CERN VOMS upgrade

Andrea Ceccanti, Laurence Field

GDB Meeting
October, 14th 2020

Outline

The VOMS 10-20 release

CERN VOMS service upgrade

VOMS legacy clients support statement

The VOMS 10-20 release

VOMS 10-20 release

Code freezed, documentation being finalised, server components already deployed @ CERN

- ETA: 23/10/2020

Provides updates for all VOMS components

- VOMS Admin server 3.8.0, VOMS Admin client 2.0.20
- VOMS 2.0.15
- VOMS Clients 3.3.2, VOMS API Java 3.3.2

VOMS GDPR-compliance changes

HR db integration refactoring

CENTOS 7/SystemD porting

Bug fixes and enhancements

VOMS Admin 3.8.0: GDPR compliance

GDPR-compliance changes: GGUS ticket

Remove all data for users who have been in status EXPIRED for more than a configurable period (default: 1 month)

- Users that failed to sign the AUP are not removed

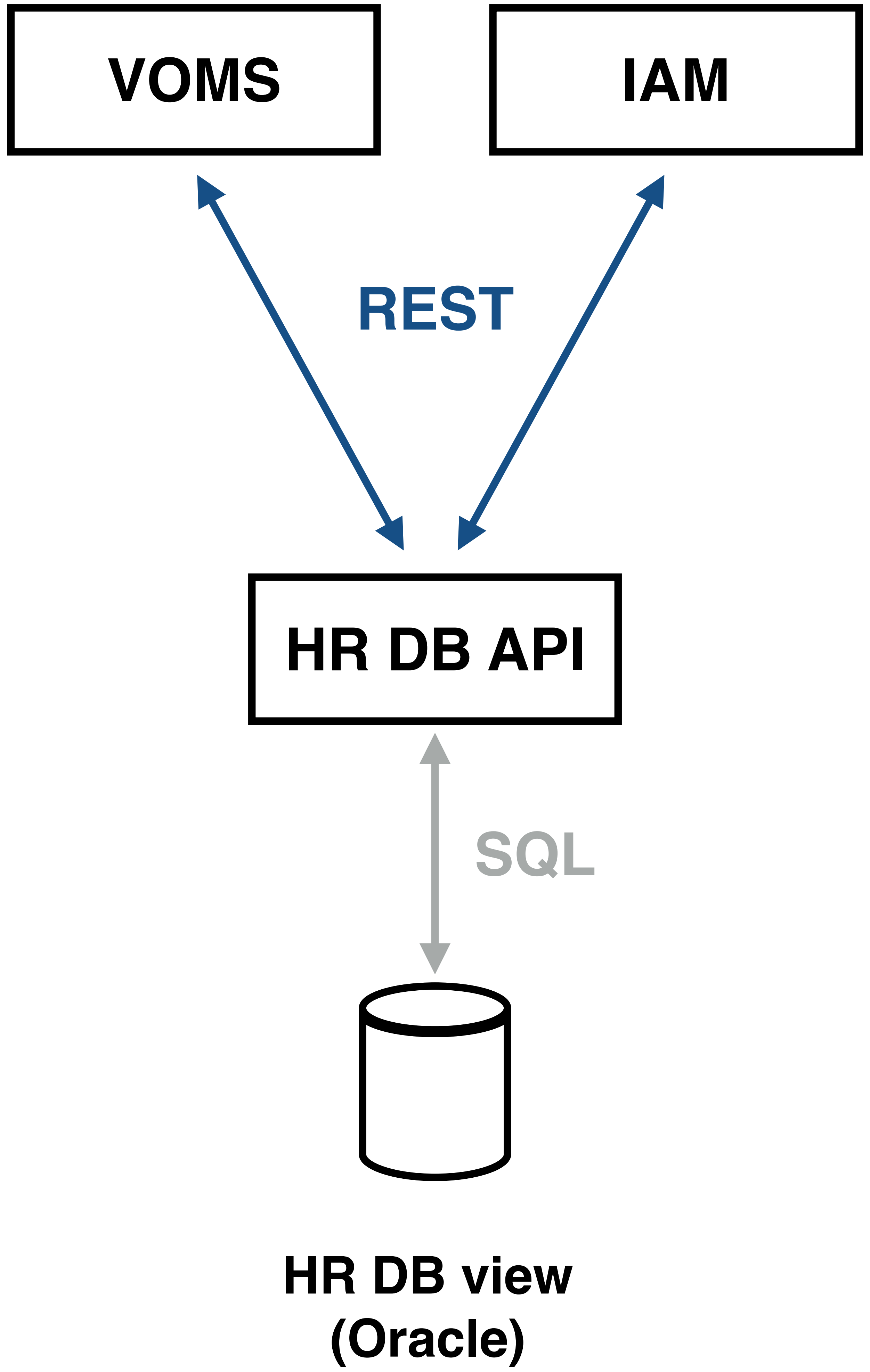
Restrict what can be seen by any authenticated user: only the list of certificate subject DNs for a given VOMS group or role shall be exposed to any authenticated user, because that functionality is needed for constructing grid-mapfiles.

