

# Der große SSO-Vergleich

Keycloak, Authentik, ... oder doch ein SaaS-Service?

Karlsruhe, Januar 2025

Einleitung

## Wer bin ich?

**Florian Schick**

// Unabhängiger Software Entwickler //

## Mit Fokus auf

Full-Stack mit .NET/Core, C#, Angular, Vue.js

Clean code //einfach zu lesen, einfach zu warten //

## Creator of

**PLAINQUIRE**.com  
Filtering, sorting & pagination for ASP .NET Core

## Kontakt

📞 florian.schick@schick-software.de

@ +49 771 8979378

Übersicht

# SSO

## Ein Login für alle Anwendungen

Single Sign-On bietet eine einfache und sichere Lösung, um mit einem einzigen Login Zugriff auf verschiedene Systeme und Apps zu erhalten

## Vorteile

Applikationen selbst kennen oder sehen das Passwort des Benutzers nicht

Die Benutzer müssen sich nur ein Passwort merken

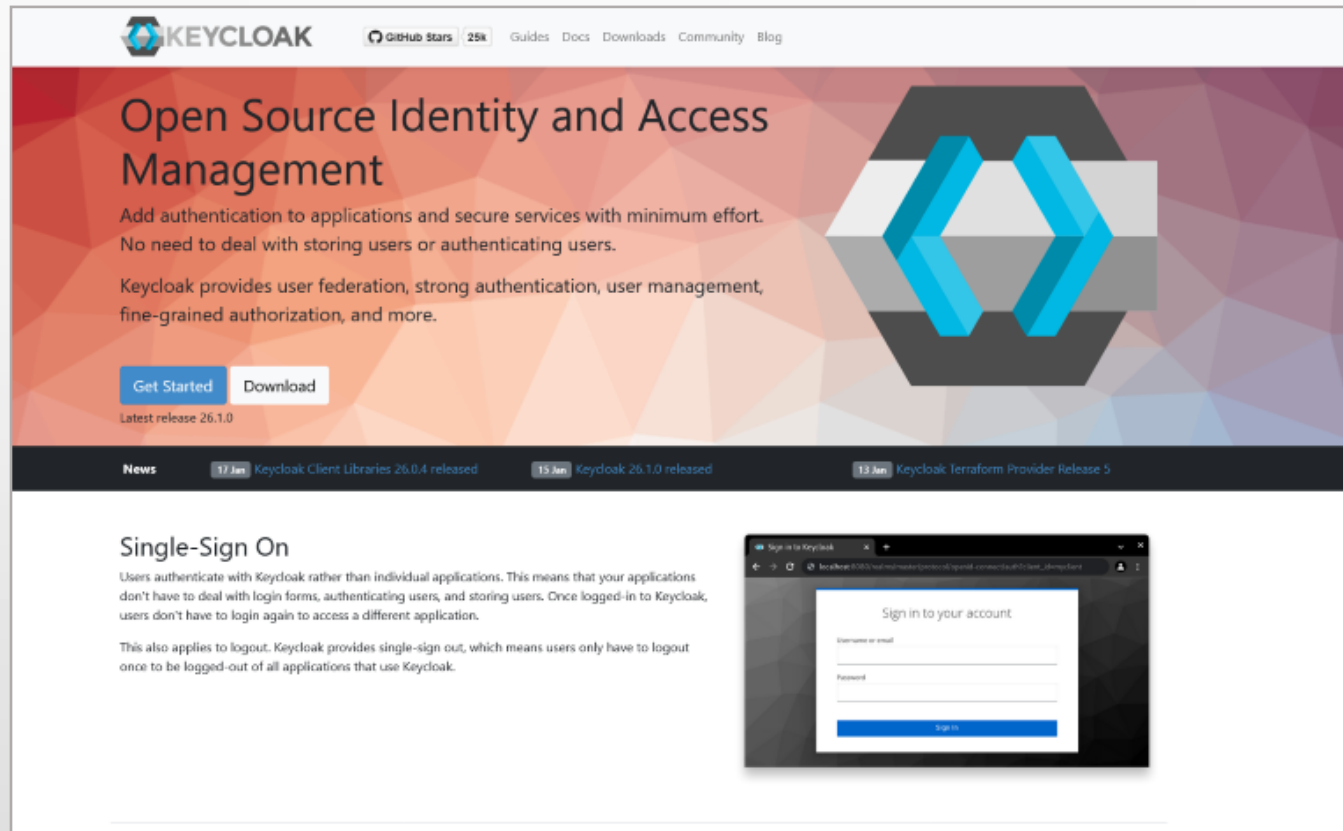
Neue Sicherheitsmechanismen (z.B. Passkey) können an zentraler Stelle implementiert werden

Logins können zentral administriert werden



Übersicht

# Keycloak



## Gründung

2014

## Lizenz

Apache-2.0

## Eigentümer

bis 2023: WildFly / Red Hat  
seit 2013: Cloud Native  
Computing Foundation

Keycloak ist eine der  
beliebtesten SSO-Lösungen. Es  
hat eine aktive Community  
und ein breites Ökosystem

