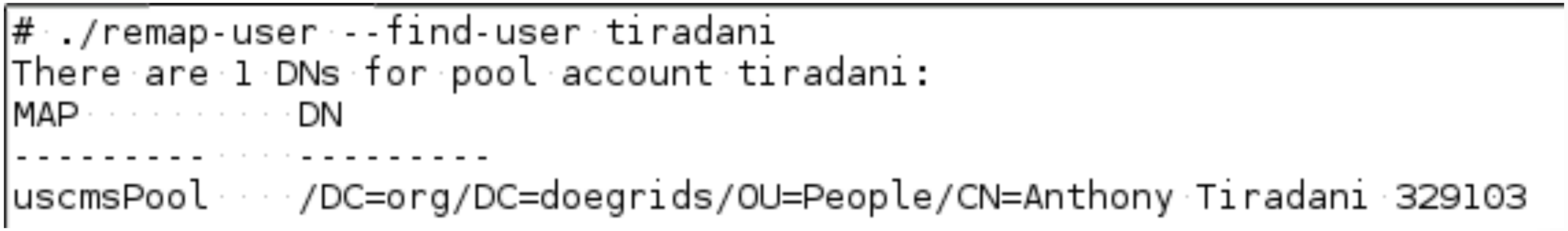
- Analyze output:  Shows potential problems in the database



```
# ./remap-user --analyze

----------------------------------------------------------
--- Users with multiple entries in a pool account MAP. ---
----------------------------------------------------------
You may want to run the --unmap-user option on some of these.
This will free up pool accounts.
Before doing so, you should determine which account this user is currently
being mapped to using the 'Map Grid Identity to Account' option on the UI.

Count MAP        DN
----- -----      -------------------
   3  uscmsPool  /C=IT/O=INFN/OU=Personal Certificate/L=Firenze/CN=Elisabetta Gallo

Account    MAP        DN
-------    -----      -------------------
uscms1400  uscmsPool  /C=IT/O=INFN/OU=Personal Certificate/L=Firenze/CN=Elisabetta Gallo
uscms1401  uscmsPool  /C=IT/O=INFN/OU=Personal Certificate/L=Firenze/CN=Elisabetta Gallo
uscms1402  uscmsPool  /C=IT/O=INFN/OU=Personal Certificate/L=Firenze/CN=Elisabetta Gallo

-------------------------------------------------------
--- Accounts both allocated and consumed - not good ---
-------------------------------------------------------
The following user pool accounts have records where the specified
account appears to be mapped, yet also available for assignment (DN is NULL).

... be patient.. this next one takes a little longer

MAP                     Account DN
--------              --------- --------------
uscmsPool             uscms1415 /DC=ch/DC=cern/OU=Organic Units/OU=Users/CN=szillasi/CN=434573/CN=Zoltan Szillasi
uscmsPool             uscms1415 NULL

To correct this condition, user the '--remove-null' option of this script.

----------------------------------------
-- Pool account MAP groups statistics --
----------------------------------------


MAP                   Allocated   Consumed  Available
------                ---------   --------  ---------
uscmsPool                  5619       5300        319
```

# (Re)Map Tool

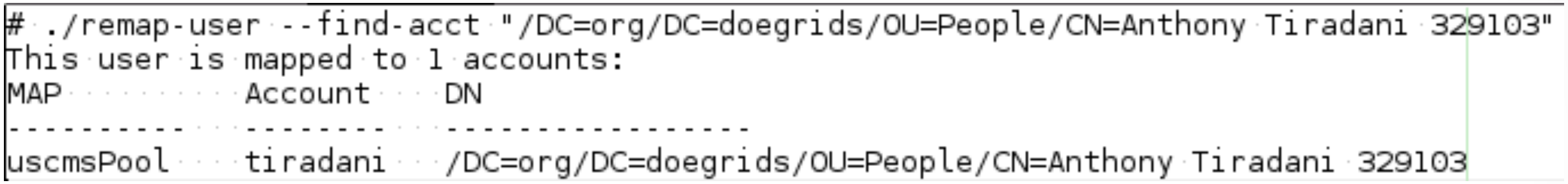
- In this context, user is the unix pool account
- Shows all DNs associated with the pool account



```
# ./remap-user --find-user tiradani
There are 1 DNs for pool account tiradani:
MAP         DN
---------   ---------
uscmsPool   /DC=org/DC=doegrids/OU=People/CN=Anthony Tiradani 329103
```

