Development of HPCI AAI in Japan

Eisaku SAKANE <sakane@nii.ac.jp>

National Institute of Informatics

Japan

Development of HPCI

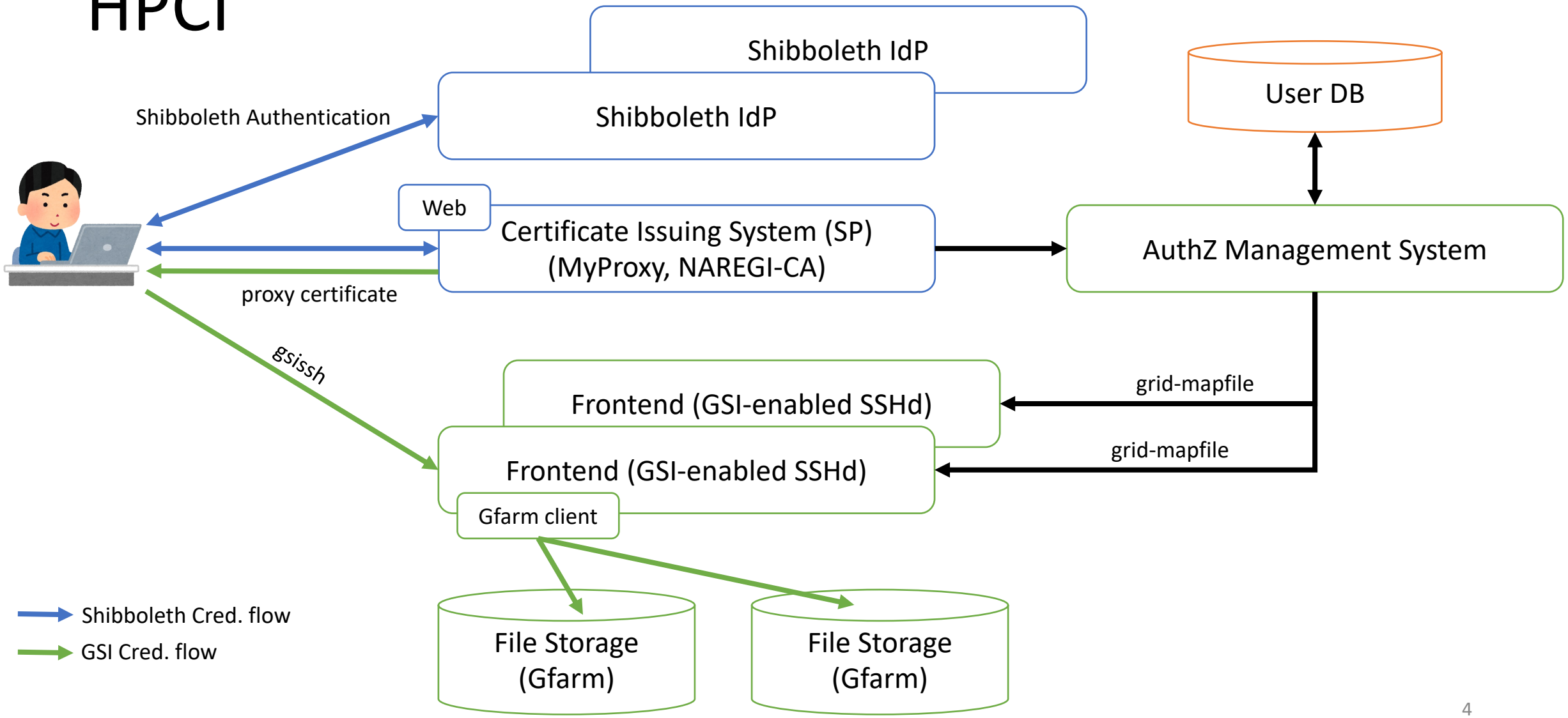
Background

- HPCI: High Performance Computing Infrastructure in Japan
  - composed of super computers that connected with SINET
- Authentication and authorization system in HPCI uses GSI.

- We must replace GSI depending components with the other authentication technology because GSI supports will end eventually.

