IHRE SOFTWARE **EFFIZIENTER** ENTWICKELT

Self-made Identity
Zentrale Authentifizierung in der Cloud

Dustin Baron | Consultant
Florian Bader | Senior Consultant

Mit wem habt ihr es zu tun?

AIT – Applied Information Technologies GmbH & Co KG.

Dustin Baron

+49 151 550526-43

Dustin.Baron@aitgmbh.de

Florian Bader

+49 151 550526-21

@FlorianBaderDE

Florian.Bader@aitgmbh.de

Leitzstraße 45
70469 Stuttgart
GERMANY

www.aitgmbh.de

@aitgmbh

Take aways

Was war die Problemstellung?

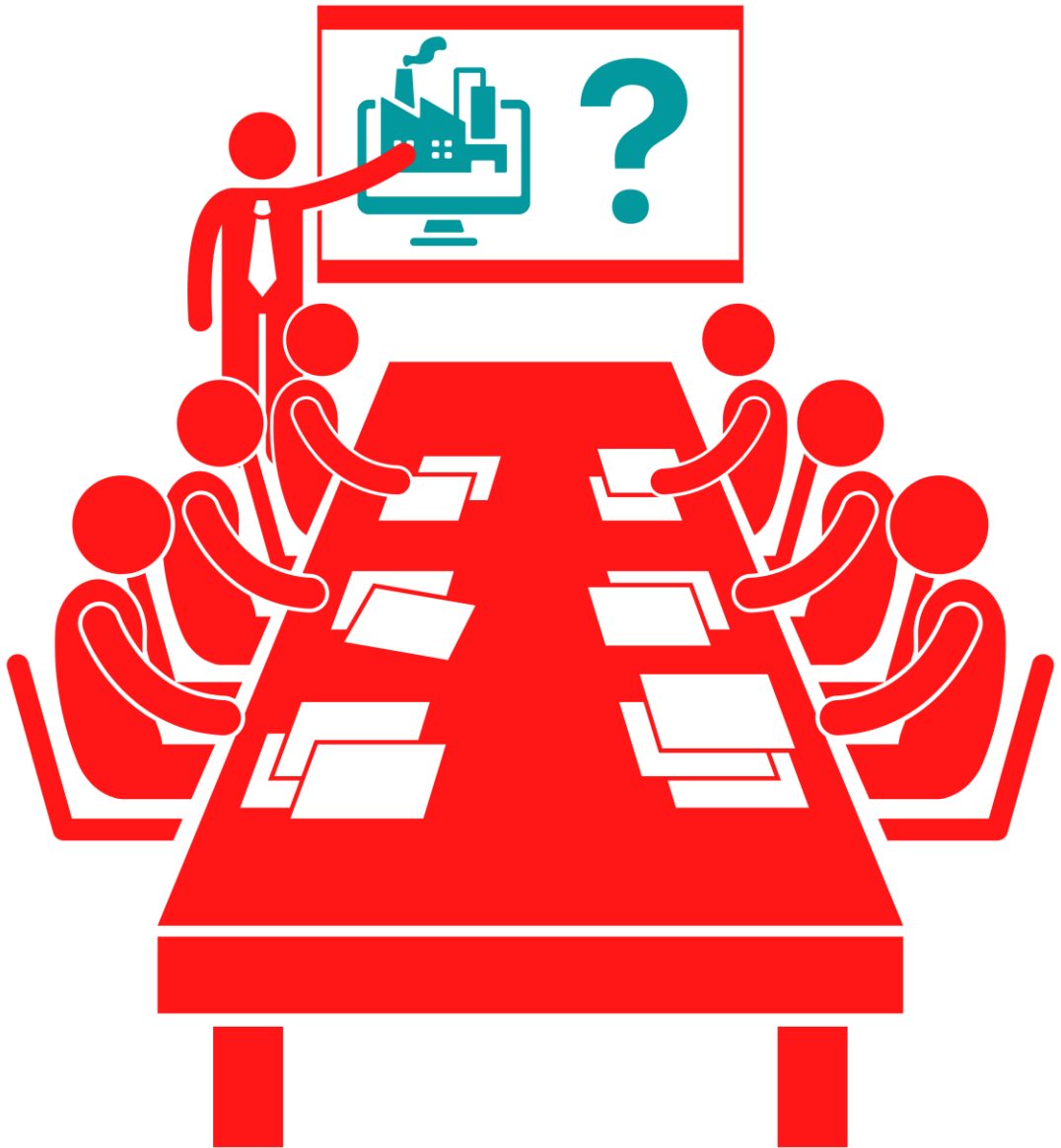
Wofür haben wir uns entschieden?

Wie sind wir vorgegangen?

Wie sieht die Zukunft aus?

Die eigentliche Problemstellung

- Frage: "Wieso einen eigenen Identity Provider?"
- Problem des Kunden: Digitalisierung der Prozesse
- Ziel: Eine ID für alle Anwendungen



Einfach oder nicht?

