



What could Keycloak be for International Research?

KeyConf26 Prague

Hannah Short*, Berk Balci, Juliette Bricot, Sebastian Lopienski, Antonio Nappi

October 8th 2026

What is CERN?

WORLD-LEADING LABORATORY

We are the world's largest particle physics laboratory

ESTABLISHMENT & FUNDING

Founded in 1954 and funded by CERN's member states

PRIMARY MISSION

CERN's primary mission is to **study the fundamental building blocks** of the universe using highly advanced, purpose-built scientific machinery and **computing facilities**

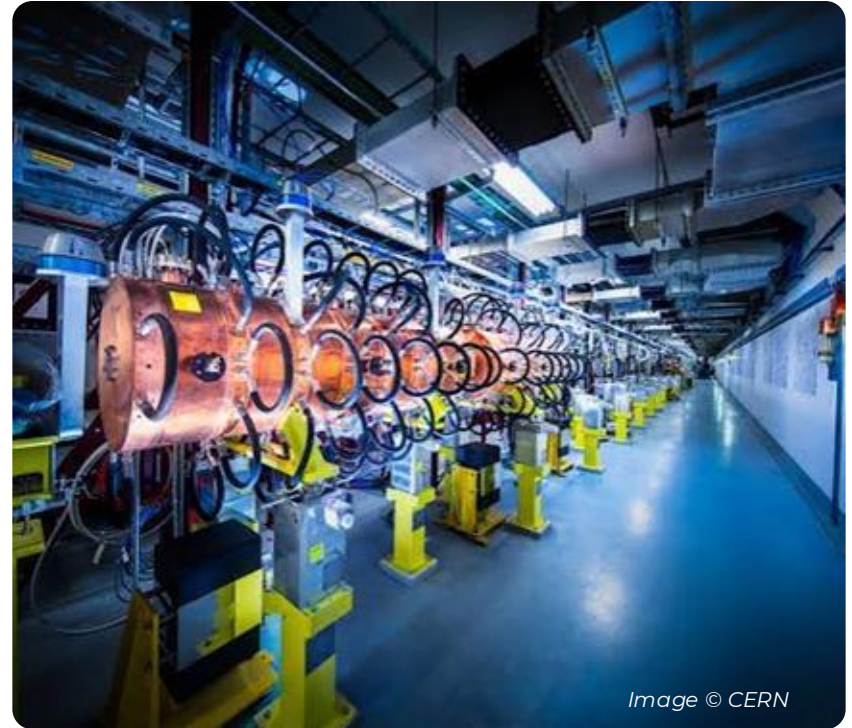


Image © CERN

CERN: Research. Innovation. Collaboration. Inspiration.

CERN GOAL

Deliver world-class scientific results and knowledge

IAM CONNECTION

Fundamental service to securely provide researchers with access to the data and tools they require

CERN GOAL

Use our flagship accelerator, the LHC, to its maximum potential during its high-luminosity phase

IAM CONNECTION

Stability and reliability is paramount

CERN GOAL

Provide, maintain and continually update a diverse, complementary scientific programme serving a broad community

IAM CONNECTION

Must support a dynamic, growing set of registered services/clients, accessed via a range of Identity Providers

CERN GOAL

Be a politically neutral voice for science, advocating investment in fundamental research and evidence-based policy

IAM CONNECTION

Must support Open Science and data sovereignty



Who is authenticating at CERN?

CERN account holders

CERN account holders using Kerberos, in a dedicated realm

CERN Accelerating science

Directory

CERN Single Sign-On

English

Sign in with a CERN account

Username

Password

Sign in

[Forgot Password?](#)

Or use another login method

Kerberos

Sign in with your email or organisation

Home Organisation - eduGAIN

Email - Guest Access

Sign in with a social account

By clicking on the buttons below, you consent to CERN's transfer of your login request to the social provider and to receive your account name, name and e-mail for authenticating you. See more details in our [Privacy Notice](#).

