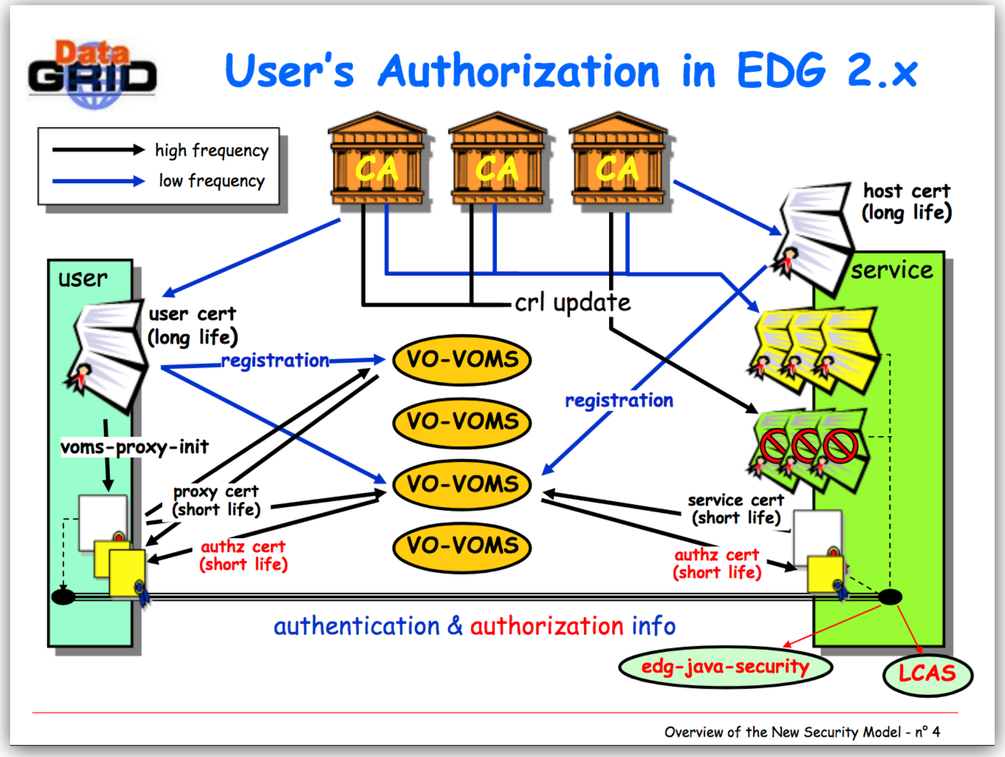
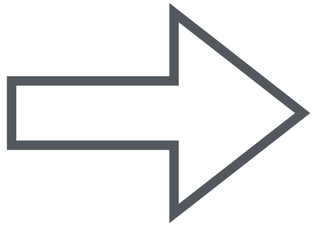
Beyond X.509: token-based authentication and authorization in practice

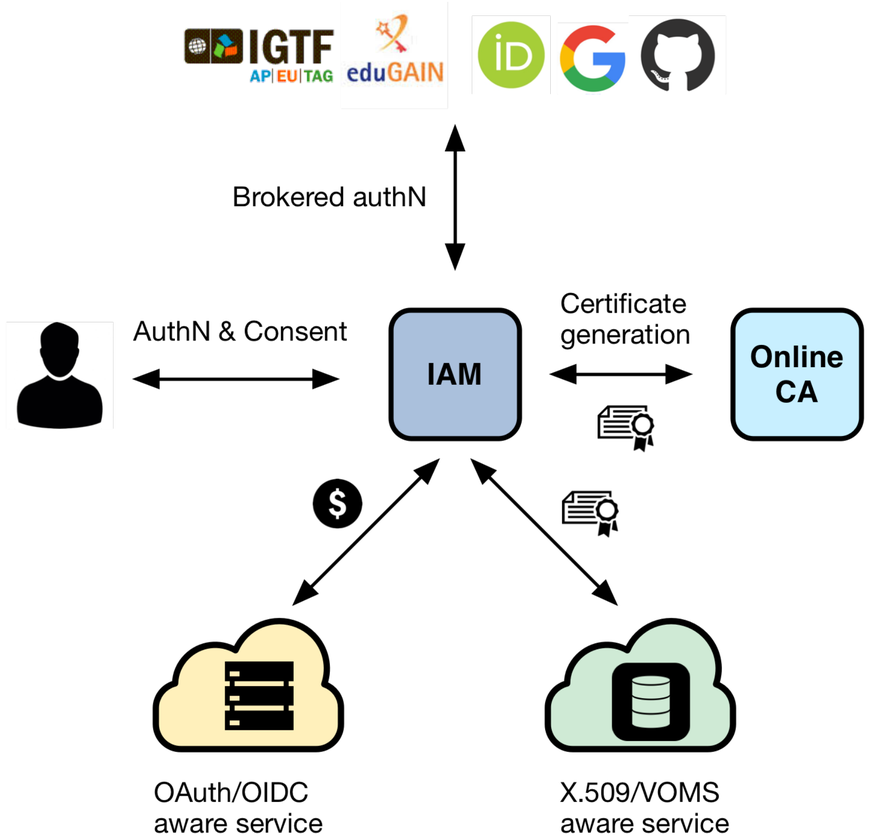
Andrea Ceccanti, Enrico Vianello, Francesco Giacomini
INFN CNAF

INFN
CNAF

Evolving the WLCG AAI beyond X.509







This is a followup for the CHEP 2018 plenary talk (and paper)

Moving beyond X.509: main challenges

Authentication

- **Flexible**, able to accomodate various authentication mechanisms
  - X.509, username & password, EduGAIN, …

Identity harmonization & account linking

- Harmonize multiple identities & credentials in a single account, providing a **persistent identifier**

Authorization

- **Orthogonal** to authentication, **attribute** or **capability-based**

Delegation

- Provide the ability for **services to act on behalf of users**
- Support for **long-running applications**

Provisioning

- Support provisioning/de-provisioning of identities to services/relying resources

Token translation

- Enable **integration with legacy services through controlled credential translation**

Moving beyond X.509: main challenges

Authentication

- **Flexible**, able to accomodate various authentication n
  - X.509, username

Identity harmon
linking

- Harmonize mult
in a single accou
identifier

Authorization

- **Orthogonal** to authentication, **attribute** or **capability-based**

Delegation

- Provide the ability for **services to act on**

g applications

-provisioning of
ing resources

- Enable **integration with legacy services through controlled credential translation**

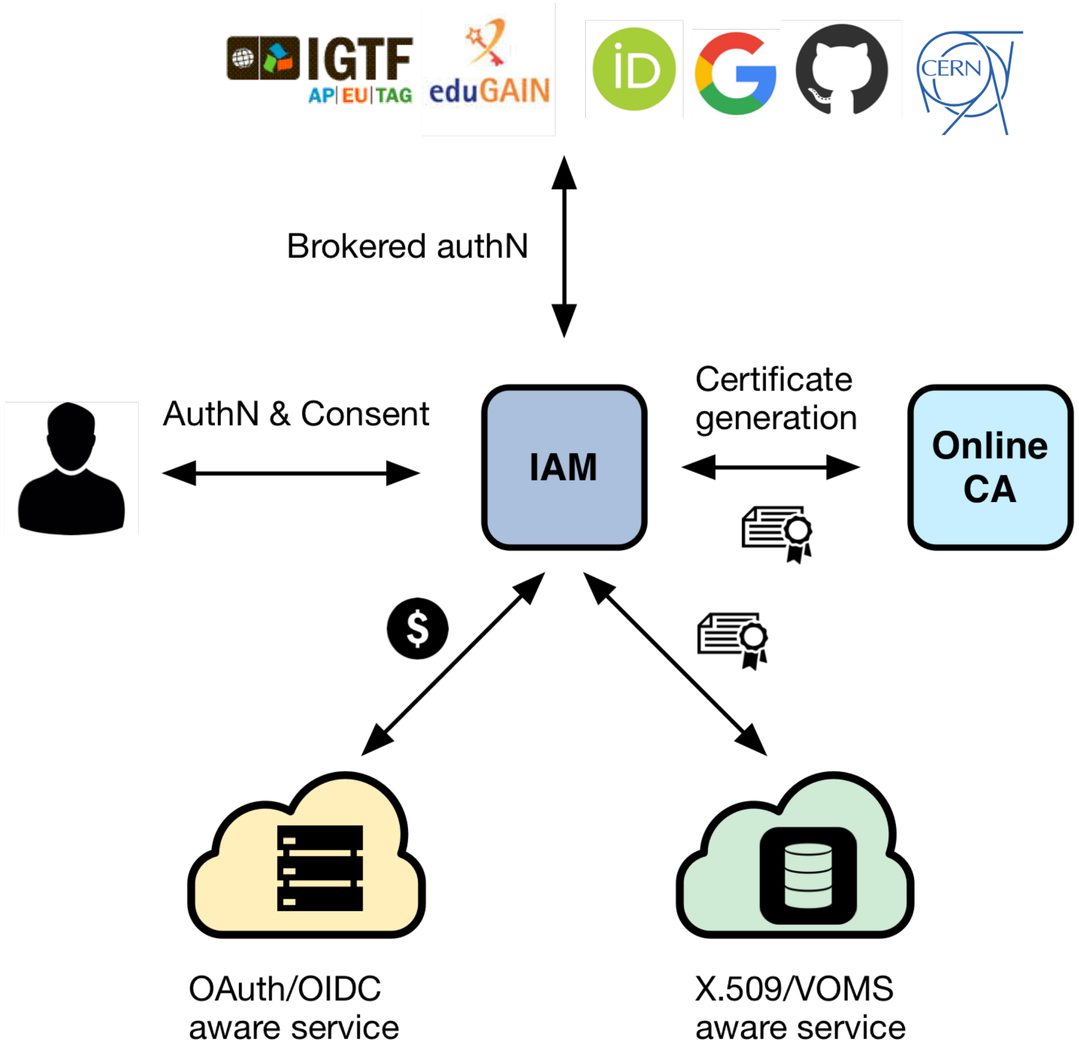
Key challenge:

allow a gradual transition to the new AAI!

INDIGO Identity and Access Management Service

A **VO-scoped** authentication and authorization service that

- supports **multiple authentication mechanisms**
- provides users with a **persistent, VO-scoped** identifier
- exposes **identity information**, **attributes** and **capabilities** to services via **JWT** tokens and standard **OAuth & OpenID Connect** protocols
- can integrate existing **VOMS**-aware services
- supports **Web** and **non-Web access**, **delegation** and **token renewal**



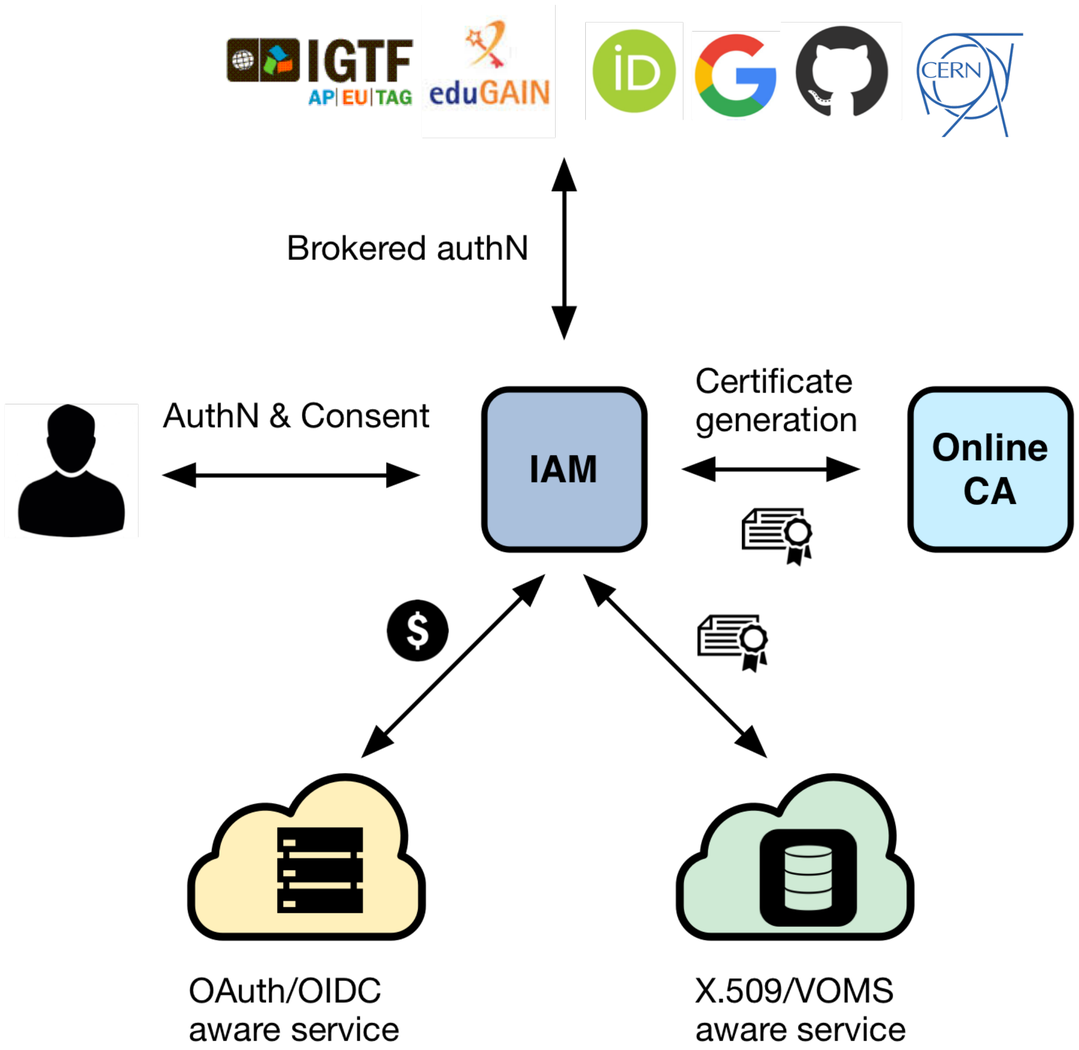
INDIGO Identity and Access Management Service