- Identity Provider aufsetzen
- Eigene Clients und externe Partner anbinden
- Identitäten anlegen

Zu Anfang leider viele Unbekannte...

- Blackbox "Kundendomäne"
- Altlasten
- Kundenwünsche
- Technische Anforderungen
- Externe Partner
- Ressourcen
- ...

Digitalisierung des Unternehmens

- Mitarbeiter müssen Prozesse noch analog durchführen
  - Szenario 1: B2B Kunde möchte eine Bestellung tätigen
    - Können nur designierte Personen vom Kunden
    - Eigene Konditionen je nach Kunde
    - Eigene Ansprechpartner innerhalb der Firma
    - Eigene Bestellprozesse
    - Sonderwünsche
    - …

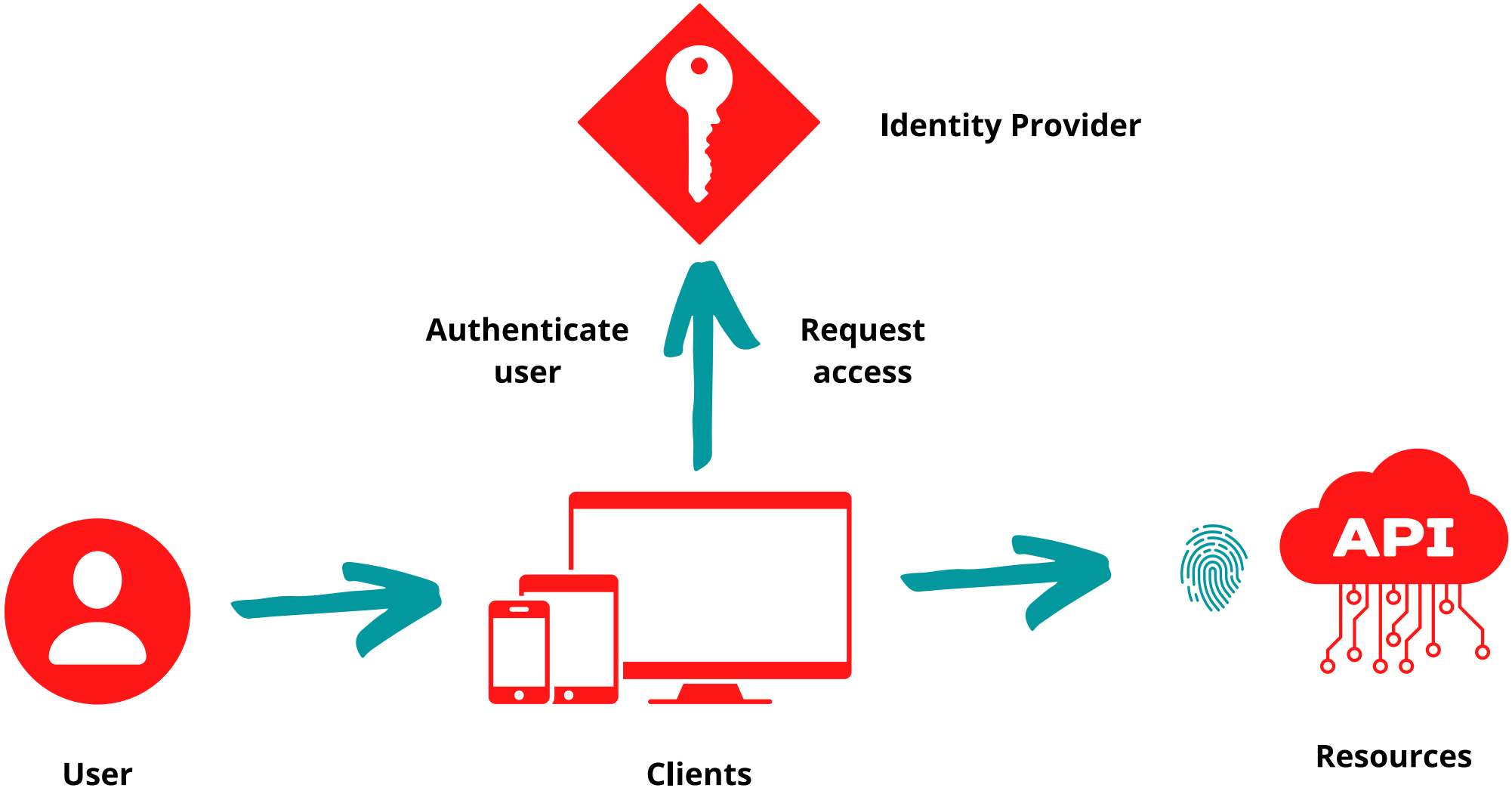
Digitalisierung des Unternehmens

- Mitarbeiter müssen Prozesse noch analog durchführen
  - Szenario 2: Kunde A ruft an und möchte Informationen zu einem Produkt haben
    - Mitarbeiter muss in der Firma Informationen zusammensuchen
    - Altdokumente z.B. früherer Firmenzusammenschluss
    - unterschiedliche Dokumentensysteme
    - Wissen von anderen Mitarbeitern

Das akute Problem – Wer bin ich?