Übersicht

# Keycloak

## Gründung

2014

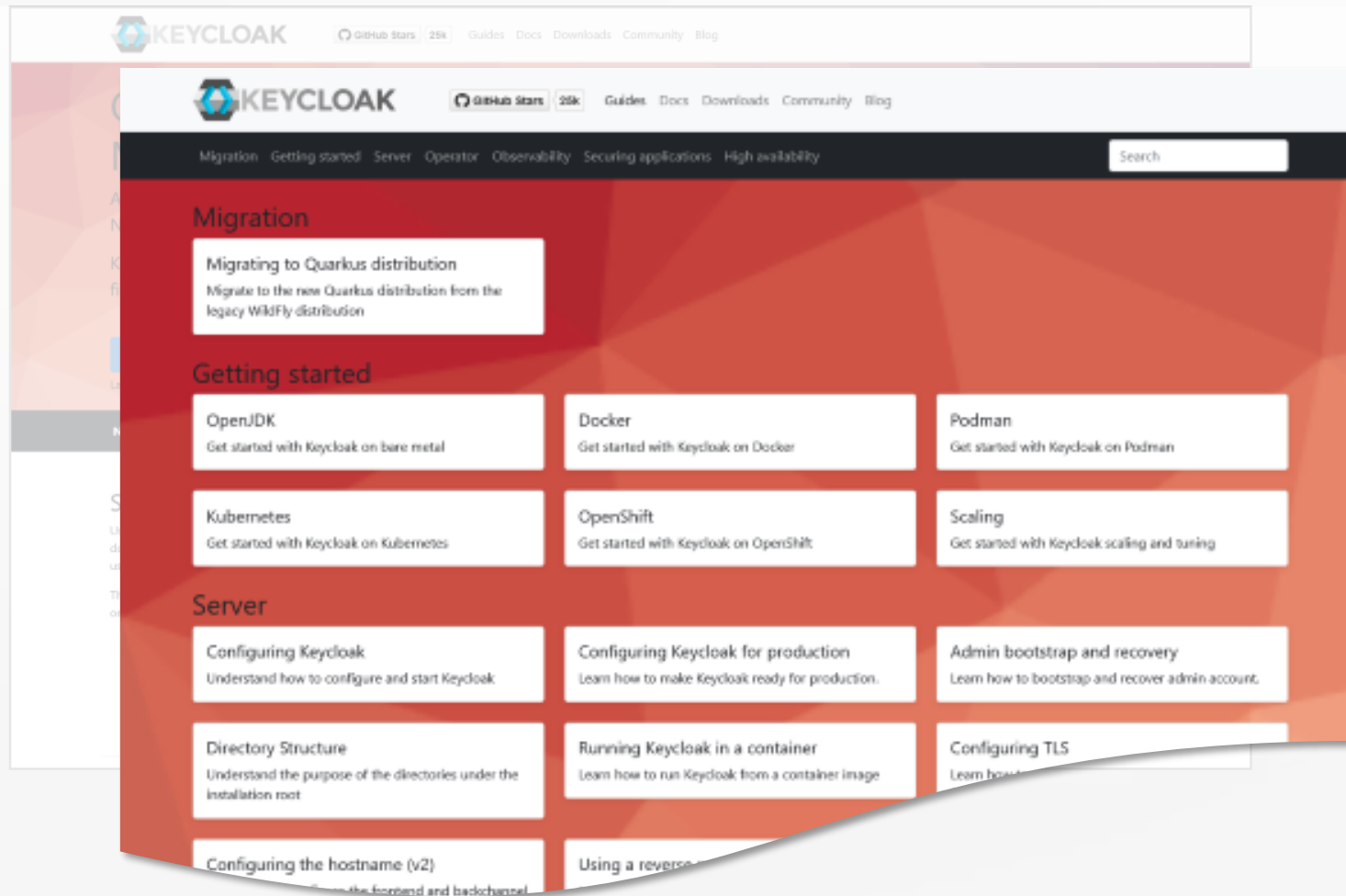
## Lizenz

Apache-2.0

## Eigentümer

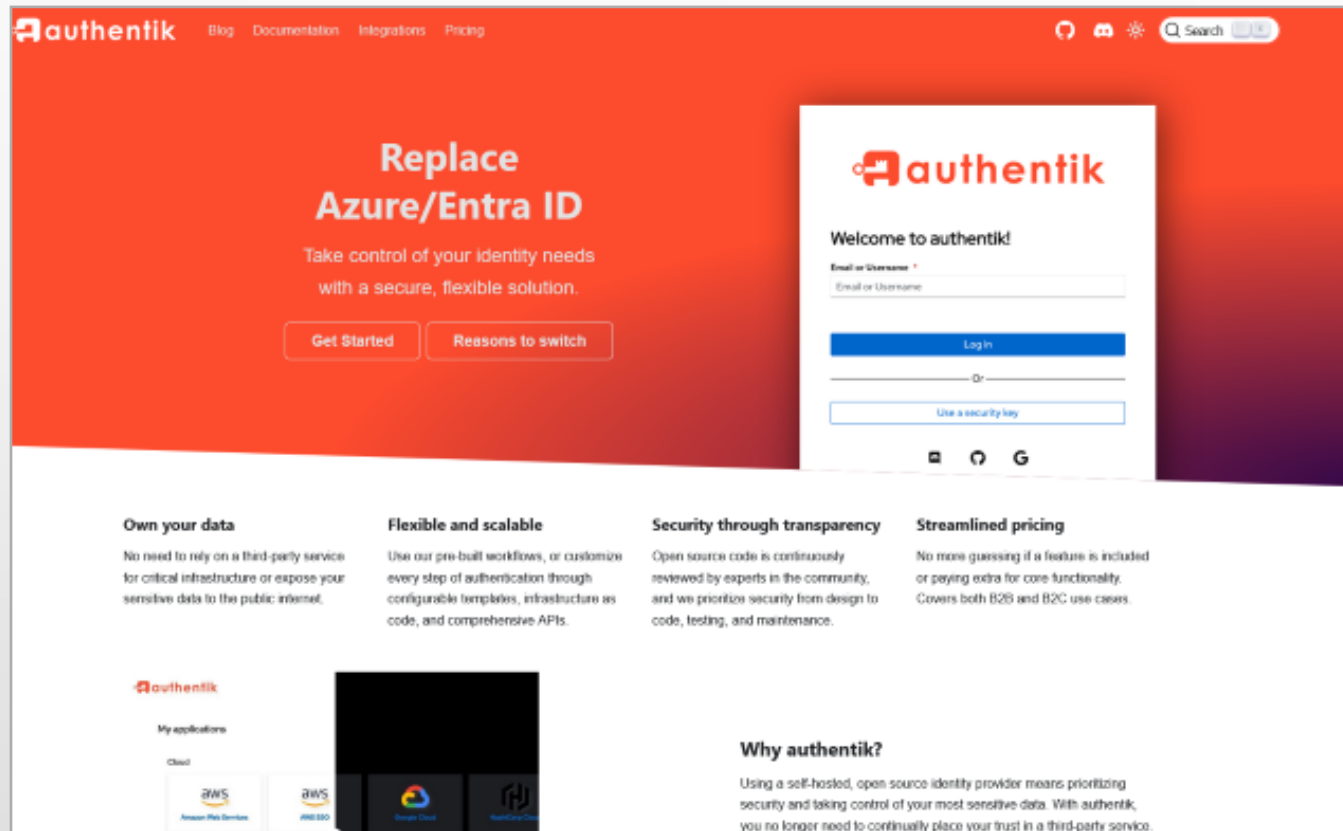
bis 2023: WildFly / Red Hat  
seit 2013: Cloud Native  
Computing Foundation

Keycloak ist eine der  
beliebtesten SSO-Lösungen. Es  
hat eine aktive Community  
und ein breites Ökosystem



Übersicht

# Authentik



**Gründung**

2021

**Lizenz**

verschiedene

**Eigentümer**

Authentik Security Inc.

Junger und inzwischen viel beachteter Identity-Provider mit wachsender Community.

Über den Hersteller gib es so gut wie keine Informationen.



# Authentik

Do more with authentik						
	authentik	Keycloak	Microsoft ADFS	Azure/Entra ID	Okta	Du
<b>Capabilities included</b>						
Self-host anywhere	✓	✓	⚠	✗	✗	✗
MFA ⓘ	✓	✓	✗	✓	✓	✓
Conditional Access	✓	✓	✓	⚠	✓	⚠
Open-source/Source available	✓	✓	✗	✗	✗	✗
Application Proxy ⓘ	✓	⚠	⚠	✓	✗	✗
Enterprise support ⓘ	✓	⚠	✗	✓	✓	✓
<b>Protocol Support (as a provider)</b>						
SAML2	✓	✓	✓	✓	✓	✓
OAuth2 and OIDC	✓	✓	✓	✓		
SCIM	✓	⚠				

## Gründung

2021

## Lizenz

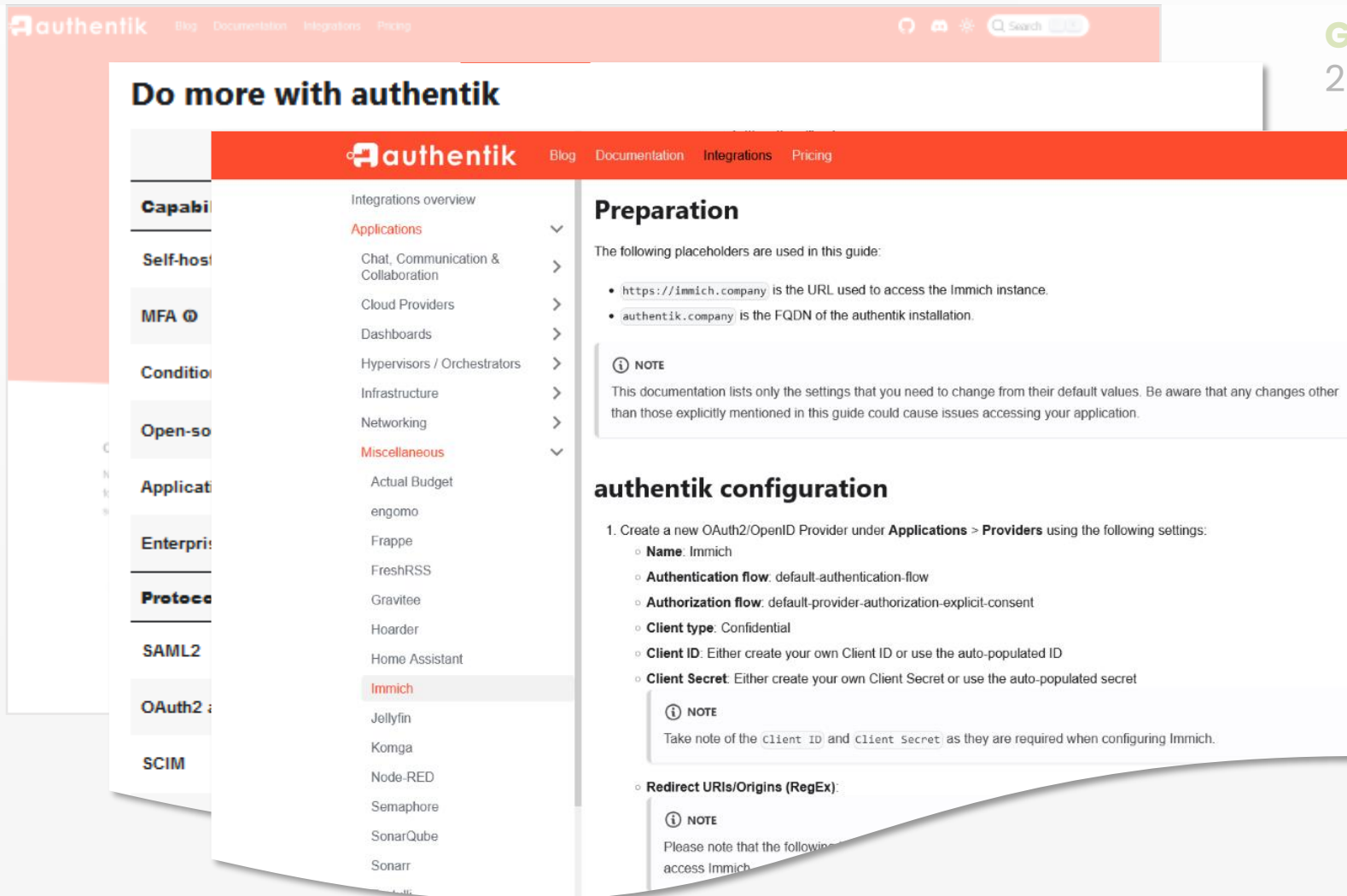
verschiedene

## Eigentümer

Authentik Security Inc.

Junger und inzwischen viel beachteter Identity-Provider mit wachsender Community.

Über den Hersteller gib es so gut wie keine Informationen.



The screenshot displays the Authentik documentation website. The top navigation bar includes links for Blog, Documentation, Integrations, and Pricing. The main content area is titled "Do more with authentik" and features a sidebar with a list of integration categories: Capabilities, Self-hosted, MFA, Conditional Access, Open-source, Applications, Enterprise, Protection, SAML2, OAuth2, and SCIM. The "Applications" category is expanded, showing a list of integrations including Chat, Communication & Collaboration, Cloud Providers, Dashboards, Hypervisors / Orchestrators, Infrastructure, Networking, Miscellaneous, Actual Budget, engomo, Frappe, FreshRSS, Gravitee, Hoarder, Home Assistant, Immich (highlighted), Jellyfin, Komga, Node-RED, Semaphore, SonarQube, and Sonarr.