VOMS Admin 3.8.0: HR db integration refactoring

VOMS Admin used to integrate directly with the Oracle HR DB for experiment membership checks

The HR integration has been refactored to call out to the HR DB API, a thin REST layer in front of the new HR DB VOMS views

The same API is used by IAM WLCG deployments



VOMS Admin 3.8.0: CENTOS 7/SystemD porting

VOMS Admin daemon lifecycle now managed with SystemD

Dedicated utility to enable/disable active VOs:

- `voms-vo-ctl deploy atlas`
- this was previously done by the init-script, difficult to port to SystemD

VOMS Admin 3.8.0: MySQL connector update

MySQL connector updated to version 8.0.16

Requires timezone set in the database or in the database URL **or the connection to the database will fail and the service will not start**

`voms-configure` utility updated to allow setting the timezone URL at VO configuration time

VOMS Admin client 2.0.20: CENTOS 7 porting

No significant code changes

Requires python-zsi package, no longer in EPEL

Package provided in our VOMS-external repo

VOMS 2.0.15: CENTOS 7/SystemD porting

Move to SystemD instantiated services

```
systemctl start|stop|status voms@atlas
```

To run commands on all configured VOs:

```
systemctl start|stop|status voms@‘*’
```

VOMS 2.0.15: OSG patches merged upstream

Patches by B. Bockelman and M. Selmeci merged upstream:

- Github commit

Validate top-level VOMS group

Make RFC proxies by default for legacy VOMS clients

Disable TLS1.1 and older

Disable Weak ciphers

VOMS API Java 3.3.2, VOMS clients 3.3.2

Bug fixes and improvements:

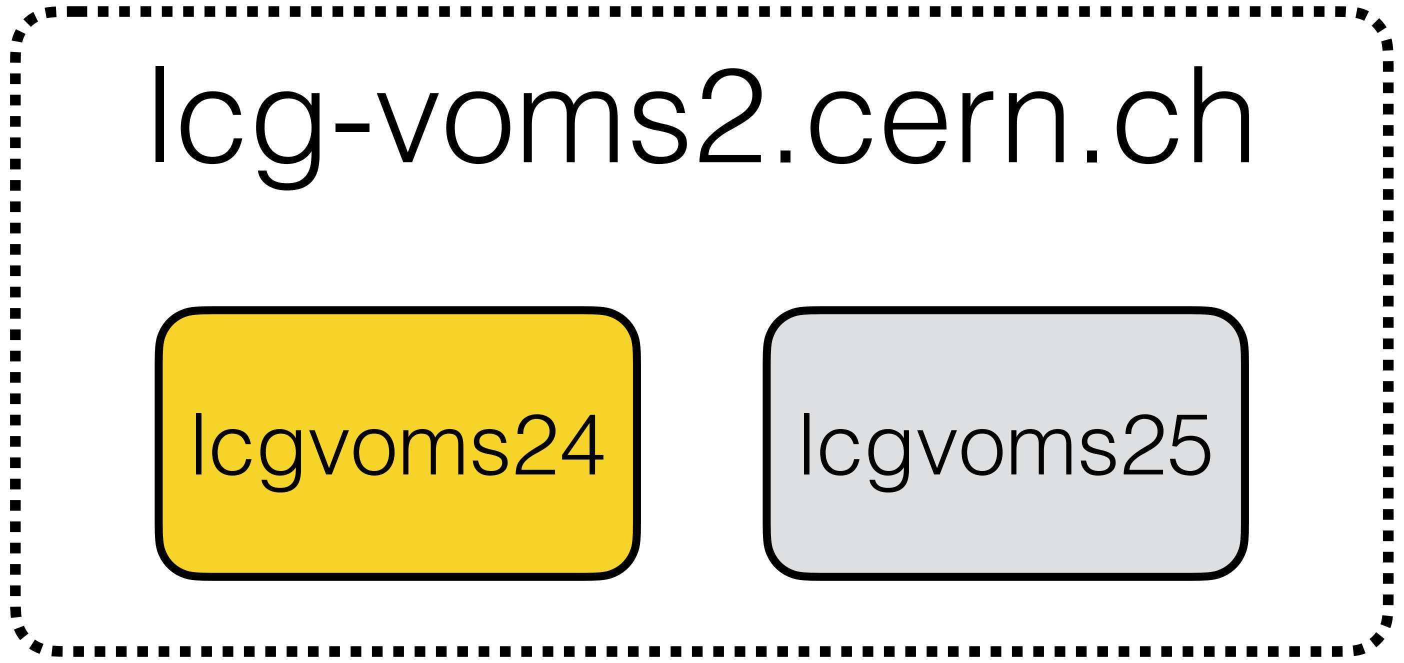
- https://issues.infn.it/jira/browse/VOMS-876: VOMS Java APIs authorityKeyIdentifier AC extension validation is not aligned with C/C++ VOMS APIs (more on this later)
- https://issues.infn.it/jira/browse/VOMS-878: Update to CANL 2.2.6
- https://issues.infn.it/jira/browse/VOMS-877: Make fallback to VOMS legacy protocol optional

CERN VOMS upgrade

CERN VOMS Service

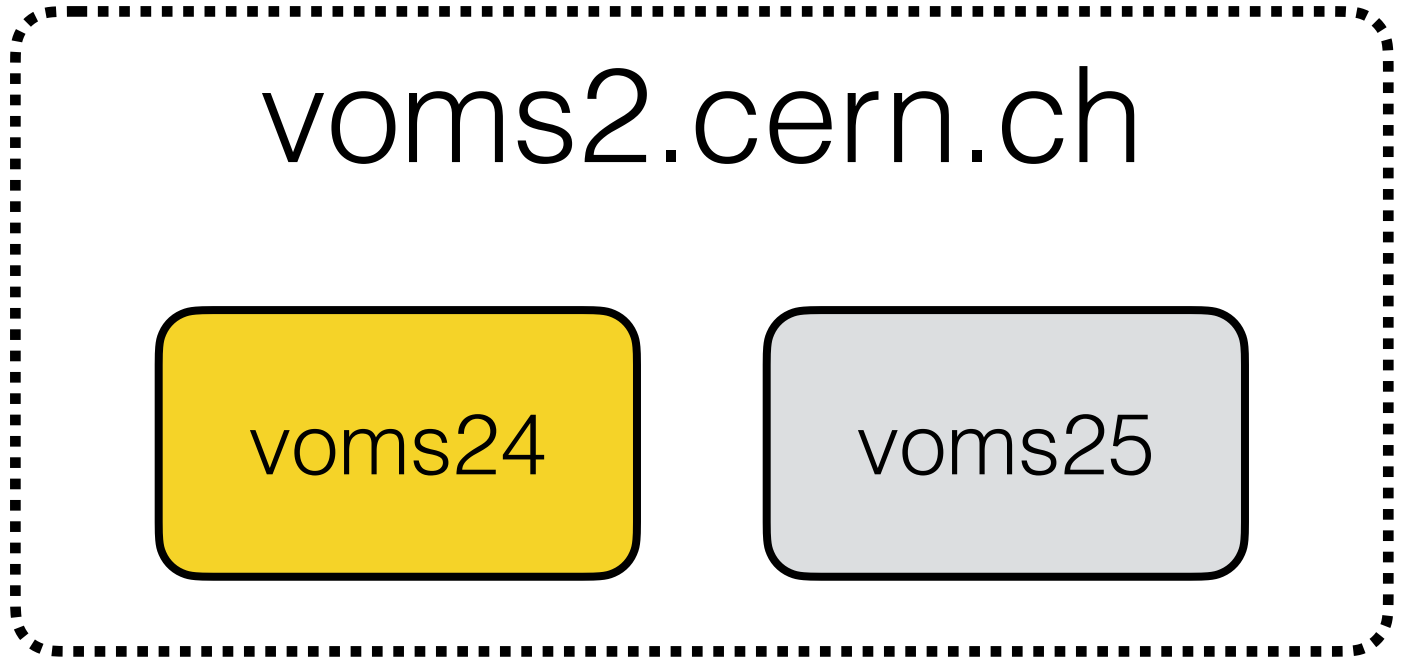
Two load balanced aliases: lcg-voms2.cern.ch and voms2.cern.ch