Selected by the WLCG MB to be the core of the future, token-based WLCG AAI

Sustained by INFN for the foreseeable future, with current support from:

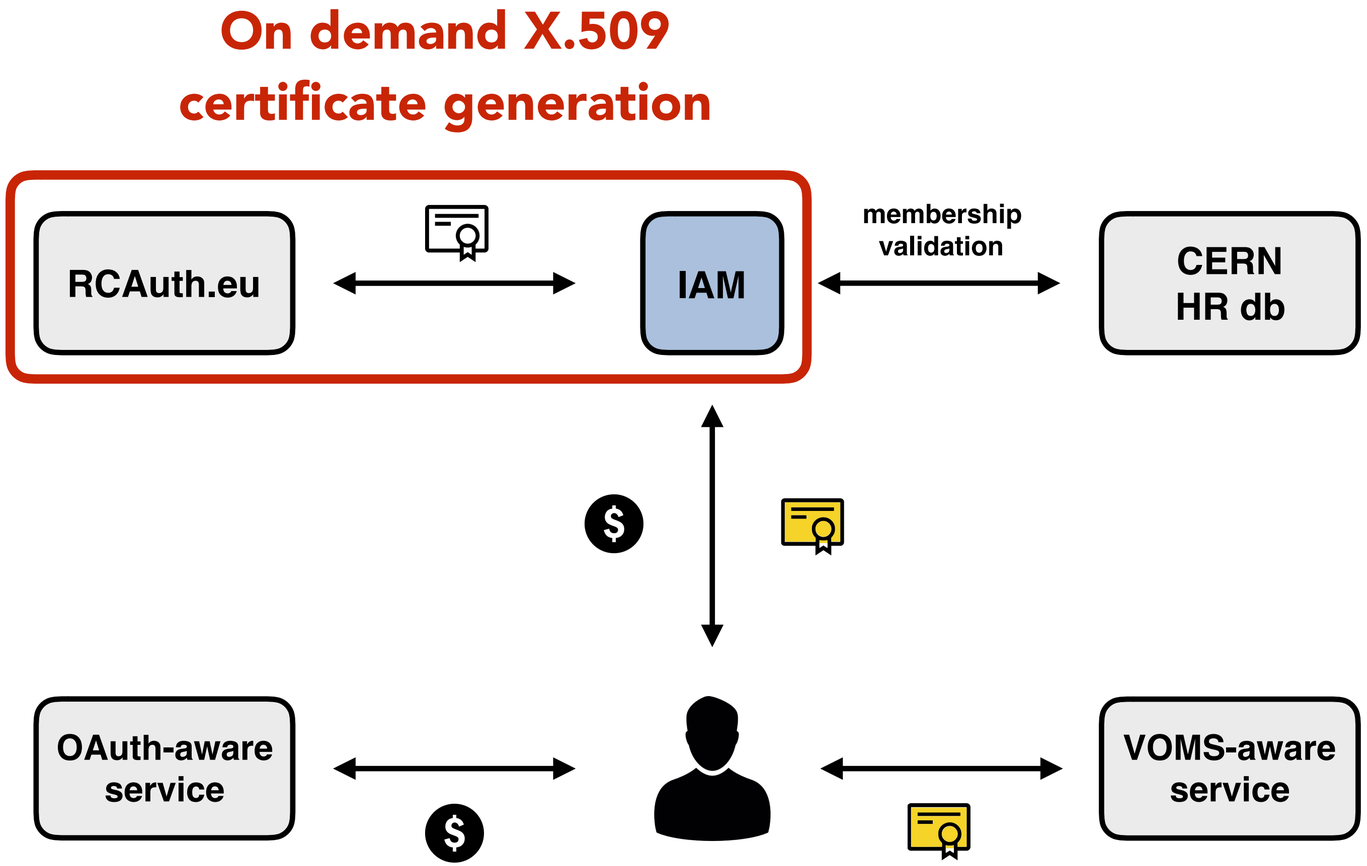
EOSC-hub

ESCAPE
European Science Cluster of Astronomy & Particle physics ESFRI research Infrastructures