The main content area is titled "Preparation" and contains the following text:

The following placeholders are used in this guide:

- `https://immich.company` is the URL used to access the Immich instance.
- `authentik.company` is the FQDN of the authentik installation.

**NOTE**  
This documentation lists only the settings that you need to change from their default values. Be aware that any changes other than those explicitly mentioned in this guide could cause issues accessing your application.

**authentik configuration**

1. Create a new OAuth2/OpenID Provider under **Applications > Providers** using the following settings:

- **Name:** Immich
- **Authentication flow:** default-authentication-flow
- **Authorization flow:** default-provider-authorization-explicit-consent
- **Client type:** Confidential
- **Client ID:** Either create your own Client ID or use the auto-populated ID
- **Client Secret:** Either create your own Client Secret or use the auto-populated secret

**NOTE**  
Take note of the Client ID and Client Secret as they are required when configuring Immich.

◦ **Redirect URIs/Origins (Regex):**

**NOTE**  
Please note that the following...  
access Immich...

Gründung  
2021

Lenz

verschiedene

gentümer

Authentik Security Inc.

nger und inzwischen viel  
achteter Identity-Provider  
it wachsender Community.

er den Hersteller gib es so  
it wie keine Informationen.



Übersicht

# ZITADEL

**Gründung**

2020

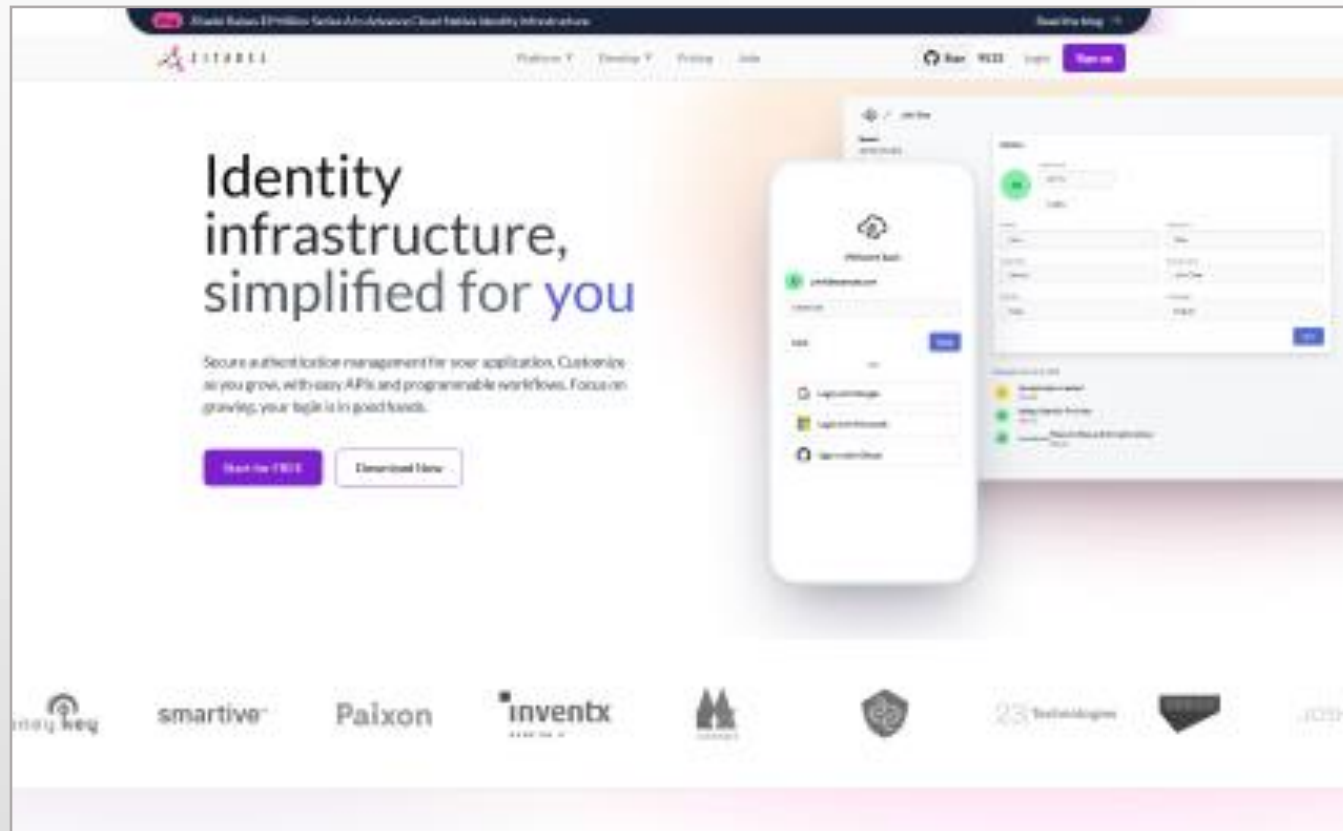
**Lizenz**

Apache-2.0

**Eigentümer**

vermutlich CAOS AG

Entstanden bei der CAOS AG (Schweiz), inzwischen ein globales Remote-Team. Starke Präsenz in Europa, besonderer Wert auf Datenschutz



Übersicht

# ZITADEL

## Gründung

2020

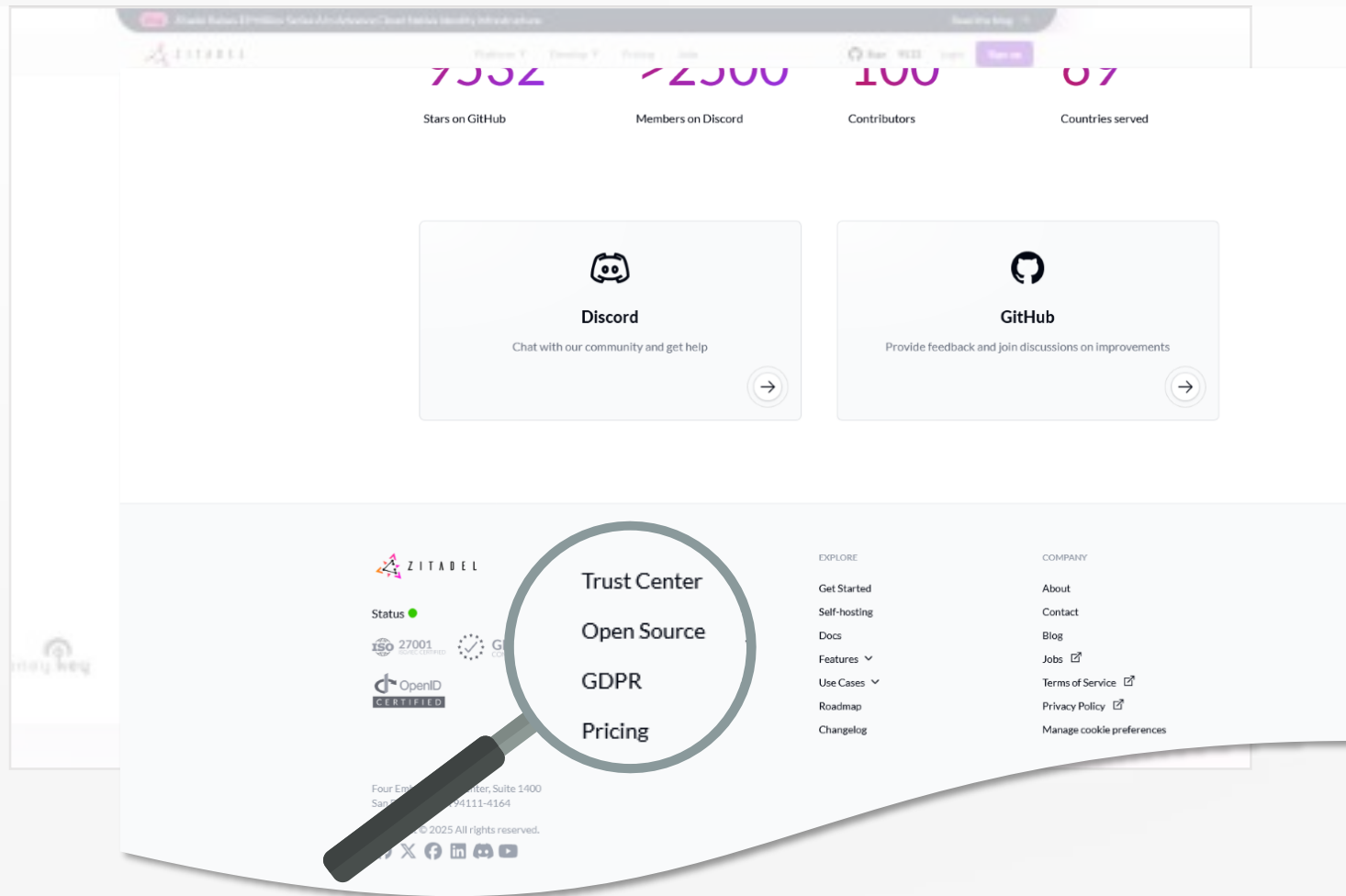
## Lizenz

Apache-2.0

## Eigentümer

vermutlich CAOS AG

Entstanden bei der CAOS AG (Schweiz), inzwischen ein globales Remote-Team. Starke Präsenz in Europa, besonderer Wert auf Datenschutz



Übersicht

# auth0

## Gründung

2013

## Lizenz

kommerziell

## Eigentümer

Okta Inc.

