EPJ Web of Conferences **245**, 03021 (2020) https://doi.org/10.1051/epjconf/202024503021
CHEP 2019

Beyond X.509

Token-based authentication and authorization in practice

Andrea Ceccanti[1,*], *Enrico* Vianello[1], and *Francesco* Giacomini[1]

[1]INFN CNAF, Viale Berti Pichat 6/2, 40127 Bologna, Italy

Abstract. One of the key challenges identified by the HEP R&D roadmap for software and computing is the ability to integrate heterogeneous resources in support of the computing needs of HL-LHC. In order to meet this objective, a flexible Authentication and Authorization Infrastructure (AAI) has to be in place, to allow the secure composition of computing and storage resources provisioned across heterogeneous providers (e.g., Grid, private and commercial Clouds, HPC centers). At CHEP 2018, we presented how a flexible AAI based on modern, standard Web technologies (OpenID Connect, OAuth and JSON Web Tokens) and centered on the INDIGO Identity and Access Management (IAM) service could support the transition of the WLCG infrastructure to a token-based AAI. In the meanwhile, INDIGO IAM has been selected by the WLCG Management Board as the solution that will be adopted by LHC experiments, and is also at the core of the AAI envisioned to support the computing needs of the ESCAPE project. In this contribution, which represents a follow up to last-year plenary talk, we describe the work done recently on the IAM service to support WLCG requirements.

1 Introduction

Last year we presented how a flexible AAI based on modern, standard Web technologies, namely OpenID Connect [1], OAuth [2] and JSON Web Tokens (JWTs) [3], and centered on the INDIGO Identity and Access Management (IAM) service could be realized to support WLCG use cases [4].

In this contribution we describe the work done in the past year to enable this vision, covering in more detail development, testing and integration activities done on the IAM service to support the requirements emerging from the WLCG Authorization working group [5, 6].

2 The INDIGO IAM service

The INDIGO IAM Service provides a central authorization server, dealing with user authentication, registration and high-level authorization for a Virtual Organization. Conceptually, IAM serves the same role that in the present WLCG AAI is served by VOMS [7], without being limited to a single authentication mechanism, as depicted in Figure 1.

IAM has been initially developed at INFN in the context of the INDIGO Datacloud [8] project, and later extended with the support of various European projects ([9, 10]) to support the needs of the various research communities served by INFN and by other computing

*e-mail: andrea.ceccanti@cnaf.infn.it

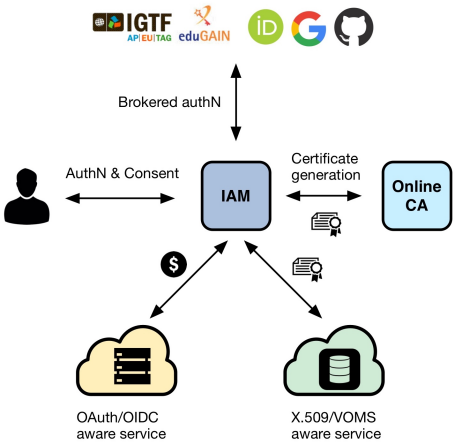

Figure 1. IAM enables a modern AAI for WLCG, with a transition path from X.509 certificates.

centers distributed in Europe [11]. IAM provides the main functionality needed to operate successfully a VO authorization server:

- A registration service that implements a moderated enrollment flow similar to the one used in production by WLCG, with support for periodic Acceptable Usage Policy (AUP) enforcement;
- An administration dashboard, that provides an intuitive tool for common administrative tasks, such as group membership and OAuth/OpenID Connect client management;
- A flexible OAuth/OpenID Connect implementation, providing support for multiple OAuth grant types (e.g., device [12], token exchange [13]);
- Support for account linking, allowing users to link multiple identities to their accounts;
- SCIM [14] provisioning APIs, to give relying services the ability to query and modify membership information.

More details on the service can be found in previous publications [4, 15] or on the IAM website [16]. In the following sections, we discuss recent developments that address WLCG requirements.

