Development in HPCI and GakuNin

Eisaku SAKANE

National Institute of Informatics, Japan

Contents

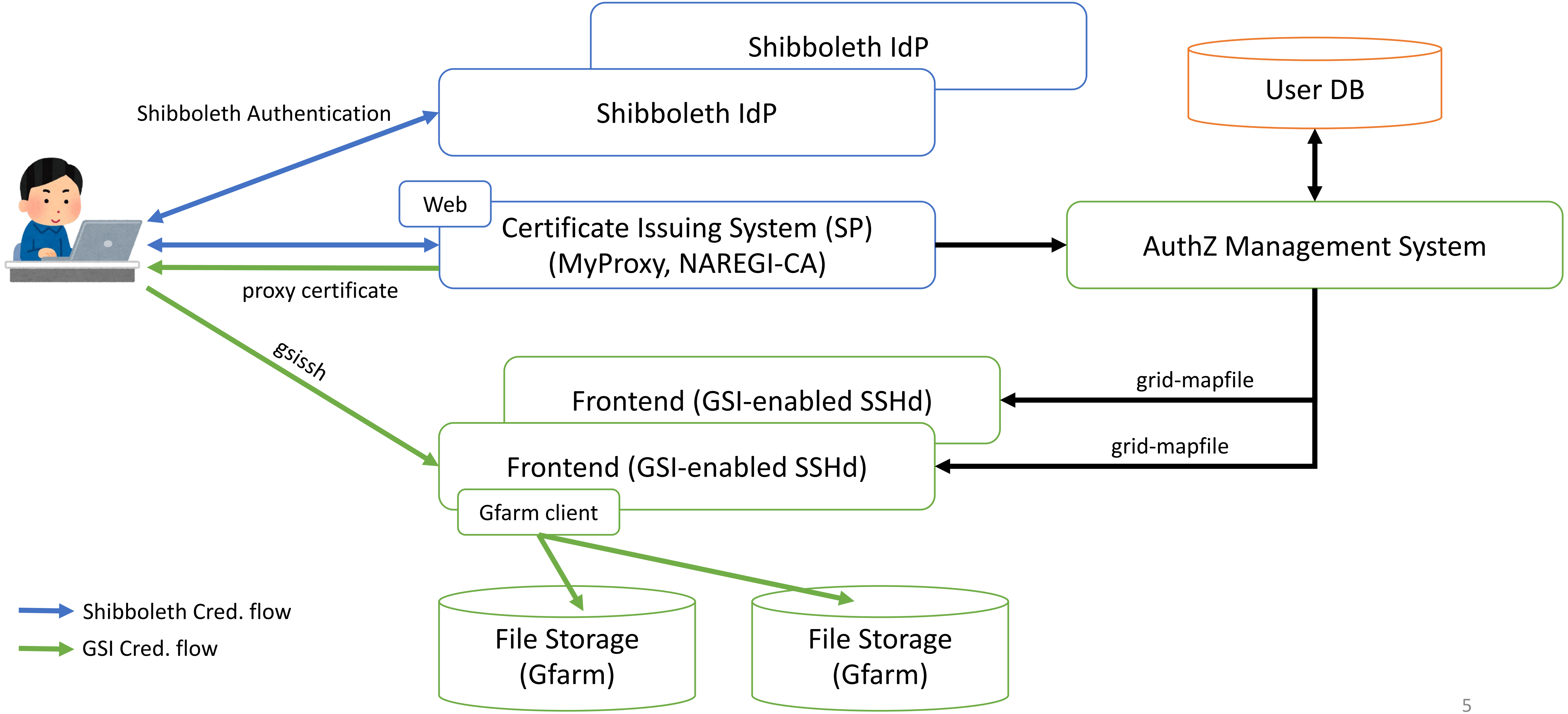
- Development in HPCI
  - Token-based AAI
- Development in GakuNin
  - New trust framework

