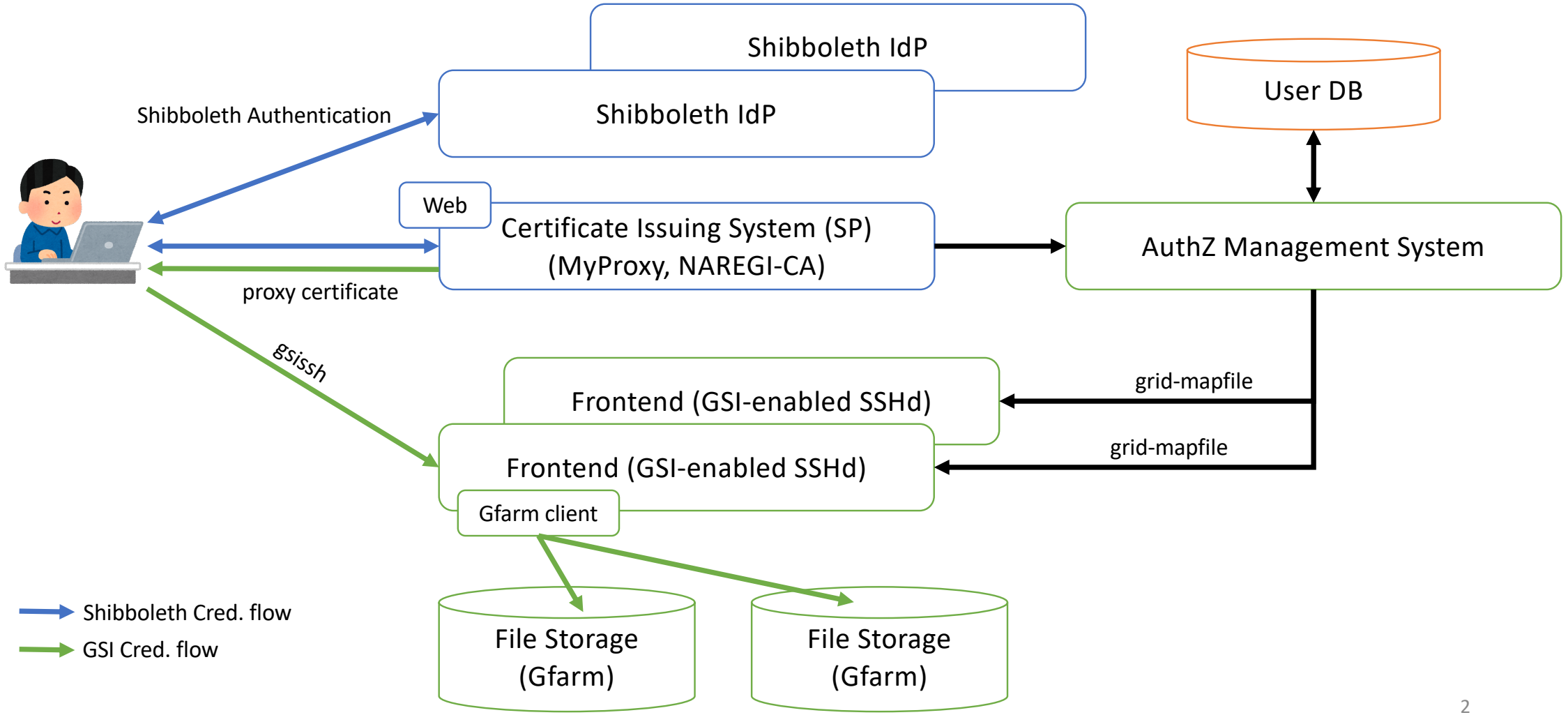
Consideration of Token-based AuthN/Z for Command-line Applications