IAM evolution work

Enabling a smooth transition beyond X.509

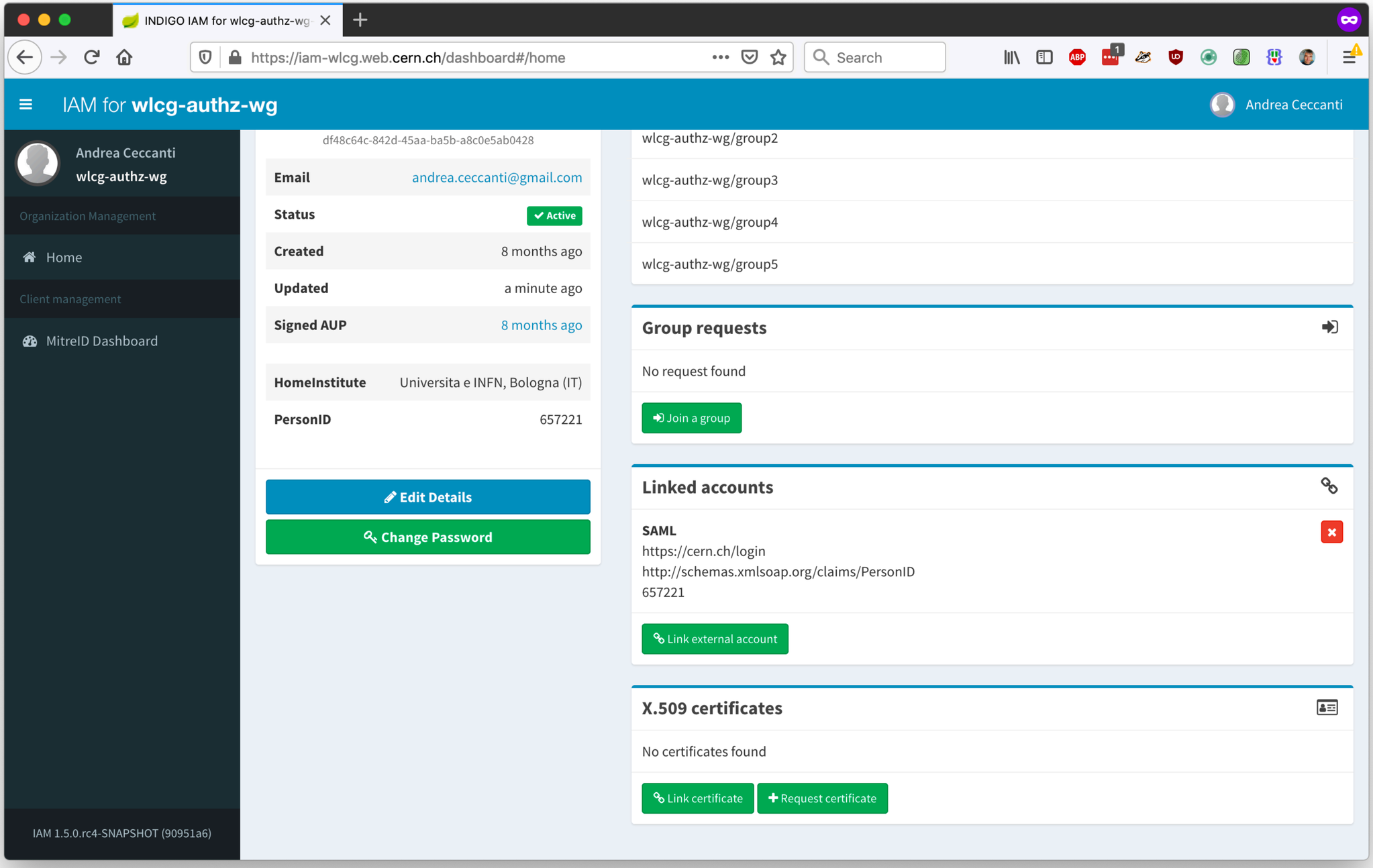


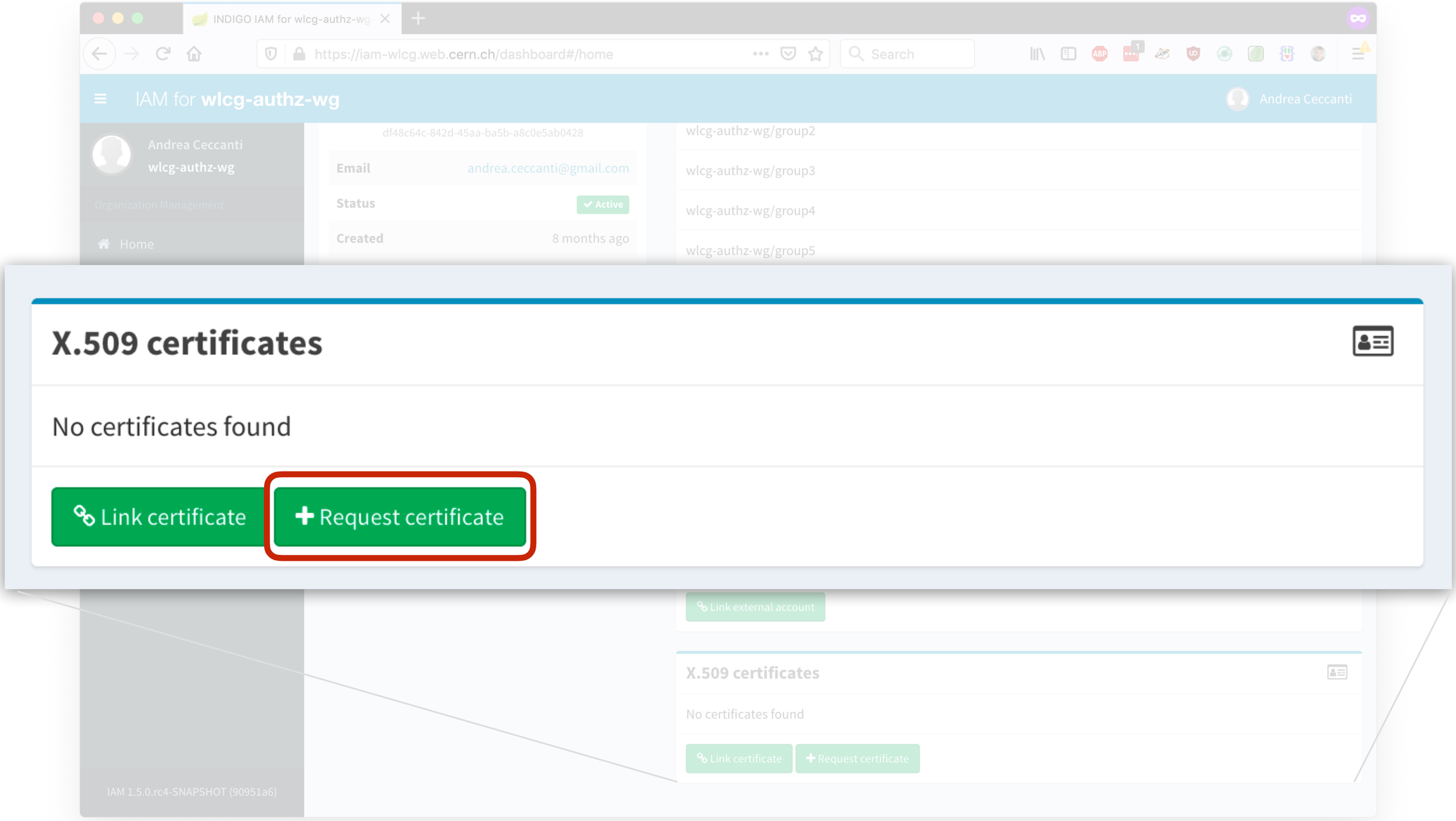
On-demand X.5O9 certificate generation

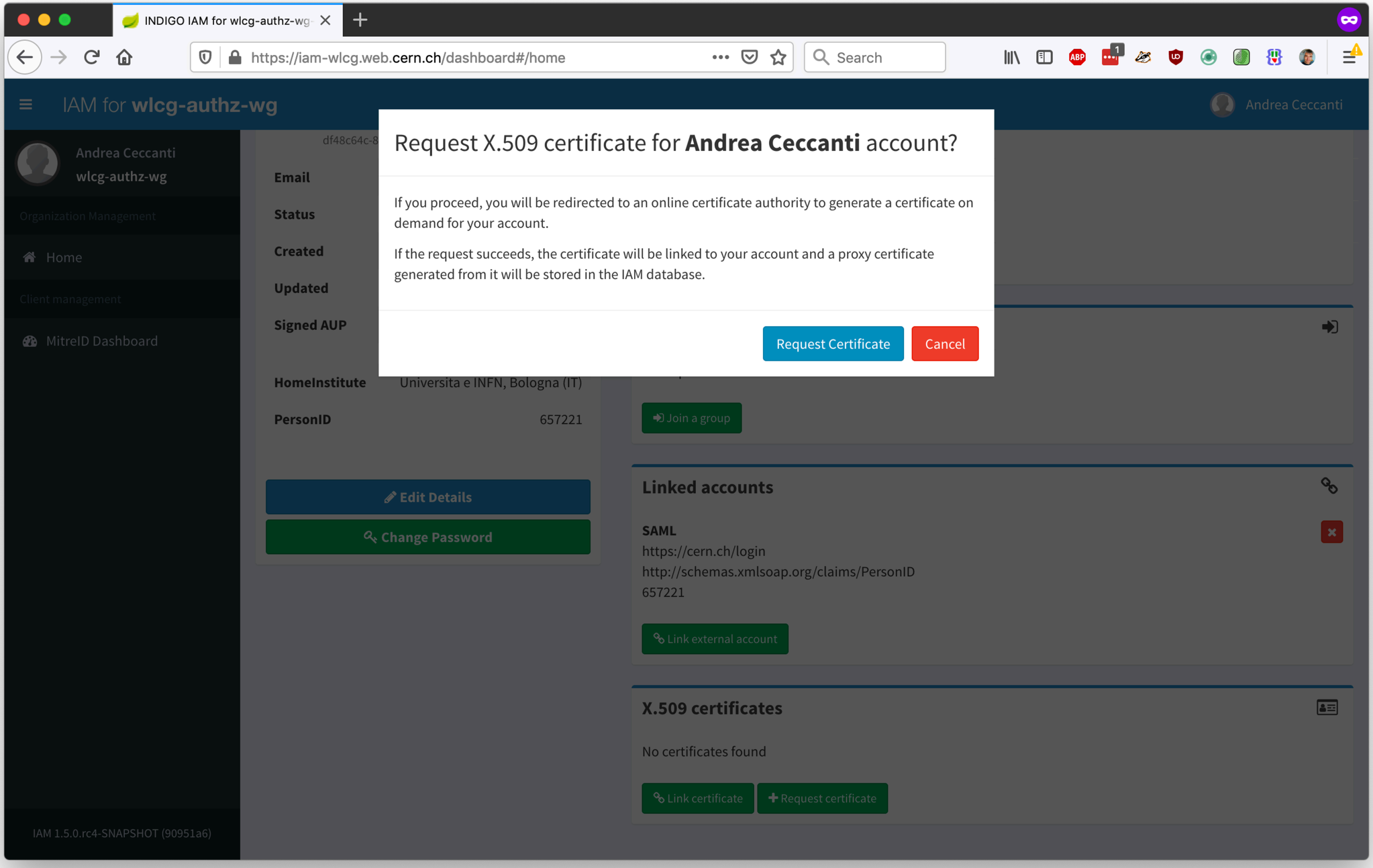
IAM integrates with the RCAuth.eu online certificate authority so that **users without an X.509 certificate can easily request one and link it to their membership**, via the IAM dashboard

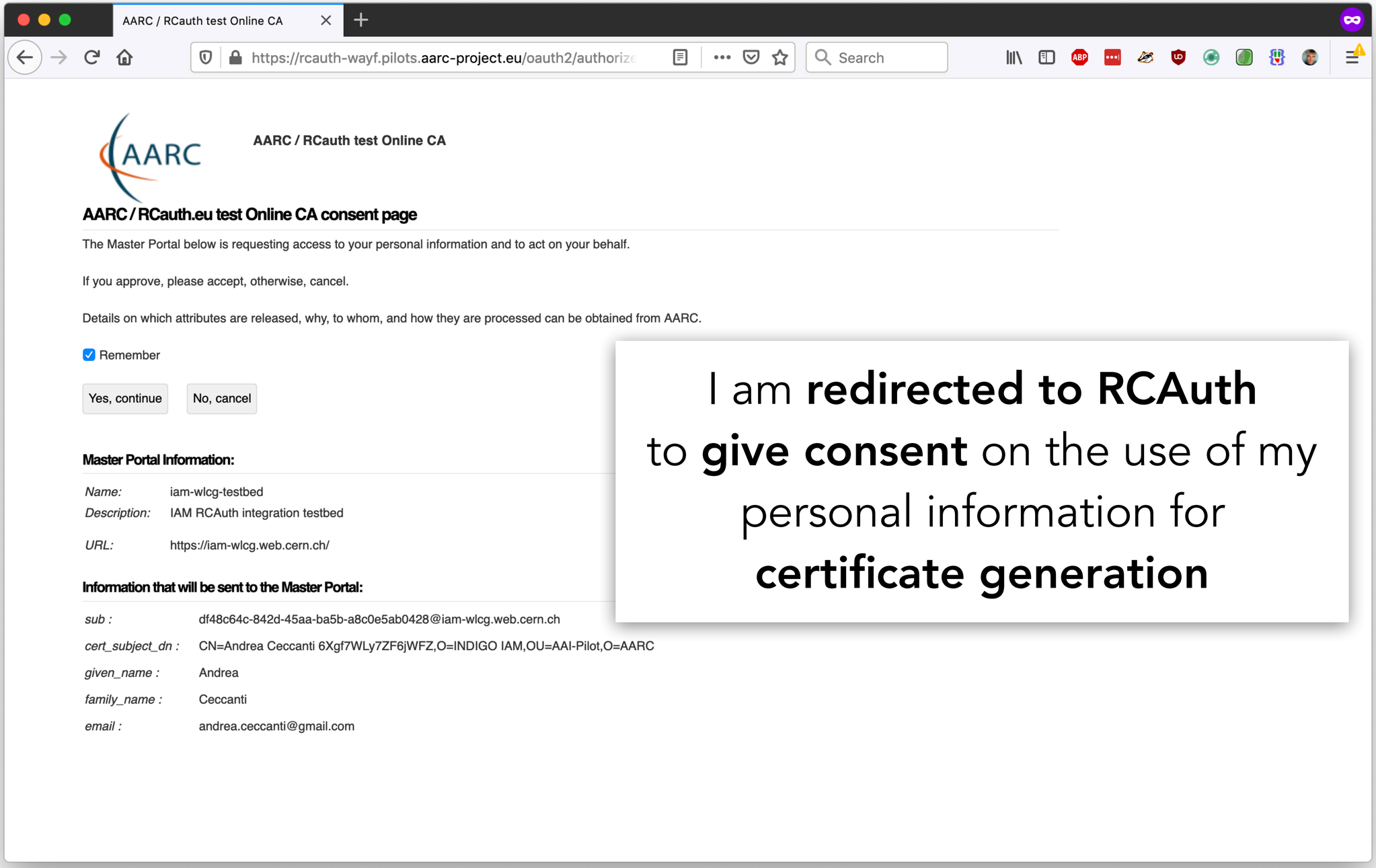
A long-lived X.509 proxy certificate is generated from the certificate obtained from RCAuth and stored in the IAM database

An **RESTful API** provides access to the certificate **to trusted clients**

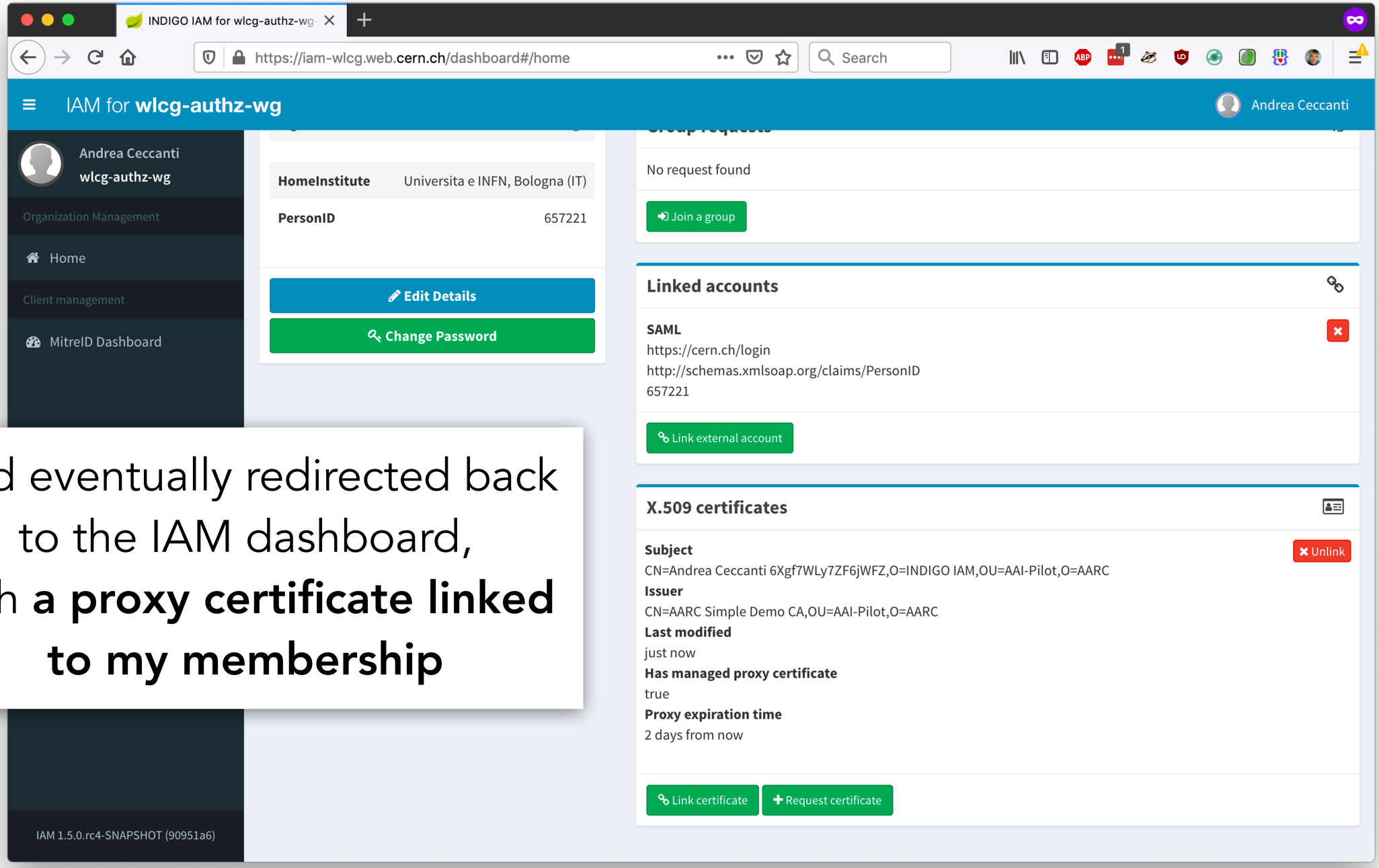

INDIGO IAM for wlcg-authz-wg
https://iam-wlcg.web.cern.ch/dashboard#/home
Search
IAM for wlcg-authz-wg
Andrea Ceccanti
Andrea Ceccanti
wlcg-authz-wg
Organization Management
Home
Client management
MitreID Dashboard
IAM 1.5.0.rc4-SNAPSHOT (90951a6)
df48c64c-842d-45aa-ba5b-a8c0e5ab0428
Email
andrea.ceccanti@gmail.com
Status
Active
Created
8 months ago
Updated
a minute ago
Signed AUP
8 months ago
HomeInstitute
Universita e INFN, Bologna (IT)
PersonID
657221
Edit Details
Change Password
wlcg-authz-wg/group2
wlcg-authz-wg/group3
wlcg-authz-wg/group4
wlcg-authz-wg/group5
Group requests
No request found
Join a group
Linked accounts
SAML
https://cern.ch/login
http://schemas.xmlsoap.org/claims/PersonID
657221
Link external account
X.509 certificates
No certificates found
Link certificate
Request certificate