Gegründet von Eugenio Pace und Matias Woloski in Argentinien. 2021 akquiriert von Okta für 6,5 Milliarden US-Dollar



Übersicht

# auth0

Gründung

2013

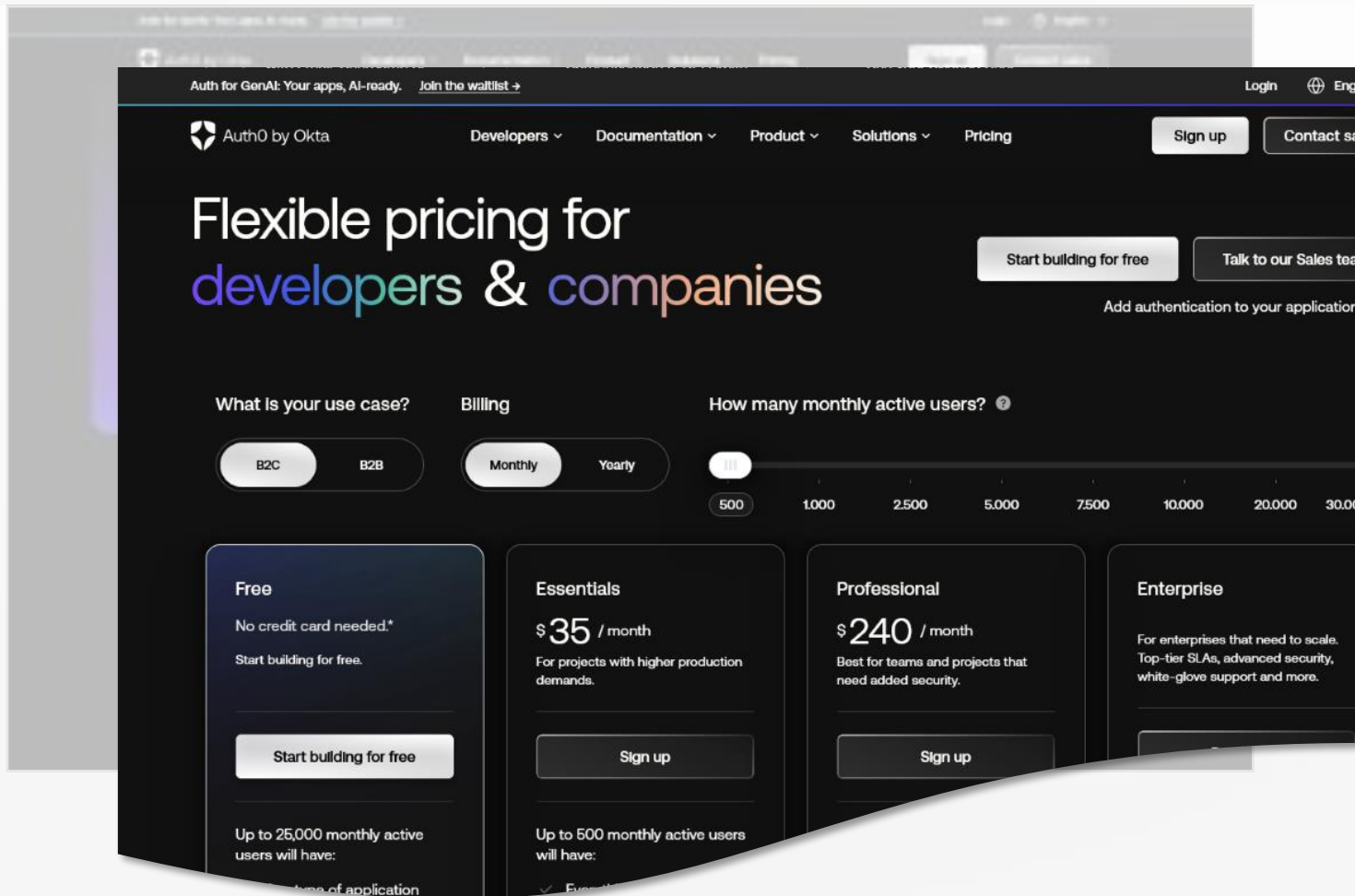
Lizenz

kommerziell

Eigentümer

Okta Inc.

Gegründet von Eugenio Pace und Matias Woloski in Argentinien. 2021 akquiriert von Okta für 6,5 Milliarden US-Dollar



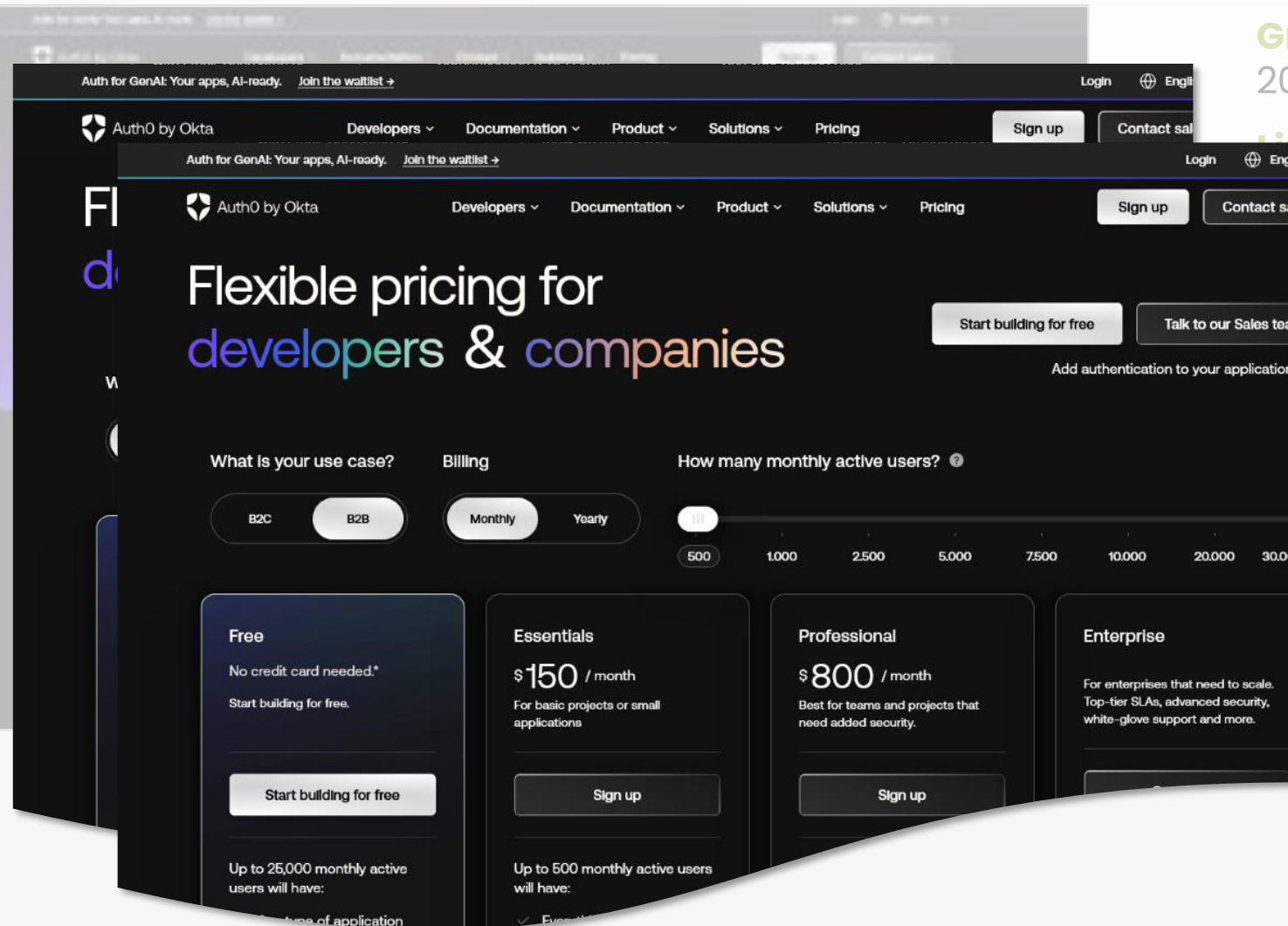
Übersicht

# auth0

Gründung  
2013

Lizenz  
kommerziell  
Eigentümer  
Okta Inc.

gegründet von Eugenio Pace  
und Matias Woloski in  
Argentinien. 2021 akquiriert von  
Okta für 6,5 Milliarden US-  
Dollar



Übersicht

# curity

## Gründung

2015

## Lizenz

kommerziell

## Eigentümer

Curity AB

Fokus auf hochsichere  
Enterprise-SSO-, API- und IAM-  
Infrastrukturen, insbesondere  
für regulierte Branchen