- Wer ist ein Mitarbeiter?
- Unterschiedliche Arten von Kunden
  - Privatkunden
  - Geschäftskunden
- Zugriff auf unterschiedliche Services
  - Eigene Services
  - Externe Partner
  - PIM Systeme (Product Information Management)
  - ERP System (Enterprise Resource Planning)
- Unterschiedliche Berechtigungen innerhalb der Cloud
- **Ziel: Eine Identität für "ALLES"**

Konzept und Terminologie

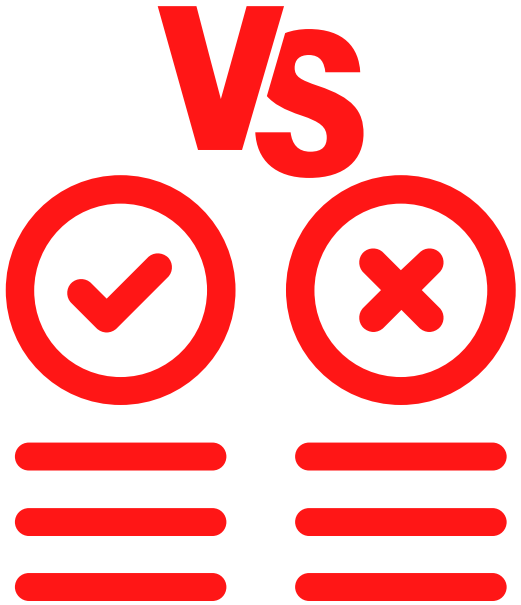


Was sind die Möglichkeiten?

- Software-as-a-Service (SaaS) vs. Platform-as-a-Service (PaaS)
  - Eigenes Hosting einer Lösung
  - Fully Managed Lösung

- SaaS
  - Azure Active Directory
  - Auth0
  - …

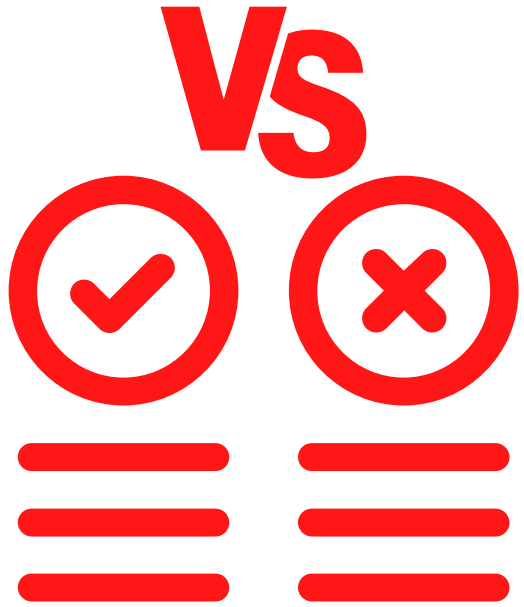
- PaaS
  - Identity Server
  - Keycloak
  - …



- Entscheidung für PaaS
  - Volle Kontrolle über den Identity Provider und die Daten
  - Vollumfängliches Customizing

Was sind die Möglichkeiten?

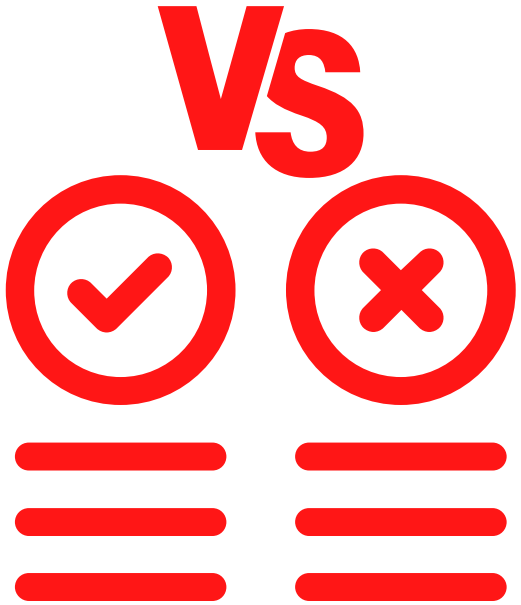
- Keycloak
  - Kostenlos und Open Source
  - Java
  - Umfangreiche Features, Doku zum Teil lückenhaft
- Identity Server
  - Kostenlos (mittlerweile kostenpflichtig) und Open Source
  - .NET
  - Umfangreiche Features, Doku und Beispiele sehr gut