INDIGO IAM for wlcg-authz-wg
https://iam-wlcg.web.cern.ch/dashboard#/home
Search
IAM for wlcg-authz-wg
Andrea Ceccanti
Andrea Ceccanti
wlcg-authz-wg
Organization Management
Home
df48c64c-842d-45aa-ba5b-a8c0e5ab0428
Email
andrea.ceccanti@gmail.com
Status
Active
Created
8 months ago
wlcg-authz-wg/group2
wlcg-authz-wg/group3
wlcg-authz-wg/group4
wlcg-authz-wg/group5
X.509 certificates
No certificates found
Link certificate
Request certificate
Link external account
X.509 certificates
No certificates found
Link certificate
Request certificate
IAM 1.5.0.rc4-SNAPSHOT (90951a6)

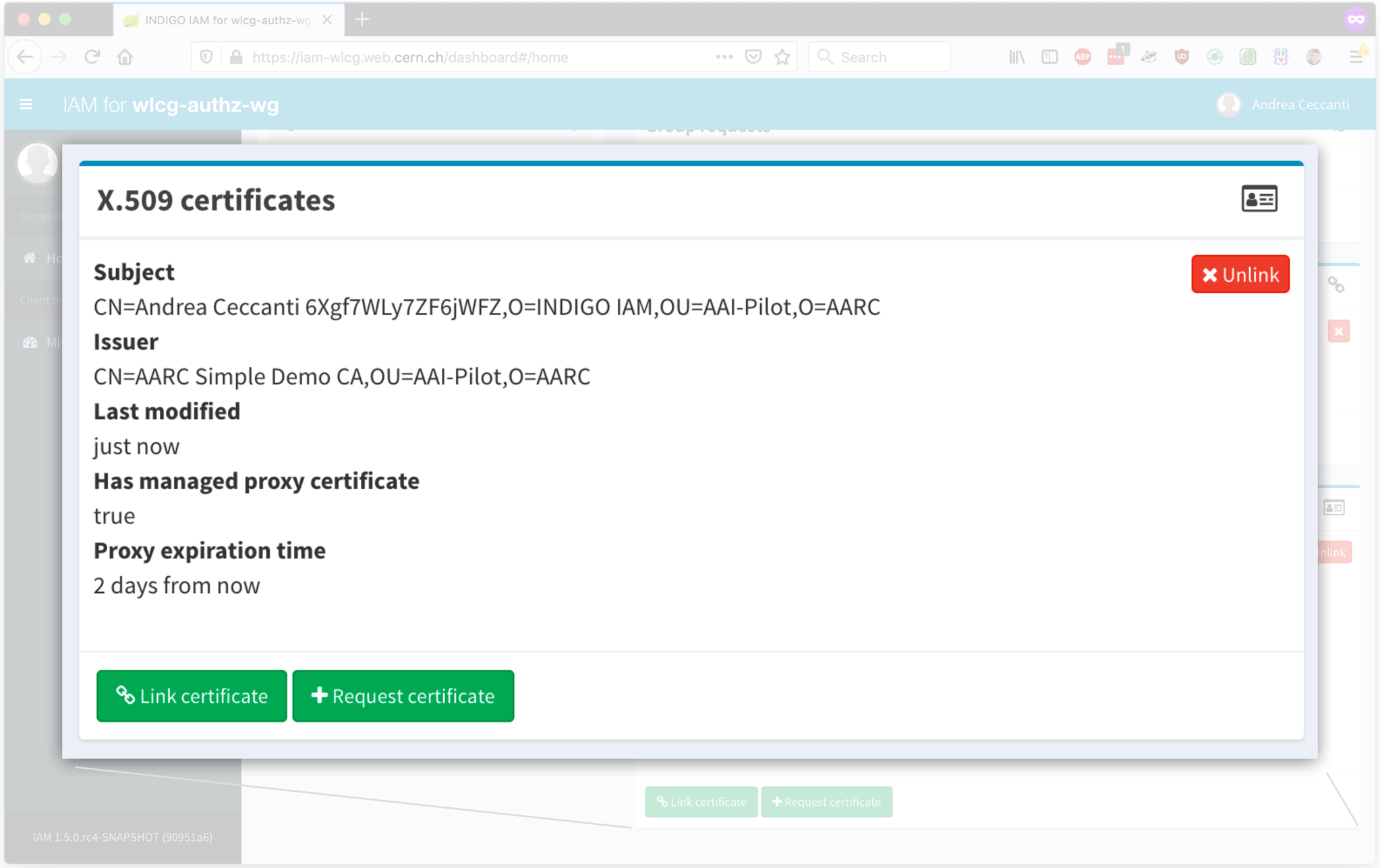

INDIGO IAM for wlcg-authz-wg
https://iam-wlcg.web.cern.ch/dashboard#/home
Search
IAM for wlcg-authz-wg
Andrea Ceccanti
Andrea Ceccanti
wlcg-authz-wg
Organization Management
Home
Client management
MitreID Dashboard
IAM 1.5.0.rc4-SNAPSHOT (90951a6)
Email
Status
Created
Updated
Signed AUP
HomeInstitute
Universita e INFN, Bologna (IT)
PersonID
657221
Edit Details
Change Password
Request X.509 certificate for Andrea Ceccanti account?
If you proceed, you will be redirected to an online certificate authority to generate a certificate on demand for your account.
If the request succeeds, the certificate will be linked to your account and a proxy certificate generated from it will be stored in the IAM database.
Request Certificate
Cancel
Join a group
Linked accounts
SAML
https://cern.ch/login
http://schemas.xmlsoap.org/claims/PersonID
657221
Link external account
X.509 certificates
No certificates found
Link certificate
Request certificate

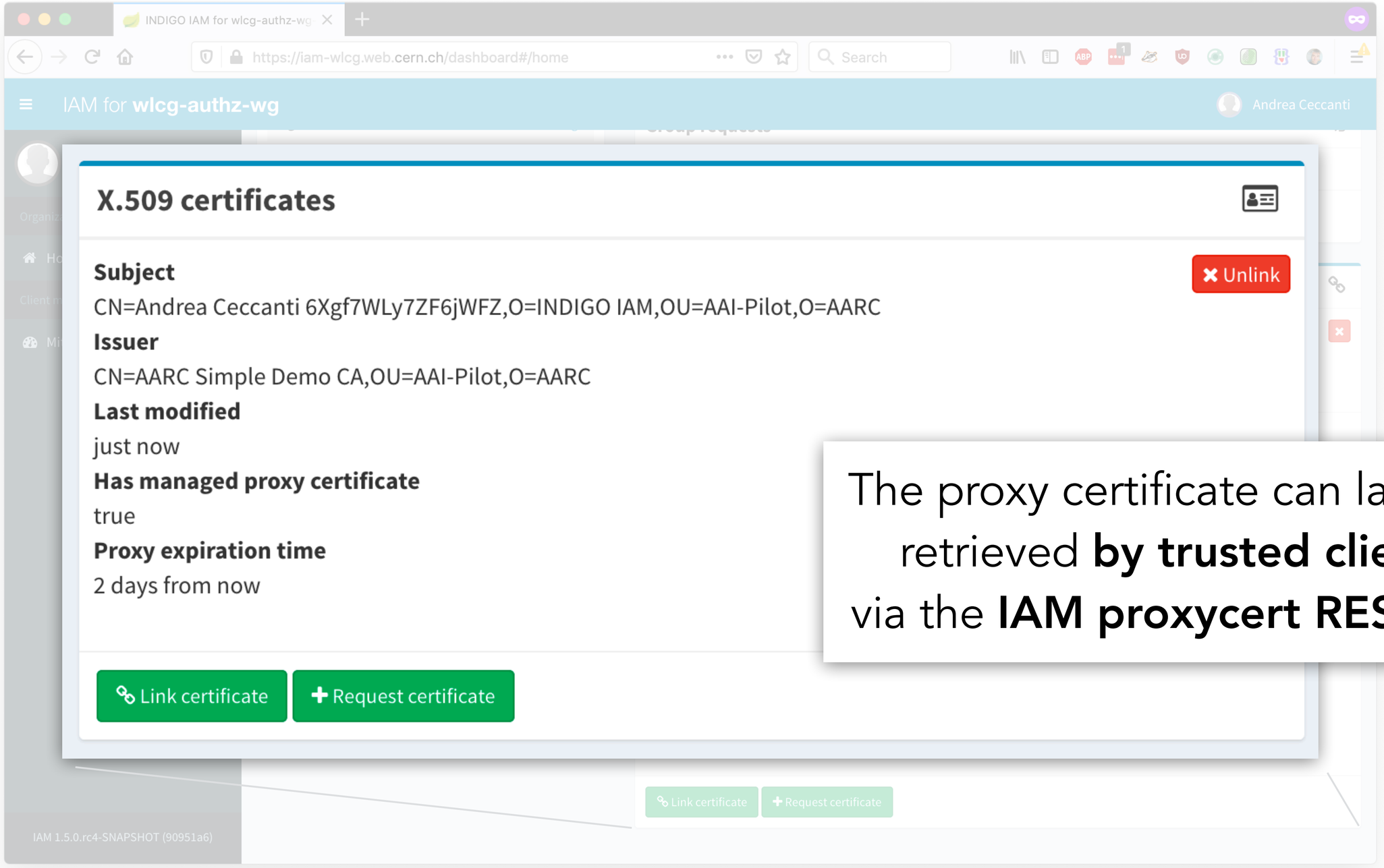


I am **redirected to RCAuth** to **give consent** on the use of my personal information for **certificate generation**



And eventually redirected back to the IAM dashboard, with **a proxy certificate linked to my membership**


INDIGO IAM for wlcg-authz-wg
https://iam-wlcg.web.cern.ch/dashboard#/home
Search
IAM for wlcg-authz-wg
Andrea Ceccanti
X.509 certificates
Subject
CN=Andrea Ceccanti 6Xgf7WLy7ZF6jWFZ,O=INDIGO IAM,OU=AAI-Pilot,O=AARC
Issuer
CN=AARC Simple Demo CA,OU=AAI-Pilot,O=AARC
Last modified
just now
Has managed proxy certificate
true
Proxy expiration time
2 days from now
Unlink
Link certificate
Request certificate
IAM 1.5.0.rc4-SNAPSHOT (90951a6)