Development in 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

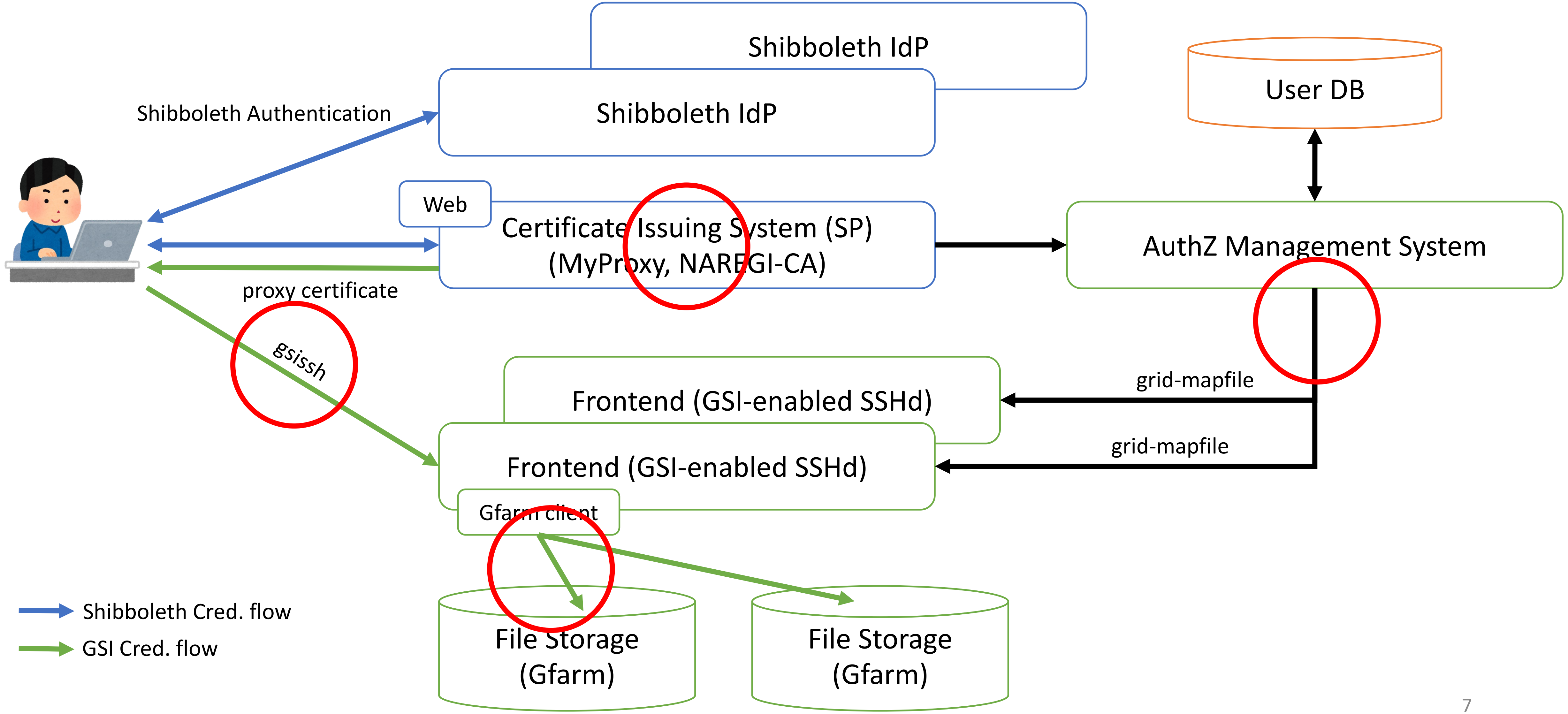


Basic Idea

- 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.