lcg-voms2 is the legacy alias. It is being kept to support client-side fail-over.



Each alias has a primary and secondary configuration.

- voms2: voms24 (primary), voms25 (secondary)
- lcg-voms2: lcgvoms24 (primary), lcgvoms25 (secondary)



The deployment uses the DBoD Service at CERN for the MySQL DB instance and

each VO has a separate database in this instance.

VOMS standard upgrade procedure

1. Upgrade lcgvoms25
2. Switch lcg-voms2 alias
3. Upgrade lcgvoms24
4. Switch lcg-voms2 alias back
5. Upgrade voms25
6. Switch voms2 alias
7. Upgrade voms24
8. Switch voms2 alias back

If no DB upgrade is required, the upgrade can be done live without scheduling any downtime. Otherwise all services will need to be stopped (downtime required) and the DB upgraded before the standard upgrade procedure can be followed.

VOMS Admin 3.8.0 testing

Required in depth testing due to new GDPR DB cleanup & move to CENTOS 7

A test node was used to validate initial install

For ALICE, ATLAS, CMS and LHCb, a local copy of the production DB was used to evaluate the GDPR cleanup task using the new HR sync code

The VO-Admins were invited to check the result

Further, testing of the configuration (new systemd, etc.), fresh installations, reboot tests etc.

VOMS service upgrade timeline

Tue 22nd Sept

AM: Test instance switched to the production DB.
Cleanup tasks executed

PM: lcgvoms25 and voms25 upgraded

Wed 23rd Sept

9:30 Switched lcg-voms2 to lcgvoms25

10:39 First report of issues

12:47 Switched voms2 to voms25

15:45 Issue confirmed, switched voms2 back to old instance

17:09 Switched lcg-voms2 back to old instance

Fri 25th Sept

New VOMS packages fixing the problem installed and tested

Mon 28th Sept

9:30 Switched lcg-voms2 to updated lcgvoms25

15:25 Switched voms2 to updated voms25

Tue 29th Sept

Upgraded lcgvoms24 and voms24

Switched aliases back to primary instances

What went wrong?