Google GitHub

Facebook Apple

LinkedIn

By logging in, you agree to comply with the [CERN Computing Rules](#), in particular OCS. CERN implements the measures necessary to ensure compliance.

Account
Manage your account

Privacy
Privacy Notice

Support
Service Desk - +41 22 76 7777
Service Status

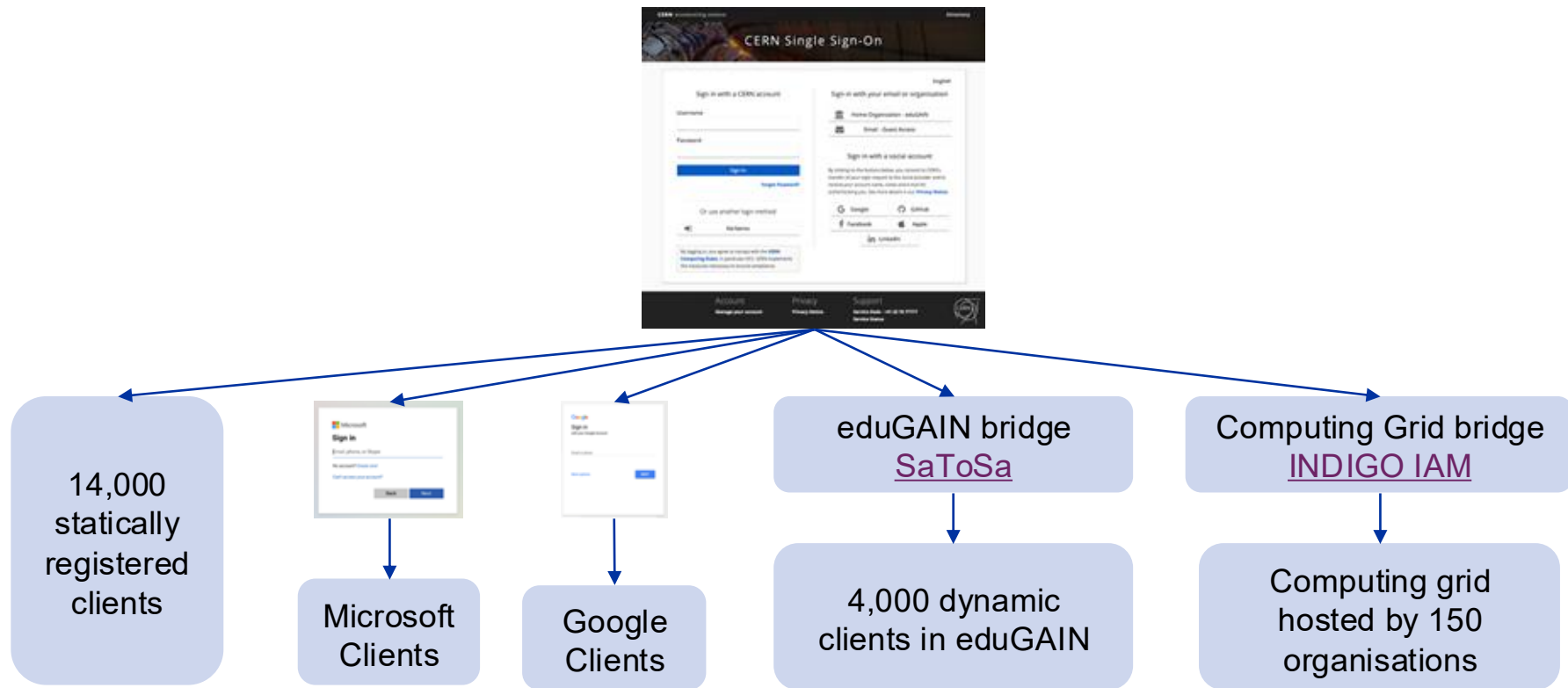
CERN

Universities and Institutes in eduGAIN, mostly **researchers, collaborators**

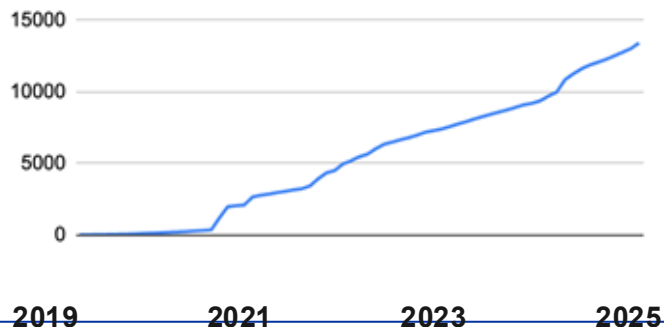
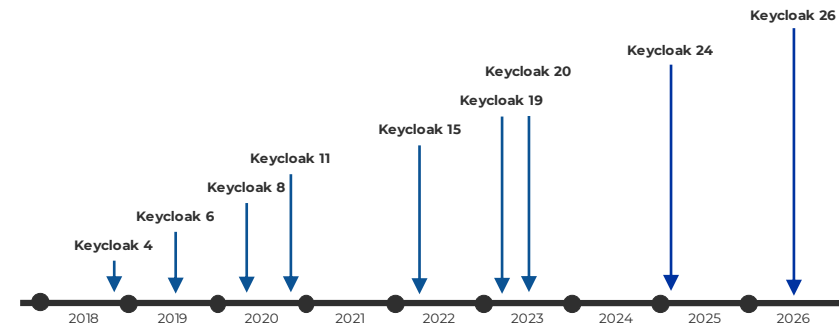
Self-registered guest accounts (Keycloak users), mostly **contractors, suppliers, alumni**

Users with an account at a social provider, mostly **visitors**

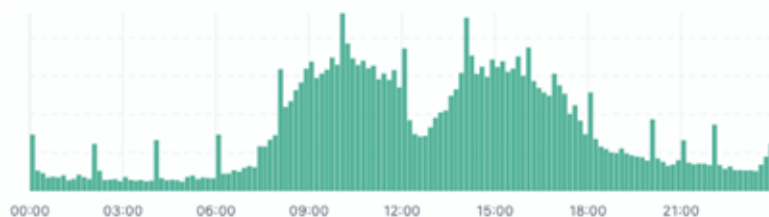
Where are they going?



CERN's journey to Keycloak



- **Migration from On-site ADFS began in 2019**
 - High cost due to number of existing clients and legacy debt
- **Launched on puppet managed VMs, then migrated to Kubernetes in 2023**
 - Now exceeds cloud AAI SLAs, over 99.99% availability



CERN's Keycloak Stats

Identity Landscape

250,000

Personal Accounts

Social logins and external email-password accounts

60,000

CERN Accounts Primary accounts managed directly by CERN

34,000

eduGAIN Accounts

From Identity Providers in eduGAIN supporting the Sirtfi trust framework

14,000

SSO Clients Registered clients and applications integrated with Keycloak

Daily Traffic & Volume

User Logins **140,000**/day

Client Logins **240,000**/day

Tokens Requests **800,000**/day

How do we handle CERN's complexity?



IBM computer and
CERN operator, 7 Mar
1963 © CERN

Client Registration

Self-Service & APIs

(Small!!) team cannot scale:

- **API Wrapper:**
Developed custom wrapper over Keycloak's API and a web interface to allow self service client registration.
- **Customisation:** Callout to CERN's group system during login to make use of central authorisation systems (not LDAP)

Security

Proactive Protection

A mix of inbuilt Keycloak features and our own:

- **Announcements:** "Message of the day" injects security messages to login page.
- **Checks during authentication:**
Passwords validated against compromised hashes and complexity rules.
Security course completion.
- **Captcha:** In house software used for account registration to ensure global accessibility.
- **2FA:** Mandatory for CERN account holders.

Upgrades

Lifecycle & QA

Managing change across highly technical departments:

- **Lead Time:** 4 months of rigorous pre-upgrade testing and validation with stakeholders.
- **QA Integration:** Core services integrate their QA with our Keycloak QA.
- **"Innovation":** Creative usage by technical users means every upgrade brings surprises.

