



A look at Keycloak from the IAM Point of View



Hi, my name is Robert

Developer by heart

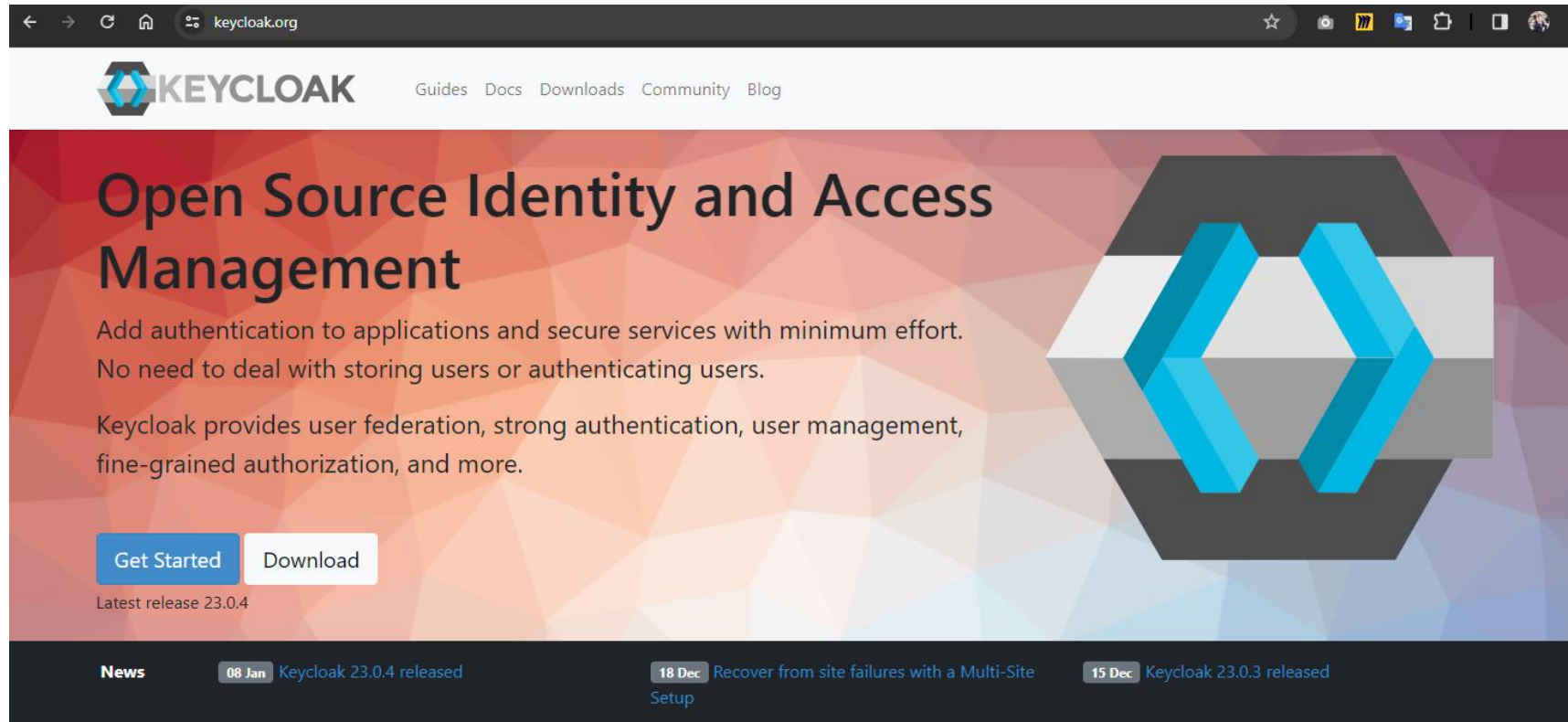
Product Management
@intension

Keycloak Afficionado
since 2014





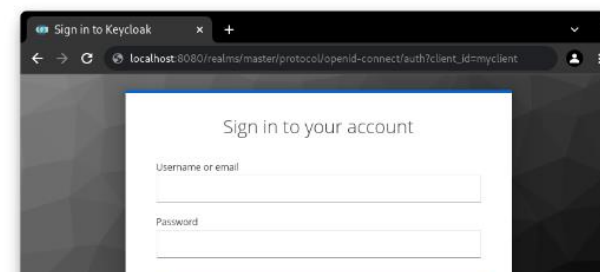
What actually does Keycloak?

A screenshot of the Keycloak website homepage. The browser address bar shows 'keycloak.org'. The navigation menu includes 'Guides', 'Docs', 'Downloads', 'Community', and 'Blog'. The main heading is 'Open Source Identity and Access Management'. Below this, there is a sub-heading 'Add authentication to applications and secure services with minimum effort. No need to deal with storing users or authenticating users.' followed by 'Keycloak provides user federation, strong authentication, user management, fine-grained authorization, and more.' There are two buttons: 'Get Started' and 'Download'. Below the buttons, it says 'Latest release 23.0.4'. At the bottom, there is a 'News' section with three items: '08 Jan Keycloak 23.0.4 released', '18 Dec Recover from site failures with a Multi-Site Setup', and '15 Dec Keycloak 23.0.3 released'. A large Keycloak logo is on the right side of the main content area.