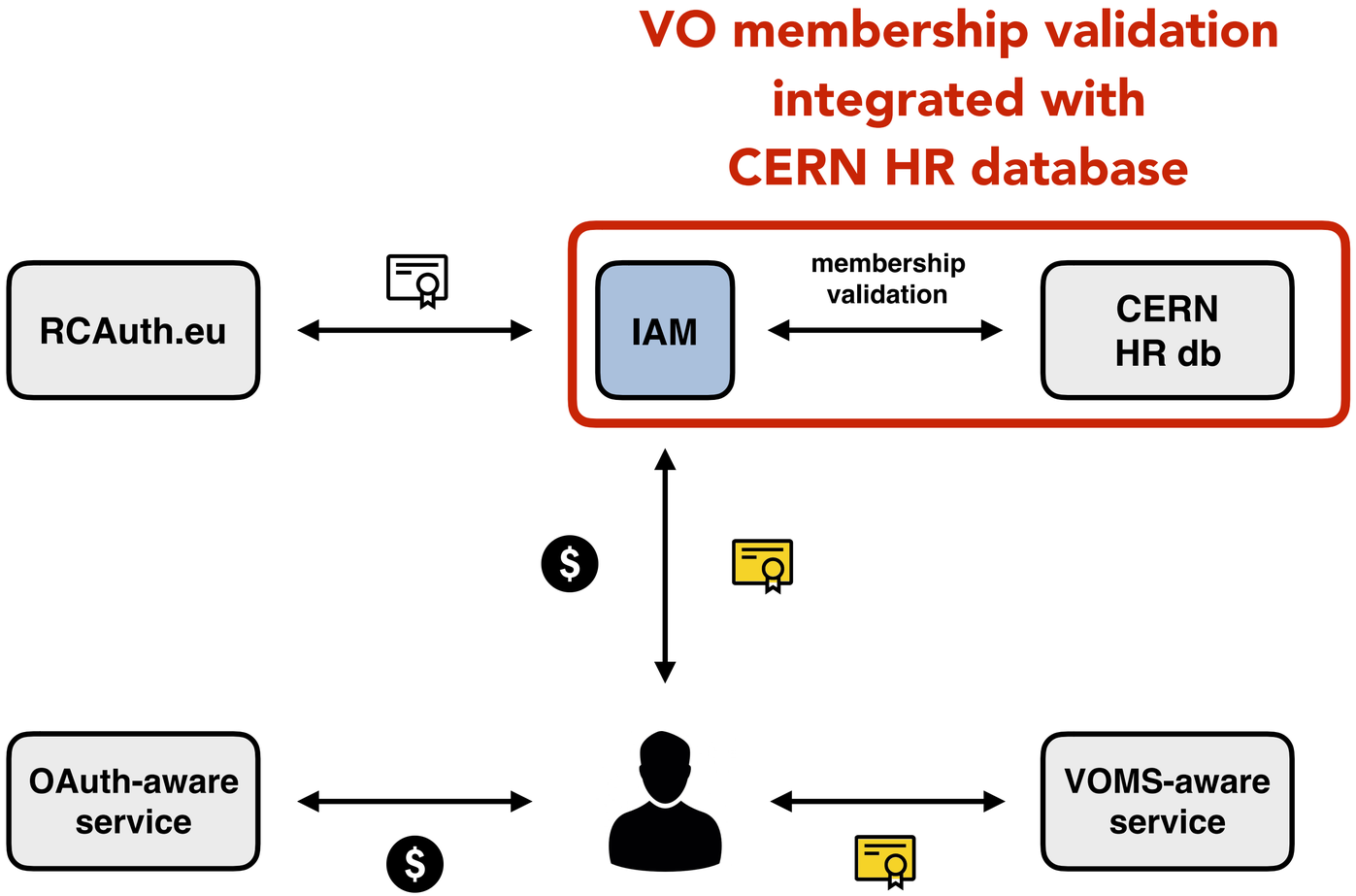
The proxy certificate can later be retrieved **by trusted clients** via the **IAM proxycert REST API**

```
06/11, 10:07 AM   ~   ssh ◂ bash   5%   12 GB
echo "Requesting proxy certificate from IAM..."
proxyresponse=$(mktemp)
chmod 600 ${proxyresponse}
curl -s -XPOST -H "Authorization: Bearer ${access_token}" \
      -d client_id=${IAM_DEVICE_CODE_CLIENT_ID} \
      -d client_secret=${IAM_DEVICE_CODE_CLIENT_SECRET} \
      ${IAM_PROXYCERT_ENDPOINT} > ${proxyresponse}

if [ $? -ne 0 ]; then
  echo "Error requesting proxy certificate"
  cat ${response}
  exit 1
fi

identity=$(jq -r .identity ${proxyresponse})
proxy_file=${X509_USER_PROXY:-$(echo /tmp/x509up_u$(id -u))}
touch ${proxy_file}
chmod 600 ${proxy_file}

jq -r .certificate_chain ${proxyresponse} > ${proxy_file}

echo
echo "A proxy certificate for identity:"
echo
echo ${identity}
echo
echo "has been saved to:"
echo
echo ${proxy_file}

rm -f ${response}
rm -f ${proxyresponse}
```

This is an excerpt from a script that calls **the** IAM proxycert API and saves the proxy in the usual location

See this in action in WLCG AuthZ WG demo (IAM starts at minute 46)

Enabling a smooth transition beyond X.509



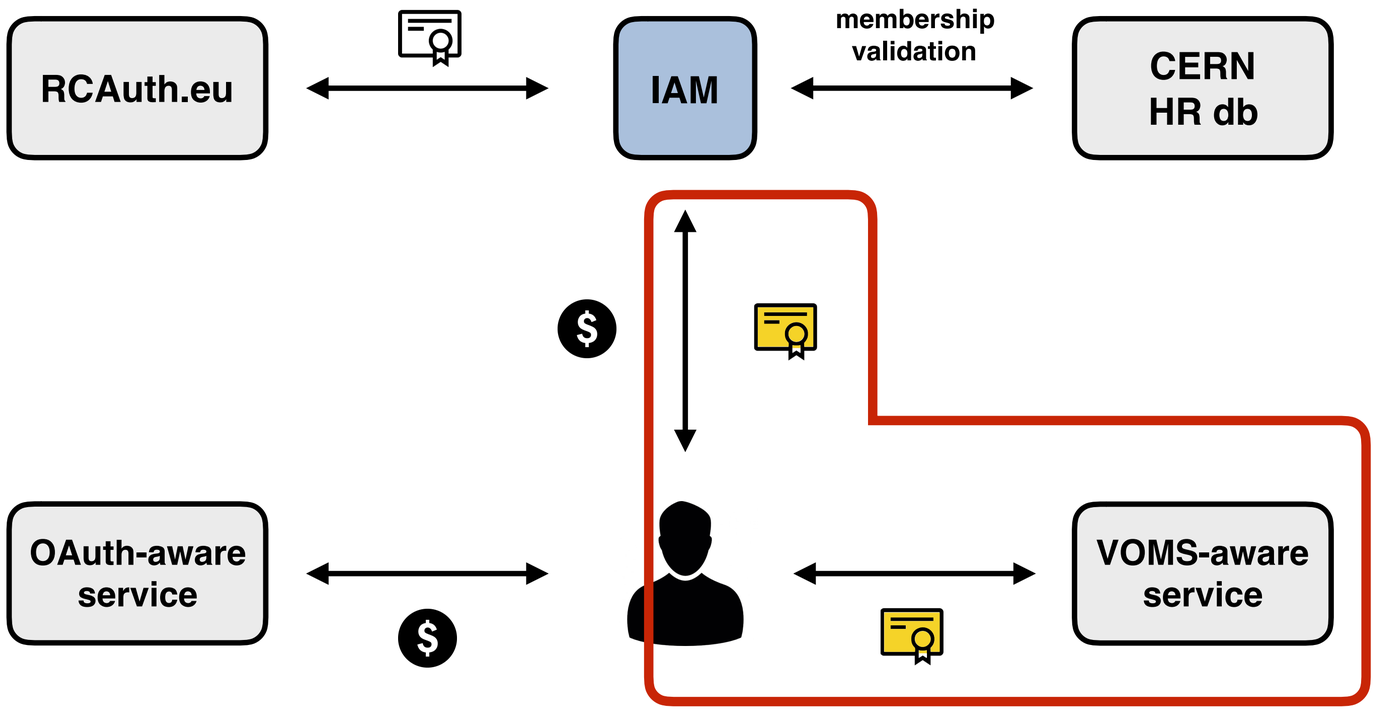
CERN HR db membership validation

The CERN HR db integration code extracted from the VOMS Admin codebase and **refactored as a standalone micro-service**, exposing a REST API

A test instance has been deployed @ CERN and used for integration activities in the WLCG AuthZ WG

The service will be deployed in production @ CERN in 2020 to support the current VOMS Admin deployment and the future IAM integration

Enabling a smooth transition beyond X.509



VOMS provisioning compatible with existing clients

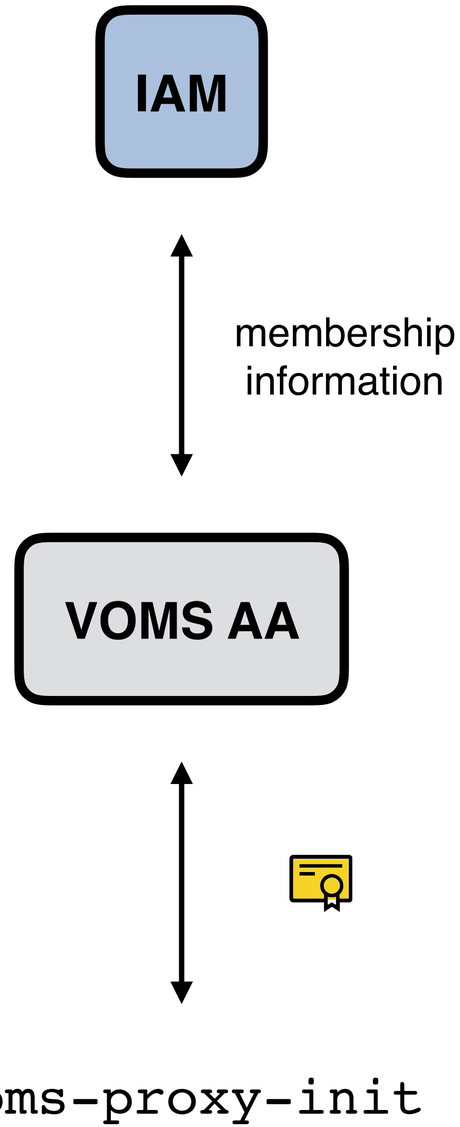
X.509 certificate

VOMS credential

JWT access token

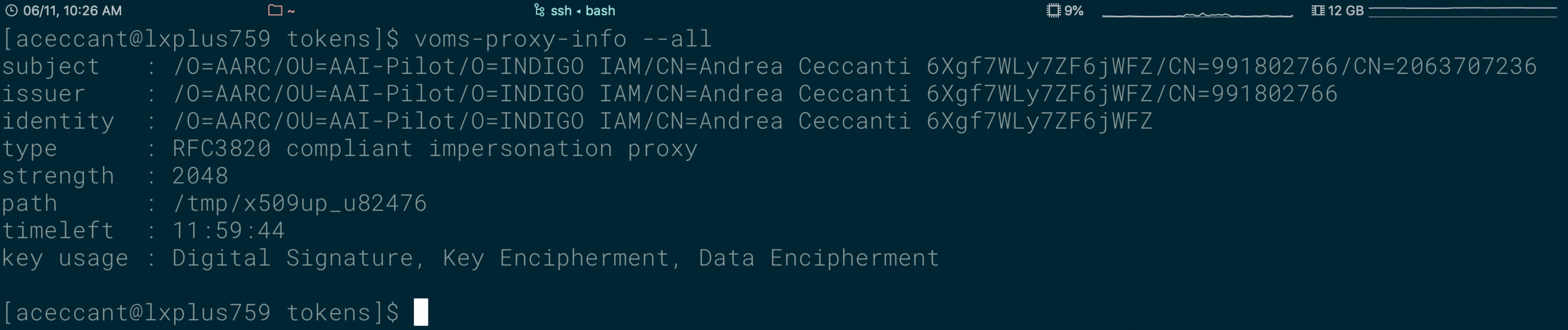
VOMS provisioning

A VOMS attribute authority micro-service gets information about user identity from IAM and generates a **standard VOMS Attribute Certificate**

