KEK IdP: Production Deployment and Future SSO Strategy for CRC Services

Konomi Omori
Computing Research Center, KEK

FJPPN - Japan-France workshop on computing technologies
10 - 11 February 2026

Introduction

- KEK has been working to enable federated authentication with other academic institutions by joining **GakuNin**, Japan's academic authentication federation.

- By participating in GakuNin, users can access services provided by other member institutions using a single institutional account.

- The Identity Provider (IdP) built for GakuNin is also expected to enable **single sign-on (SSO)** across **KEK CRC services**.

About GakuNin: Japan's Academic Authentication Federation

- **GakuNin** is Japan's academic authentication federation.
  - Managed by the National Institute of Informatics (NII).
  - It enables cross-institutional **SSO** using **Shibboleth**.
    - **Shibboleth** is middleware that implements **SAML (Security Assertion Markup Language)**.
- **GakuNin can connect with eduGAIN** to share services with the European Academic Access Management Federations.
- In GakuNin, there are two key components:
  - **Identity Provider (IdP)** :
    Handles authentication for each institution.
    It filters and provides user attributes to **Service Provider**s after authentication.
  - **Service Provider (SP)** :
    Offers services and uses the IdP for authentication.

cooperate

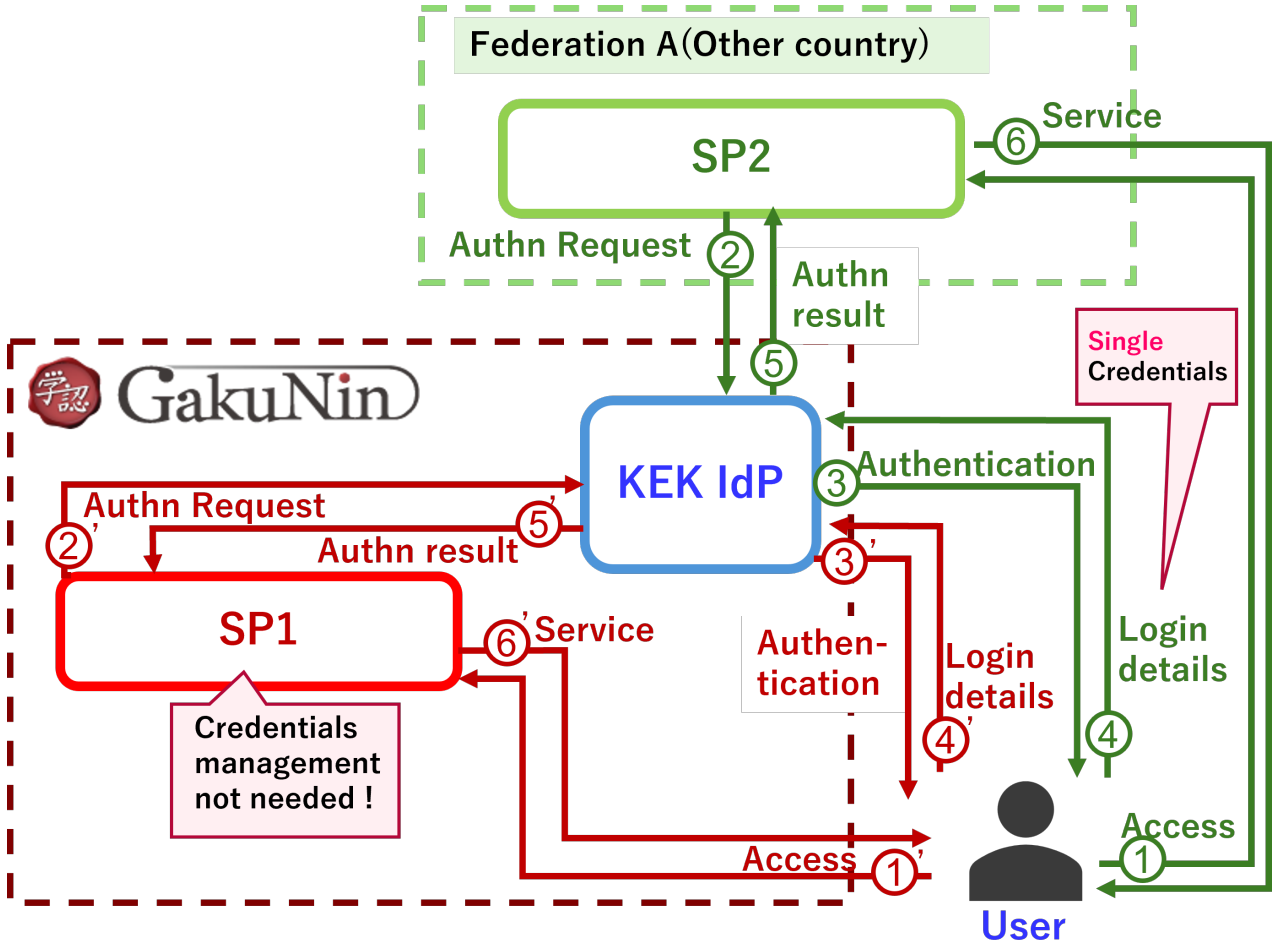
Benefits of Federation Participation

Usability (better user experience)

- Users can seamlessly access multiple GakuNin / eduGAIN-federated services using a single set of credentials.
- Users only need to remember and manage a single set of credentials from their home institution, improving both usability and security.

Security

- Authentication strength at each SP is aligned with the security level of the IdP.
- SPs no longer need to manage user credentials locally, reducing the risk of security incidents.



Updates from FJPPL 2025

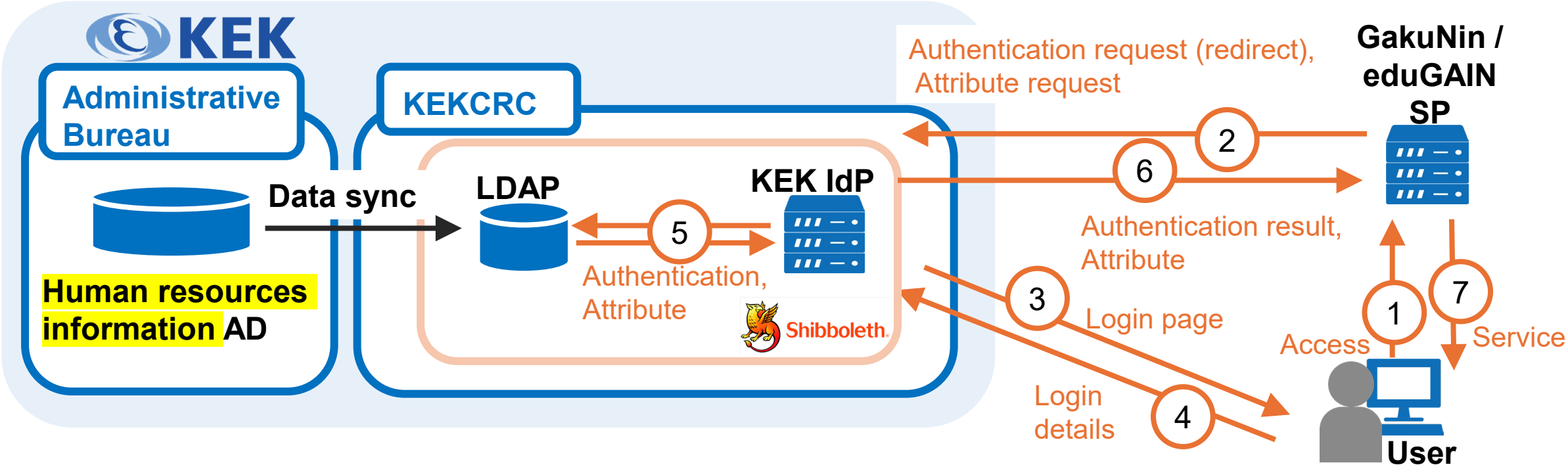
Previous Report

- We presented our plan and testing for joining GakuNin at the previous FJPPL workshop.
  - https://indico.in2p3.fr/event/35206/

Updates

- The production IdP server (KEK IdP) has been successfully deployed.
- KEK has officially joined GakuNin, and the IdP is now connected to eduGAIN.
- Distribution of GakuNin accounts to KEK users has begun.
- We have started planning the next steps.
  - Integrate authentication of KEK CRC services using the KEK IdP.
  - Enable selected KEK CRC services to be federated via GakuNin and eduGAIN.

