NRC·CNRC

Towards Federation in CADC Authentication, Authorization and Identity (AA&I)

Adrian Damian - Canadian Astronomy Data Centre (CADC)
IVOA InterOp Meeting, June 2025

Federated Identities - Overview

- Current status
- Requirements for federated identity
- Approach
- Conclusion

Cartoon credit: https://www.toonpool.com/cartoons/Onlinprofilepicture_279153

CADC Authentication & Authorization

A&A has been used for a long time for proprietary data (and metadata) distribution. More recently also used to control access to other resources: disk space (user and project), computing, user catalogues, etc.

- 9-10k user accounts
- AccessControl (`ac`) - LDAP-backed in-house Web service

Very complex environment:

- Authentication methods: username/password, cookies, X509 Certificates, OpenID (partial)
- Web and command line applications
- Single Sign On (SSO) over 3 domains
- Authorization based on group membership (GMS). Scalable. Group of groups.
- Support for interactive and batch sessions on distributed cloud infrastructure
- Local POSIX identities
- ~~Credential delegation service using X509 Proxy Certificates~~

From SSO to Federated Identity Management (FIM)

SSO: with a Single Organization

FIM: one single digital identity to access multiple entreprises and domains that are part of a federation and share a sense of mutual **trust**

Seamless integration with 2 federations (SKA, Rubin)

Support for OpenID Connect (OIDC) technologies

Maximum flexibility as access policies not clearly defined yet

Considered a few solutions:

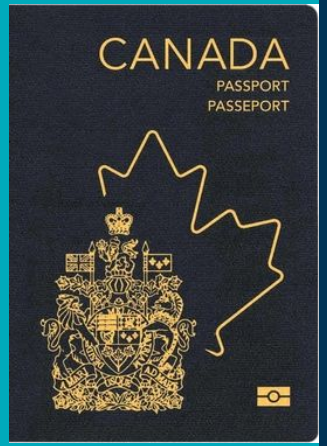
- CILogon (Rubin)
- Indigo IAM (SKA)
- keycloak (Many others)

For now decided to adapt/enhance the CADC `ac`

X509 Certificates vs OAuth2.0/OIDC Identity Approach

X509 certificates are similar to passports:

- Issued by a local office (authority) on behalf of a central (country) authority with large recognition
- Unique identity within the central authority
- A lot of embedded security
- Long time validity
- Hard to impersonate
- Bulky to use daily
- Certified photocopies
- used to work (proxy certificates)



Bearer tokens are similar to daily ski passes:

- Issued by a local authority
- Different identities at each ski resort
- Recognized at other ski resorts that participate in a collective
- Valid only for the day/half day
- Easy to use by anyone in its possession (easy to impersonate)
- Not a lot of security embedded (QRCode)
- Sometimes issued for a specific purpose

Big paradigm shift

Implementation Guidelines

Planned features (open to feedback):

1. Support OIDC token in JWT format only (to be able to validate the IdP)
2. Configure trusted Identity Providers (SKA, Rubin) and their GMS services
    a. Industry solution in the works (OpenID Federation)
3. Automatic CADC account creation when local identities required:
    a. Resource owner such as UWS Job owner
    b. POSIX identities (uid and gid)
4. Support for UI authentication with trusted IdPs
5. Ability to link existing CADC account with external identities - preferred
6. Ability to merge existing CADC accounts
7. Implement credential exchange (token->X509, X509->token, token->token)
8. Replace `ac` or just the authorization side with a off the shelf solution (keycloak) - long term