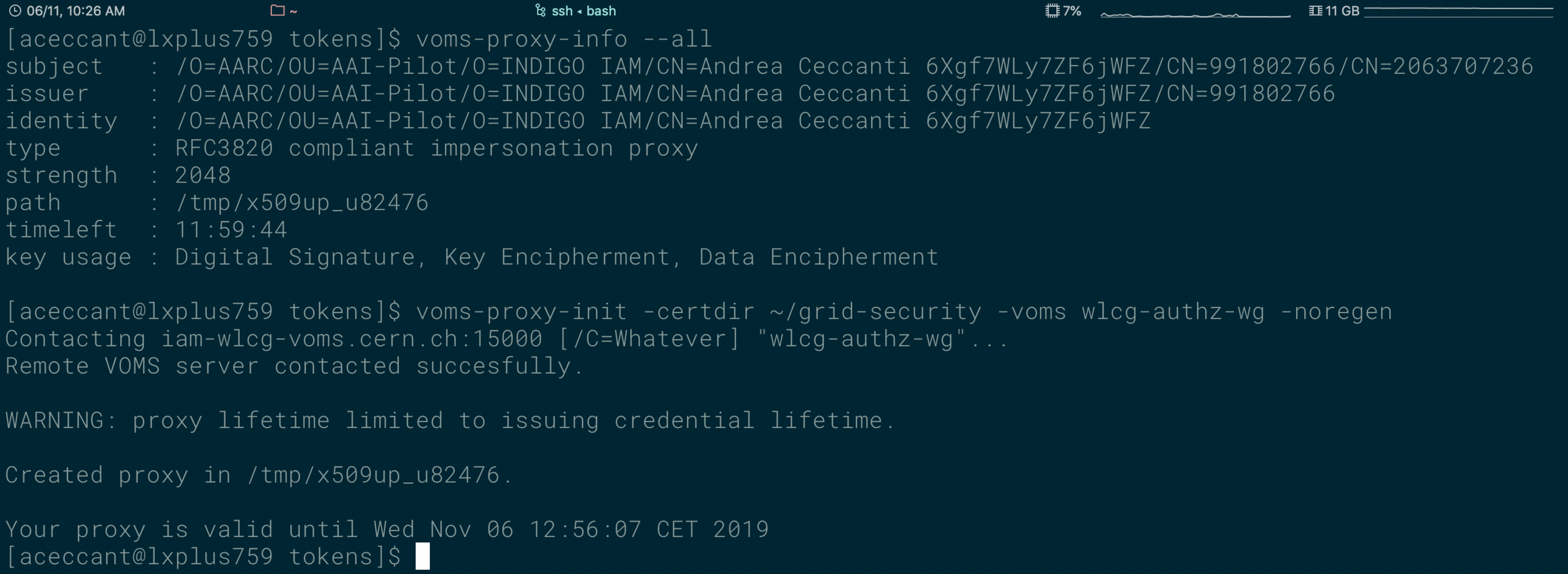


Proven compatibility with existing latest supported clients and Grid services

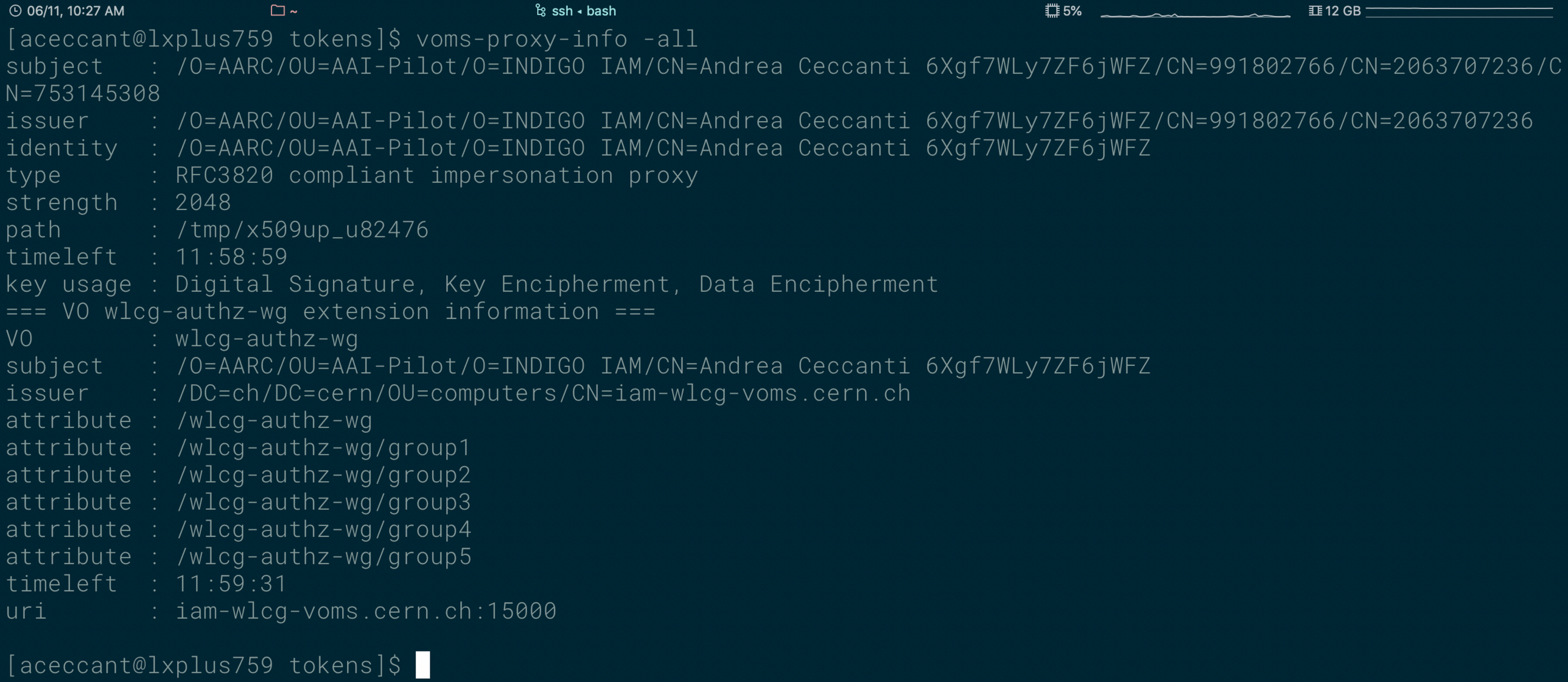
- e.g., data transfers in the ESCAPE data lake testbed rely on this



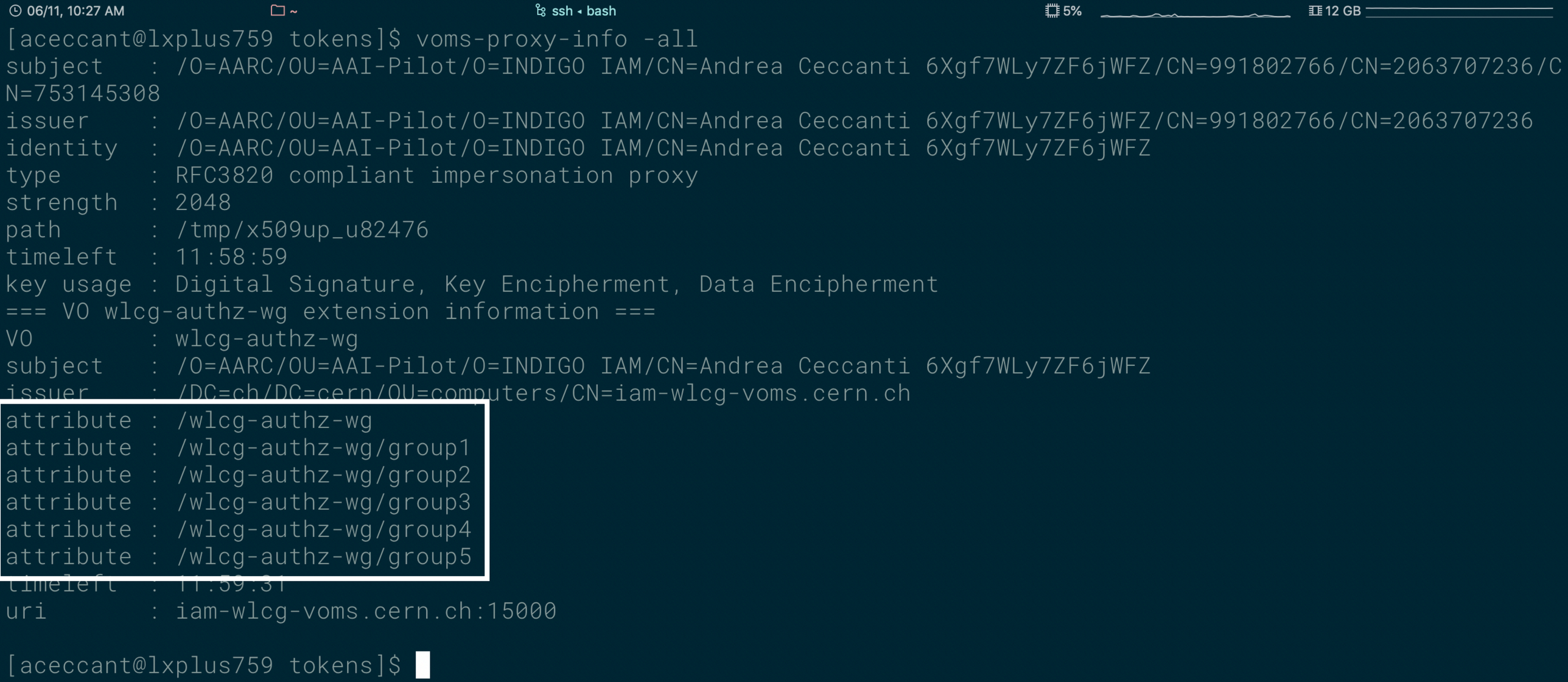
This is the output of voms-proxy-info when run on the proxy certificate obtained from the IAM proxy API



Then I run voms-proxy-init against the IAM VOMS attribute authority



This is the output of voms-proxy-init on the generated voms proxy



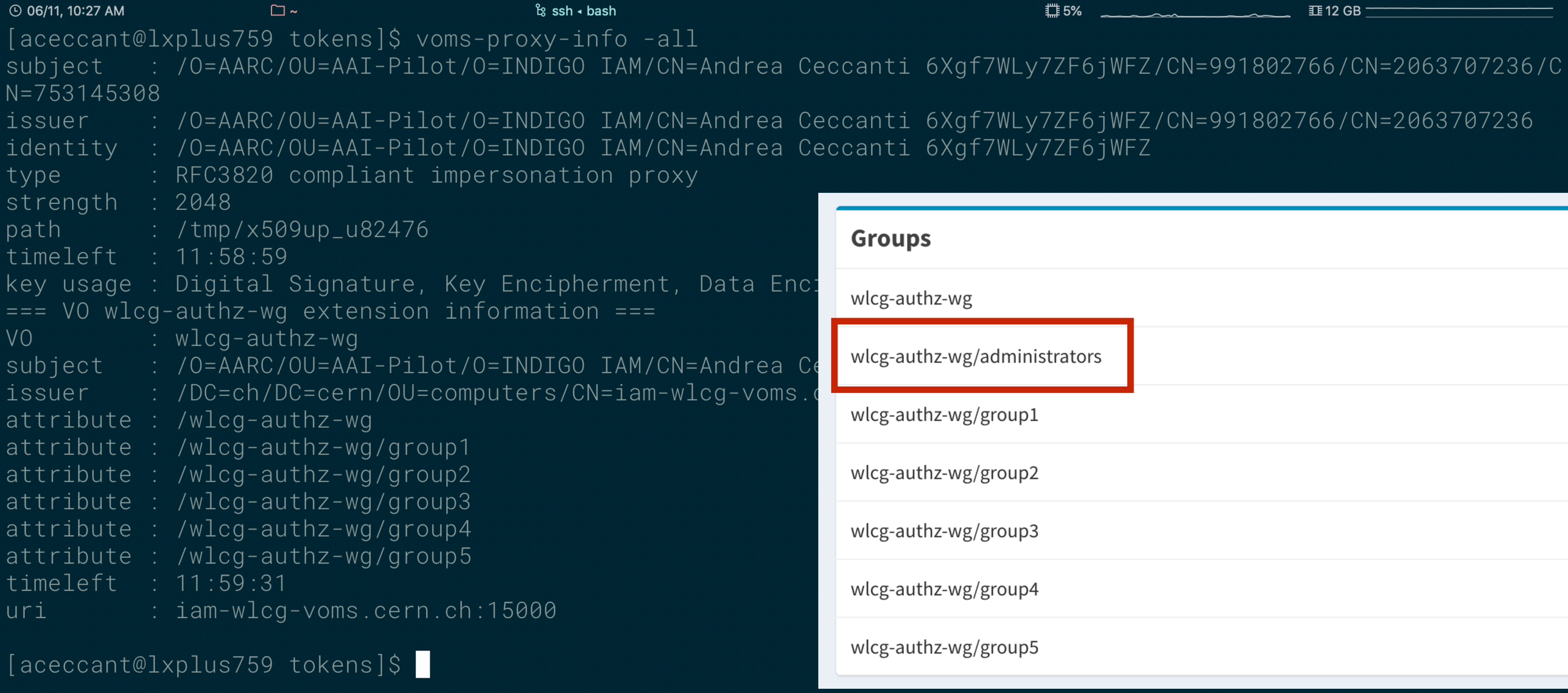
IAM group membership is reflected in the VOMS attribute certificate

```
06/11, 10:27 AM   ~   ssh ◂ bash   5%   12 GB
[aceccant@lxplus759 tokens]$ voms-proxy-info -all
subject   : /O=AARC/OU=AAI-Pilot/O=INDIGO IAM/CN=Andrea Ceccanti 6Xgf7WLy7ZF6jWFZ/CN=991802766/CN=2063707236/C
N=753145308
issuer    : /O=AARC/OU=AAI-Pilot/O=INDIGO IAM/CN=Andrea Ceccanti 6Xgf7WLy7ZF6jWFZ/CN=991802766/CN=2063707236
identity  : /O=AARC/OU=AAI-Pilot/O=INDIGO IAM/CN=Andrea Ceccanti 6Xgf7WLy7ZF6jWFZ
type      : RFC3820 compliant impersonation proxy
strength  : 2048
path      : /tmp/x509up_u82476
timeleft  : 11:58:59
key usage : Digital Signature, Key Encipherment, Data Enci
=== VO wlcg-authz-wg extension information ===
VO        : wlcg-authz-wg
subject   : /O=AARC/OU=AAI-Pilot/O=INDIGO IAM/CN=Andrea Ce
issuer    : /DC=ch/DC=cern/OU=computers/CN=iam-wlcg-voms.c
attribute : /wlcg-authz-wg
attribute : /wlcg-authz-wg/group1
attribute : /wlcg-authz-wg/group2
attribute : /wlcg-authz-wg/group3
attribute : /wlcg-authz-wg/group4
attribute : /wlcg-authz-wg/group5
timeleft  : 11:59:31
uri       : iam-wlcg-voms.cern.ch:15000

[aceccant@lxplus759 tokens]$
```