- We must satisfy the following requirements:
  - Single Sign-on access to resources (computing and file storage)
  - Unchanged in the other components as possible

Overview of Current GSI-based system in HPCI

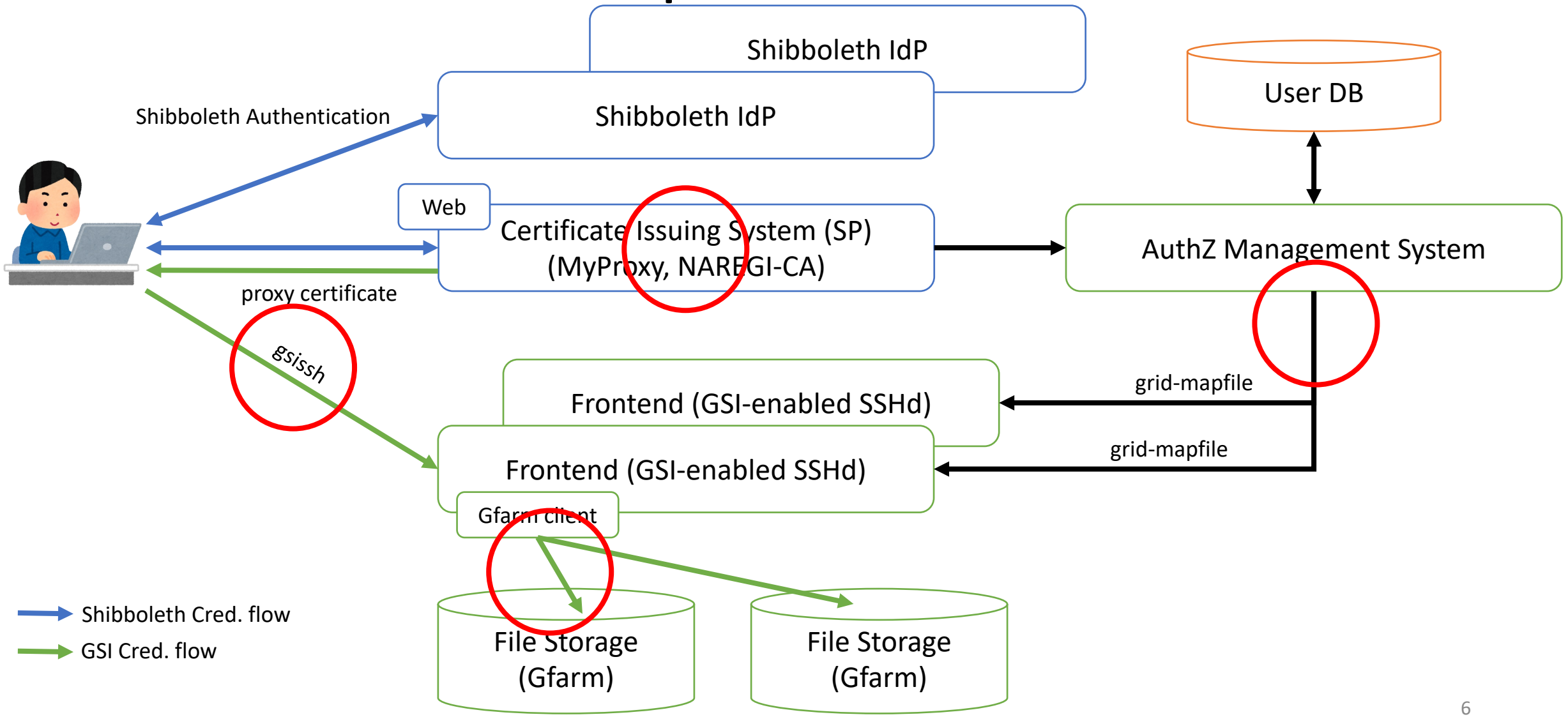


Basic Idea

- We selected OAuth for the next HPCI AA system.
- We migrate smoothly from current GSI-based AA system to token-based AA system.
- System components that use GSI are replaced with those that use OAuth tokens.

- Web services in HPCI continuously use SAML authentication.
  - The X.509/proxy certificate issuing system is a web service with SAML.
  - In this sense, SAML assertion is primary in HPCI.