VOMS 2.1.0, originally included in this update, generated attribute certificates (ACs) incompatible with the VOMS 2.0.x C/C++ APIs

- https://issues.infn.it/jira/browse/VOMS-875

The bug was introduced in a refactoring of the code needed to support OpenSSL 1.1.0

The issue was not observed during testing since the incompatibility was not visible from VOMS Java clients due to

- a bug in the VOMS Java APIs which validated successfully the invalid AC issued by VOMS 2.1.0 https://issues.infn.it/jira/browse/VOMS-876
- incomplete automated testing

Corrective actions

Postpone the VOMS 2.1.0 release to a later date

- Understand and fix the AC encoding issue **DONE**

Release VOMS 2.0.15 including minimal changes w.r.t. production

- VOMS 2.0.14 + SystemD unit + OSG patches **DONE**

Fix VOMS Java API incompatibility **DONE**

Include stronger backward compatibility testing in our CI pipeline

- Test against legacy voms clients **IN PROGRESS**
- Test against services that rely on the VOMS APIs (e.g., StoRM, XRootD) **IN PROGRESS**

A word about legacy VOMS clients support

The supported VOMS clients are the Java ones, but **we have no plans to break interoperability with the legacy clients**

- No active development is foreseen but contributions/patches from the community are welcome

In support of this statement

- legacy clients interoperability testing is being included in our CI testing pipeline
- the IAM VOMS implementation has been modified to support VOMS legacy clients

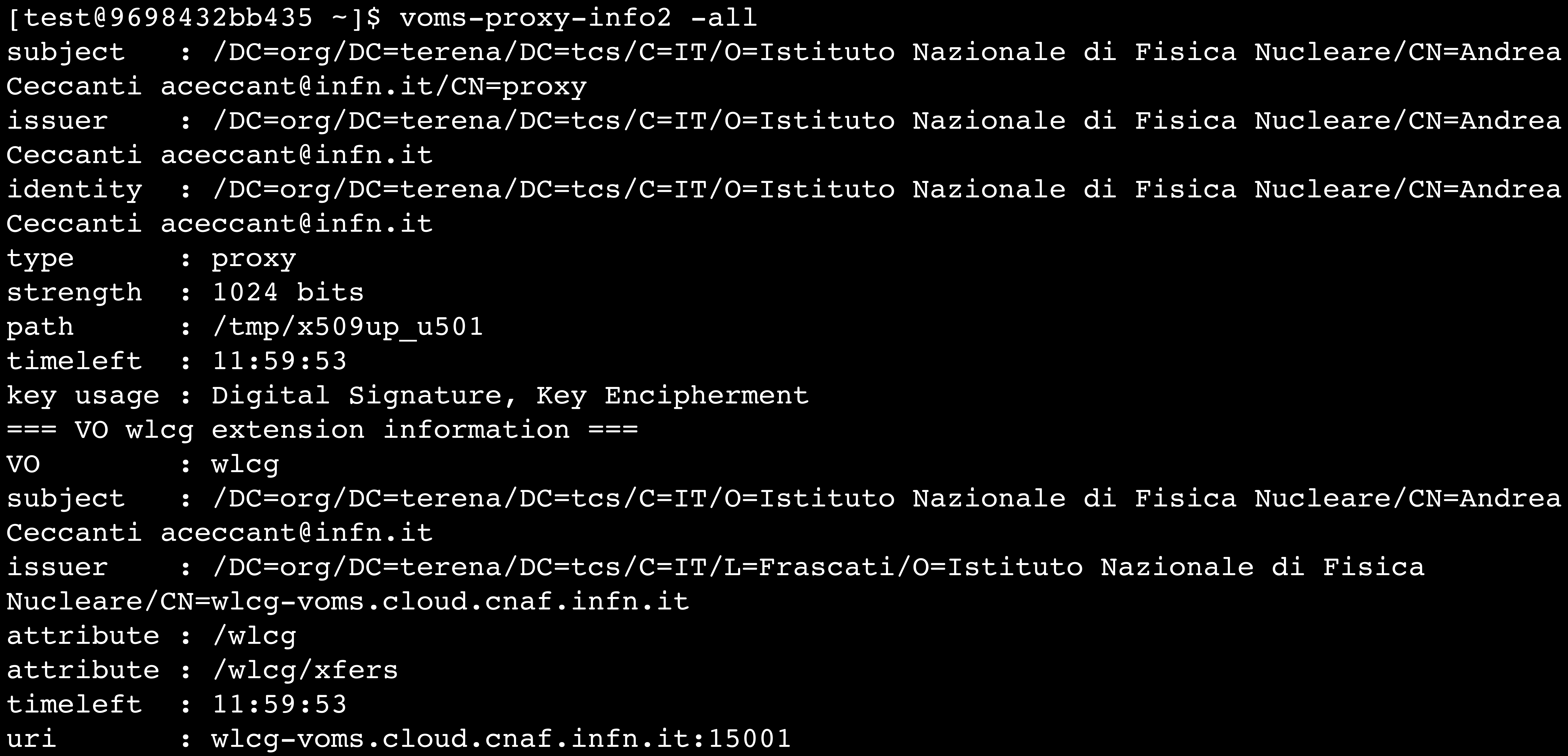
```
[test@9698432bb435 ~]$ voms-proxy-init2 -voms wlcg
Enter GRID pass phrase:
Your identity: /DC=org/DC=terena/DC=tcs/C=IT/O=Istituto Nazionale di
Fisica Nucleare/CN=Andrea Ceccanti aceccant@infn.it
Creating temporary proxy ............................ Done
Contacting  wlcg-voms.cloud.cnaf.infn.it:15001 [/DC=org/DC=terena/DC=tcs/
C=IT/L=Frascati/O=Istituto Nazionale di Fisica Nucleare/CN=voms-
wlcg.cloud.cnaf.infn.it] "wlcg" Done
Creating proxy ................................. Done

Your proxy is valid until Wed Oct 14 02:26:31 2020
```