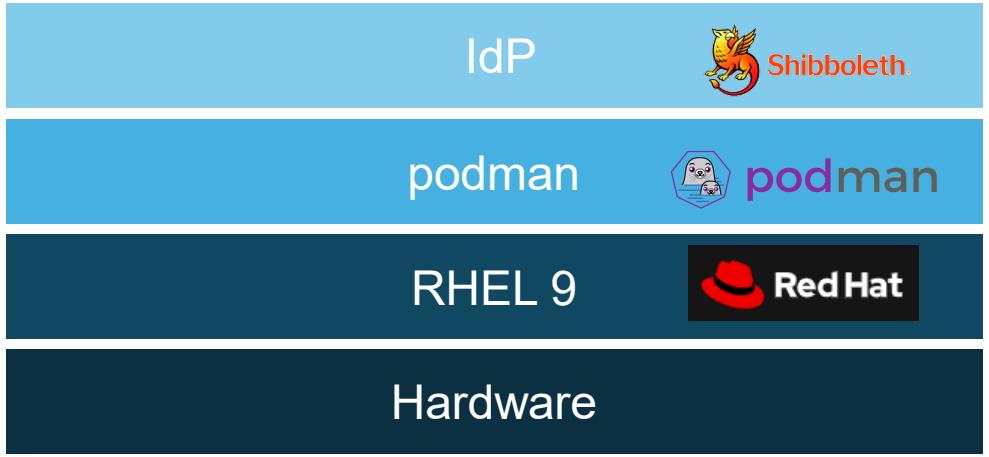
KEK IdP System Overview



- When a KEK user accesses a SP, the SP redirects the user to the KEK IdP and requests authentication.
- User information in LDAP is synchronized from Active Directory (AD) which is managed by the Administrative Bureau.
  - This AD serves as the source of up-to-date human resource attributes required by the IdP.

Technical Stack of the KEK IdP

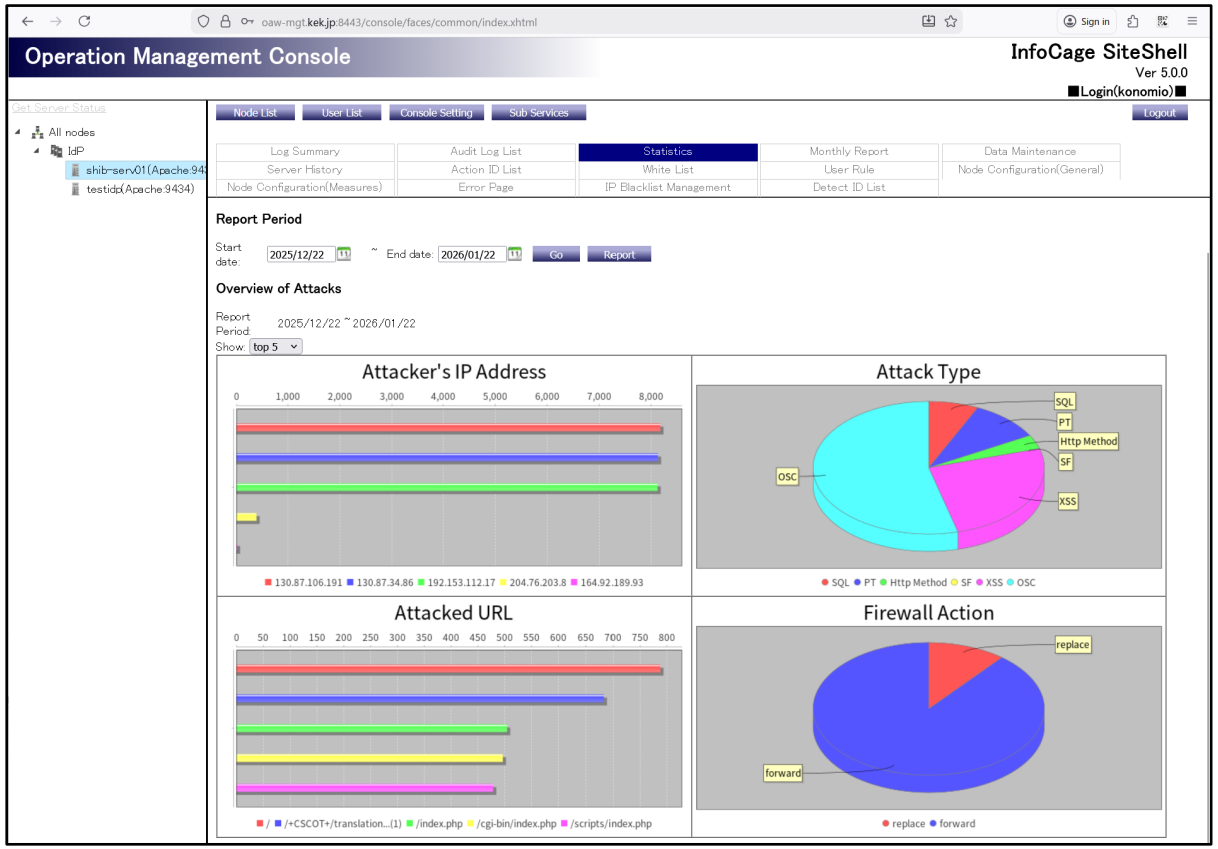
- The KEK IdP is deployed using **container technology**.
  - Designed to be easily updated and scaled using container images.
  - We successfully completed a smooth migration from the test environment to production.
- The server is built using **Shibboleth v5 (**the latest major release**)**.
- The KEK IdP is integrated with a dedicated LDAP for user information and attribute release.
- All configurations are managed via **Git** to ensure reproducibility and traceability.