Eisaku SAKANE <sakane@nii.ac.jp>

National Institute of Informatics

Japan

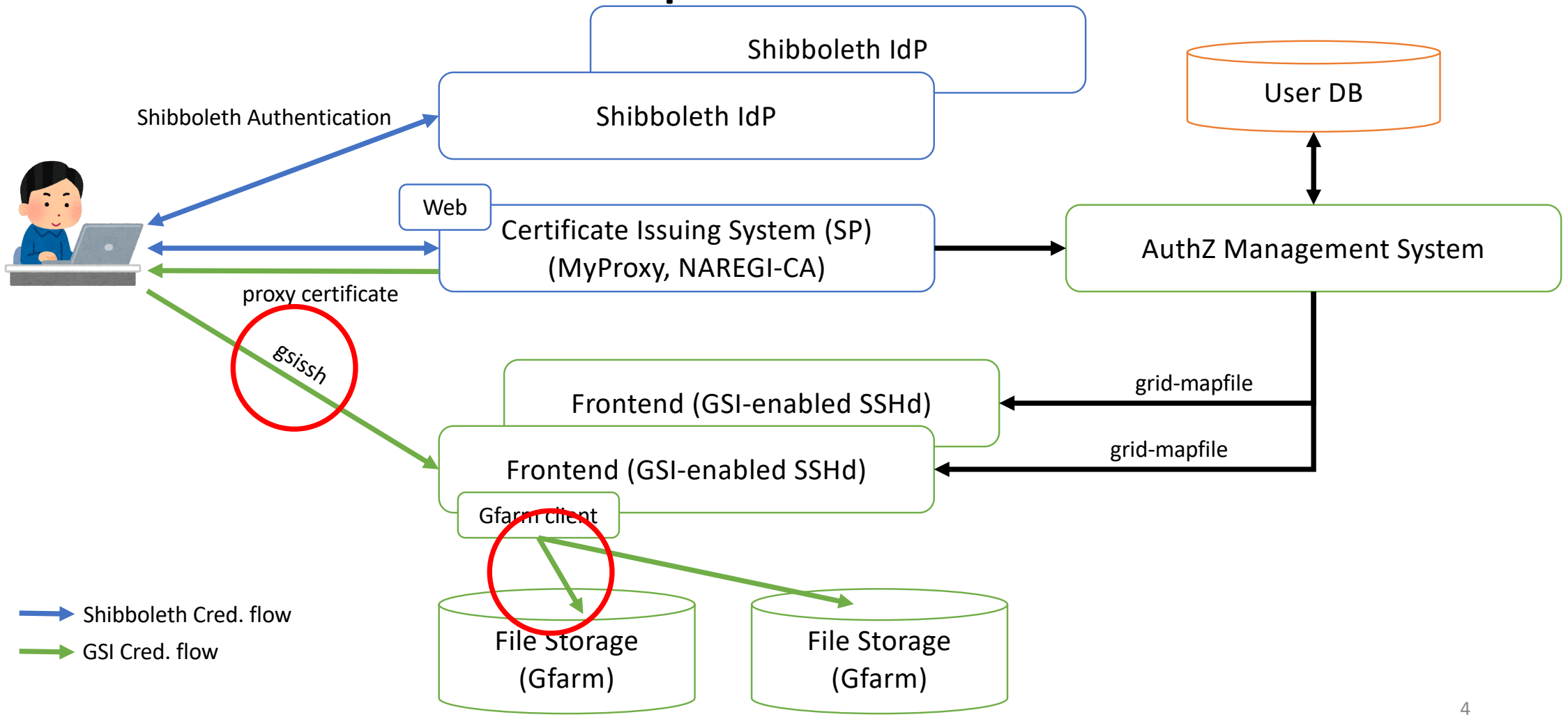
Overview of Current GSI Use Cases in HPCI



GSI-enabled Apps. used in HPCI

- Certificate Issuing System
  - a web service as a Shibboleth service.
  - certificate repository with MyProxy.
- GSI-enabled OpenSSH
  - access to frontends of supercomputers.
- GSI-enabled Gfarm
  - Gfarm is a distributed file system: http://oss-tsukuba.org/en/software/gfarm
  - Gfarm is linked against GSI library and uses proxy certificates for client authentication.

