

SciTokens Project

- Introduces a **capabilities-based authorization infrastructure** for distributed scientific computing,
- Provides a **reference platform**, combining CILogon, HTCondor, CVMFS, and XRootD, and
- Implements specific use cases** to help our science stakeholders (LIGO and LSST) better achieve their scientific aims.

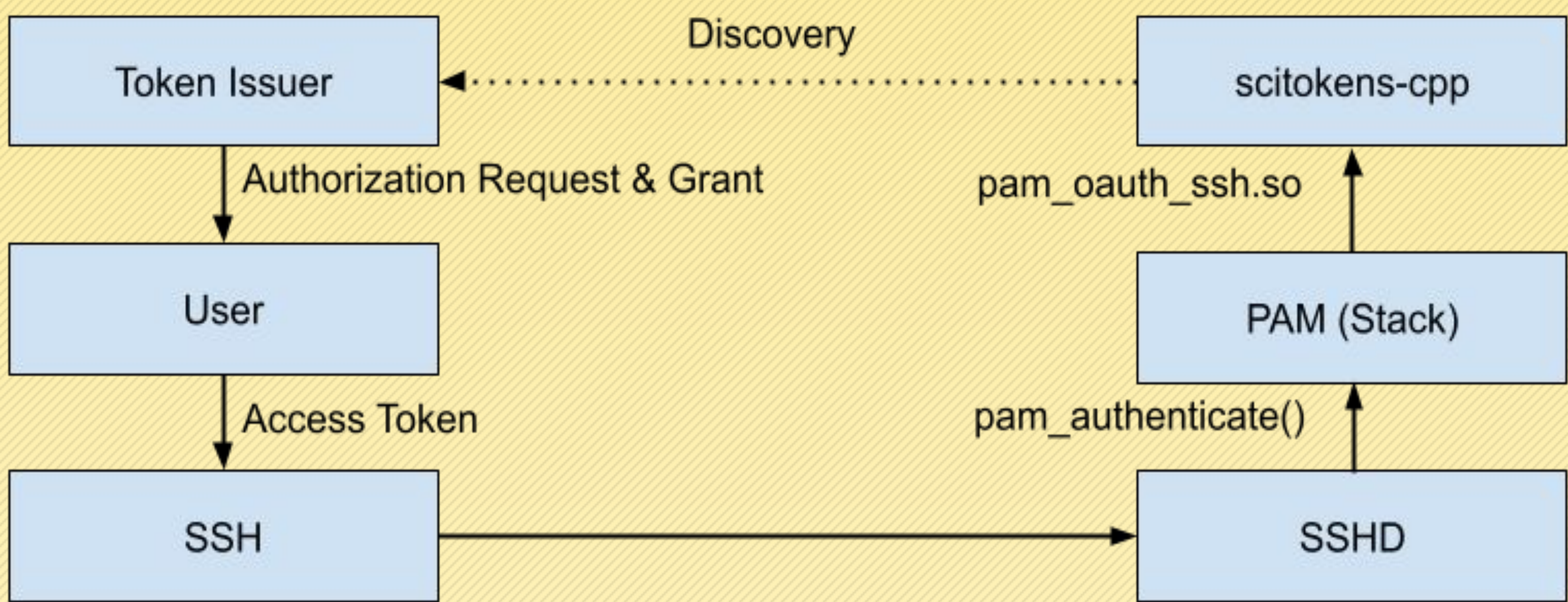
Using Standards

- RFC 6749: OAuth 2.0 Authorization Framework
 - token request, consent, refresh
- RFC 7519: JSON Web Token (JWT)
 - self-describing tokens, distributed validation
- RFC 8414: OAuth 2.0 Authorization Server Metadata
 - token signing keys, policies, endpoint URLs
- OAuth 2.0 Token Exchange (IETF OAuth WG I-D)
 - token delegation, drop privileges.

SciTokens SSH

- A token-based authentication method for remote login through SSH authentication via SciTokens
- Based on XSEDE OAuth SSH, SciTokens SSH routes SSH authentication requests to a PAM stack in which the module pam_oauth_ssh.so is used for sshd authentication.
- Can be configured to use Globus Auth and/or SciTokens for authentication.
- Verifies SciTokens using the SciTokens C++ Library, scitokens-cpp.