3 Enabling a smooth transition beyond X.509

Transitioning the WLCG to token-based authentication and authorization represents a sea change for the infrastructure and will likely take years to be fully realized. Services, at various levels, will have to be modified, new tools and approaches for computing, operations, accounting and many other aspects will have to be investigated, realized, and deployed without disrupting the ability to keep supporting the HEP community research efforts.

For this reason, a key aspect is creating the conditions for a gradual transition away from X.509. To this end, development on IAM has focused on two aspects:

- VOMS provisioning: IAM ability to to act as a VOMS attribute authority compatible with existing WLCG resources;

- RCAuth.eu integration: IAM ability to integrate with a trusted, online certificate authority providing X.509 certificates on-demand.

3.1 VOMS provisioning

IAM has supported X.509 certificate authentication and linking since version 1.0, released in 2017. The certificate linking process requires that the user proves ownership of the certificate by successfully authenticating with such certificate. This represents an improvement over previous approaches, like the one implemented in VOMS Admin [17], because the procedure does not require administrator vetting. Another advantage is that users do not have to know and manually enter details about their certificate, a process that has proved to be error-prone in VOMS and has led to the submission of several support tickets.

On top of this functionality, we have developed a VOMS [7] attribute authority (VOMS AA) micro-service integrated with IAM. There are several advantages in implementing VOMS support as a separate service:

- Not all IAM deployments will require VOMS support; having this functionality separated from the core IAM code gives more flexibility at deployment time;
- The VOMS AA will typically expose a TLS endpoint secured using IGTF trust roots, as required by the WLCG infrastructure, while typically the IAM service will use a certificate signed by a widely recognized CA, like Let's Encrypt [18], in order to improve usability for end-users. Having two separate services allows for an easy implementation of this approach;
- the two services can be deployed and scaled independently according to the needs of the deployment.

The IAM VOMS AA is a Spring Boot [19] micro-service, which relies on VOMS Java libraries [20] to implement VOMS attribute certificate generation and signing. User subject, group information and other attributes are obtained from the IAM database.

Since IAM does not provide a *role* abstraction and since VOMS roles can be seen as group membership assertions that are included only if explicitly requested, a mechanism based on labels is used to flag some IAM groups as VOMS roles. These groups are not automatically included in the generated VOMS attribute certificates, but are instead returned only if explicitly requested by a client, preserving the original VOMS role syntax and semantics.

3.2 RCAuth.eu integration

The RCAuth.eu [21] Pilot Certificate Authority (CA) is an online CA operated by NIKHEF, which issues certificates to end-entities based on a successful authentication to a Federated Identity Management System (FIMS) operated by an eligible Registration Authority. The certificates issued by the RCAuth Pilot CA are valid for a period of at most 13 months, but may be as short as 11 days.

RCAuth.eu has been integrated with IAM in order to provide on-demand X.509 certificates to users without a certificate. The certificate is obtained using a simple OAuth-based protocol [22].

When the RCAuth.eu integration is enabled, IAM provides users with the ability to request a new certificate from the IAM dashboard, as shown in Figure 2.

What happens under the hood is that the user is redirected to the RCAuth.eu instance to authenticate and to give consent for the generation of an X.509 certificate and for that certificate to be accessible by IAM. IAM can then fetch the generated certificate, from which it

creates a proxy certificate that is stored in the IAM database and linked to the user membership.

A certificate-provisioning API has also been developed to give authorized users and agents access to the proxy certificates stored in the IAM database.

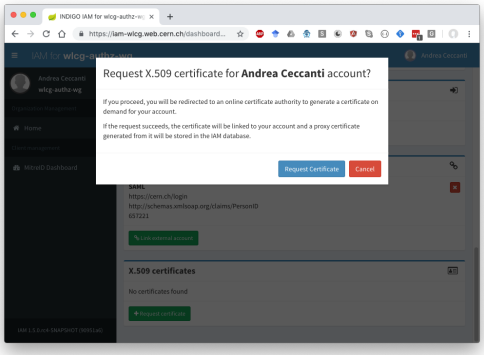

Figure 2. The generation of an X.509 certificate can be requested directly from the IAM dashboard.