Groups

- wlcg-authz-wg
- wlcg-authz-wg/administrators
- wlcg-authz-wg/group1
- wlcg-authz-wg/group2
- wlcg-authz-wg/group3
- wlcg-authz-wg/group4
- wlcg-authz-wg/group5

Actually looking more closely there's a difference…



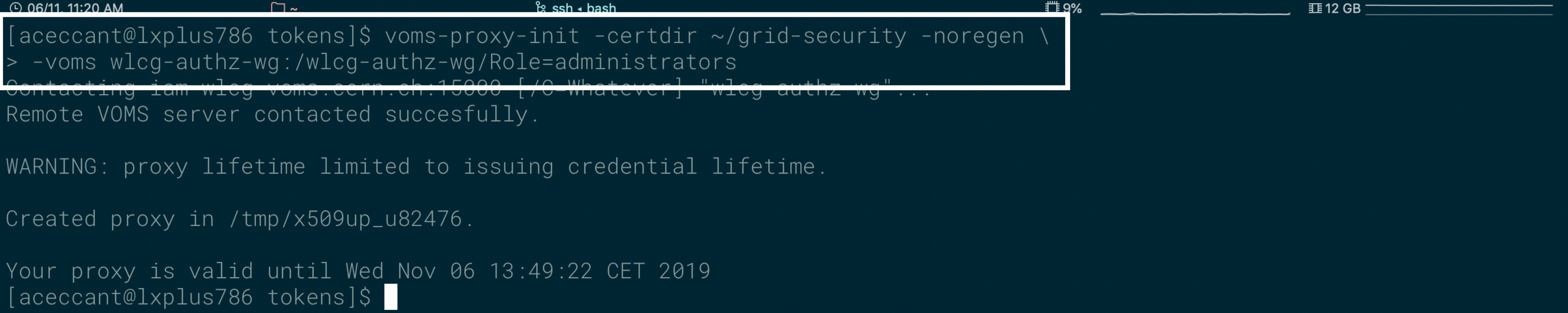
The wlcg-authz-wg/administrators group is missing since it's configured to be an optional group

```
06/11, 10:27 AM   ~   ssh ◂ bash   5%   12 GB
[aceccant@lxplus759 tokens]$ voms-proxy-info -all
subject   : /O=AARC/OU=AAI-Pilot/O=INDIGO IAM/CN=Andrea Ceccanti 6Xgf7WLy7ZF6jWFZ/CN=991802766/CN=2063707236/C
N=753145308
issuer    : /O=AARC/OU=AAI-Pilot/O=INDIGO IAM/CN=Andrea Ceccanti 6Xgf7WLy7ZF6jWFZ/CN=991802766/CN=2063707236
identity  : /O=AARC/OU=AAI-Pilot/O=INDIGO IAM/CN=Andrea Ceccanti 6Xgf7WLy7ZF6jWFZ
type      : RFC3820 compliant impersonation proxy
strength  : 2048
path      : /tmp/x509up_u82476
timeleft  : 11:58:59
key usage : Digital Signature, Key Encipherment, Data Enci
=== VO wlcg-authz-wg extension information ===
VO        : wlcg-authz-wg
subject   : /O=AARC/OU=AAI-Pilot/O=INDIGO IAM/CN=Andrea Ce
issuer    : /DC=ch/DC=cern/OU=computers/CN=iam-wlcg-voms.c
attribute : /wlcg-authz-wg
attribute : /wlcg-authz-wg/group1
attribute : /wlcg-authz-wg/group2
attribute : /wlcg-authz-wg/group3
attribute : /wlcg-authz-wg/group4
attribute : /wlcg-authz-wg/group5
timeleft  : 11:59:31
uri       : iam-wlcg-voms.cern.ch:15000

[aceccant@lxplus759 tokens]$
```

Groups

- wlcg-authz-wg
- wlcg-authz-wg/administrators
- wlcg-authz-wg/group1
- wlcg-authz-wg/group2
- wlcg-authz-wg/group3
- wlcg-authz-wg/group4
- wlcg-authz-wg/group5

In VOMS, we would call that a **role**



So I do a “traditional” VOMS role request

```
WARNING: proxy lifetime limited to issuing credential lifetime.

Created proxy in /tmp/x509up_u82476.

Your proxy is valid until Wed Nov 06 13:49:22 CET 2019
[aceccant@lxplus786 tokens]$ voms-proxy-info -all
subject   : /O=AARC/OU=AAI-Pilot/O=INDIGO IAM/CN=Andrea Ceccanti 6Xgf7WLy7ZF6jWFZ/CN=991802766/CN=768203330/CN=
7
issuer    : /O=AARC/OU=AAI-Pilot/O=INDIGO IAM/CN=Andrea Ceccanti 6Xgf7WLy7ZF6jWFZ/CN=991802766/CN=768203330
identity  : /O=AARC/OU=AAI-Pilot/O=INDIGO IAM/CN=Andrea Ceccanti 6Xgf7WLy7ZF6jWFZ
type      : RFC3820 compliant impersonation proxy
strength  : 2048
path      : /tmp/x509up_u82476
timeleft  : 11:58:34
key usage : Digital Signature, Key Encipherment, Data Encipherment
=== VO wlcg-authz-wg extension information ===
VO        : wlcg-authz-wg
subject   : /O=AARC/OU=AAI-Pilot/O=INDIGO IAM/CN=Andrea Ceccanti 6Xgf7WLy7ZF6jWFZ
issuer    : /DC=ch/DC=cern/OU=computers/CN=iam-wlcg-voms.cern.ch
attribute : /wlcg-authz-wg/Role=administrators
attribute : /wlcg-authz-wg
attribute : /wlcg-authz-wg/group1
attribute : /wlcg-authz-wg/group2
attribute : /wlcg-authz-wg/group3
attribute : /wlcg-authz-wg/group4
attribute : /wlcg-authz-wg/group5
timeleft  : 11:59:42
uri       : iam-wlcg-voms.cern.ch:15000

[aceccant@lxplus786 tokens]$
```

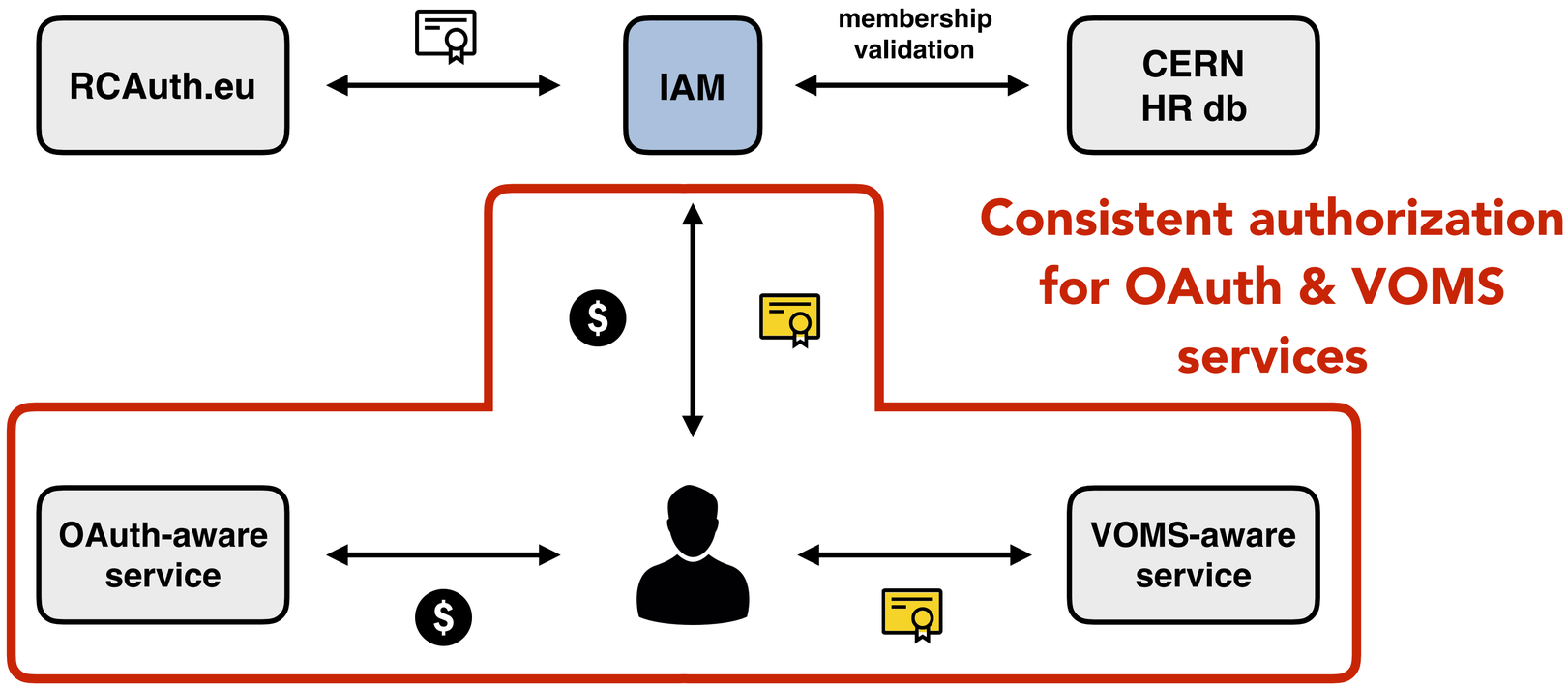
And in the end I get the *administrators* role as VOMS primary attribute

```
WARNING: proxy lifetime limited to issuing credential lifetime.

Created proxy in /tmp/x509up_u82476.

Your proxy is valid until Wed Nov 06 13:49:22 CET 2019
[aceccant@lxplus786 tokens]$ voms-proxy-info -all
subject   : /O=AARC/OU=AAI-Pilot/O=INDIGO IAM/CN=Andrea Ceccanti 6Xgf7WLy7ZF6jWFZ/CN=991802766/CN=768203330/CN=
7
issuer    : /O=AARC/OU=AAI-Pilot/O=INDIGO IAM/CN=Andrea Ceccanti 6Xgf7WLy7ZF6jWFZ/CN=991802766/CN=768203330
identity  : /O=AARC/OU=AAI-Pilot/O=INDIGO IAM/CN=Andrea Ceccanti 6Xgf7WLy7ZF6jWFZ
type      : RFC3820 compliant impersonation proxy
strength  : 2048
path      : /tmp/x509up_u82476
timeleft  : 11:58:34
key usage : Digital Signature, Key Encipherment, Data Encipherment
=== VO wlcg-authz-wg extension information ===
VO        : wlcg-authz-wg
subject   : /O=AARC/OU=AAI-Pilot/O=INDIGO IAM/CN=Andrea Ceccanti 6Xgf7WLy7ZF6jWFZ
issuer    : /DC=ch/DC=cern/OU=computers/CN=iam-wlcg-voms.cern.ch
attribute : /wlcg-authz-wg/Role=administrators
attribute : /wlcg-authz-wg
attribute : /wlcg-authz-wg/group1
attribute : /wlcg-authz-wg/group2
attribute : /wlcg-authz-wg/group3
attribute : /wlcg-authz-wg/group4
attribute : /wlcg-authz-wg/group5
timeleft  : 11:59:42
uri       : iam-wlcg-voms.cern.ch:15000

[aceccant@lxplus786 tokens]$
```