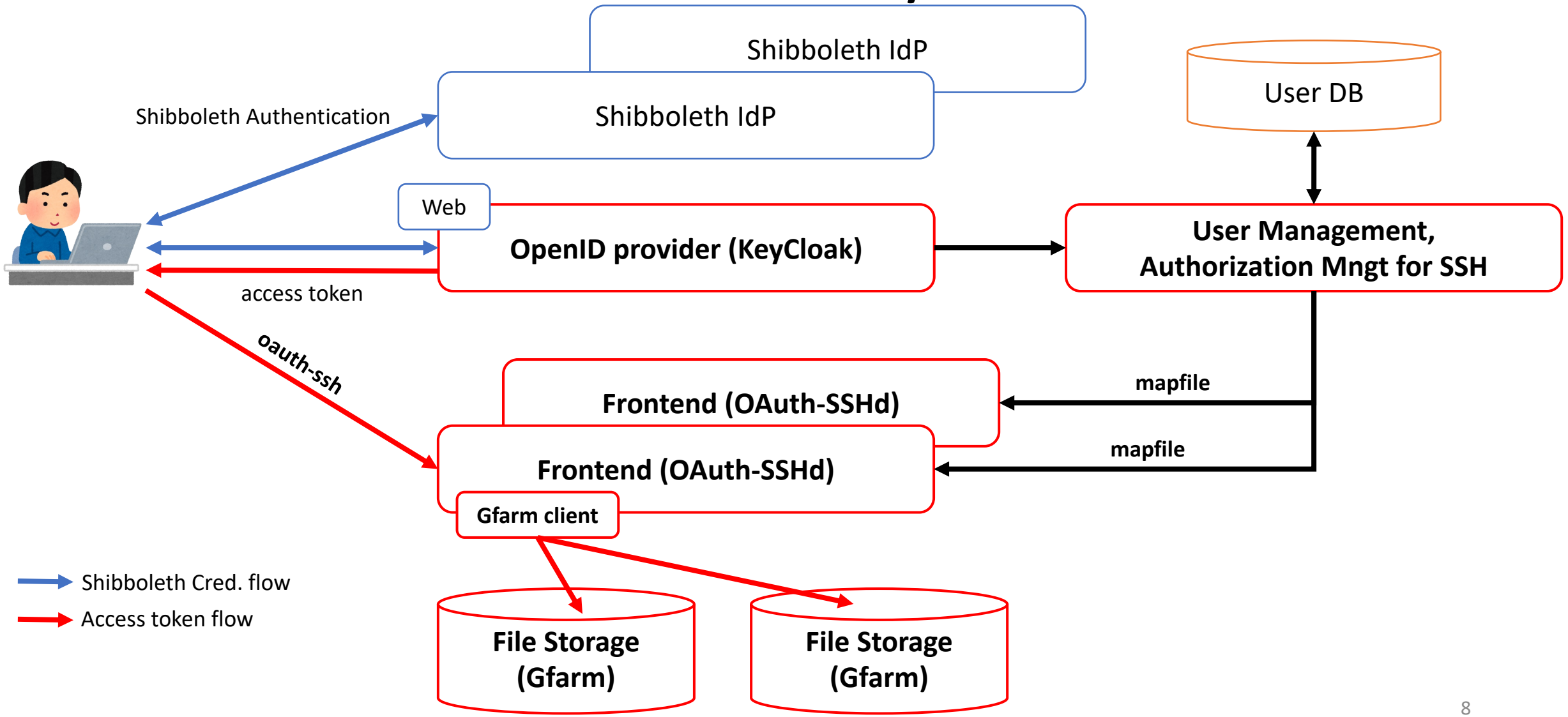
What should we replace GSI with ?



Issues

- How do we authenticate users who the system can issue tokens?
- How do we map the tokens onto the local accounts ?
- What claims should we include access token ?
- We should provide the usability of the same as or more than gsissh and myproxy.

Overview of Token-based system in HPCI



Design & Implementation

- OAuth-enabled SSH: OAuth-SSH (SciTokens SSH)
  - https://github.com/XSEDE/oauth-ssh/

- Access token
- OpenID provider : KeyCloak
- User management : HPCI specfic
- Authorization management for SSH : mapping file provided by OAuth-SSH
- Usability improvement of OAuth-SSH client

Claims in HPCI Access token

Claim	Description
aud	Audience claim defined by RFC 7519, “JSON Web Token (JWT)”
exp	Expiration time claim defined by RFC 7519
hpci.id	HPCI-ID
hpci.ver	Version of HPCI access token
iat	Issued at claim defined by RFC 7519
iss	Issuer claim defined by ditto
jti	JSW ID claim defined by ditto
nbf	Not before claim defined by ditto
scope	Scopes claim defined by RFC 6749, “The OAuth 2.0 Authorization Framework”
sub	Subject claim defined by RFC 7519
ver	Version of the token defined by SciTokens Claims
(the others)	acr, auth_time, azp, sesstion_state, sid, typ (automatically added by KeyCloak)

OpenID Provider & User management

- KeyCloak : https://www.keycloak.org/
- SAML authentication support
  - Identity brokering provided by KeyCloak can use authentication by an external IdP.
  - KeyCloak behaves as a SAML service provider.

