

Dr. Johannes C. Schneider

Zentrale Authentifizierung mit OAuth2 in einem technologisch heterogenen App-Ökosystem



Über mich

- Fraunhofer IESE, Kaiserslautern
- Software-Entwickler
- Software-Architekt
- Abteilung Software-Architektur
 - Architektur-Schulung
 - Architektur-Bewertung



Digitale Dörfer Kurzvorstellung

Digitale Dörfer Phase 2



Schauen sie sich unser Erklärvideo zu Phase 2 an:
<https://www.youtube.com/watch?v=fHYpKpZzklo&t=1s>

Digitale Dienste



DorfNews



DorfFunk



DorfDigital



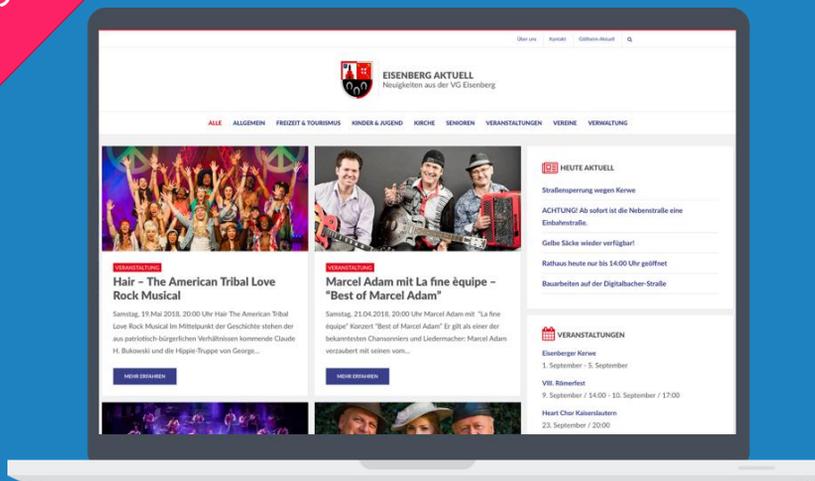
BestellBar



LieferBar

WordPress, PHP

DorfNews Immer auf dem Laufenden!



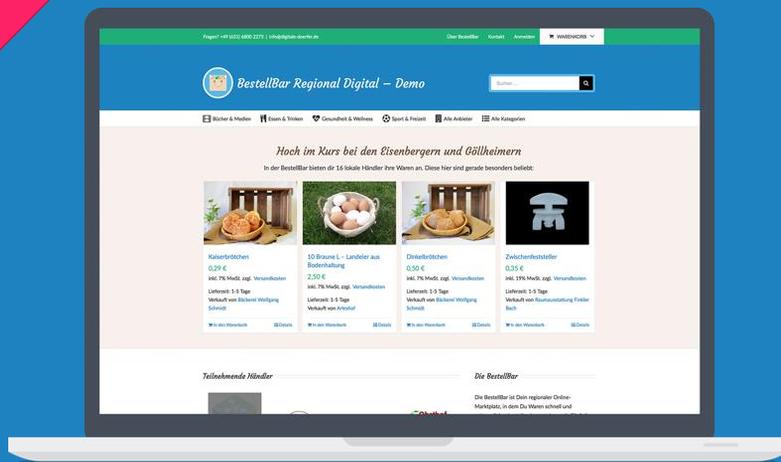
Xamarin, iOS/Android



DorfFunk
Das Digitale Dorf in der
Tasche!