See this in action in WLCG AuthZ WG demo (IAM starts at minute 46)

And in the end I get the *administrators* role as VOMS primary attribute

Enabling a smooth transition beyond X.509



WLCG JWT profile implementation

WLCG JWT profile has reached v1.0

IAM **implements it today** in the latest development branch

Example WLCG JWT access token:


```
{
  "wlcg.ver": "1.0",
  "sub": "a1b98335-9649-4fb0-961d-5a49ce108d49",
  "scope": "openid wlcg.groups profile",
  "iss": "https://wlcg.cloud.cnaf.infn.it/",
  "exp": 1571989553,
  "iat": 1571985953,
  "jti": "a535baea-0f7b-461e-a5de-cd7bceb8be3c",
  "wlcg.groups": [
    "/wlcg"
  ]
}
```

The WLCG IAM instance

A WLCG-managed, **experiment-agnostic VO in support of WLCG development, integration and testing activities** focusing on **the transition to token-based AuthN/Z**

https://wlcg.cloud.cnaf.infn.it

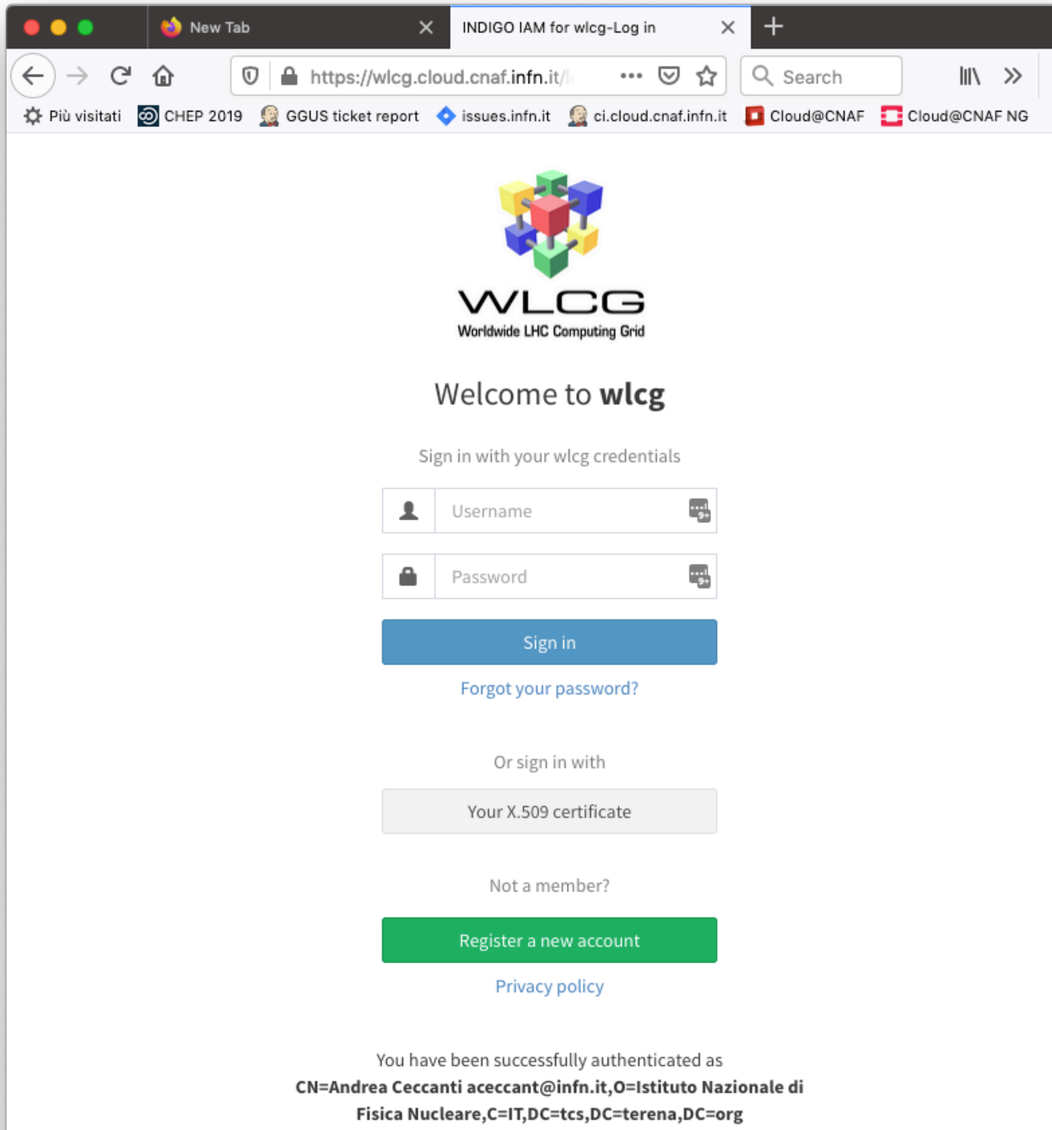
Deployed at INFN-CNAF, managed with IAM, registered in EduGAIN*

- Providing support for VOMS and token/based AuthN/AuthZ

Short term: supported by sites for DOMA integration activities

- TPC, …

Long term: replace dteam for WLCG integration testing



* ETA: Dec. 2019

Integration activites

Standard OAuth/OpenID Connect enables **easy integration** with off-the-shelf services and libraries.

IAM has been successfully integrated with

- Openstack, Atlassian JIRA & Confluence, Moodle, Rocketchat, Grafana, Kubernetes, JupyterHub
- **dCache, StoRM, XRootD (HTTP), FTS, RUCIO, HTCondor**

IAM related talks/posters @ CHEP 2019

Beyond X.509: token-based authentication and authorization in practice

WLCG Authorisation: from X.509 to tokens

Dynamic integration of distributed, Cloud-based HPC and HTC resources using JSON Web Tokens and the INDIGO IAM Service

ESCAPE prototypes a Data Infrastructure for Open Science

Modernizing Third-Party-Copy Transfers in WLCG

The iTHEPHY project and its software platform: enhancing remote teacher-student collaboration

Building an IRIS trust framework

Token-based authorization in the StoRM WebDAV service

Future work

Support integration activities

- DOMA and beyond
- ESCAPE
- EOSC

Transition IAM codebase to 

Thanks for your attention.
Questions?

References

IAM @ GitHub: https://github.com/indigo-iam/iam

IAM documentation: https://indigo-iam.github.io/docs

WLCG Authorization WG: https://twiki.cern.ch/twiki/bin/view/LCG/WLCGAuthorizationWG

WLCG AuthZ WG Demos: https://indico.cern.ch/event/791175/attachments/1806605/2948665/demos.mp4 (IAM starts at minute 46)

IAM in action video: https://www.youtube.com/watch?v=1rZlvJADOnY

Contacts:

- andrea.ceccanti@cnaf.infn.it
- indigo-iam.slack.com

Backup slides

Software Quality in IAM

Aim to have **~90% unit test coverage on all code**:

- now 30K LoC, 86% branch coverage, >1.1K tests

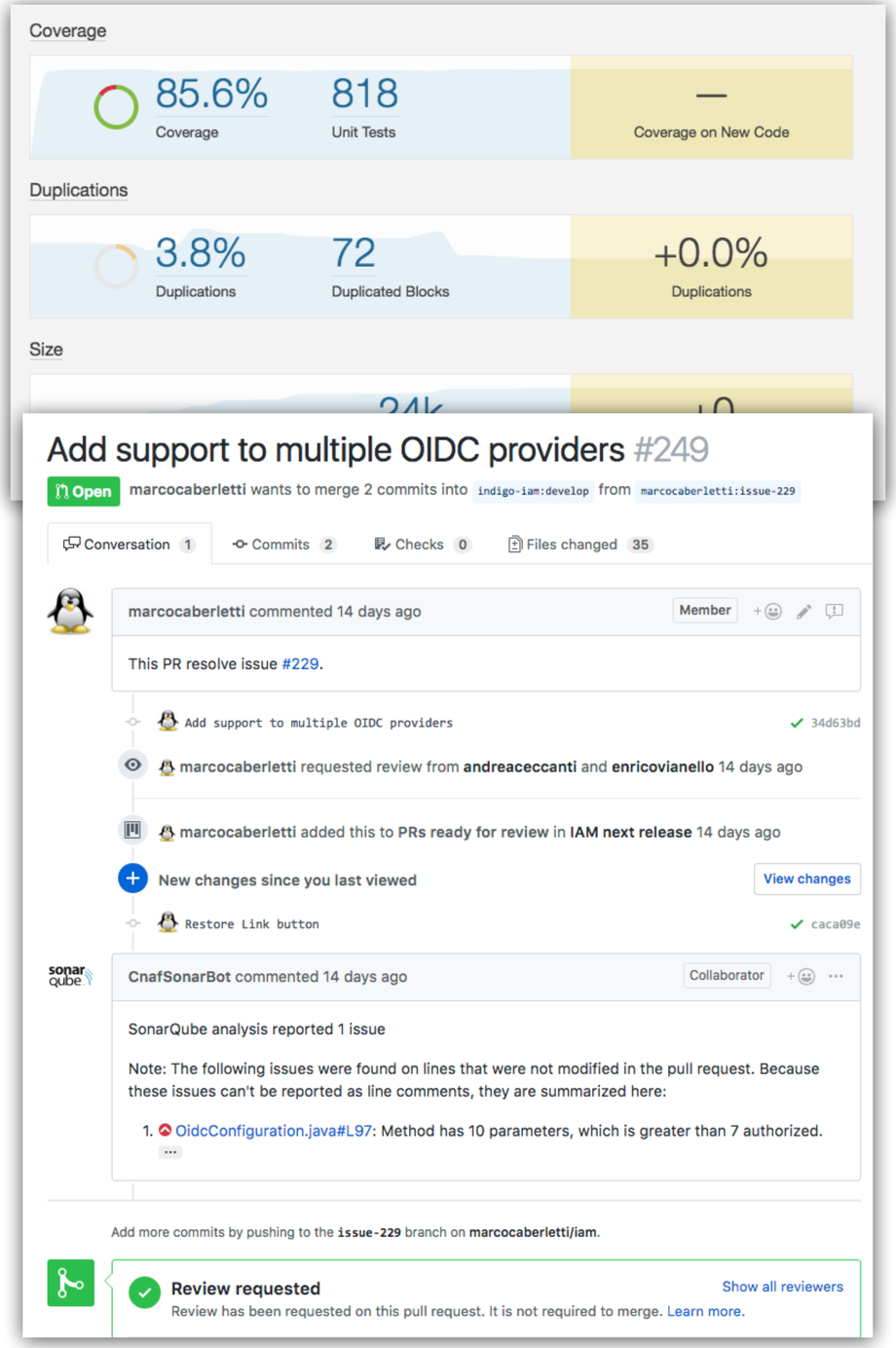
Open, **test-driven** development process

Static analysis tools

- SonarCloud IAM page

Multiple test suites

- **Unit tests**
- **Frontend test suite** (based on Selenium and Robot framework)
- **Deployment tests** (in CI)



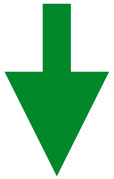
IAM evolution: porting to Keycloak

IAM 2 (currently in development) **will be based on Keycloak**

- Powerful RedHat SSO solution
- Vibrant community: > 250 GitHub contributors
- LDAP/Kerberos integration
- Multi-tenancy

IAM codebase will **focus on what not already provided by Keycloak**

- registration service and user/group management
- X.509 and VOMS authentication support



Improved flexibility and sustainability