The WLCG VO is served by the IAM VOMS implementation

```
[test@9698432bb435 ~]$ voms-proxy-init2 -voms wlcg
Enter GRID pass phrase:
Your identity: /DC=org/DC=terena/DC=tcs/C=IT/O=Istituto Nazionale di
Fisica Nucleare/CN=Andrea Ceccanti aceccant@infn.it
Creating temporary proxy ............................... Done
Contacting  wlcg-voms.cloud.cnaf.infn.it:15001 [/DC=org/DC=terena/DC=tcs/
C=IT/L=Frascati/O=Istituto Nazionale di Fisica Nucleare/CN=voms-
wlcg.cloud.cnaf.infn.it] "wlcg" Done
Creating proxy ................................... Done

Your proxy is valid until Wed Oct 14 02:26:31 2020
```



```
[test@9698432bb435 ~]$ voms-proxy-info2 -all
subject   : /DC=org/DC=terena/DC=tcs/C=IT/O=Istituto Nazionale di Fisica Nucleare/CN=Andrea
Ceccanti aceccant@infn.it/CN=proxy
issuer    : /DC=org/DC=terena/DC=tcs/C=IT/O=Istituto Nazionale di Fisica Nucleare/CN=Andrea
Ceccanti aceccant@infn.it
identity  : /DC=org/DC=terena/DC=tcs/C=IT/O=Istituto Nazionale di Fisica Nucleare/CN=Andrea
Ceccanti aceccant@infn.it
type      : proxy
strength  : 1024 bits
path      : /tmp/x509up_u501
timeleft  : 11:59:53
key usage : Digital Signature, Key Encipherment
=== VO wlcg extension information ===
VO        : wlcg
subject   : /DC=org/DC=terena/DC=tcs/C=IT/O=Istituto Nazionale di Fisica Nucleare/CN=Andrea
Ceccanti aceccant@infn.it
issuer    : /DC=org/DC=terena/DC=tcs/C=IT/L=Frascati/O=Istituto Nazionale di Fisica
Nucleare/CN=wlcg-voms.cloud.cnaf.infn.it
attribute : /wlcg
attribute : /wlcg/xfers
timeleft  : 11:59:53
uri       : wlcg-voms.cloud.cnaf.infn.it:15001
```

Thanks for your attention.

Questions?