Authentication Flow



Example SciToken

```
{
  "scope": "ssh:vt20",
  "aud": "martok.ncsa.illinois.edu",
  "iss": "https://demo.scitokens.org",
  "exp": 1583855836,
  "iat": 1583855236,
  "nbf": 1583855236,
  "jti": "073ac358-4f07-4090-ae5f-b5c5be273269"
}
```

Example PAM modification (PAM Stack)

```
auth required pam_sepermit.so
auth required pam_env.so
auth [success=done maxtries=die new_authok_reqd=done default=ignore] pam_oauth_ssh.so
auth requisite pam_succeed_if.so uid >= 1000 quiet_success
auth required pam_deny.so
```

Using SciTokens SSH

```
[$ssh vt20@martok.ncsa.illinois.edu
Enter your OAuth token:
Last login: Wed Apr  8 15:57:57 2020 from vt20.security.ncsa.illinois.edu
[vt20@martok ~]$
```

Authentication
Succeeds

```
Enter your OAuth token:
Enter your OAuth token:
Enter your OAuth token:
vt20@martok.ncsa.illinois.edu's password:
Permission denied, please try again.
vt20@martok.ncsa.illinois.edu's password:
Received disconnect from 141.142.236.2 port 22:2: Too many authentication failures
Authentication failed.
```

Password prompt after token authentication fail

Decoded	Encoded
<div>EDIT THE PAYLOAD</div> <div>HEADER: ALGORITHM & TOKEN TYPE</div> <div><pre>{ "typ": "JWT", "alg": "RS256", "kid": "key-rs256" }</pre></div> <div>PAYLOAD: DATA</div> <div><pre>{ "scp": "read:/protected", "aud": "https://demo.scitokens.org", "iss": "https://demo.scitokens.org", "exp": 1585674839, "iat": 1585674239, "nbf": 1585674239, "jti": "15f40958-d1e1-4b74-9438-98843aeeb5d9" }</pre></div>	<div><pre>eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6ImtleS1yc2I1NiJ9.eyJzY3AiOiJyZWFrOi9wcm90ZWN0ZWQiLCJhdWQiOiJodHRwczovL2RlbW8uc2NpdG9rZW5zLm9yZyIsImIzcyI6Imh0dHBzOi8vZGVyby5zY2I0b2t1bnMub3JnIiwiaXhwIjoxNTg1Njc0ODM5LCJpYXQiOiJlODU2NzQyMzksIm5iZiI6MTU4NTY3NDIzOSwianRpIjoiaMTVmNDA5NTgtZDFlMS00Yjc0LTk0MzgtOTg4NDNhZWVlNWQ5In0.e8C16h-ctm4rHKZ8msmuH-_kWyFwVikW3Ph1IM5KKVSUPvALIdDr1w4a8tLf78Py9QB57vJ9ztrHBdgETQpc3rTiis4_4cJ3D1DL0TjMq7RaF2-SC3yvvU83-cXWh5cNUiR-MeUaZZTZrq-ntE9F1DkFG4Jra4Hn6nWC1ErwY0dxq5kSFeBX7NIdeWGMurN6APAt_r_5f0A4q7uVbg_TA3J5QQakn0ZS8qd429b6-6Q4JMMOGdDSiiZpDn25zc90az-</pre></div>

SciTokens Issuer

Related Work

- GSI-OpenSSH:
Standard solution for remote login to scientific computing resource.
- Globus Auth SSH:
Provides a pluggable authentication module (PAM) that accepts OAuth tokens for authentication.
- SciTokens:
A JWT profile and associated open source implementation.

Evaluation and Security Analysis

- Eavesdropping access tokens:
Attempt to obtain an access token when transported between the SSH client and server.
 - Countermeasure:
Rely on the SSH protocol to encrypt the access token via an SSH public key encrypted channel.
- Leakage of tokens via log files:
Access tokens may be logged.
 - Countermeasure:
Log with just enough information to allow administrators and user to debug

Conclusions and Future Work

SciTokens SSH is a modification to Globus Auth SSH (a.k.a. XSEDE OAuth SSH) that adds support for SciTokens JWTs alongside the existing support for opaque Globus Auth tokens.

Future Work:

- Fine-grained access control:
SciTokens can be issued with a restricted scope of claims. In the future, SciTokens SSH can integrate other SSH solutions that allow fine-grained access control.
- Automate authentication process:
Currently, users will need to manually cut-n-paste the token to respond prompt.
- Account mapping and grouping:
Globus Auth SSH allows mapping requested account to local account but currently, there is no need for SciTokens SSH to perform account mapping

<https://scitokens.org/>