CILogon & SciTokens OIDC/OAuth Federation

Jim Basney <jbasney@ncsa.illinois.edu>

EUGridPMA 2018-01-22

CILogon

SCITOKENS

XSEDE

Extreme Science and Engineering Discovery Environment

- Planning for Globus migration from X.509 to Globus Auth
  - https://www.globus.org/blog/support-open-source-globus-toolkit-ends-january-2018
  - https://software.xsede.org/display/XCI-127
- Maintain credential assurance for XSEDE users and systems
  - https://software.xsede.org/display/XCI-205
- Continue to benefit from IGTF trust community
- IGTF OIDC / OAuth Federation?

CILogon

SCITOKENS

OIDC/OAuth Federation

- Namespace Ownership
  - DNS
  - Federation Registrar
- Key Exchange
  - Trust HTTPS (basic OIDC / OAuth 2.0 trust model)
  - Signed Metadata (https://openid.net/specs/openid-connect-federation-1_0.html)
- Policy Certification
  - https://refeds.org/sirtfi
  - https://wiki.refeds.org/display/GROUPS/Assurance+Working+Group
  - https://www.igtf.net/ap/authn-assurance/
  - https://www.eugridpma.org/guidelines/trustedstores/
  - https://www.eugridpma.org/guidelines/aaops/

CILogon

- Federated IAM
- OpenID Connect
- ID Tokens
- iss, sub, name, email
- R&E claims
  - isMemberOf
  - eppn
  - affiliation

www.cilogon.org/oidc

SciTokens

- Federated Authorization
- OAuth 2.0
- Access Tokens
- iss, sub, scope
- OAuth Token Exchange
  - act (Actor)
  - scp (Scopes)
  - cid (Client Identifier)

scitokens.org

CILogon

SCI TOKENS

CILogon ID Token


```
{
 "iss": "https://cilogon.org",
 "sub": "http://cilogon.org/users/534",
 "exp": 1516573433,
 "iat": 1516572533,
 "aud": "myproxy:oa4mp:/cli/6e8fda42",
 "name": "Jim Basney",
 "isMemberOf": ["ncsa-ca","org_cisr"],
 "email": "jbasney@illinois.edu",
 "idp": "https://ncsa.illinois.edu/",
 "idp_name": "NCSA",
 "eppn": "jbasney@ncsa.illinois.edu"
}
```


SciTokens Access Token


```
{
 "iss": "https://scitokens.org/cms",
 "sub": "u534",
 "exp": 1509991790,
 "iat": 1509988190,
 "aud": "https://scitokens.org/cms",
 "scp": "read:/data write:/home/u534",
}
```


CILogon

SCITOKENS

OIDC Discovery Metadata

- REQUIRED: issuer, authorization_endpoint, token_endpoint, jwks_uri, response_types_supported, subject_types_supported, id_token_signing_alg_values_supported
- RECOMMENDED: userinfo_endpoint, registration_endpoint, scopes_supported, claims_supported
- OPTIONAL: service_documentation, claims_locales_supported, op_policy_uri, op_tos_uri, ...

http://openid.net/specs/openid-connect-discovery-1_0.html#ProviderMetadata

CILogon Metadata

https://cilogon.org/.well-known/openid-configuration


```
{
 "issuer": "https://cilogon.org",
 "jwks_uri": "https://cilogon.org/oauth2/certs",
 "authorization_endpoint": "https://cilogon.org/authorize",
 "registration_endpoint": "https://cilogon.org/oauth2/register",
 "token_endpoint": "https://cilogon.org/oauth2/token",
 "userinfo_endpoint": "https://cilogon.org/oauth2/userinfo",
 ...
}
```

CILogon Metadata

https://cilogon.org/oauth2/certs


```
{ "keys": [
            { "n": "...", "e": "AQAB", "alg": "RS256",
              "kid": "...", "use": "sig", "kty": "RSA" },
            { "n": "...", "e": "AQAB", "alg": "RS384",
              "kid": "...", "use": "sig", "kty": "RSA" },
            { "n": "...", "e": "AQAB", "alg": "RS512",
              "kid": "...", "use": "sig", "kty": "RSA" }
          ]
}
```


CILogon

SCITOKENS

SciTokens Metadata

https://scitokens.org/cms/.well-known/openid-configuration


```
{
 "issuer":"https://scitokens.org/cms",
 "jwks_uri":"https://scitokens.org/cms/oauth2/certs",
 "token_endpoint":"https://cms.scitokens.org/token"
}
```

IGTF CA metadata (CILogon Basic)

```
alias = cilogon-basic
url = http://ca.cilogon.org/
ca_url = https://cilogon.org/cilogon-basic.pem
crl_url = http://crl.cilogon.org/cilogon-basic.crl
email = ca@cilogon.org
status = accredited:iota
version = 1.82
sha1fp.0 = 21:D6:E3:AE:1E:D0:A7:02:77:67:B3:6B:A9:6D:69:70:60:07:F9:B1
subjectdn = "/DC=org/DC=cilogon/C=US/O=CILogon/CN=CILogon Basic CA 1"
```

CILogon

SCI TOKENS

IGTF OIDC metadata (CILogon Basic)

```
alias = cilogon-basic
url = http://www.cilogon.org/oidc
iss = https://cilogon.org
metadata = https://cilogon.org/.well-known/openid-configuration
ca_url = https://cilogon.org/cilogon-basic.pem
crl_url = http://crl.cilogon.org/cilogon-basic.crl
email = help@cilogon.org
status = accredited:iota
version = 1.82
sha1fp.0 = 21:D6:E3:AE:1E:D0:A7:02:77:67:B3:6B:A9:6D:69:70:60:07:F9:B1
subjectdn = "/DC=org/DC=cilogon/C=US/O=CILogon/CN=CILogon Basic CA 1"
```

CILogon

SCITOKENS

Discussion