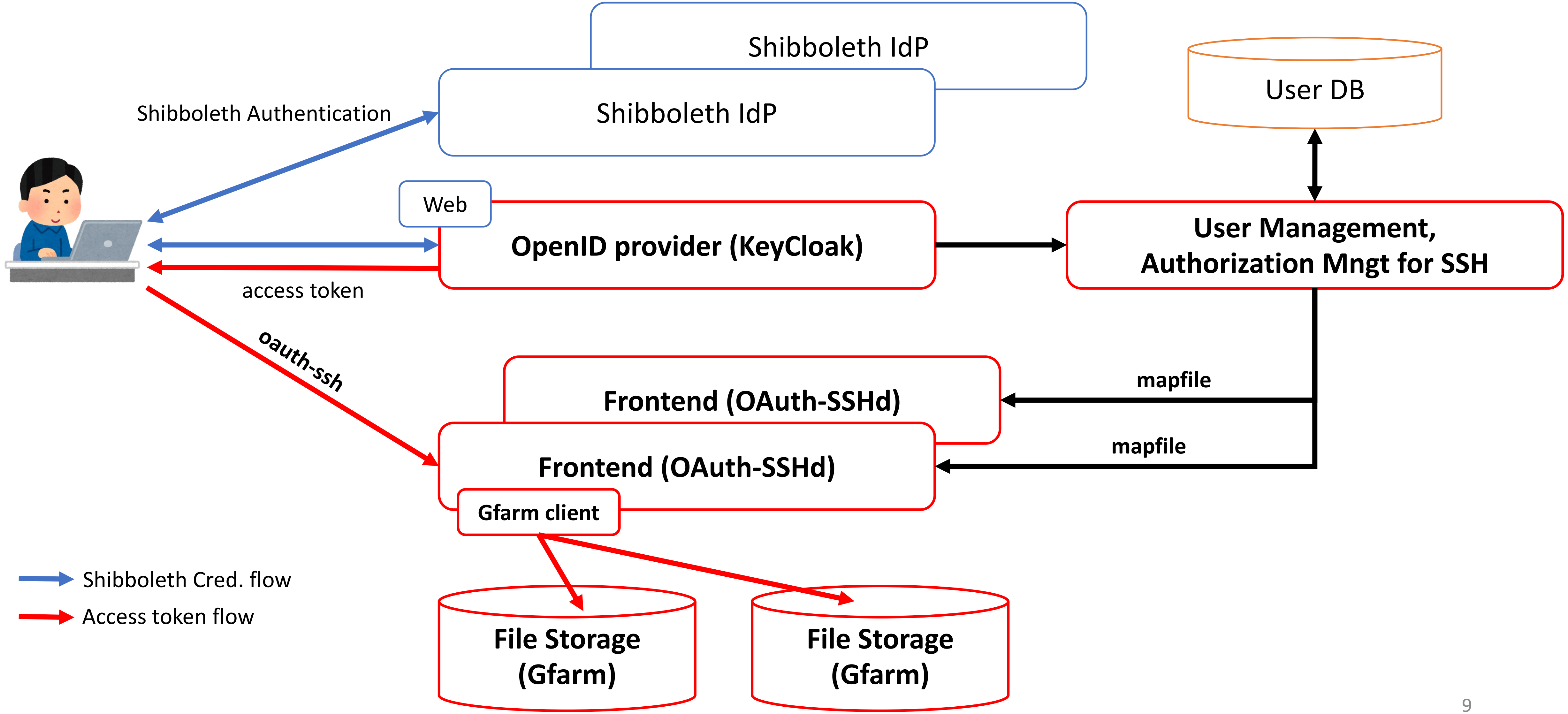
What should we replace GSI with ?



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

HPCI Access token

- All around access token
- 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 *hpci.id* claim onto local UNIX account.
    - The hpci.id claim has the value of the identifier of HPCI user.
- 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 hpci.id claim and UNIX local account.
    - 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”
  - Client type: Public – not distinguishing clients
- 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

Now in progress

- Consideration of validity period of access and refresh tokens and revocation flow if needed.