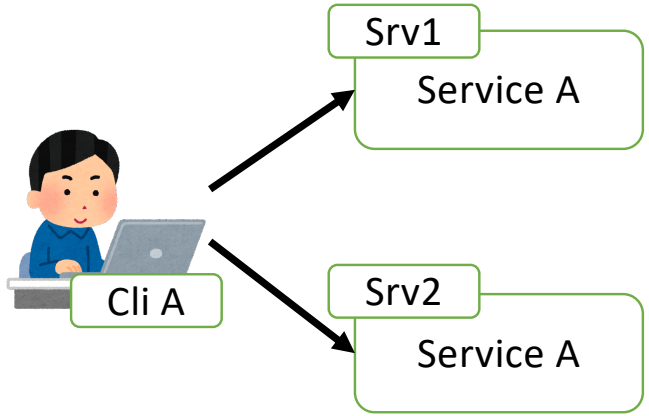
What should we replace GSI with ?

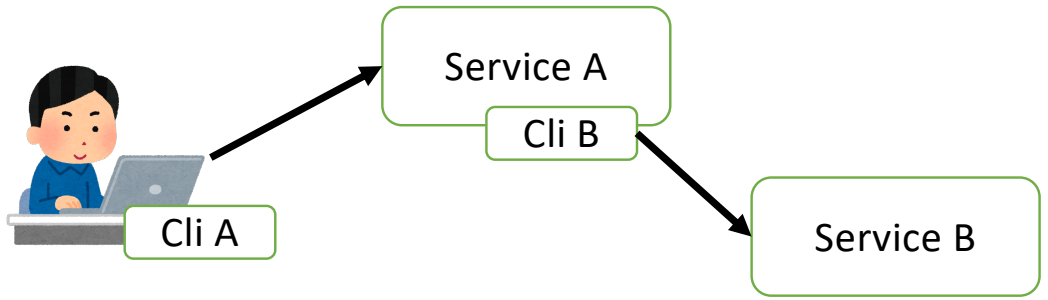


Requirements

- Realize Single Sign-on to supercomputers (SSH) and file storages (Gfarm)
  - No interactive authentication is needed except when user get the first credential.

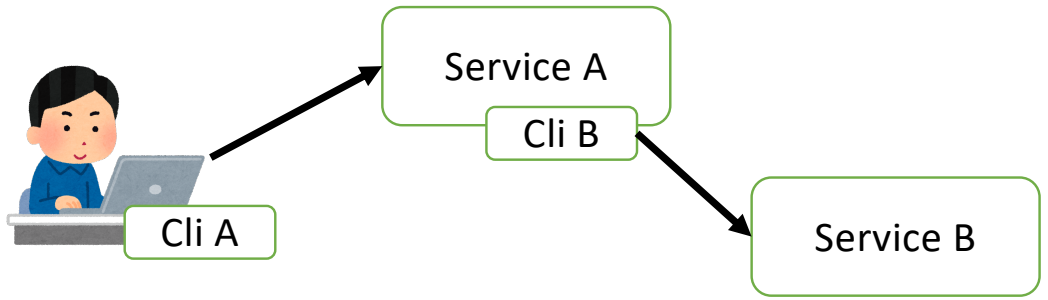
- Types of SSO





Candidate

- OpenID Connect & OAuth
  - realize SSO to Web services with cookie
- Issues
  - How can we do SSO to different command-line applications ?