# (Re)Map Tool

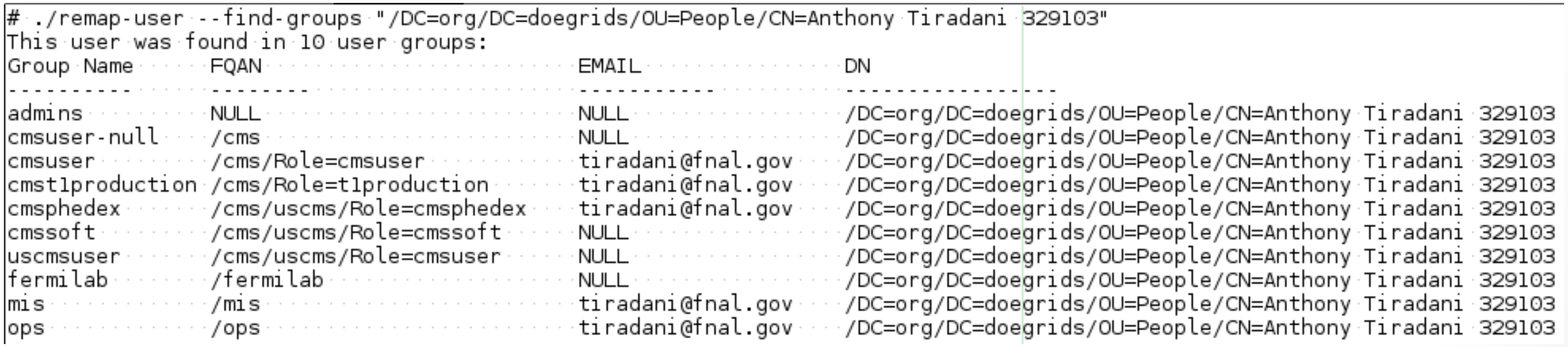
- Displays all pool accounts for a specific DN



```
# ./remap-user --find-acct "/DC=org/DC=doegrids/OU=People/CN=Anthony Tiradani 329103"
This user is mapped to 1 accounts:
MAP          Account    DN
----------   --------   -----------------
uscmsPool    tiradani   /DC=org/DC=doegrids/OU=People/CN=Anthony Tiradani 329103
```

# (Re)Map Tool

- Occasionally, you may encounter a user user in the mapping table but have trouble finding the user in the GUMS user interface
- The --find-groups option will display all the groups the DN has been assigned to
- If no groups are returned, that means the user no longer has any valid certificates registered with the VOMS server
- GUMS does not remove the user from the mapping table



```
# ./remap-user --find-groups "/DC=org/DC=doegrids/OU=People/CN=Anthony Tiradani 329103"
This user was found in 10 user groups:
Group Name      FQAN                           EMAIL                DN
----------      --------                       -----------          -----------------
admins          NULL                           NULL                 /DC=org/DC=doegrids/OU=People/CN=Anthony Tiradani 329103
cmsuser-null    /cms                           NULL                 /DC=org/DC=doegrids/OU=People/CN=Anthony Tiradani 329103
cmsuser         /cms/Role=cmsuser              tiradani@fnal.gov    /DC=org/DC=doegrids/OU=People/CN=Anthony Tiradani 329103
cmst1production /cms/Role=t1production         tiradani@fnal.gov    /DC=org/DC=doegrids/OU=People/CN=Anthony Tiradani 329103
cmsphedex       /cms/uscms/Role=cmsphedex      tiradani@fnal.gov    /DC=org/DC=doegrids/OU=People/CN=Anthony Tiradani 329103
cmssoft         /cms/uscms/Role=cmssoft        NULL                 /DC=org/DC=doegrids/OU=People/CN=Anthony Tiradani 329103
uscmsuser       /cms/uscms/Role=cmsuser        NULL                 /DC=org/DC=doegrids/OU=People/CN=Anthony Tiradani 329103
fermilab        /fermilab                      NULL                 /DC=org/DC=doegrids/OU=People/CN=Anthony Tiradani 329103
mis             /mis                           tiradani@fnal.gov    /DC=org/DC=doegrids/OU=People/CN=Anthony Tiradani 329103
ops             /ops                           tiradani@fnal.gov    /DC=org/DC=doegrids/OU=People/CN=Anthony Tiradani 329103
```

# OSG PKI Transition Questions

Questions?