- User management
  - creation of KeyCloak account associated with ePPN sent by HPCI IdP
    - obtain user information from HPCI user database
    - operate KeyCloak with REST API provided by KeyCloak

Authorization management for SSH

- Mapping file provided by OAuth-SSH maps the sub claim onto local UNIX account.
  - The sub claim is the name of KeyCloak account.
- Authorization management system for SSH creates a template of mapping file that the front end server uses.
  - obtain user information from HPCI user database.
  - obtain account information from KeyCloak.
  - combine the sub claim and UNIX local account via HPCI-ID.
  - finally create a template of mapping file.

Usability improvement of SSH client

- We developed the following functions:
  - Simplifying acquisition of access token
  - Automatically input of access token at SSH login

- Simplifying acquisition of access token
  - use the oidc-agent : https://github.com/indigo-dc/oidc-agent
  - based on “Device Authorization Grant”
- Automatically input of access token at SSH login
  - use the sshpass : http://sshpass.sourceforge.net/
  - develop wrapper shell scripts
    - oidc-ssh, oidc-scp, odic-sftp

Discussion

- All round access tokens vs access token for each service
  - Token exchange approach can be used for token for each service.
- Prohibition of Password authentication of KeyCloak (not SAML)
  - It seems that KeyCloak cannot be restricted to SAML authentication only.
- Consideration of validity period of access and refresh tokens and revocation flow if needed.

Summary

- We designed and implemented a token-based AAI for HPCI.
  - Access token (claims)
  - OpenID Provider: Keycloak with SAML
  - User management
  - Authorization management for SSH: mapping file creation
  - Usability improvement of OAuth-SSH client: oidc-agent, sshpass, wrapper scripts

- We plan to evaluate the token-based AAI in FY2022
  - build the AAI on the production environment in FY2023
  - start full-scale operation in FY2024

Development of GakuNin

Background

- Necessity for a new trust framework in Japan
  - GakuNin has provided a stable trust framework to academia in Japan.
  - There are research communities in Japan, but they don’t always rely on IdPs in GakuNin because all GakuNin IdP do not satisfy the requirement of the communities.
  - As a result, a trust framework has been formed in each research community.
  - Many of users in the research communities are also members of IdPs that join GakuNin.
  - It is natural for users to demand to use home organization account for services in the research communities.

  - In order to solve the situation, we have launched a new working group in GakuNin.

Goal

- The goal of the working group is to build a new trust framework focused on identification and authentication:
  - useful for research communities in Japan,
  - collaborating business sector,
  - promoting international collaboration,
  - interoperable with the IGTF Authentication Assurance Profiles as well as the REFEDS Assurance Framework.
- Software development
  - Authentication proxy service
    - support for the new GakuNin trust framework,
    - bridge between IdPs and SPs,
    - enabling IAL/AAL management and attribute assurance.

GakuNin IAL2/AAL2

- The results of the working group for the next generation of IAM federation
  - Proposals: Operation policy of IAL2/AAL2 in the next generation of GakuNin (in Japanese)
    - Stakeholders, RIKEN, NIMS, RCOS, HPCI, now are reviewing the proposals
  - CrP/CrPS sample
- The future plan
  - publishing the policies version 1.0,
  - checking the interoperability with existing trust framework such as RÉFEDS and IGTF,
  - conducting experiments in the implementation of new trust framework and evaluating the results.

Future Work

- Interoperability with IGTF Authentication Assurance
  - We want to prove that GakuNin IAL2 is interoperable with the IGTF AA.
  - What should we do ?
    - We should translate the GakuNin IAL2 document into English.
    - We must compare the GakuNin IAL2 with the IGTF AA. How should we do ?

- We would like to collaborate with IGTF !!