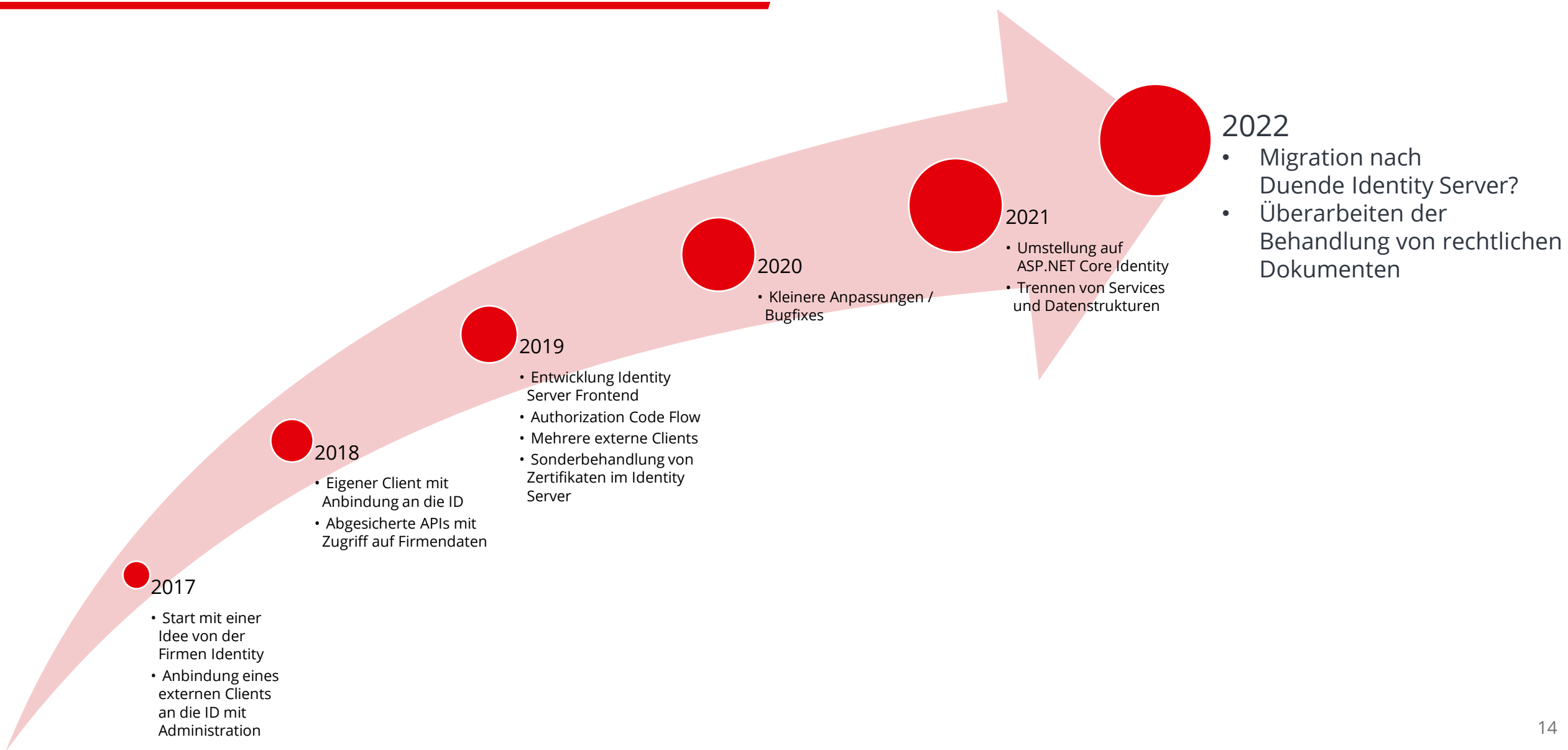
- Open ID Connect, OAuth 2.0, SAML 2.0, LDAP Integration
- 2017: Entscheidung für Identity Server

Wieso Identity Server 4.0 ?