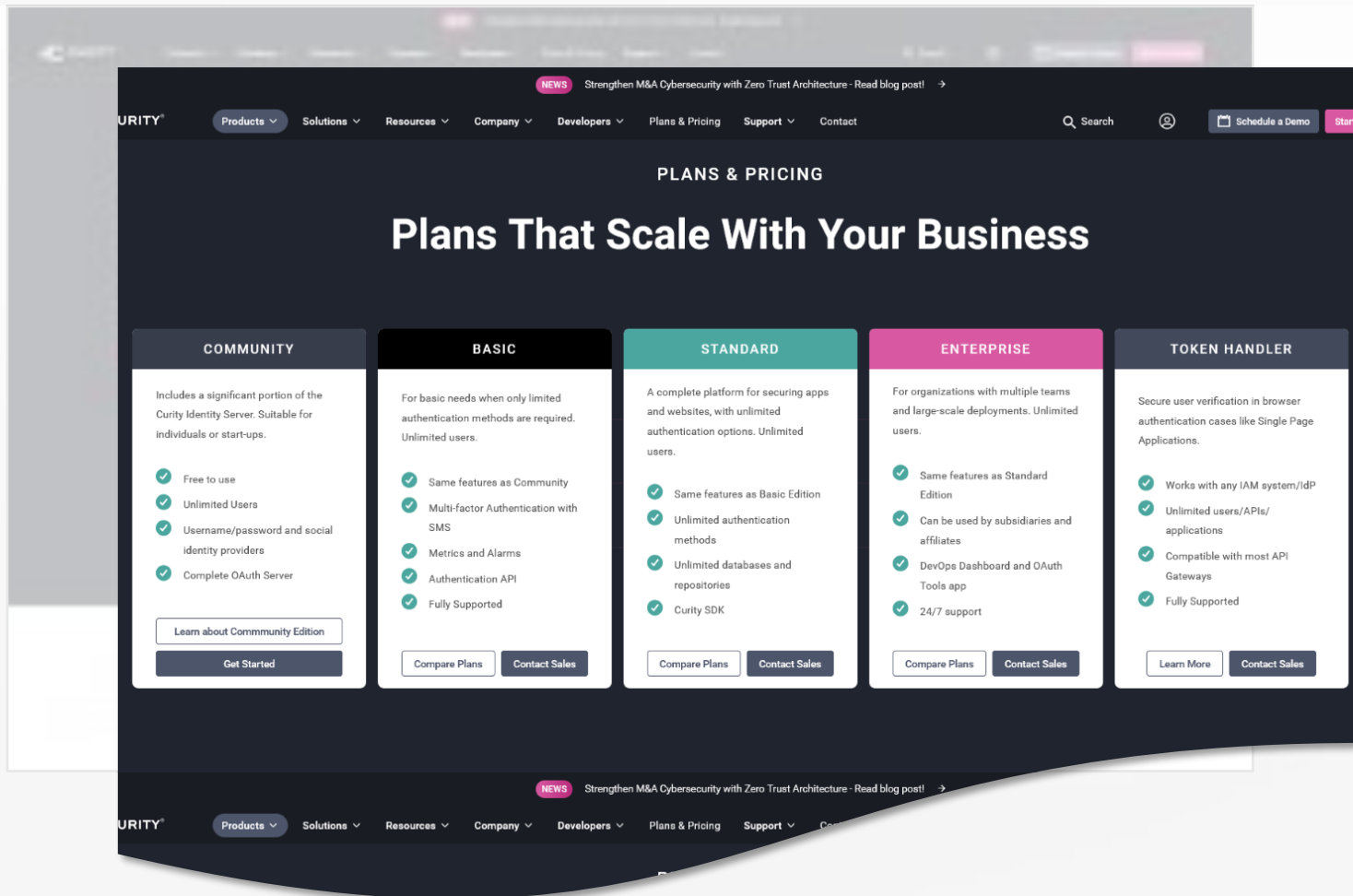


Gründung  
2015

Lizenz  
kommerziell

Eigentümer  
Curity AB

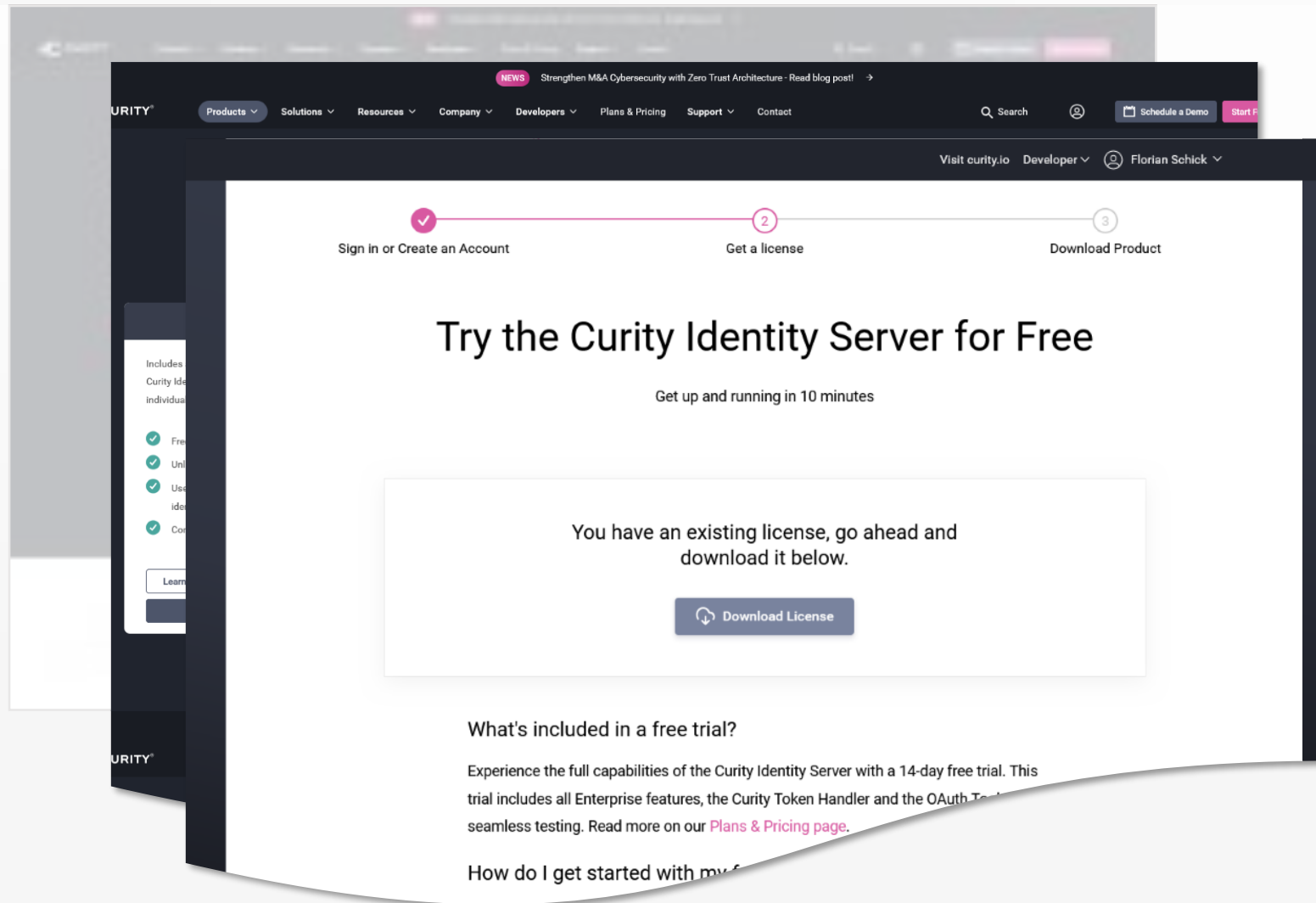
Fokus auf hochsichere  
Enterprise-SSO-, API- und IAM-  
Infrastrukturen, insbesondere  
für regulierte Branchen



Gründung  
2015

Lizenz  
kommerziell  
Eigentümer  
Curity AB

Fokus auf hochsichere  
Enterprise-SSO-, API- und IAM-  
Infrastrukturen, insbesondere  
für regulierte Branchen



Übersicht

# Entra ID

**Gründung**

2010

**Lizenz**

kommerziell

**Eigentümer**

Microsoft

In Azure integrierte Identity-  
Provider-Lösung.