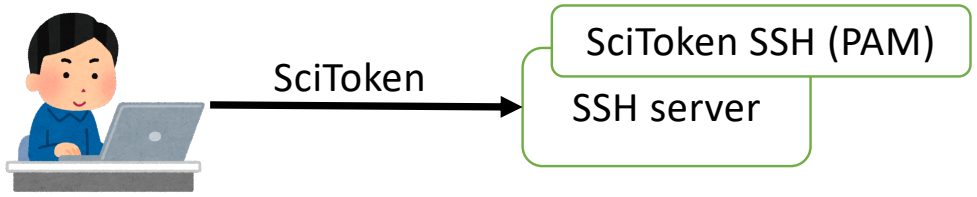


Development Environment

- SciTokens SSH: OAuth-enabled SSH
  - https://scitokens.org/
  - OAuth-enabled PAM module
- KeyCloak
  - https://www.keycloak.org/
  - Access token endpoints
- oidc-agent
  - https://indigo-dc.gitbook.io/oidc-agent/
  - a set of tools to manage OpenID Connect tokens and make them easily usable from the command line

SciTokens SSH

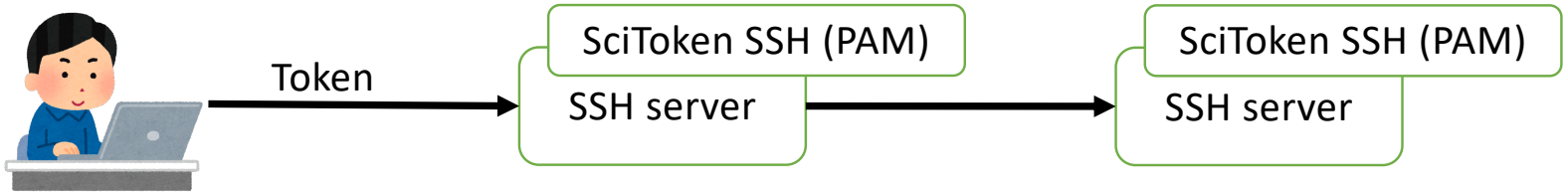
- Based on OAuth-SSH https://github.com/XSEDE/oauth-ssh/
- A PAM module that can handle SciTokens
  - The PAM module does not keep a token on the SSH server.



  - We decided to keep the access token obtained initially on the SSH server.

Prototype for multi-stage SSH connections

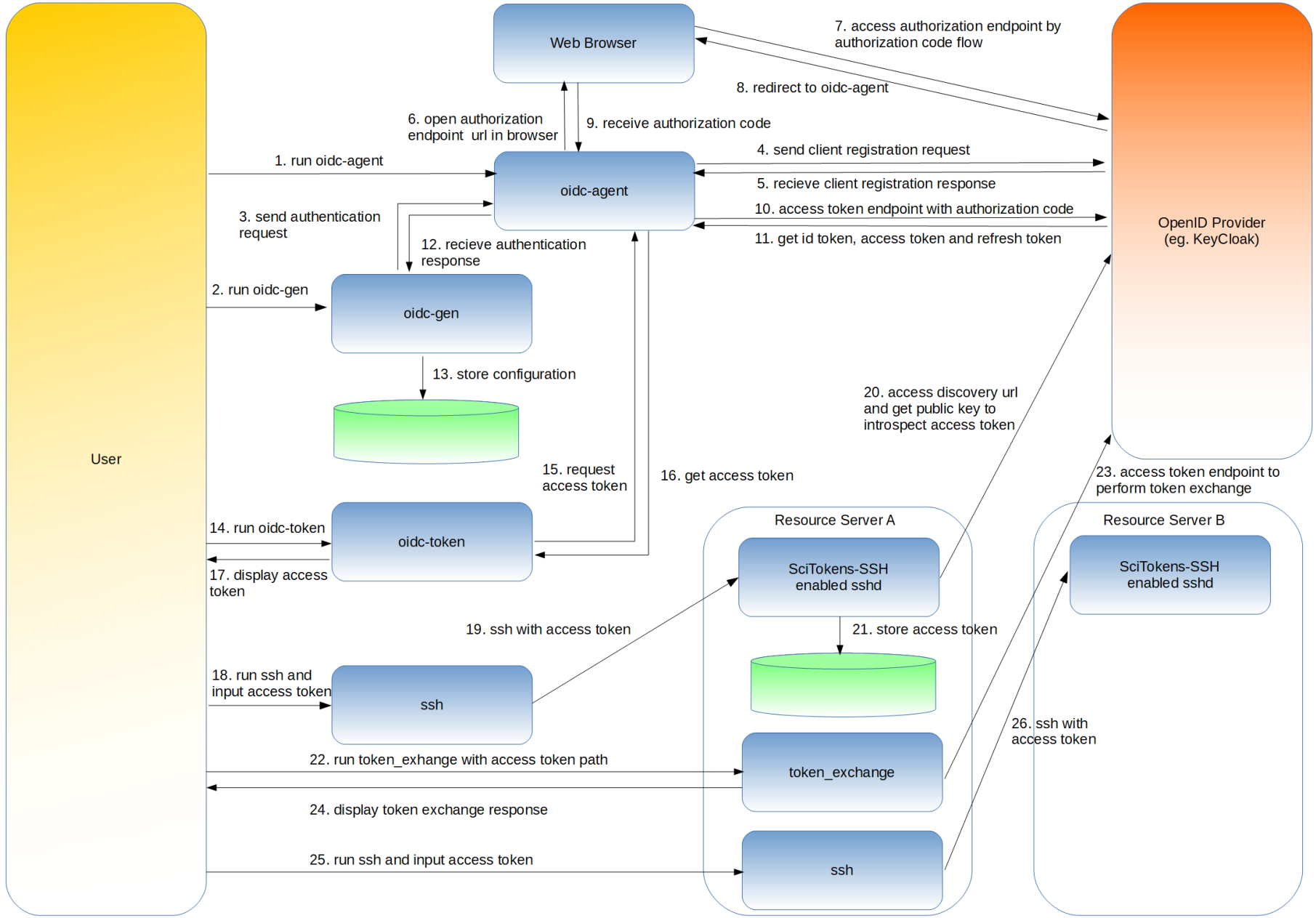
- Scenario
  - User logins to the first SSH server, and from the first SSH server the user logins to the second server.