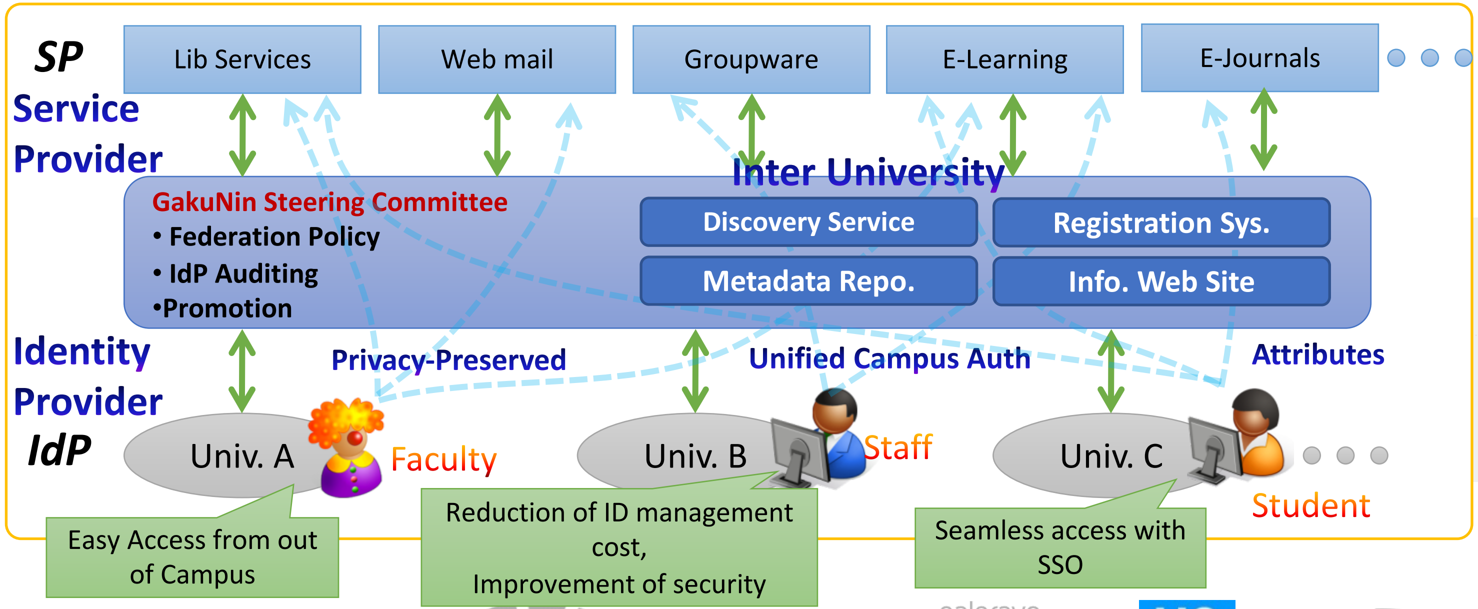
- We are building the AAI environment for the production operation in FY2023.
- We plan to start the production operation in FY2024.

Development in GakuNin

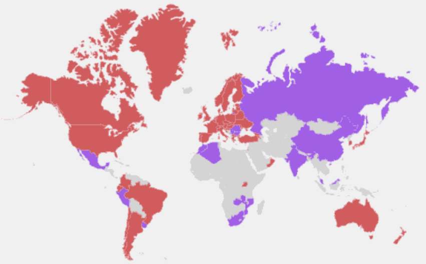
A new trust framework supporting more research communities in Japan

GakuNin Academic Identity Federation in Japan

- Build up new ICT infrastructure to support R&E based on SSO technologies
- Provides trust framework (technologies, policies and assessment)
- Offers value added services (academic discount, etc.) by collaboration with commercial
- Improves usability and security with continuous R&D (including multifactor/cert. auth.)



Academic Federations have been established per country basis



Background

- Necessity for a new trust framework in Japan
    - GakuNin has provided a stable trust framework to academia in Japan.
    - There are many 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 constituent 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 other words, users shouldn’t want to manage several accounts.

    - 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,
  - ensuring world-wide interoperability.

Request from Research Communities

- Authenticating users that don’t have suitable IdP accounts.
  - Users that RC offers services not always possess the account of an IdP joining GakuNin.
  - RC want to rely on IdP that provides sufficient identity assurance.
- Grasping authenticator level
  - Password only or multi-factor authentication
  - For certain services RC want users to impose MFA.