WordPress, PHP

BestellBar
Der lokale Online-Marktplatz





LieferBar

Der flexibel einsetzbare Mitbringservice

Xamarin, iOS/Android

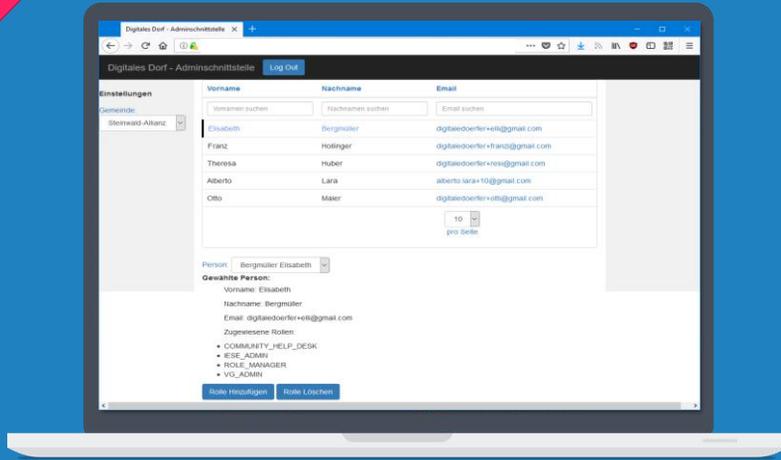
AngularJS

Admin-UI LieferBar/BestellBar

Status	Bestellt	Verpackt	Shop	Empfänger	akt. Lieferant	Inhalt
	von	bis				
	03.05.2016	03.05.2016	Ausdauer Shop	Herbert Wolf	-	1* Digitale Dörler ...
	05.2016, 12:05 Uhr	05.2016, 12:05 Uhr	Bären-Apotheke	Herbert Wolf		1* Aspirin Plus C, ...
Warten auf Abholung	05.2016, 12:05 Uhr	05.2016, 12:05 Uhr	Bären-Apotheke	Elisabeth Maier	Herbert Wolf	1* Aspirin Plus c 1* Pramenbol
Warten auf Abholung	03.05.2016, 09:54 Uhr	03.05.2016, 12:08 Uhr	Bären-Apotheke	Marc Peters	Julia Müller	1* ...

???. (Web-Technologien,
OSGi Backend)

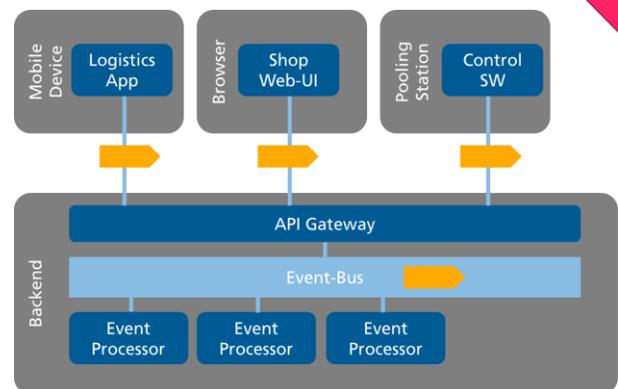
Admin-UI Rechteverwaltung



Backend Basis für alle Dienste

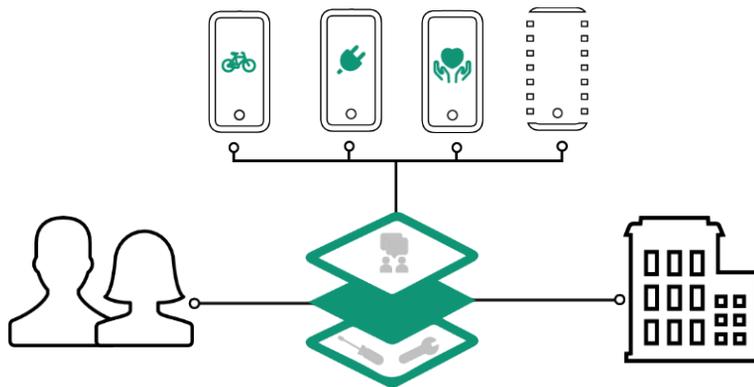
Java

- Event-orientiert
- REST-Schnittstelle





Reallabor PFaff



© 2018 alle Rechte vorbehalten. Alle Rechte vorbehalten.



Bundesministerium
für Wirtschaft
und Energie



Bundesministerium
für Bildung
und Forschung



Feststellungen

- heterogene Technologien
- Benutzer-Login erforderlich z.B. für
 - DorfNews-Beitrag erstellen
 - DorfFunk-Plausch erstellen
 - BestellBar-Bestellung abgeben
 - Benutzerrollen verwalten
- Auch Drittanbieter-Anwendungen brauchen Zugriff auf Benutzerdaten

Kernfragen

**Wie kann ein Benutzer
unabhängig von der verwendeten
Client-Technologie überall eine
gleiche Login-Erfahrung machen?**

**Wie können wir es einem
Benutzer ermöglichen,
vorhandene Accounts zum Login
zu verwenden?**

Wie kann eine Anwendung über längere Zeit Aufrufe im Namen des eingeloggten Benutzers tätigen, ohne dass sich der Benutzer neu einloggen muss oder die Anwendung das Passwort des Benutzers speichert?

