



Sovereign identities for your cloud-native architecture with Keycloak

Alexander Schwartz | Keycloak Maintainer

Sebastian Łaskawiec | Defense Unicorns

KubeCon EU (Amsterdam, NL) | 2026-03-25

The Epic Quest of Single Sign On



Share your identity and delegate resource access to selected services.

The Epic Quest of Single Sign On



Share your identity and delegate resource access to selected services.



Keep your credentials secure.
Let applications operate on your data when permitted.

The Epic Quest of Single Sign On



Share your identity and delegate resource access to selected services.

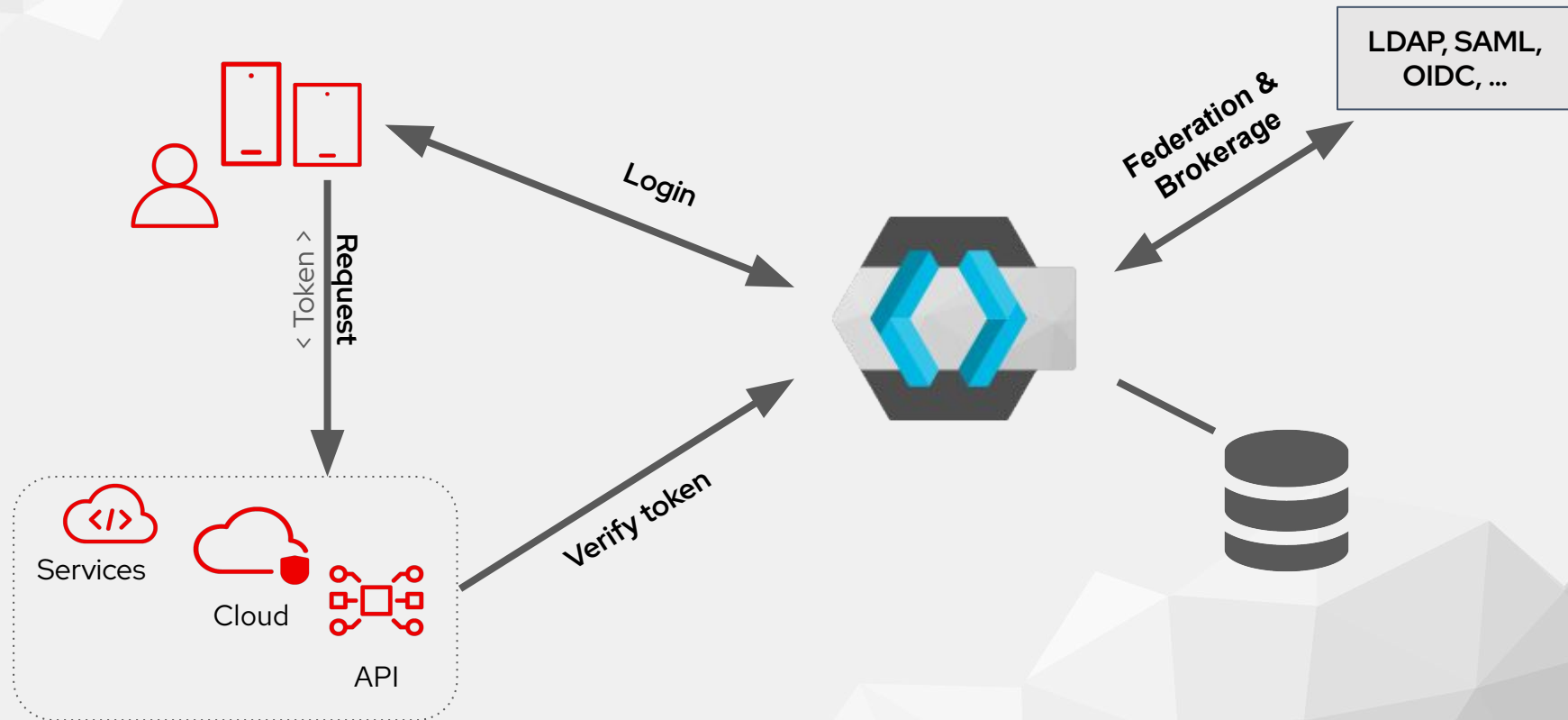


Keep your credentials secure.
Let applications operate on your data when permitted.



Digital Sovereignty depends on who can pull the plug,
and who owns the roadmap.

Own your identities with Keycloak



First contact

Sign in to your account

Username or email

Password

☐

Sign In

New: Better security for humans and machines



Standard Token Exchange

Exact and secure tokens with the right audience and scopes.

New: Better security for humans and machines



Standard Token Exchange

Exact and secure tokens with the right audience and scopes.



JWT Authorization Grant

Authenticate locally, then use trust relationships.

New: Better security for humans and machines



Standard Token Exchange

Exact and secure tokens with the right audience and scopes.



JWT Authorization Grant

Authenticate locally, then use trust relationships.