CERN is not an island

- **CERN is part of an interconnected web of scientific organisations**
 - There is a long history of sharing computing infrastructure and allowing cross domain authentication
 - Worldwide Large Hadron Collider Computing Grid ([WLCG](#)): 150 organisations
 - [eduGAIN](#): 84 (mostly) national SAML federations, combining 10,000+ Identity Providers and Service Providers
- **Participant in EU projects for shared identity infrastructure e.g. [AARC](#)**

Many of the challenges felt at CERN are common to other research organisations and laboratories



CERN is not an island unto itself

Laboratories != Commercial Organisations

Distributed Trust

Multi-Domain Reality

Trusted, distributed computing between scientific organisations has a long and successful history.

- **Federation:** Many assumptions about IT services being in a single domain do not hold true.
- **Protocols:** User federation and distributed protocols are critically important.

Atypical Users

Beyond Standard Roles

Researchers are not typical customers or employees.

- **Mobility:** Users may move institutes multiple times for funding reasons but remain users of the laboratory throughout.
- **Technical ability:** We must provide usable solutions or they will invent insecure workarounds.

24/7 Operations

Stability During Runs

The ultimate "product" (data leading to publications) is paramount.

- **No Downtime:** Systems must remain perfectly stable during active beam/runtimes.
- **Isolated networks:** local sites may duplicate core services for redundancy in case of physical disconnection



Schedule Constraints

Example of CERN's Large Hadron Collider schedule: Coordinating a breaking change upgrade during runtime remains a major technical and operational challenge.

Where is Keycloak a good match for Research?



Early tape robot © CERN

Digital Sovereignty

Independence & Universal Access

Scientific collaboration must remain global, resilient, and fully under the institution's control:

- **No Geopolitical Barriers:** Avoids risks of external sanctions or geographical restrictions on research collaborators.
- **Data Sovereignty:** Keeps sensitive identities under lab control - core asset!

Operational Control

Aligned with Experimental Lifecycles

Updates and downtime must match laboratory runs:

- **Custom Release Cycles:** Align system maintenance, upgrades, and patches with experimental shutdowns.
- **Network configuration:** By hosting our SSO we can define all firewall rules and maintain segregation. Multisite evolution looks promising.

Extensible & Scalable

Open-Source Flexibility

Meets non-standard requirements inherent in research setups:

- **No Vendor Lock-In:** FOSS alignment ensures custom integrations remain modular and easily maintained. Mitigates risk of forced migration.
- **Custom Protocols:** Extends to support custom token exchanges, pam-module integration for SSH

What are the opportunities for Keycloak?

Identity Federation

Dynamic Needs

Research operates at a global scale requiring flexible, standard-driven trust frameworks:

- **Federated Identity:** Crucial dependence on researchers being able to use their institutional identity rather than create a new one for the laboratory/research project.
- **Future Protocols:** Keycloak must support dynamic identity provider and client federation to be truly useful for research - SAML federation is operational now, native OpenID Federation will come soon.