KEK IdP server configuration diagram

Security Measures for the KEK IdP

- Since the KEK IdP is accessible from the Internet, security is critically important.
  - Implementing a **Web Application Firewall (WAF)** to protect against common web vulnerabilities.
  - When an attack is detected, the WAF performs defensive actions, such as forwarding traffic from the source IP address to an alternative page.
  - Attack logs can be monitored in real time via a **web-based management UI**.



Authentication of the KEK IdP

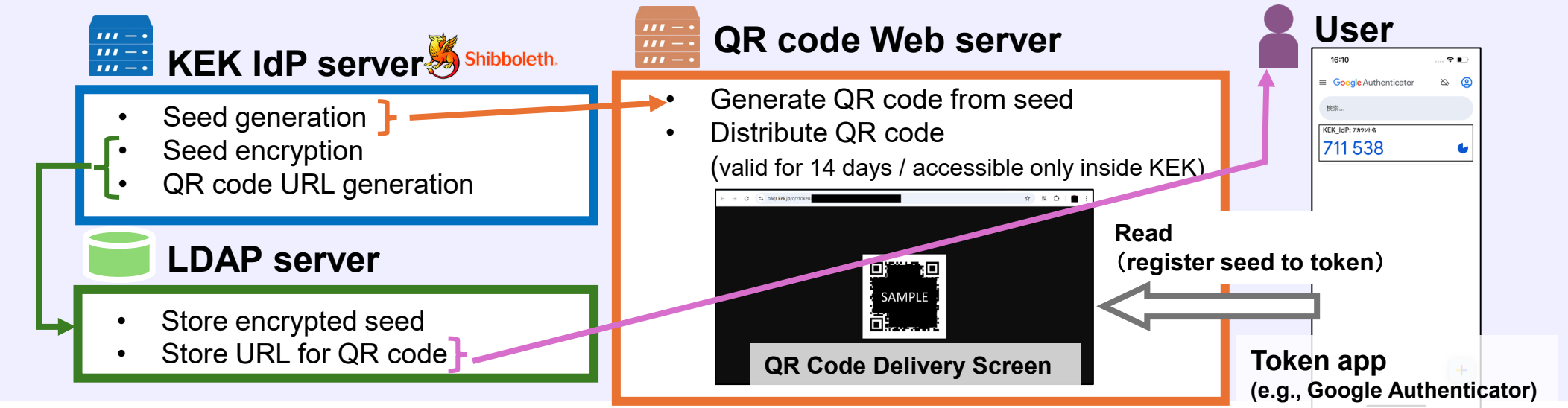
- The KEK IdP uses **two-factor authentication (2FA)**, combining a **password** and a **one-time password (OTP) generated by a smartphone**.
  - OTP is implemented by adding a **TOTP plugin** to Shibboleth.
  - The OTP seed is generated and encrypted by the IdP.
  - The seed is stored in LDAP.

