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

Andrea Ceccanti, Enrico Vianello, Francesco Giacomini
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 accommodate 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 accommodate 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
- 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
IAM evolution work
Enabling a smooth transition beyond X.509

On demand X.509 certificate generation

RCAuth.eu  IAM  CERN HR db

membership validation

OAuth-aware service  $  VOMS-aware service

$  $
On-demand X.509 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.
X.509 certificates

No certificates found

- Link certificate
- Request certificate
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.
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.
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
The proxy certificate can later be retrieved by trusted clients via the IAM proxycert REST API.
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

VO membership validation integrated with CERN HR database

- RCAuth.eu
- IAM
- CERN HR db
- OAuth-aware service
- VOMS-aware service

X.509 certificate
VOMS credential
JWT access token
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

RCAuth.eu ← IAM ← CERN HR db

OAuth-aware service ← IAM ← VOMS-aware service

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

---

IAM

VOMS AA

membership information

voms-proxy-init
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
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.
In VOMS, we would call that a role
So I do a “traditional” VOMS role request
And in the end I get the *administrators* role as VOMS primary attribute.
And in the end I get the `administrators` role as VOMS primary attribute
Enabling a smooth transition beyond X.509 membership validation

Consistent authorization for OAuth & VOMS services

- RCAuth.eu
- IAM
- CERN HR db
- OAuth-aware service
- VOMS-aware service

X.509 certificate
VOMS credential
JWT access token
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:

```json
{
    "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 activities

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 KEYCLOAK
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