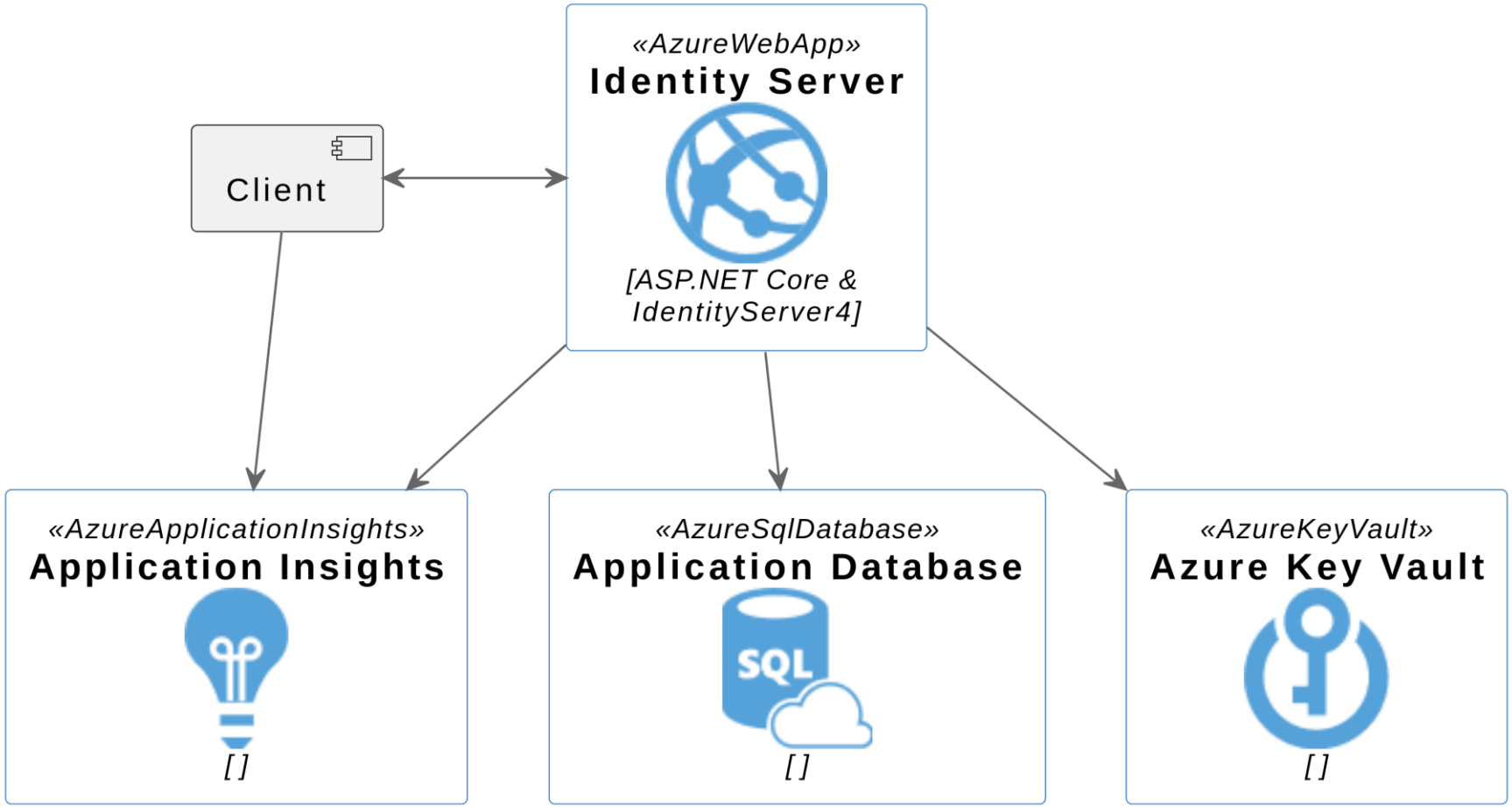
- Zum Start des Projektes: Wohin geht die Reise eigentlich?
- Vorhandene Erfahrungen bei Teammitgliedern
  - Microsoft Welt
- Einfacher Einstieg mit dem Identity Server
  - Fluktuation im Projektteam
- Flexible Anpassungsmöglichkeiten für Kundenwünsche
  - Abbildung der Domäne und ihren Eigenheiten
- Keine Kosten für die Nutzung des Identity Servers 4.0
  - Änderung mit **Duende Identity Server!**