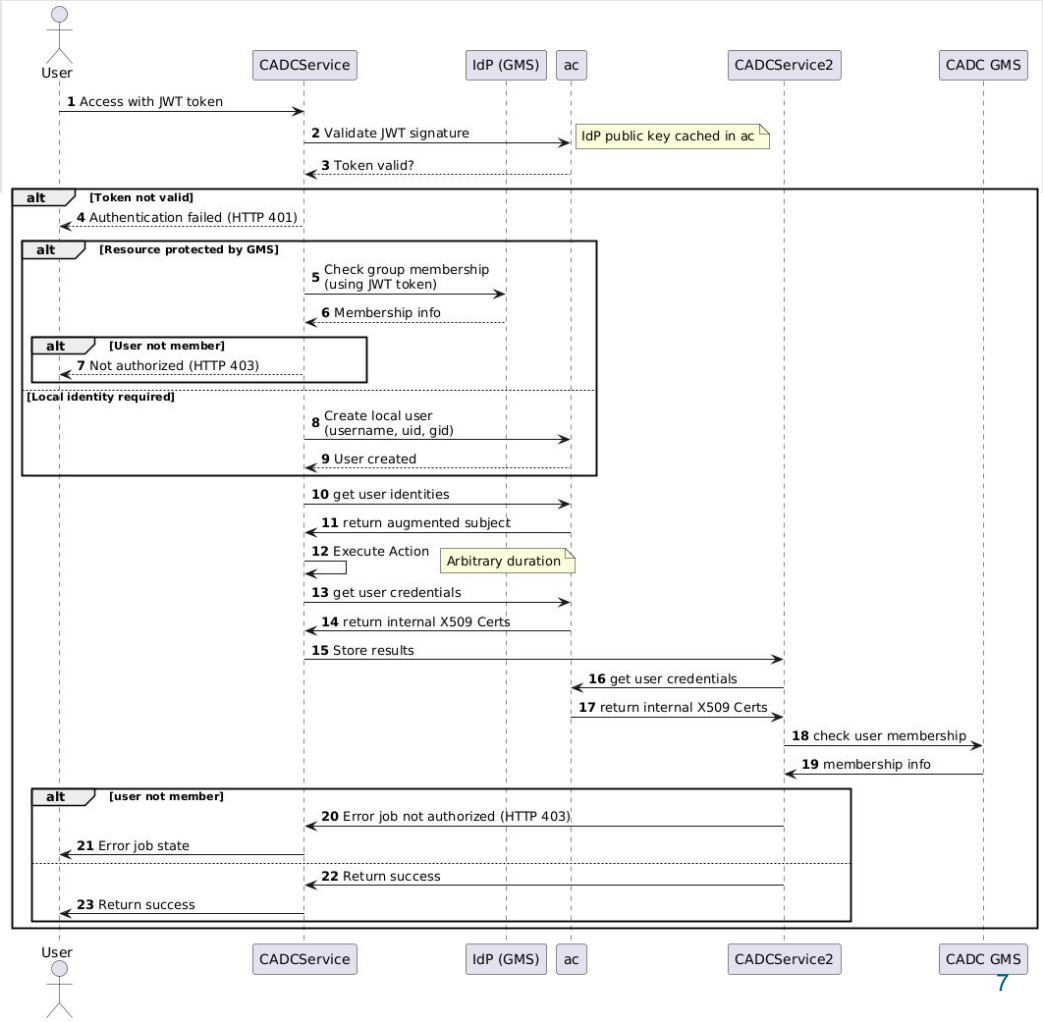
Example of call sequence

OIDC claims mapping:

Unique OIDC Identity is the `iss` and `sub` mandatory claims combination:
"`iss=https://ska-iam.stfc.ac.uk sub=ecaa76d2-964c-4d7a-b6a2-fba67c4b7c31`"

`preferred_username` - optional POSIX name

`allowed_origins, allowed_domains, audience` - trusted domains?



User info for external vs CADC users

Default User Account:

```
<?xml version="1.0" encoding="UTF-8"?>
<user>
  <internalID>
<uri>ivo://cadc.nrc.ca/gms?00000000-0000-0000-0000-000000203045</uri>
  </internalID>
  <identities>
    <identity type="HTTP">ska-joedoe</identity>
    <identity type="CADC">00000000-0000-0000-0000-000000203045</identity>
    <identity type="POSIX">23021</identity>
    <identity type="OPENID">iss=https://ska-iam.stfc.ac.uk
sub=abcd76e2-977c-4d7a-b6a2-fba88d9b7c43</identity>
    <identity type="X500">CN=Joe Doe,OU=myorg,O=Grid,C=CA</identity>
  </identities>
  <personalDetails/>
  <posixDetails>
    <username>ska-doej</username>*
    <uid>23021</uid>
    <gid>23021</gid>
    <homeDirectory>/home/23021</homeDirectory>
  </posixDetails>
</user>
```

*User name filled in only if `preferred_username` claim is present.

User personal details only filled in when corresponding claims provided

CADC User Account with Linked :

```
<?xml version="1.0" encoding="UTF-8"?>
<user>
  <internalID>
<uri>ivo://cadc.nrc.ca/gms?00000000-0000-0000-0000-000000203045</uri>
  </internalID>
  <identities>
    <identity type="HTTP">joedoe</identity>
    <identity type="CADC">00000000-0000-0000-0000-000000203045</identity>
    <identity type="POSIX">23021</identity>
    <identity type="OPENID">iss=https://ska-iam.stfc.ac.uk
sub=abcd76e2-977c-4d7a-b6a2-fba88d9b7c43</identity>
    <identity type="OPENID">iss=https://test.cilogon.org
 sub=http://cilogon.org/serverE/users/123456"</identity>
    <identity type="X500">CN=Joe Doe,OU=myorg,O=Grid,C=CA</identity>
  </identities>
  <personalDetails>
    <firstName>Joe</firstName>
    <lastName>Doe</lastName>
    <email>Joe.Doe@myemail.com</email>
    <institute>INST</institute>
    <city>Victoria</city>
    <country>Canada</country>
  </personalDetails>
  <posixDetails>
    <username>doej</username>
    <uid>23021</uid>
    <gid>23021</gid>
    <homeDirectory>/home/23021</homeDirectory>
  </posixDetails>
</user>
```

CADC Service to External Service Calls

- Appropriate user credentials must be used for CADC service to external service calls
- Can use the proposed Interoperable Authentication Protocol (IAP) to determine the domain (federation) of the target service and the user credential that are required to access it
- For longer lasting jobs, a new token-based credential delegation service similar to the Credential Delegation Protocol (CDP) is required
- Exchange Credentials Service?
- evil is in the details

Conclusions

- As the new facilities come online, a solution for federated AA&I is required
- Authentication/Authorization is no longer just for data access - resources also need to be protected
- We might need temporary solutions before standards catch up
- User experience is center stage
- We have to go fast but not necessarily alone
- Please be in touch if interested in the subject

Thank you

Adrian Damian • CADC • Adrian.Damian@nrc-cnrc.gc.ca