- Approaches
  - *all-round* access tokens that are accessible to wide services
  - token exchange (RFC 8693)
    - issue access token to each resource server
    - obtain an access token for different resource server from the exist access token with token exchange method

What we have done

- Improved SciToken SSH PAM module
  - to keep the access token used at SSH client authentication,
  - to map the subject claim onto the local account and save mapping information in a file that obeys the same format as OAuth-SSH.
- Developed a token exchange program.
- Confirmed that the *all-round* access tokens approach works.
- Confirmed that the token exchange approach works.
  - KeyCloak supports experimentally the token exchange.


User
Web Browser
oidc-agent
oidc-gen
oidc-token
ssh
OpenID Provider
(eg. KeyCloak)
Resource Server A
SciTokens-SSH
enabled sshd
token_exchange
ssh
Resource Server B
SciTokens-SSH
enabled sshd
1. run oidc-agent
2. run oidc-gen
3. send authentication
request
4. send client registration request
5. recieve client registration response
6. open authorization
endpoint url in browser
7. access authorization endpoint by
authorization code flow
8. redirect to oidc-agent
9. receive authorization code
10. access token endpoint with authorization code
11. get id token, access token and refresh token
12. recieve authentication
response
13. store configuration
14. run oidc-token
15. request
access token
16. get access token
17. display access
token
18. run ssh and
input access token
19. ssh with access token
20. access discovery url
and get public key to
introspect access token
21. store access token
22. run token_exhange with access token path
23. access token endpoint to
perform token exchange
24. display token exchange response
25. run ssh and input access token
26. ssh with
access token

Future work

- There are many many things we must consider…
- design of access token
  - *all-round* access token approach, but only accessible for HPCI services
  - token exchange approach
  - we must evaluate these approaches under security consideration.
- revocation of access tokens
  - how can we do?
- Some technical issues
  - We cannot send access token whose size is equal to or greater than 1024B to SSH server. (related to CVE-2016-6515?)

Comments are welcome !

Thanks !