Single-Sign On

Users authenticate with Keycloak rather than individual applications. This means that your applications don't have to deal with login forms, authenticating users, and storing users. Once logged-in to Keycloak, users don't have to login again to access a different application.

This also applies to logout. Keycloak provides single-sign out, which means users only have to logout once to be logged-out of all applications that use Keycloak.

A screenshot of a web browser showing a login form. The browser tab is 'Sign in to Keycloak' and the address bar shows 'localhost:8080/realms/master/protocol/openid-connect/auth?client_id=myclient'. The form has a title 'Sign in to your account' and two input fields: 'Username or email' and 'Password'.



What actually does Keycloak?

The screenshot shows a web browser window with the URL `access.redhat.com/products/red-hat-single-sign-on/`. The page header includes the Red Hat Customer Portal logo and navigation links for Subscriptions, Downloads, Containers, and Support Cases. The main content area features the title "Red Hat Single Sign-On" and a description: "Red Hat Single Sign-On provides Web single sign-on and identity federation based on SAML 2.0, OpenID Connect and OAuth 2.0 specifications." A blue "Download" button is visible. A dark blue banner at the bottom of the main content area contains the text: "Red Hat Single Sign-On 7.6 is the last planned feature release for version 7" and "Maintenance of all releases of version 7 will be available through regular, cumulative patch updates in the 7.6 release, according to the lifecycle policy. You can migrate Red Hat Single Sign-On to Red Hat build of Keycloak." Below this banner, there is a link "Go to Red Hat build of Keycloak" with a right-pointing arrow. At the bottom of the page, there is a section titled "Browse the latest documentation" with a dropdown menu labeled "Select a version".

access.redhat.com/products/red-hat-single-sign-on/

Subscriptions Downloads Containers Support Cases

Red Hat Customer Portal Products & Services Tools Security Community Search English All Red Hat Log in

Red Hat Single Sign-On

Red Hat Single Sign-On provides Web single sign-on and identity federation based on SAML 2.0, OpenID Connect and OAuth 2.0 specifications.

[Download](#)

Red Hat Single Sign-On 7.6 is the last planned feature release for version 7

Maintenance of all releases of version 7 will be available through regular, cumulative patch updates in the 7.6 release, according to the lifecycle policy. You can migrate Red Hat Single Sign-On to Red Hat build of Keycloak.

[Go to Red Hat build of Keycloak](#) →

Browse the latest documentation



What actually does Keycloak?

access.redhat.com/products/red-hat-build-of-keycloak/

Subscriptions Downloads Containers Support Cases

Red Hat Customer Portal Products & Services Tools Security Community Search English All Red Hat Log in

Red Hat build of Keycloak

Red Hat build of Keycloak is a cloud-native Identity Access Management solution based on the popular open source Keycloak project. Red Hat build of Keycloak replaces any planned future releases of Red Hat Single Sign-On. You can migrate Red Hat Single Sign-On to Red Hat build of Keycloak now.

[Download](#)

Browse the latest documentation

Release Notes Release Notes for Red Hat build of Keycloak	Red Hat build of Keycloak Component Details Supported Configurations and Component Details	Getting Started Guide Installing Red Hat build of Keycloak	Server Guide Managing the Red Hat build of Keycloak Server
Migration Guide Migrating to Red Hat build of Keycloak	Securing Applications and Services Guide Using Red Hat build of Keycloak		



And what was IAM about?

Identification

Authentication

Autorisierung

Identity and Access Management Identity Governance and Administration



IAM und IGA "feature" categories

Identity Management & Administration	Access Management	Access Governance	Access Intelligence
--	----------------------	----------------------	------------------------



IAM Use Cases

Scenarios with specific requirements

- Enterprise / Workforce IAM
- B2B Customer IAM
- B2C Customer IAM (CIAM)
- IAM for IOT

- OnPrem vs. Cloud

Industries with specific requirements

- Healthcare
- Education
- Public Administration
- NGOs, Clubs, Associations

Identity Management und Administration

1. Category



Management of the identity objects

- Central Identity Store / Meta Directory
- Lifecycle Management
- Organizational Management
- Credentials Management
- Provisioning

Identity Management und Administration

Keycloak Check



Management of the identity objects

- Central User Store / Meta Directory ✓
- Lifecycle Management ?
- Organizational Management ✓
- Credentials Management ✓
- Provisioning ✗

Access Management

2nd category



User Identification und Authentication

- Single Sign On
- Secure access to web applications
- Secure access to APIs
- Multifactor Authentication
- Adaptive Authentication
- Identity Brokering
- Social Logins