4 Integration with the CERN Human Resources database

The identity vetting procedure deployed at CERN for the LHC VOs relies on the VOMS Admin [17] integration with the CERN Human Resource database [23]. This integration ensures that each member has a valid LHC experiment membership while registered in VOMS.

In order to expose that functionality also to IAM, the logic of the HR database querying has been extracted from the VOMS Admin code base. A Spring boot micro-service has been developed to provide a convenient REST API to query information about LHC experiment membership [24]. This micro-service has been deployed at CERN and integrated in IAM to demonstrate identity-vetting based on HR information, supporting a registration flow similar to the one implemented in production by VOMS Admin and that would satisfy the requirements expressed by the WLCG Authorization Working Group.

All the functionality described above has been demonstrated in the context of the WLCG Authorization Working Group, as described in another contribution to this journal [6].

5 The common WLCG JWT profile implementation

One of the major achievements of the WLCG Authorization Working Group was the definition of a JWT profile that would help supporting WLCG authentication and authorization use cases. Version 1.0 of the profile has been published at the end of September, 2019 [25]. The document, building in large part on consolidated standards [1–3, 13], defines important aspects for the future WLCG AAI, such as how trust is established in the infrastructure, what information should be included in tokens and how tokens should be verified by client applications.

Support for the WLCG JWT profile has been implemented in IAM during October 2019, and demonstrated during the conference.

In more detail, IAM has been extended to support *token profiles*. In IAM, a token profile defines how membership and authorization information should be encoded in issued tokens

and in OpenID Connect userinfo and OAuth token introspection responses. Currently, IAM implements two token profiles: the default profile and the WLCG JWT profile. The profile can be selected both at IAM instance level, by setting a default value, and at client application level. This approach allows to integrate applications using different profiles in the context of the same IAM instance.

The IAM Scope Policy API, which allows to define policies that regulate access to OAuth scopes in IAM, has been extended to support more flexible scope matching rules, so that, besides exact string matching, it is possible to match scopes by regular expression or following the WLCG JWT storage capabilities path semantics, where permissions granted on a path are applied transitively to sub-paths.

As an example, a policy granting members of the `transfers` group access to the `storage.read:/data` scope will also grant the group members access to scopes targeting sub-resources, e.g. `storage.read:/data/sub/path`.

This flexibility in the Scope Policy API allows the definition of fine-grained data access authorization policies at the IAM level, that will be then enforced at storage elements, as envisioned in the WLCG JWT profile.

6 The WLCG IAM instance

In March 2019, the WLCG Management Board selected IAM as the future solution for LHC experiments, after an evaluation pilot where IAM ability to support WLCG requirements was assessed [6].

In late 2019, once the JWT profile implementation was ready for external testing, a WLCG IAM instance integrated with CERN Single Sign On [26] was set up at the Istituto Nazionale di Fisica Nucleare (INFN) to provide a stable platform against which software enhancements could be tested.

This instance was mainly deployed in support of DOMA Third-Party Copy Working Group [27] activities, but in the future could be used for deployment and authorization testing purposes at WLCG sites, replacing the `dteam` VO. A VOMS attribute authority linked to this IAM instance has also been deployed, to allow users to get VOMS attribute certificates for the `wlcg` VO, with the objective of demonstrating IAM interoperability with the current X.509-based WLCG AAI.

7 Conclusions and future work

Moving beyond X.509 is recognized as a key challenge for HEP computing to improve usability, simplify the middleware stack and enable interoperability with heterogeneous computing and storage resource providers.

In this contribution we have described in more detail recent work done on INDIGO IAM to address WLCG requirements, focusing on developments targeted at enabling a gradual transition towards a token-based AAI.

In the future, we will focus on three main activities: supporting IAM integration at various levels of the WLCG software stack (from storage elements, to experiment workload management frameworks); supporting the deployment of IAM in production in support of LHC experiments and other interested communities [10]; migrating the IAM code base to Keycloak [28], to enable support for multi-tenancy and increase IAM sustainability.