Gründung

2018

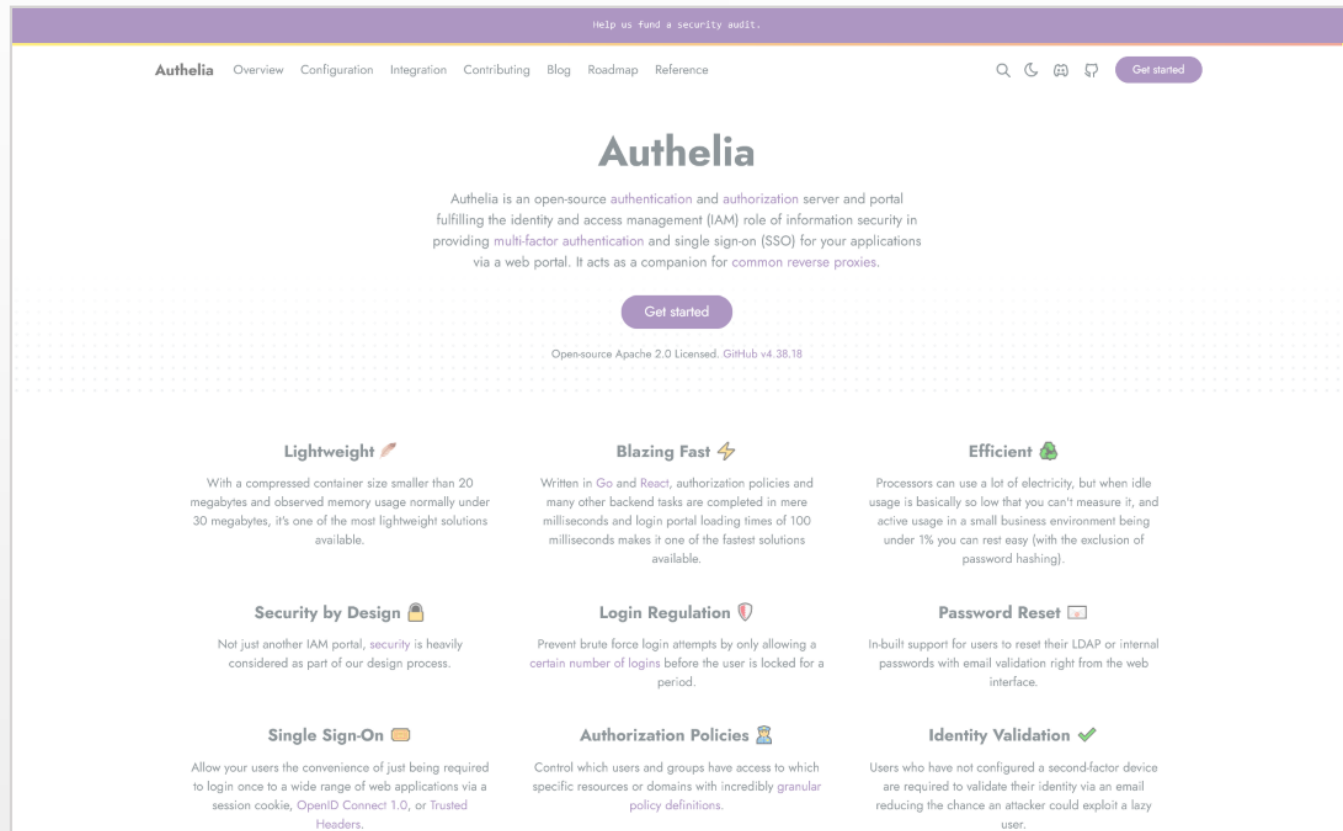
Lizenz

Apache-2.0

Eigentümer

keiner

Fokussiert sich stark auf  
Privacy und Sicherheit , mit  
einer speziellen Zielgruppe von  
technisch versierten Nutzern  
oder Admins



Help us fund a security audit.

Authelia Overview Configuration Integration Contributing Blog Roadmap Reference

Authelia

Authelia is an open-source authentication and authorization server and portal fulfilling the identity and access management (IAM) role of information security in providing multi-factor authentication and single sign-on (SSO) for your applications via a web portal. It acts as a companion for common reverse proxies.

Get started

Open-source Apache 2.0 Licensed. GitHub v4.38.18

**Lightweight** 🍌

With a compressed container size smaller than 20 megabytes and observed memory usage normally under 30 megabytes, it's one of the most lightweight solutions available.

**Blazing Fast** ⚡

Written in Go and React, authorization policies and many other backend tasks are completed in mere milliseconds and login portal loading times of 100 milliseconds makes it one of the fastest solutions available.

**Efficient** 🌿

Processors can use a lot of electricity, but when idle usage is basically so low that you can't measure it, and active usage in a small business environment being under 1% you can rest easy (with the exclusion of password hashing).

**Security by Design** 🛡️

Not just another IAM portal, security is heavily considered as part of our design process.

**Login Regulation** 🛑

Prevent brute force login attempts by only allowing a certain number of logins before the user is locked for a period.

**Password Reset** 🔄

In-built support for users to reset their LDAP or internal passwords with email validation right from the web interface.

**Single Sign-On** 🍷

Allow your users the convenience of just being required to login once to a wide range of web applications via a session cookie, OpenID Connect 1.0, or Trusted Headers.

**Authorization Policies** 👤

Control which users and groups have access to which specific resources or domains with incredibly granular policy definitions.

**Identity Validation** ✅

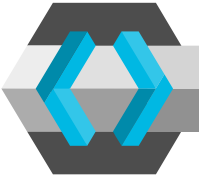
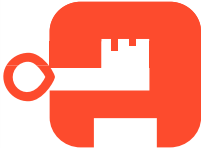




Users who have not configured a second-factor device are required to validate their identity via an email reducing the chance an attacker could exploit a lazy user.

Übersicht

# Nicht im Fokus



# Kandidaten im Test

	Keycloak	Authentik	Zitadel	auth0	curity	Entra ID
						
On-Prem	✓	✓	✓	✗	✓	✗
SaaS	✗	✗	✓	✓	✗	✓
Open Source	✓	✓	✓	✗	✗	✗
Free Plan	✓	✓	✓	limited	limited	✗