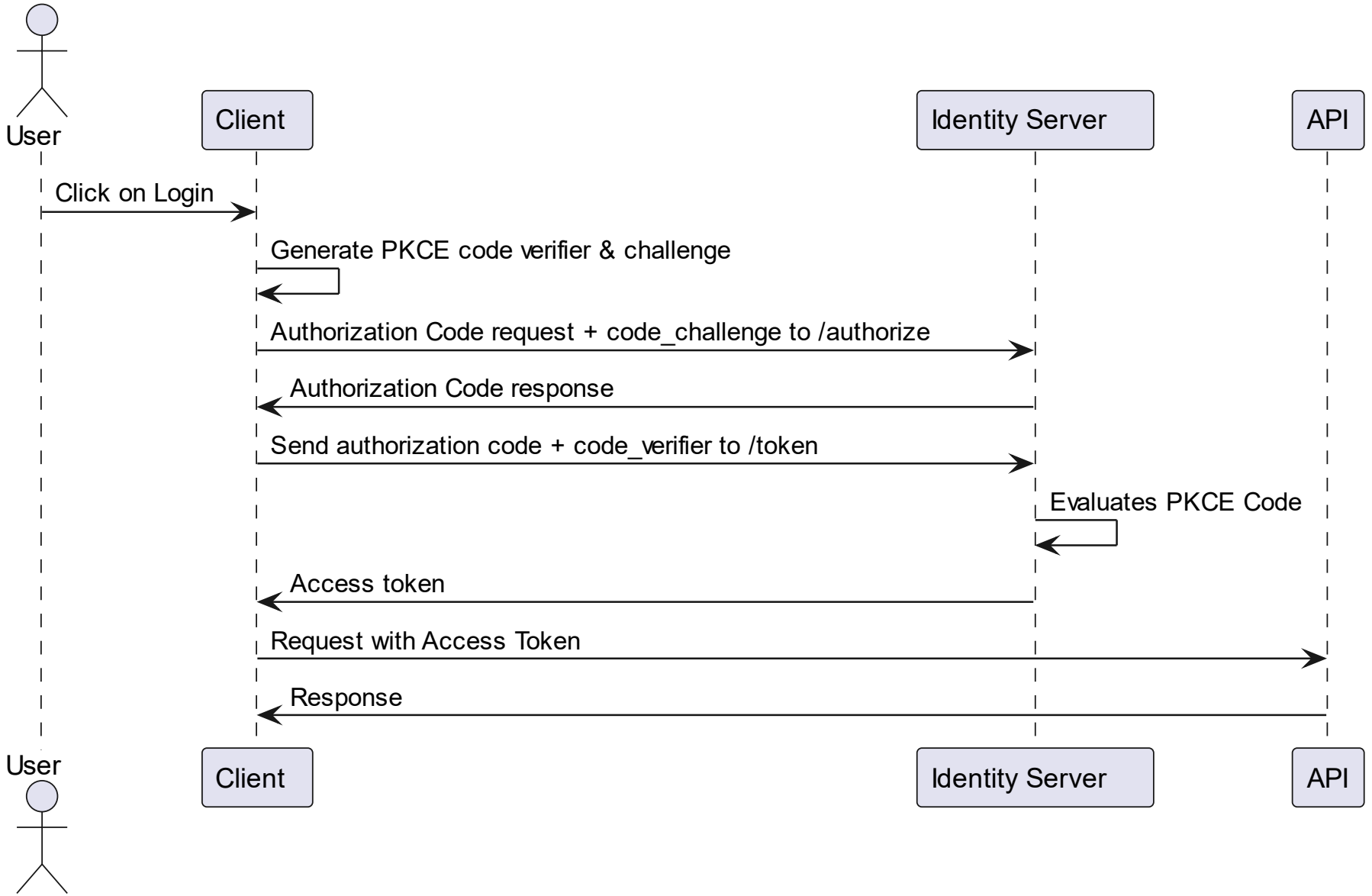
Der zeitliche Ablauf des Identity Servers im Projekt