Access Management Keycloak Check

User Identification und Authentication

- Single Sign On ✓
- Secure access to web applications ✓
- Secure access to APIs ✓?
- Multifactor Authentication ✓?
- Adaptive Authentication ✗?
- Identity Brokering ✓
- Social Logins ✓

API Exploit



November 2022
T-Mobile US

API Exploit



41 days

37 million customers affected

“limited set of customer account data”
(name, billing address, email, phone number, date of birth)

Access Governance

3rd category



- Assignment and withdrawal of authorizations
- Lifecycle Management for authorizations
- Access control mechanisms (e.g. RBAC, PBAC)

- Workflows
- Access Recertification

Access Governance Keycloak Check



- Assignment and withdrawl of authorizations ✓ ✗
- Lifecycle Management for authorizations ✗
- Access control mechanisms (e.g. RBAC, PBAC) ✓ ✓
- Workflows ✗
- Access Recertification ✗

Access Intelligence & Risk Mitigation

4th category



Q: Do all users really only own the right authorizations, and only the once they actually need?

- Segregation of Duty
- Monitoring, Auditing und Reviewing
- Role Mining

- Privileged Access Management (PAM)

Access Intelligence & Risk Mitigation

Keycloak Check



Q: Do all users really only own the right authorizations, and only the once they actually need?

- Segregation of Duty ✘
- Monitoring, Auditing und Reviewing ?
- Role Mining ✘
- Privileged Access Management (PAM) ✘



NIS2 – Identity Security

“Cyber Hygiene” for users and infrastructure nach “Stand der Technik” – State of the Art

- Zero Trust
- Secure Authentication
- Audit & Reporting



Enterprise / Workforce IAM

- Lifecycle Management
- Governance
- Organizational structures
- Externen & Partner Management
- Risiko Management
- PAM

Ransomware Attack



Mai 2021
Colonial Pipeline



Ransomware Attack

“Legacy Virtual Private Network (VPN) system,
unused but active,
that did not have multifactor authentication in place”



Ransomware Attack

VPN login belonged to an employee believed to be inactive. The firm noted that the employee "may have used" the password on a different website that was previously compromised.



B2B Customer IAM

Einsatz zur Verwaltung von Kundenorganisationen und Kundenuser

- Customer organizations, tenants
- Delegated administration: customer self service
- Automated user provisioning (SCIM)
- Onboarding

- Scalability



B2C Customer IAM

Einsatz zur Verwaltung von Endkunden

- Effortless and seamless user onboarding
- Social Logins
- Consent Management (GDPR, CCPA)
- SSO (Einmalanmeldung)
- Adaptive Authentication
- Threat detection

- Scalability

Credentials Stuffing Attack



May 2023
23andme.com

Credentials Stuffing Attack



5 Monate lang unentdeckt

14000 gehackte Accounts

6.9 Millionen Kunden betroffen



IAM für IOT Anwendungsfälle

Einsatz zur Verwaltung von Geräten

- Sichere Geräteauthentifizierung
- Usergebundene Geräte?
- Messstationen?

Branchenspezifische IAM Anforderungen



- Bildungswesen
 - Viele unterschiedliche Nutzergruppen
 - Komplexe Gruppenstrukturen mit Jahrgängen, Kursen
 - Heterogene Applikationslandschaft
 - Integration in Bildungsnetzwerken (DFN, eduGAIN, VIDIS)
- Healthcare
 - Datenschutz: Patientendaten
 - Heterogene Usergruppen
 - Viel Bewegung zb beim Pflegepersonal
 - Externe User, z.b. Niedergelassene Ärzte, Labore
 - GesundheitsID: digas, E-Rezept etc.
- NGOs und Vereine
 - Heterogene Nutzergruppen
 - Abbildung von Strukturen, Team Administration
 - Bestätigungsprozesse
 - Kosten
 - IT Fachkenntnisse
- Öffentliche Verwaltung
 - Komplexe Föderale Strukturen
 - IT Grundschutz
 - Verschlusssachen
 - Revisionsicherheit



Wo gibt's also was zu entwickeln?

- Life Cycle Management für Benutzer
- Life Cycle Management für Berechtigungen
 - Rezertifizierungen
- Genehmigungsworkflows
- Provisionierungsmechanismen (nur just in time per Token)
 - Reconciliation
 - SCIM Support
- Support für SAML / OIDC Federation
 - Anbindung DFNAAI / eduGAIN
 - Oder z.B. für DiGAs (Anbindung Gematik / GesundheitsID)
- Mechanismen zur Adaptive Authentifizierung
- Detektion von Angriffen



Ausblick: IAM Trends

Digital ID

Zero Trust Security: Never Trust, Always Verify

Biometric Authentication: Device based, Fingerprint, FaceID

AI: Adaptive Authentication, Anomaly Detection, Role Mining, User Profiling

Fokus auf User Experience -> Anmeldeprozesse einfacher und sicherer gestalten



Danke fürs Zuhören



Robert Bauer

Product Management

+49 711 45880-135

robert.bauer@intension.de