User side:

- Users register the seed on a TOTP-compatible app (token app).
- The app generates OTPs for login.

QR code distribution:

- The QR code contains the seed and can be scanned for registration.
- A web server distributes QR codes with an expiration date, accessible only from the KEK internal network.



Current Status of KEK IdP

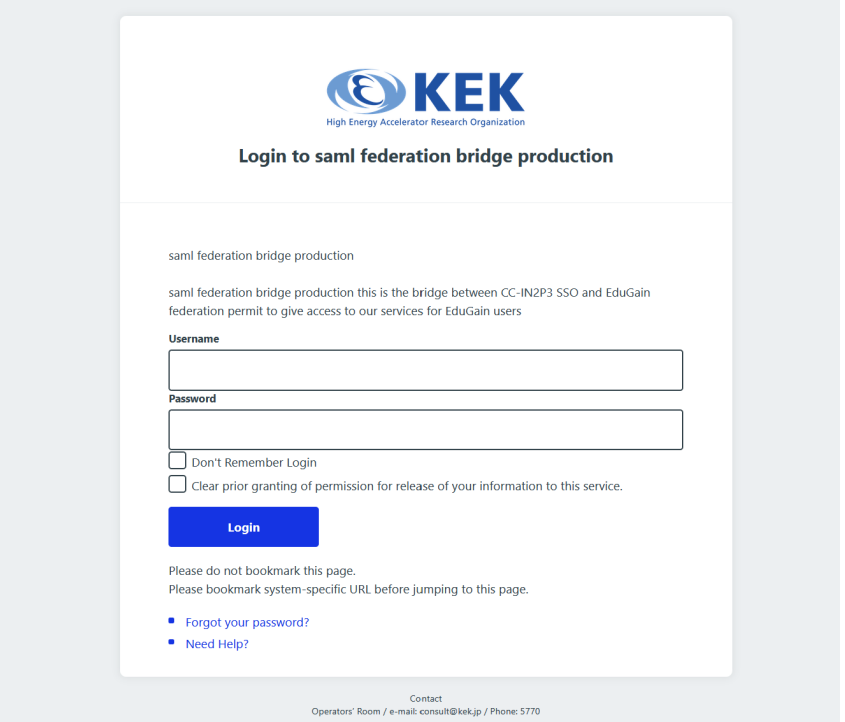
- The KEK IdP completed participation in **GakuNin** and integration with **eduGAIN**, and entered production in November 2025.
  - Total KEK IdP accounts issued： 28

GakuNin:

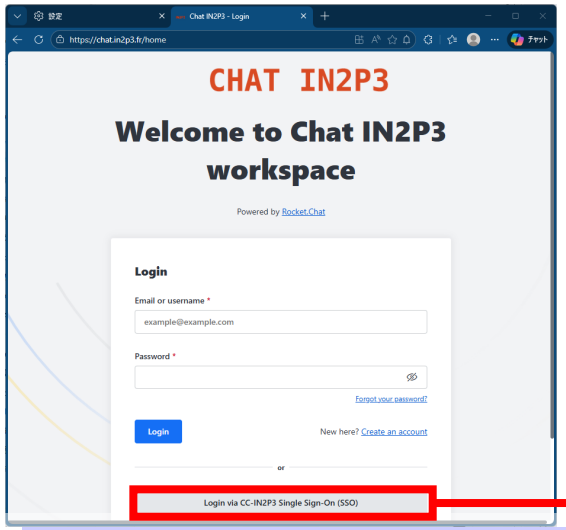
- We have started using the “EduroamJP Authentication Federation ID Service.”
  - This service eliminates the need to issue and manage separate eduroam accounts at KEK CRC.
- We are testing “GakuNin RDM” for future use.
  - This will enable collaborative management of research data with other institutions.

eduGAIN:

- The KEK IdP is now integrated with SSO services at CC-IN2P3, CERN, and DESY.