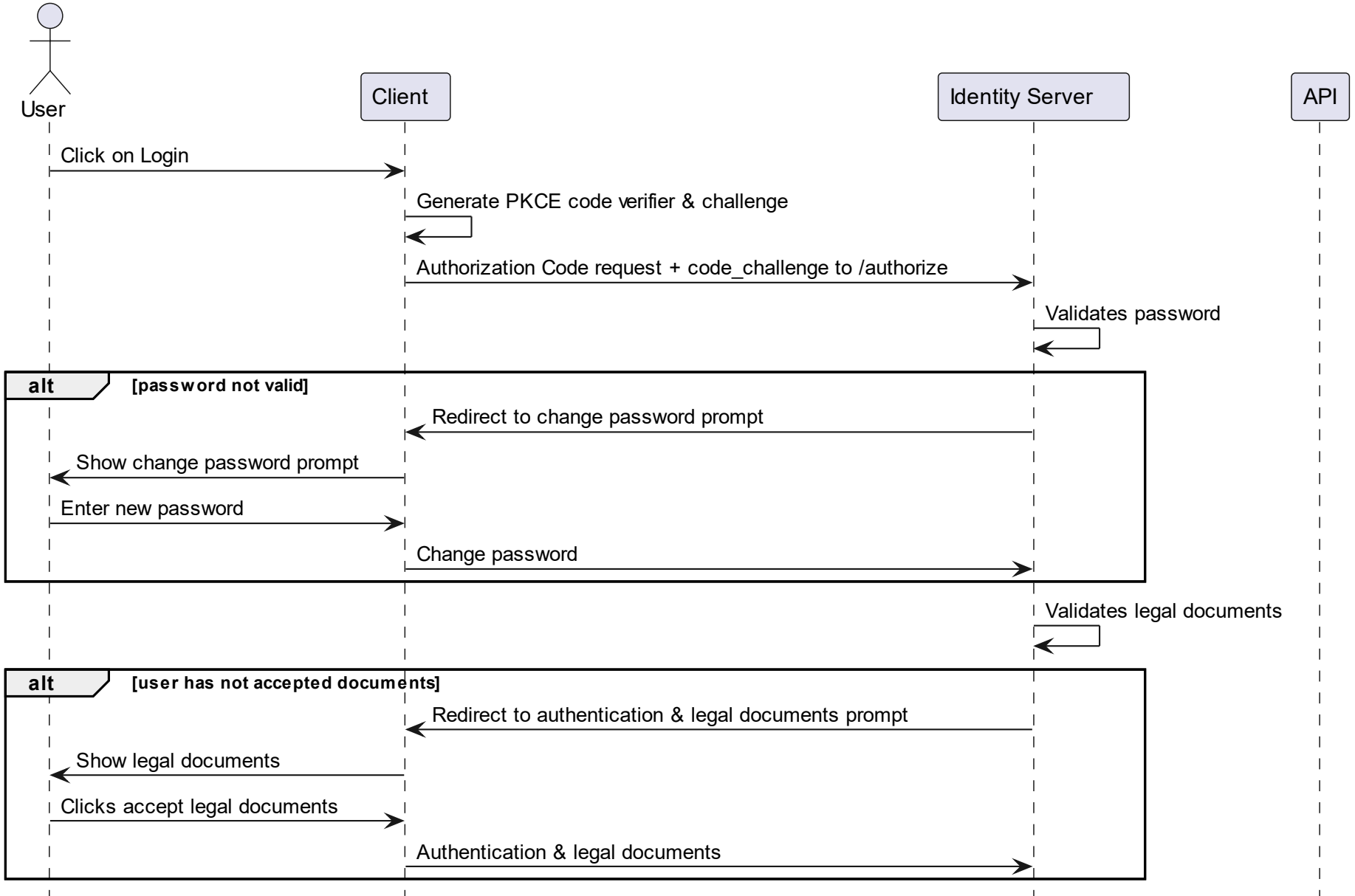
Infrastruktur in Azure



Authentication Flow - Standard

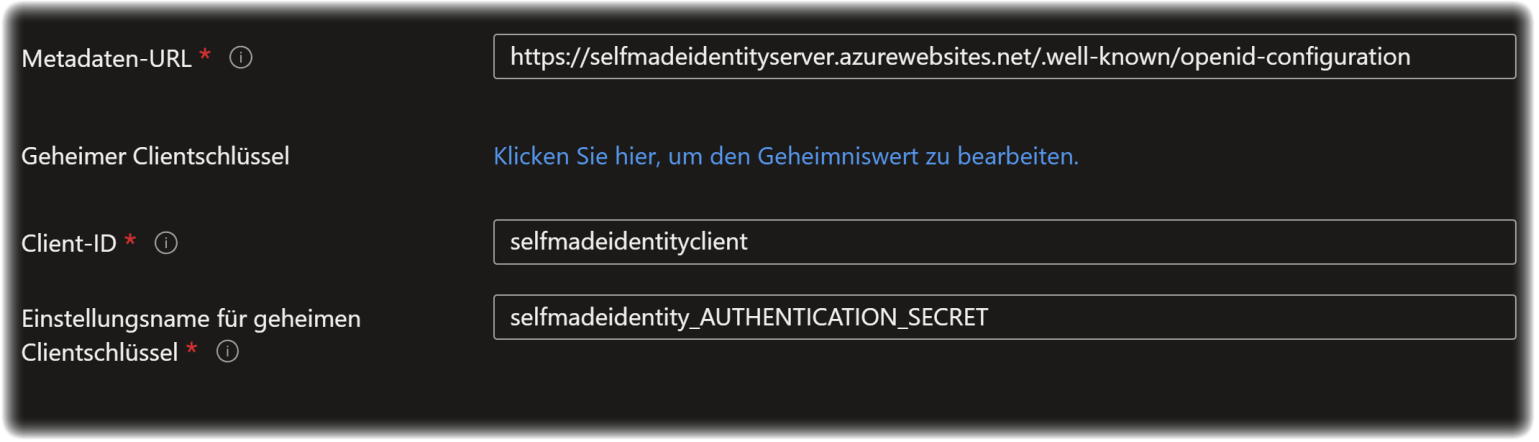


Authentication Flow - Custom



Client Konfiguration - Beispiel

- Sichern einer Azure Web Anwendung mit EasyAuth und eigenem Identity Server




```
new Client
{
    ClientId = "selfmadeidentityclient",
    ClientSecrets = { new Secret("49C1A7E1-0C79-4A89-A3D6-A37998FB86B0".Sha256()) },
    AllowedGrantTypes = GrantTypes.Code,
    RedirectUris = { "https://selfmadeidentityclient.azurewebsites.net/.auth/login/selfmadeidentity/callback" },
    RequirePkce = false,
    AllowOfflineAccess = true,
    AllowedScopes = { "openid", "profile", "email" }
},
```