References

[1] OpenID Foundation, *The OpenID Connect identity layer* (2018), `https://openid.net/connect/`

[2] D. Hardt, RFC 6749, IETF Tools (2012), https://tools.ietf.org/rfc/rfc6749.txt
[3] M.B. Jones, J. Bradley, N. Sakimura, RFC 7519, IETF Tools (2015), https://tools.ietf.org/rfc/rfc7519.txt
[4] A. Ceccanti, E. Vianello, M. Caberletti, F. Giacomini, EPJ Web Conf. **214**, 09002 (2019)
[5] *The WLCG Authorization Working Group*, https://twiki.cern.ch/twiki/bin/view/LCG/WLCGAuthorizationWG
[6] B. Bockelman, A. Ceccanti, I. Collier, L. Cornwall, T. Dack, J. Guenther, M. Lassnig, M. Litmaath, P. Millar, M. Sallé et al., *WLCG Authorisation from X.509 to Tokens*, submitted for publication to this journal
[7] V. Ciaschini, V. Venturi, A. Ceccanti, *The Virtual Organisation Membership Service*, https://doi.org/10.5281/zenodo.1875371 (2016)
[8] I.D. Collaboration, :, D. Salomoni, I. Campos, L. Gaido, J.M. de Lucas, P. Solagna, J. Gomes, L. Matyska, P. Fuhrman et al., *INDIGO-DataCloud:A data and computing platform to facilitate seamless access to e-infrastructures* (2017), arXiv:1711.01981
[9] *The EOSC-Hub project*, https://www.eosc-hub.eu
[10] *The ESCAPE project*, https://projectescape.eu/
[11] D. Crooks, D. Kelsey, I. Neilson, I. Collier, *Building an IRIS trust framework*, submitted for publication to this journal
[12] W. Denniss, J. Bradley, M. Jones, H. Tschofenig, *OAuth 2.0 Device Authorization Grant*, RFC 8628 (2019), https://rfc-editor.org/rfc/rfc8628.txt
[13] M. Jones, A. Nadalin, B. Campbell, J. Bradley, C. Mortimore, *OAuth 2.0 Token Exchange*, RFC 8693 (2020), https://rfc-editor.org/rfc/rfc8693.txt
[14] *The System for Cross Domain Identity Management website*, http://www.simplecloud.info/
[15] A. Ceccanti, M. Hardt, B. Wegh, A.P. Millar, M. Caberletti, E. Vianello, S. Licehammer, Journal of Physics: Conference Series **898** (2017)
[16] A. Ceccanti, E. Vianello, M. Caberletti, *INDIGO Identity and Access Management (IAM)*, https://doi.org/10.5281/zenodo.1874790
[17] A. Ceccanti, *The VOMS administration service*, https://doi.org/10.5281/zenodo.1875616
[18] *The Let's Encrypt Certificate Authority*, https://letsencrypt.org
[19] *The Spring Boot project*, https://spring.io/projects/spring-boot
[20] *The VOMS Java APIs*, https://github.com/italiangrid/voms-api-java
[21] *The RCAuth online CA*, https://rcauth.eu
[22] *OAuth for MyProxy*, http://grid.ncsa.illinois.edu/myproxy/oauth/
[23] A. Ceccanti, V. Ciaschini, M. Dimou, G. Garzoglio, T. Levshina, S. Traylen, V. Venturi, *VOMS/VOMRS utilization patterns and convergence plan*, in *Journal of Physics: Conference Series* (2010), Vol. 219, http://stacks.iop.org/1742-6596/219/i=6/a=062006
[24] *The CERN HR DB API service* , https://baltig.infn.it/aceccant/cern-hr-db-service
[25] M. Altunay, B. Bockelman, A. Ceccanti, L. Cornwall, M. Crawford, D. Crooks, T. Dack, D. Dykstra, D. Groep, I. Igoumenos et al., *WLCG Common JWT Profiles* (2019), https://doi.org/10.5281/zenodo.3460258
[26] E. Ormancey, Journal of Physics: Conference Series **119**, 082008 (2008)

[27] *The WLCG DOMA Third-party Copy Working Group*, https://twiki.cern.ch/twiki/bin/view/LCG/ThirdPartyCopy

[28] *The Keycloak Identity and Access Management service*, https://www.keycloak.org