Übersicht

# Hauptsitz der Firmen



Übersicht

# Hauptsitz der Firmen



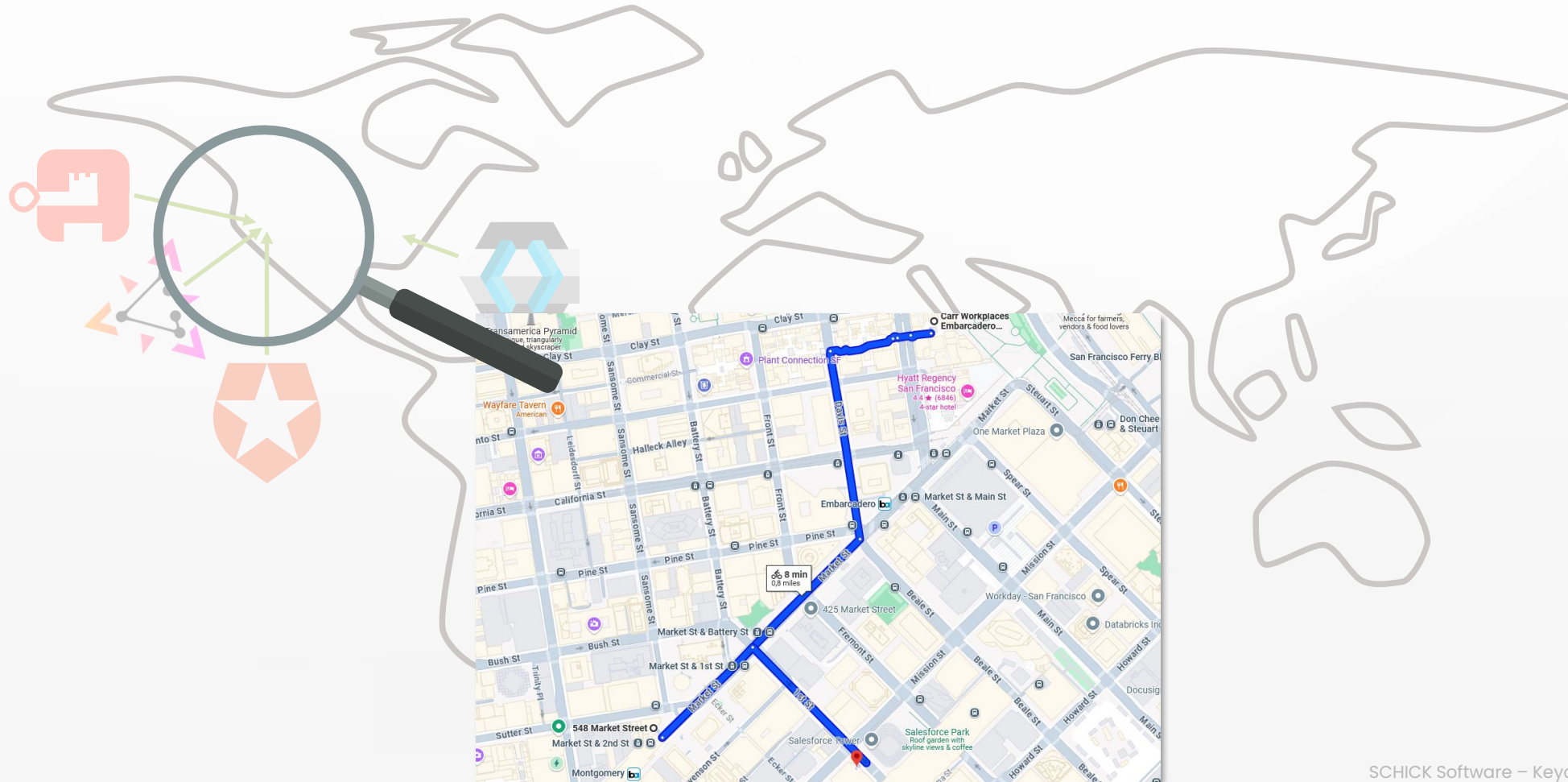
Übersicht

# Hauptsitz der Firmen



Übersicht

# Hauptsitz der Firmen



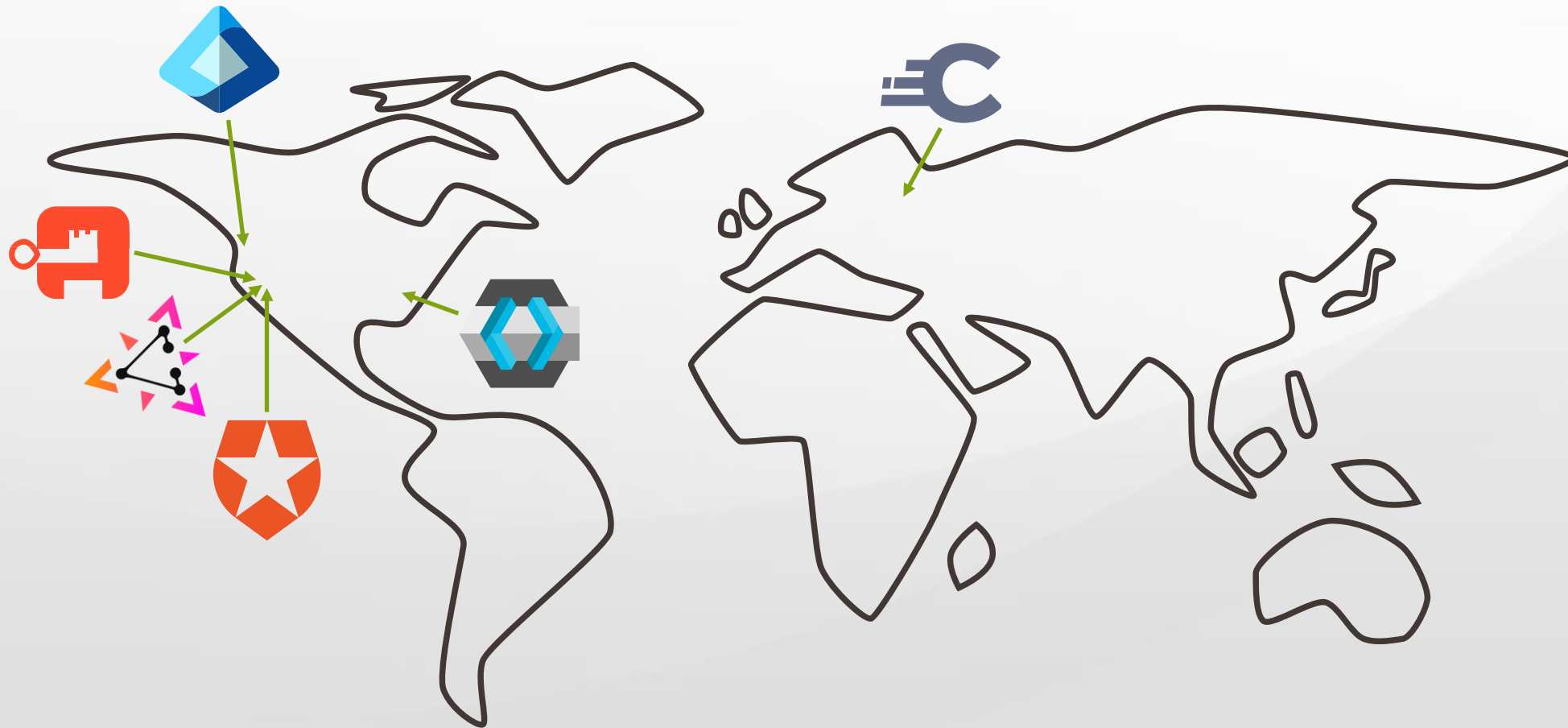
Übersicht

# Hauptsitz der Firmen



Übersicht

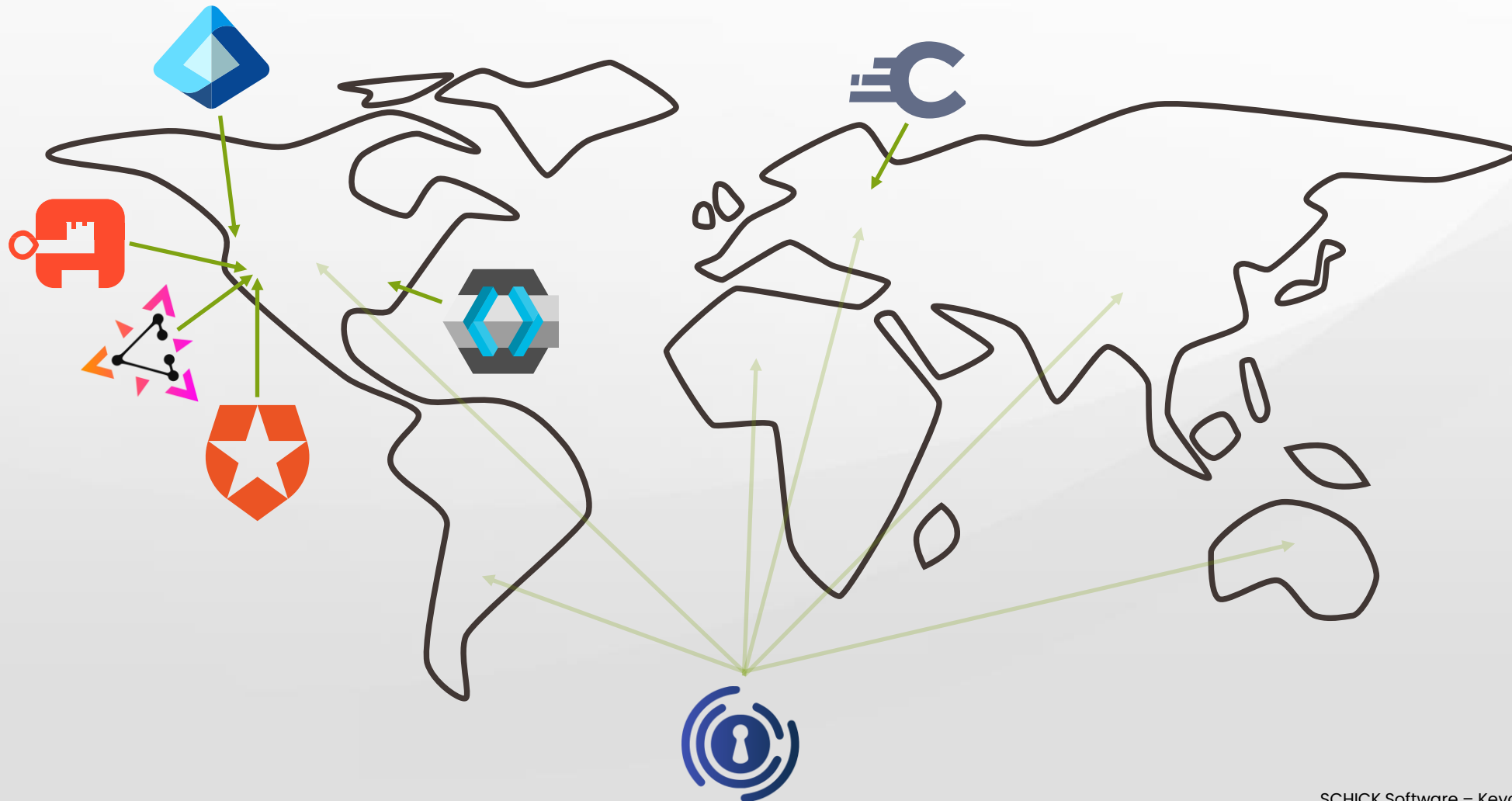
# Hauptsitz der Firmen





Übersicht

# Hauptsitz der Firmen



Features

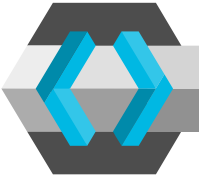
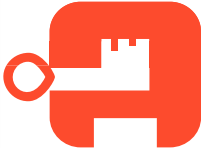




# Features



HICK  
RE-ENTWICKLUNG



# Allgemeine Features

	Keycloak	Authentik	Zitadel	auth0	curity	Entra ID
						
Branding	✓	✓	limited	paid	✓	
Plugins	✓	X	✓	paid	paid	
REST API	✓	✓	partial	✓	partial	
Swagger spec.	✓	✓	broken	limited	X	

# Authentifizierungsverfahren

## **Authorization Code Grant**

Öffentliche Clients, z.B. Single Page Applications

## **Client Credentials Grant**

Machine-to-Machine

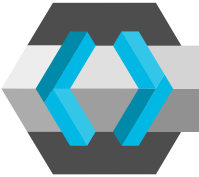
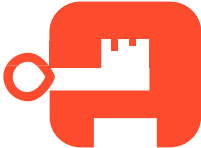




## **Device Authorization Grant**

Geräte ohne Eingabemöglichkeiten

## **Client Initiated Backchannel Authentication (CIBA)**

Geräte ohne Eingabemöglichkeiten

# Authentifizierungsverfahren

	Keycloak	Authentik	Zitadel	auth0	curity	Entra ID
						
Auth. Code	✓	✓	✓	✓	✓	
Client Cred.	✓	partial	✓	✓	✓	
Device Auth.	✓	✓	✓	✓	✓	
CIBA	✓	✗	✓	preview	✓	

# Anmeldeverfahren

## Benutzername und Passwort

Der Benutzer meldet sich mit einem Benutzernamen und Passwort an

## WebAuthn / Passkey

Schlüsselbasierte Anmeldung über ein physisches Gerät, z. B. YubiKey oder Biometrie, z. B. Fingerabdruck

## E-Mail

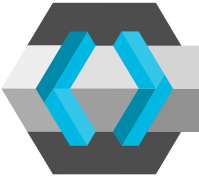
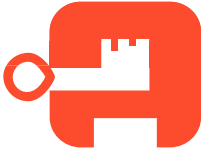




Einmal-Url zum Einloggen

## SMS

Code zum Einloggen per SMS



# Anmeldeverfahren

	Keycloak	Authentik	Zitadel	auth0	curity	Entra ID
						
Name/Passwort	✓	✓	✓	✓	✓	
WebAuthn	✓	✗	✓	paid	✓	
E-Mail	?	?	?	paid	?	
SMS	?	?	?	?	?	