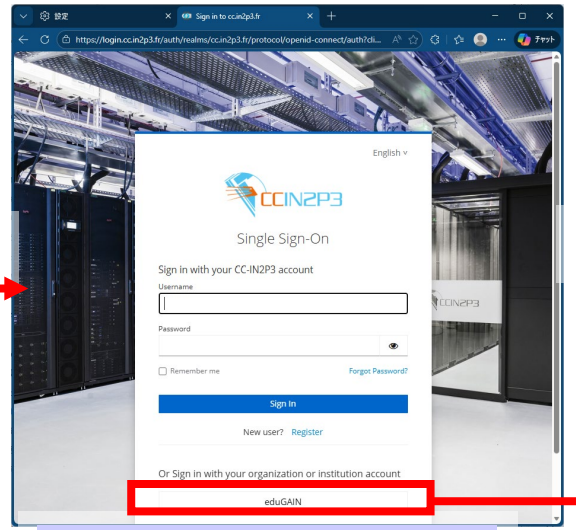


Current Status: Integrated with CC-IN2P3 Services



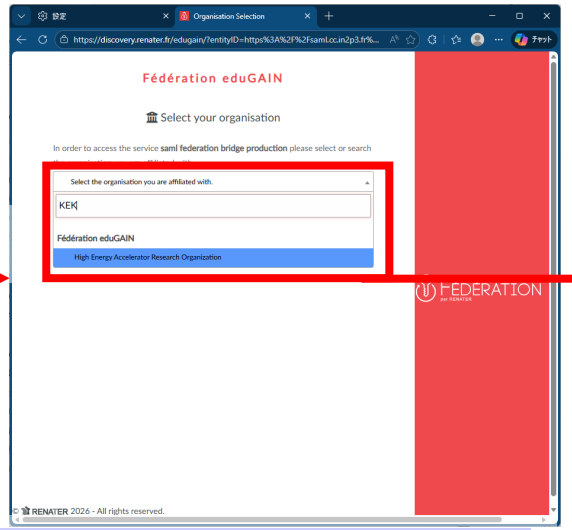
CHAT IN2P3 Login page

redirect



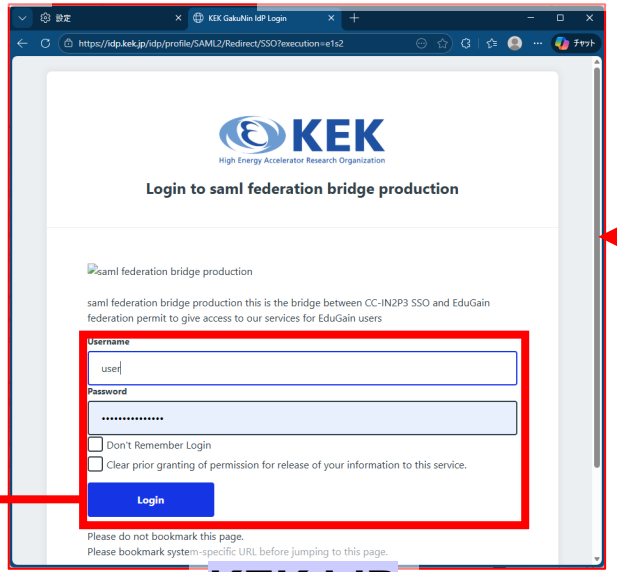
CC-IN2P3 SSO page

redirect



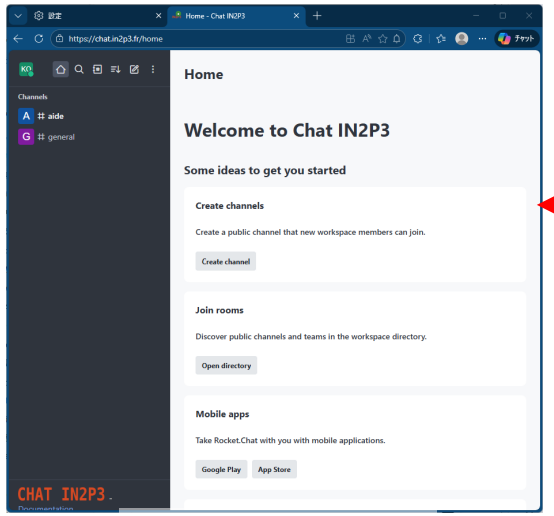
eduGAIN bridge service

redirect



KEK IdP

redirect



CHAT IN2P3

GakuNin IAL2/AAL2 Support

- Identity Assurance Level (**IAL**) / Authentication Assurance Level (**AAL**): Standards for identity verification and authentication. (NIST SP 800-63)
- KEK IdP IAL/AAL:
  - **IAL2**: Account information is obtained from AD based on personnel information.
  - **AAL2**: Two-factor authentication using TOTP is implemented.
- Currently, GakuNin has no mechanism to verify and certify that an IdP complies with IAL2/AAL2.