Identity Server - Migration

- Basierend auf https://docs.duendesoftware.com/identityserver/v6/upgrades/is4_v4_to_dis_v6/
- Migration in sieben Schritten
- Neues Problem: Lizensierung
- Neue Entscheidungen
  - Migration
  - Anderes Framework
  - Fertige Lösung

Vom Anfang bis zum Ende – Lessons Learned

- Identity Server und Client sollten **keine** Nebenbaustellen sein
- Rechtzeitig mit den Konzepten auseinandersetzen
  - Identity Server, Authorization Code Flow, OAuth, OpenID, …
- Klare Aufgabentrennung in der Cloud
  - Späteres Trennen von z.B. Services und Daten erfordert viel Migrationsaufwand
- MVC Anwendung für Identity Server Frontend anstatt Angular
- Rechtliche Dokumente für Clients trennen
  - Nutzungsbedingungen, Datenschutzbestimmungen, …
- Gestartet mit Custom-Lösung und später ASP.NET Core Identity
- Und noch mehr…

Fazit

Die Kundendomäne ist der Treiber

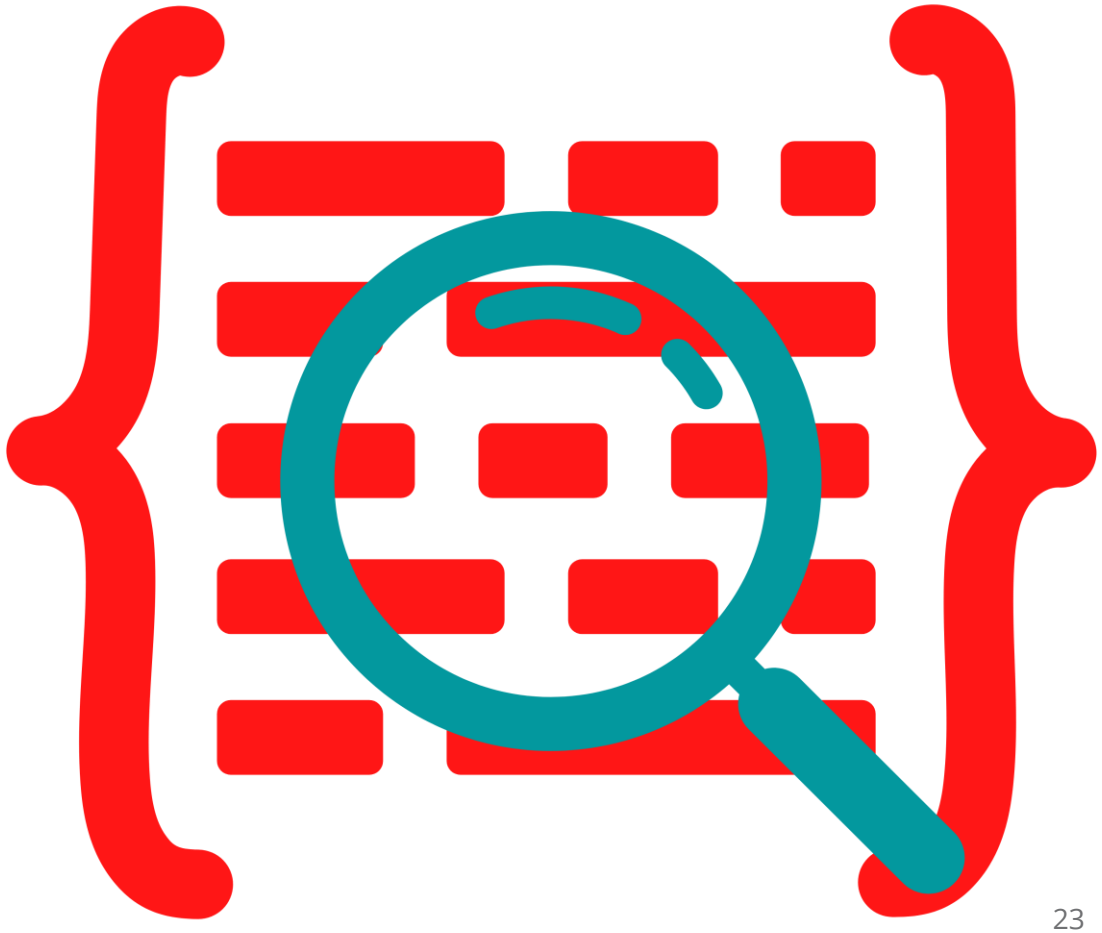
Die Konzepte beim Identity Server verstehen

Einfacher Start mit Identity Server

Nichts ist in Stein gemeißelt

Identity Server – Live Demo

- Basierend auf https://github.com/IdentityServer/IdentityServer4.Templates



Icons by canva.com

WIR SUCHEN **DIE BESTEN!**

Entwickler, Berater, Software-Architekten,
Werksstudenten, Junioren, Senioren,...

www.aitgmbh.de/jobs

Jetzt bewerben und Karrierechance sichern !