2FA recovery codes, Passkeys, FAPI 2.0, DPOP, MCP

Tightened security in all login flows.

New: Better security for humans and machines



Standard Token Exchange

Exact and secure tokens with the right audience and scopes.



JWT Authorization Grant

Authenticate locally, then use trust relationships.



2FA recovery codes, Passkeys, FAPI 2.0, DPOP, MCP

Tightened security in all login flows.



Workflows

Automate all stages of the user lifecycle management.

New: Automation and better tools for admins



Fine Grained Admin Permissions

Delegate access to administer entities in the realm to resource owners.

New: Automation and better tools for admins



Fine Grained Admin Permissions

Delegate access to administer entities in the realm to resource owners.



Secure communication, split-brain detection, rolling updates

Making an administrator's life simpler.

New: Automation and better tools for admins



Fine Grained Admin Permissions

Delegate access to administer entities in the realm to resource owners.



Secure communication, split-brain detection, rolling updates

Making an administrator's life simpler.



Federated Client Authentication

Less friction to manage credentials of clients across the infrastructure.

Observe your IAM in action with



Traces to hunt errors and latencies

Trace an incoming auth call to the database, LDAP and external IdPs.
Fully Supported since Jan 2025.

Observe your IAM in action with



Traces to hunt errors and latencies

Trace an incoming auth call to the database, LDAP and external IdPs.
Fully Supported since Jan 2025.



Logs for detailed insights

Originally for console, file and syslog. For OTel since Jan 2026.

Observe your IAM in action with



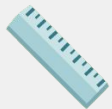
Traces to hunt errors and latencies

Trace an incoming auth call to the database, LDAP and external IdPs.
Fully Supported since Jan 2025.



Logs for detailed insights

Originally for console, file and syslog. For OTel since Jan 2026.



Metrics covering user and system activities

Find out about logins per second, cache sizes, endpoint timings.
Originally for Prometheus/OpenMetrics. For OTel since Jan 2026.

Observe your IAM in action with



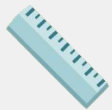
Traces to hunt errors and latencies

Trace an incoming auth call to the database, LDAP and external IdPs.
Fully Supported since Jan 2025.



Logs for detailed insights

Originally for console, file and syslog. For OTel since Jan 2026.



Metrics covering user and system activities

Find out about logins per second, cache sizes, endpoint timings.
Originally for Prometheus/OpenMetrics. For OTel since Jan 2026.



Dashboards, ready to go with Grafana

All relevant service level indicators on a single page.

Clients and users need credentials



Can we leverage existing credentials to avoid issuing new credentials and manage them?

Trust and Federation to re-use existing ~~credentials~~ tokens

- **External user wants to access resources via an external application**
Use JWT Authorization Grant (RFC 7523 & 7521) to have Keycloak issue tokens to external applications (preview in KC 26.5, supported in 26.6).
- **Client has SPIFFE, wants to talk OIDC to Keycloak**
Authenticate confidential client via SPIFFE JWT SVIDs (preview since KC 26.4, waiting for RFC to finalize)
- **Client runs on a Kubernetes cluster, wants to talk OIDC to Keycloak**
Issue a service account token to authenticate the confidential client (preview in KC 26.5, supported in KC 26.6)

It is all about issuers, signatures, and who we trust!

<https://www.keycloak.org/nightly/securing-apps/jwt-authorization-grant>
<https://www.keycloak.org/2026/01/federated-client-authentication>

What you will see in the demo



The “old way” for Client Authentication using **Client ID and Client Secret**



The “better way” - **no passwords or secrets!**



The “better way” for machine-to-machine authentication using **Client Credentials Grant**

DEMO

https://github.com/slaskawi/presentations/tree/master/2026_kubecon

Use cases and limitations

Perfect setup if Keycloak is in the same Kubernetes cluster as the secured application

Cross-cluster setup might get tricky because of CAs

Signed JWT tokens expiration time limited to 10 mins (Kubernetes limitation)

Upcoming Features in Keycloak 26.6*

- JWT Authorization Grant supported
- Federated Client Authentication supported
- Workflows supported
- Organization Groups
- Rolling updates and graceful restarts
- Better integration with Traefik, Envoy
- Simplified and opinionated DB connection setup
- New Keycloak test framework

* Due end of March, subject to change

Upcoming Features in Keycloak 26.7*

- SCIM support
- Organization Roles
- Continue the work around MCP
- Better documentation for proxy configuration
- ...

* Due end of June, subject to change

Q&A

Slides



Contact

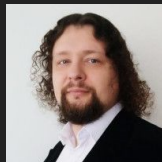


Alexander Schwartz
Keycloak Maintainer

alexander.schwartz@gmx.net
<https://www.ahus1.de>

 @ahus1.de

 @ahus1@fosstodon.org



Sebastian Łaskawiec
Defense Unicorns

sebastian.laskawiec@gmail.com