- GakuNin is running a phased pilot project to evaluate and support IAL2/AAL2.
  - KEK joined the project in 2026.
- After the completion of the pilot project, we initially aim to use GakuNin authentication instead of GRID authentication for GRID users who have GakuNin accounts.
  (GRID requires IAL2-level identity verification at account issuance.)

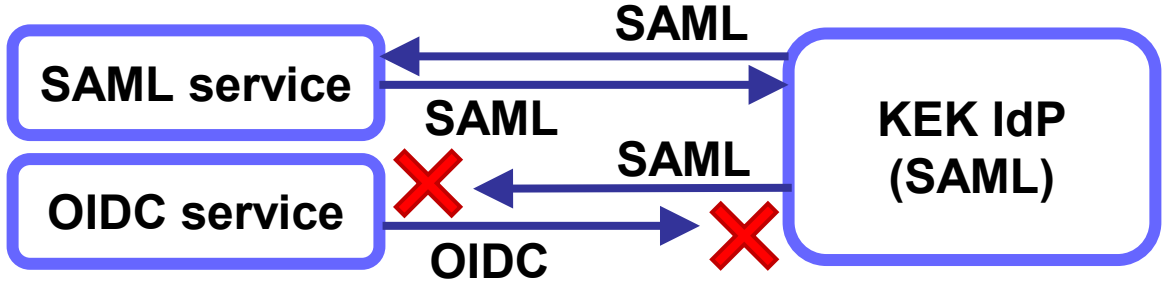
Next Steps: Seamless Access to All CRC Services

Goal:

- We aim to integrate authentication and account management for all KEK CRC services into the **KEK IdP** to enable **SSO**.
- We also aim to provide KEK CRC services to external institutions via **GakuNin** and **eduGAIN**.

Technical Challenges :

- KEK IdP supports **SAML only** (Shibboleth).
- Many modern services use **OIDC (OpenID Connect)**.
- Direct integration between the SAML IdP and OIDC services is not possible.