- Identification user that belongs to several organization.
- Ensuring user identity moving between different organizations.
  - SP want to provide continuously and efficiently services to users moving between different organizations.
- Support for suitable attributes for purpose
  - e.g., grasping whether resident or not (export control)

Key Components in New GakuNin Trust Framework

GakuNin IAL/AAL

- Stipulation of IAL and AAL

Authenticator Registry

- Evaluation of authenticators based on GakuNin AAL

Authentication Proxy Service "Orthros"

- AL matching, credential bridging, attribute coordination

IdP Hosting Service

- Addressing issues of IdP building and operation

Advanced Group Management

- Support for high and complex authorization control

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/English)
  - CrP/CrPS sample (in Japanese/English)
  - Documents are available from https://meatwiki.nii.ac.jp/confluence/x/JoSfBQ
- Now in progress
  - being reviewed by stakeholders; RIKEN, NIMS, RCOS, **HPCI**,
  - 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.

Collaboration with IGTF

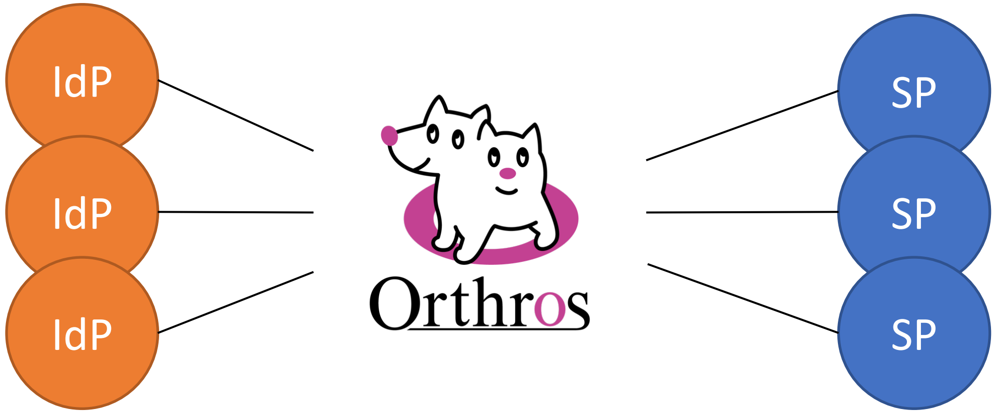
- Interoperability with IGTF Authentication Assurance
  - We want to ensure that GakuNin IAL2 is interoperable with the IGTF AA.
  - What should we do ?
    - We should translate the GakuNin IAL2 document into English. Already done.
    - We must compare the GakuNin IAL2 with the IGTF AA.
    - We will make a report on the interoperability between IGTF and GakuNin later.

Authenticator Registry

- Purpose
  - Evaluate authenticators based on GakuNin AAL, publish the results, and promote multi-factor authentication support for IdPs of universities and research institutions
- FY2022
  - Formulated authenticator evaluation criteria (document preparation)
  - Established authenticator registry operation system (documentation)
- FY2023
  - Starting trial operation
    - MS Authenticator/Google Authenticator
    - UPKI (PKIX) client certificate
    - others

Authentication Proxy Service “Orthros”

- Support for the new GakuNin trust framework
- Bridging between IdPs and SPs, and enabling IAL/AAL management and attribute assurance.
- FY2022
  - Prepared migration from OpenIdP
  - Developed systems and procedures for production-level operation
- FY2023
  - OpenIdP migration
  - External IdP linkage
  - Home IdP binding due to change of organization
  - Support for new GakuNin IAL/AAL policy
  - Enhancement of authorization attributes handling



IdP Hosting Service

- Future Vision of GakuNin
    - All universities and research institutes nationwide participate in GakuNin.
    - Fundamental ID infrastructure for researchers and students
- R&D for supporting the diversification of operation modes, and improving operational efficiency.
- FY2023
    - Demonstrative experiment starts this March.