Security Backporting

Strict Lifecycle Risks

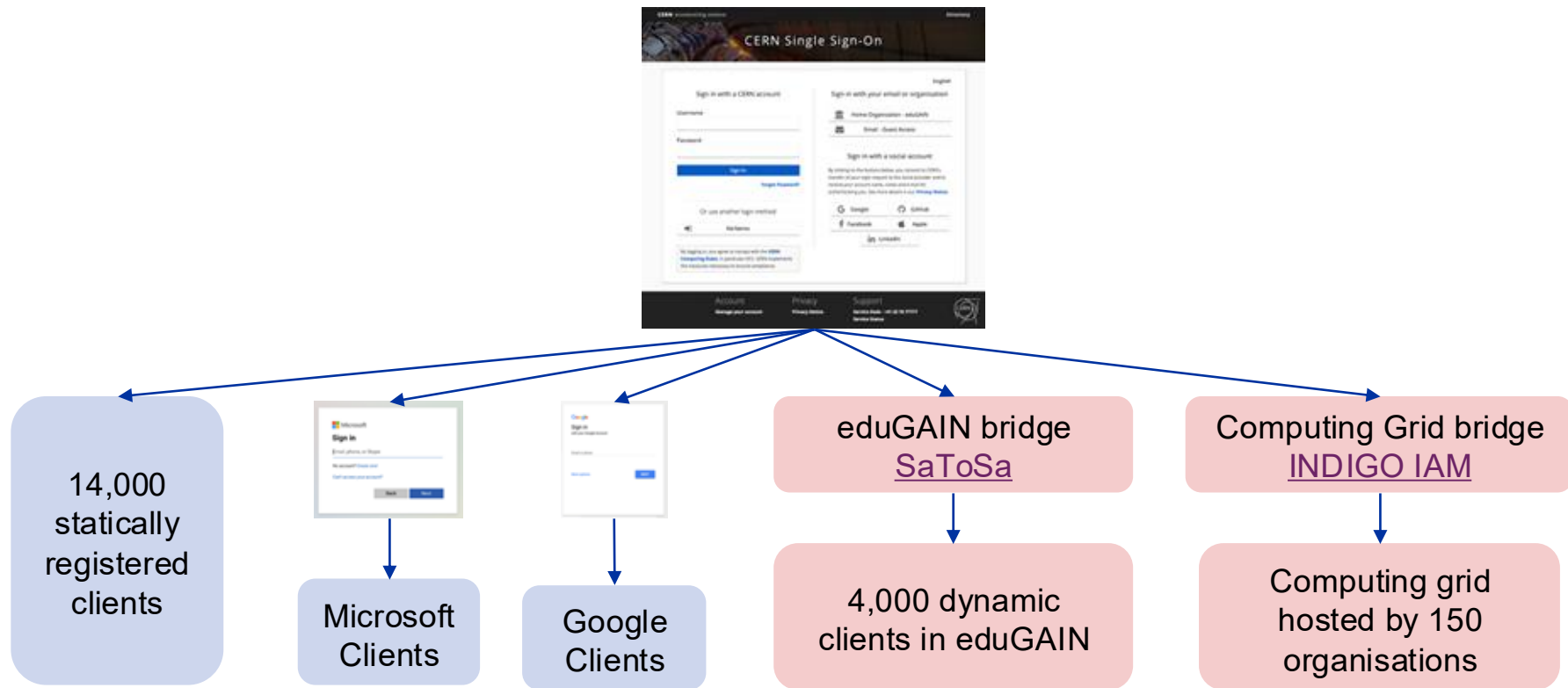
Research environments cannot easily tolerate breaking upgrades during critical operations:

- **No Backports:** Keycloak does not backport security fixes to older community versions.
- **Forced Upgrades:** Labs are forced into complex, risky major upgrades to maintain security.



CERNet, an early, homegrown packet-switching computer network developed at CERN starting in 1976
© CERN

Today, Keycloak cannot provide the full solution



Research Infrastructures of the Future

Cloud Services

Increasing % of research will use cloud services

Facilities may continue to prioritize on-site systems for core data and specialized hardware, whilst outsourcing many user facing web services.

AI & Security

AI continues to reshape security

Vulnerability discovery may plateau, but non-human identities introduce more risk.

Need to suspend rogue credentials quickly and effectively may influence token lifetimes, performance needs, key rollover, and protocol evolution.

Digital Wallets

Disrupting Research & Education

Highly beneficial for student mobility and proving research institute affiliation.

OpenID Federation

Ready for take off

OpenID Federation has been deployed in several countries proved its worth.

EOSC is the largest active venture into federated infrastructure, going live now and aiming to adopt OpenID Fed in the mid term.



*Looking to the future: Denise Heagerty, with rollerball prototype mouse circa 1980
© CERN*

Many research infrastructures are betting on Keycloak!

Thanks for inviting us!