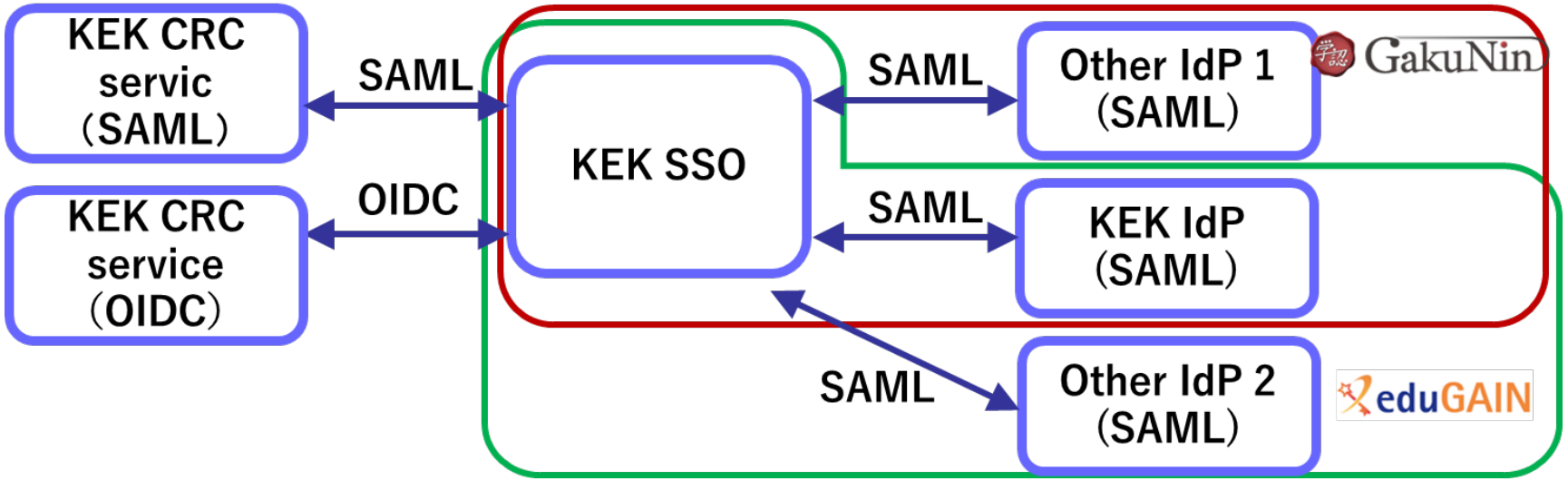
Operational Challenges :

- Registering each service as a SP in GakuNin/eduGAIN is operationally complex.

Design of KEK SSO

To enable SSO for KEK CRC services using the KEK IdP, we are designing a new system called “KEK SSO.”

- KEK SSO handles authentication for selected KEK CRC services, independent of each service’s protocol (such as **SAML** or **OIDC**).
- KEK SSO performs protocol translation between KEK CRC services and GakuNin/eduGAIN IdPs.
- Once users authenticate via KEK SSO, they can access other KEK CRC services without re-authentication.
- By registering only KEK SSO as a SP in GakuNin/eduGAIN, users will be able to access KEK CRC services using their GakuNin/eduGAIN IdP accounts.



KEK SSO Technology Candidate 1: Keycloak

- Keycloak is an open-source Identity and Access Management (IAM) solution.
  - Provides SSO to organization's applications.
  - Uses standard protocols such as OIDC and SAML.
  - Supports external Identity Providers (IdP) and social logins.
  - A growing usage in academia and research institutes. (e.g., CERN)

➢ We set up Keycloak for testing and confirmed that it can be integrated with the KEK IdP.
  ➢ To our understanding, Keycloak does not provide a built-in **discovery service** (to select and identify a user's home IdP), and relies on an external discovery service for this function.
  ➢ We have not yet found an implementation example of a GakuNin-provided, eduGAIN-compatible discovery service for use with Keycloak.

KEK SSO Technology Candidate 2: INDIGO IAM

- INDIGO IAM is an open-source Identity and Access Management (IAM) solution.
  - There are operational examples integrated with **eduGAIN**（e.g., IRIS IAM）.
    - It can **automatically retrieve metadata including IdP information,** from eduGAIN.
    - It can provide a custom IdP discovery UI using this metadata.
  - INDIGO IAM is already in production in the **KEK GRID system**, so we can leverage our operational experience.
  - However, INDIGO IAM cannot act as a SAML IdP. If a CRC service supports only SAML, an additional bridge service would be required.

⇒INDIGO IAM appears to be a strong candidate for KEK SSO, but further evaluation is needed.

In 2026, we will continue testing both INDIGO IAM and Keycloak for KEK SSO.

Summary

- KEK IdP is now in production and integrated with GakuNin and eduGAIN.
- KEK is engaged in the GakuNin IAL2/AAL2 pilot project to establish a foundation for future high-assurance and GRID authentication.
- We have started design work for the **KEK SSO** system to support SSO integration for KEK CRC services.
  - **Keycloak** and **INDIGO IAM** are being evaluated to **bridge the gap between SAML and OIDC protocols**.

- In 2026, we will continue SSO implementation for KEK CRC services and further integration with academic federations.