# Multi-Faktor-Authentifizierung

## Time-based one-time password (TOTP)

Zeitbasierter Einmalcode, von einer Authenticator-App (z. B. Google Authenticator) generiert

## E-Mail

Einmalcode oder einen Bestätigungslink per E-Mail, der zur Authentifizierung verwendet wird

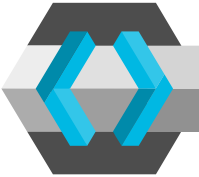
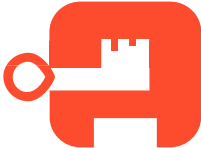




## SMS

Einmalcode per SMS, der zur Authentifizierung verwendet wird

## WebAuthn

Moderne, schlüsselbasierte Authentifizierung, bei der der Nutzer ein physisches Gerät (z. B. YubiKey) oder biometrische Daten (z. B. Fingerabdruck auf dem Smartphone) verwendet

# Multi-Faktor-Authentifizierung

	Keycloak	Authentik	Zitadel	auth0	curity	Entra ID
						
TOTP	✓	✓	✓	paid	✓	
E-Mail	✗	✗	✓	paid	✓	
SMS	✗	✗	limited	paid	✓	
WebAuthn	✓	✓	✓	paid	✓	

Rechteverwaltung

# Rechteverwaltung

# RBAC und UMA

## Role-Based Access Control

Berechtigungskonzept, welches den Zugriff auf Ressourcen basierend auf Nutzerrollen wie "Admin" oder "Mitarbeiter" festlegt.

## User-Managed Access

Granulares Berechtigungskonzept, welches den Zugriff basierend auf

- Ressourcen (z.B. API-Routen) und
- Regeln (z.B. Benutzer über MFA authentifiziert)

festlegt

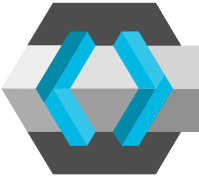
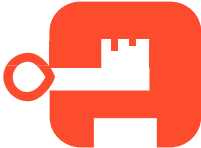




# Token Exchange (RFC 8693)

## Impersonation and Delegation

Impersonation liegt vor, wenn das Subjekt in einem Token vom ursprünglichen Subjekt nicht zu unterscheiden ist.

Im Falle einer Delegation enthält ein Token die ausdrückliche Information, dass ein Subjekt seine Rechte an eine andere Entität delegiert.

# RBAC, UMA und Token Exchange

	Keycloak	Authentik	Zitadel	auth0	curity	Entra ID
						
RBAC	✓	✓	✓	paid	✓	
UMA	✓	✗	✗	✗	✗	
Token Exchange	preview	✗	✓	preview	✓	



Setup & Integration

# Setup & Integration



SCHICK  
SOFTWARE ENTWICKLUNG





# Vorgehensweise

Die Installation, Einrichtung & Integration erfolgte

- Time-Boxed á 6 Stunden je Produkt
- ohne produkt-spezifische Vorkenntnisse
- anhand der Dokumentation auf der Homepage
- und Google-Anfragen, jeweils die ersten 5 Treffer
- in eine bestehende Demo-Anwendung
- OHNE Verwendung von ChatGPT

# Vorgehensweise

Ich habe verwendet:

- .NET 8/9, Standard-Mechanismen, keine 3rd-Party Bibliotheken
- Angular 18 mit ‚angular-oauth2-oidc‘ von Manfred Steyer

# Erkenntnisse

## Keine 5-Minuten Lösung

Keiner der Provider ist „mal eben“ ausprobiert

## Begrifflichkeiten unterschiedlich

„Roles“, „Groups“ und „Permissions“ werden munter vertauscht

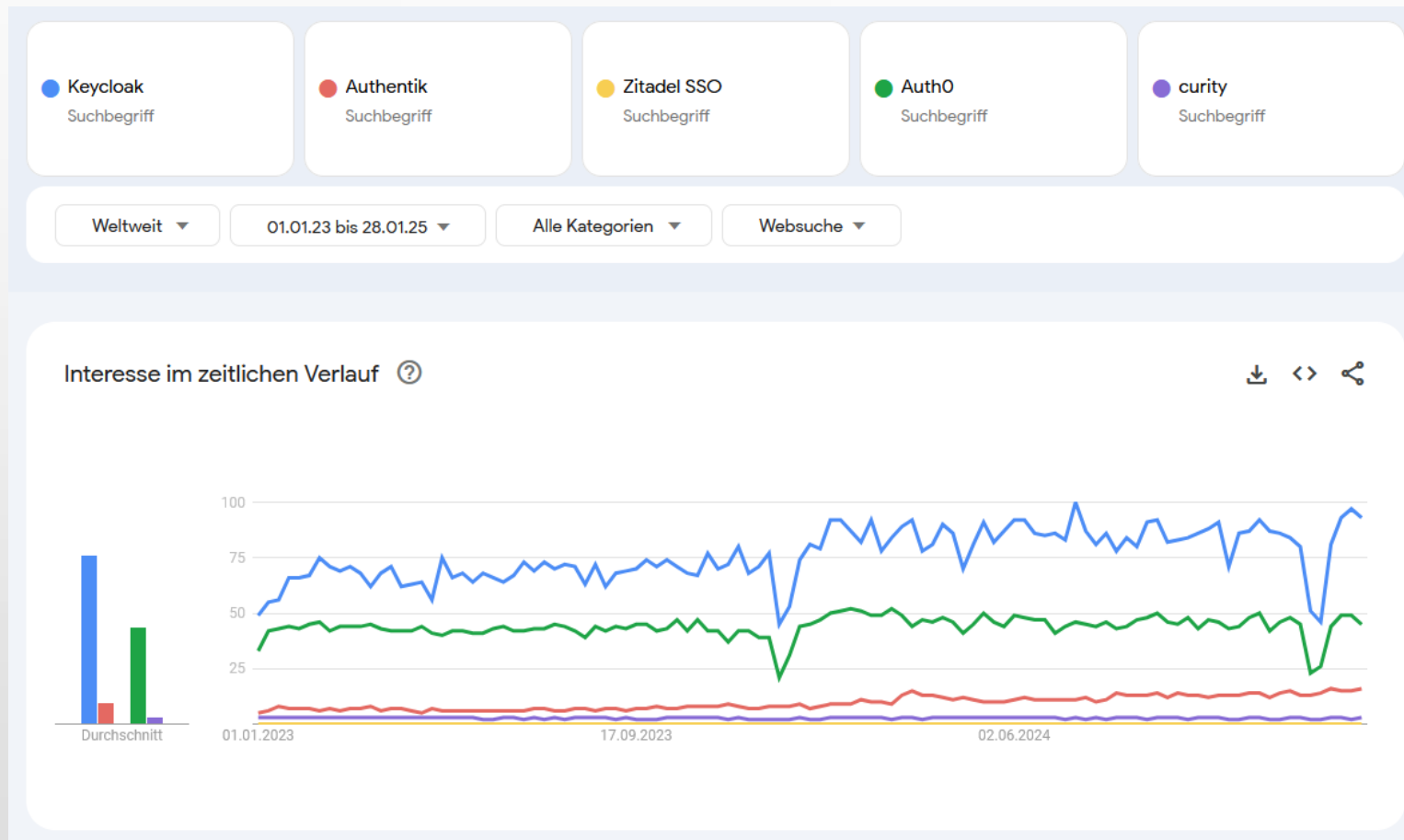
## Dokumentation

Extrem große Unterschiede bei der Qualität der Dokumentation. Sowohl zwischen den Produkten als auch zwischen den Bereichen (Installation, Einrichtung, Integration)

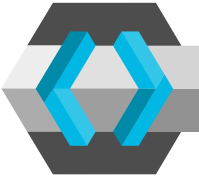
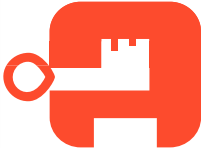




## Integration

Die eigentliche Herausforderung ist oft nicht die Integration in .NET / Angular sondern das Setup und die Einrichtung des Identity-Providers


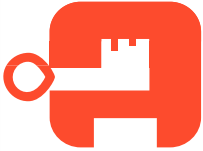




# Google Trends



# Ergebnis

	Keycloak	Authentik	Zitadel	auth0	curity	Entra ID
						
Installation	✓	✓	✓	✓	✓	
Anmeldung	✓	✓	✓	✓	✗	
RBAC	✓	✗	✓	✗	✗	
Integration	✓	✓	✓	✓	✗	

# Fazit \*

Keycloak	Authentik	Zitadel	auth0	curity	Entra ID
					
Bester Gesamteindruck	Befindet sich „in der Entwicklung“	Guter Gesamteindruck	Sinnvoll nur mit Abonnement nutzbar	Komplexes Produkt mit sehr vielen Features	

\* persönlicher, subjektiver Eindruck





# Vielen Dank

[www.schick-software.de](http://www.schick-software.de)

SCHICK Software – Keycloak, Authentik, SaaS