Wie kann ein Benutzer selbst entscheiden, welche Daten er einer Drittanbieter-Anwendung zur Verfügung stellt?

**Wie verhindern wir, dass
Drittanbieteranwendungen auf
unserer Plattform Zugriff auf das
Passwort des Benutzers erhalten?**

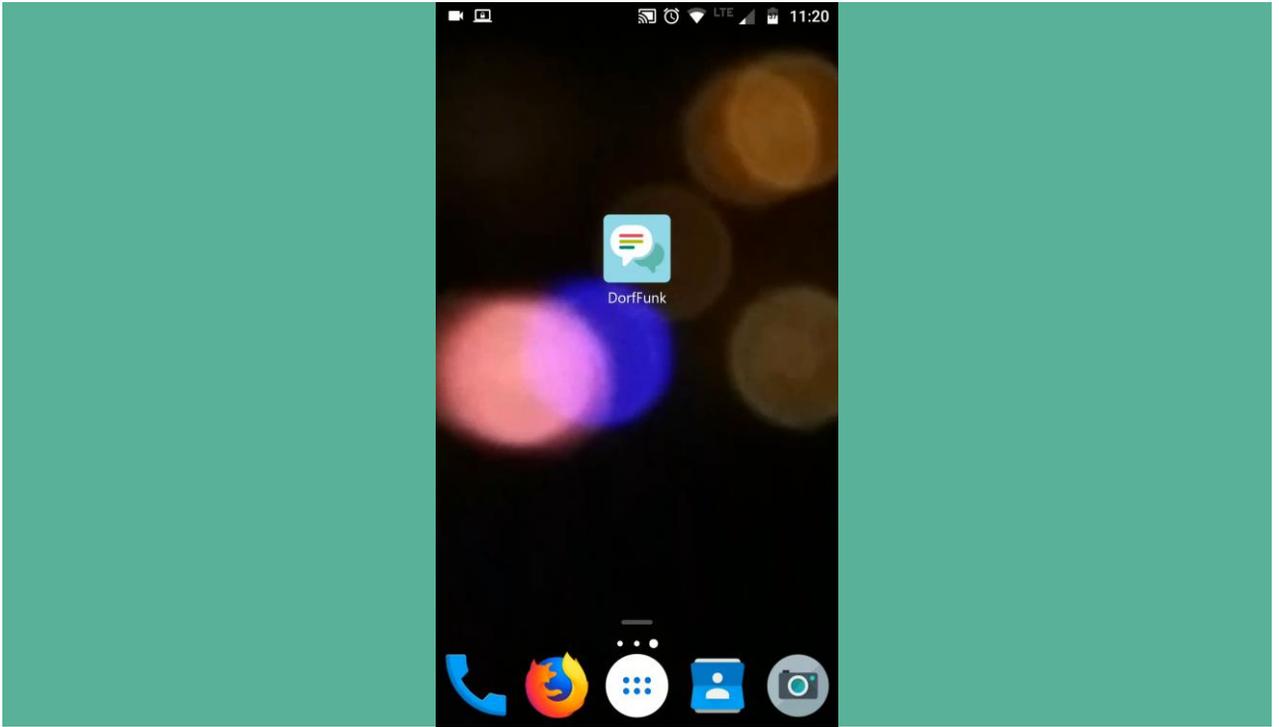
**Die Lösung:
Zentrale Authentifizierung mit
OAuth2!**

Digitale Dörfer Umsetzung aus Benutzersicht

The screenshot displays a web browser window with the URL <https://www.digital-doefer.de>. The page features a green navigation bar with links for 'Über BestellBar', 'Kontakt', 'Anmelden', and 'WARENKORB'. Below this is a blue header with the logo 'BestellBar Regional Digital – Demo' and a search bar. A white navigation bar lists categories: 'Bücher & Medien', 'Essen & Trinken', 'Gesundheit & Wellness', 'Sport & Freizeit', 'Alle Anbieter', and 'Alle Kategorien'. The main content area is titled 'Hoch im Kurs bei den Eisenbergern und Gölheimern' and states: 'In der BestellBar bieten dir 11 lokale Händler ihre Waren an. Diese hier sind gerade besonders beliebt:'. Four product cards are shown:

- Orangensaft (frisch gepresst), 1 l Flasche**: 4,99 € (4,99 € / l). Includes 7% MwSt. and shipping costs. Delivery time: 1-5 days. Sold by HIT Echte Vielfalt.
- Äpfel Rubinette Beutel a 2,5kg**: 4,00 €. Includes 7% MwSt. and shipping costs. Delivery time: 1-5 days. Sold by Obsthof Enders.
- Roggenmischbrot**: 1,90 €. Includes 7% MwSt. and shipping costs. Delivery time: 1-5 days. Sold by Bäckerei Wolfgang Schmidt.
- 10 Braune L – Landeier aus Bodenhaltung**: 2,50 €. Includes 7% MwSt. and shipping costs. Delivery time: 1-5 days. Sold by Afleshof.

Each product card includes a 'Details' link and an 'In den Warenkorb' button.



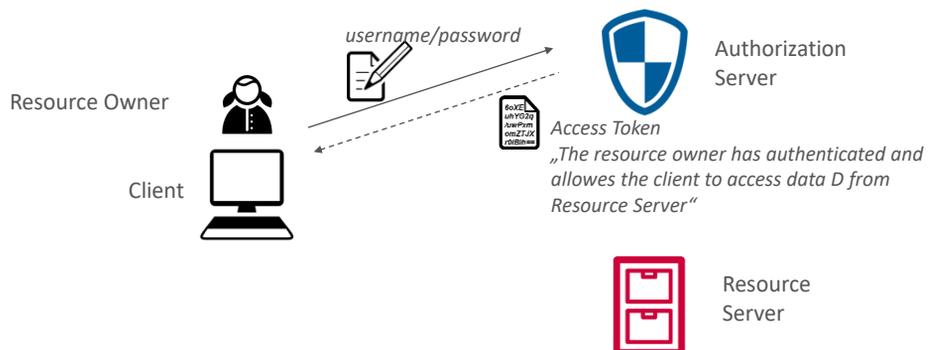
Wie OAuth2 funktioniert

Rollen



27

Genereller Ablauf



28

Genereller Ablauf



29

Scope

- frei definierbarer String, z.B. „read:profile read:location“
- OAuth2-Implementierung holt User-Consent ein
- Resource-Server muss sicherstellen, dass der übermittelte Scope zur Anforderung der Ressource berechtigt.

Hallo Johannes,

die Anwendung „DorfFunk“ möchte auf folgende Daten von dir zugreifen:

- dein Profil lesen
- deinen aktuellen Standort lesen

OK

Abbrechen

Im Detail



Access Token

- JWT-Format (JSON Web-Token)
- Base64-codiert
- Auch „Bearer Token“ genannt, weil es bei Requests im „Authentication“- Header als „Bearer <token>“ mitgeschickt wird

eyJhbGciOiJSUzI1NiIsImtpZCI6IiJFVTkROVUzZDTIRCQk1rW
HEADER kJlVTRNMEZETWpsQ05rSTBSall4UWtRNU9UVTVPQsJ9.eyJodHRwOi8vZGlnaXRhbGUtZG9lcmZlci5kZS9lbWV1LmF1dGgwLmNvbS8iLCJzdWliOiJhdXRoMHw1YWVjNDlhNGVmNzlxNTBjNjhlhYTFkYWYiLCJhdWQiOiJlc3R5bGlnaXRhbGUtZS8iLCJodHRwczovL2RkLWRldi5ldS5hdXRoMC5jb20vdXNlcmluZnVjoxNTI1NDM0ODExLCJleHAiOiE1MjU1MjEyMTEsImF6cCI6ImhZV1VCdUtlNTRpY05ienZ3Uzg0Q05VMjh5MFVIQWp4liwic2NvcGUiOiJvcGVuaWQgZW1haWwifQ.Gr_M8lphA2T1DTqiKDpgl79FfE8vEsdzRfqt1CZL3QnrFmvU-tjv63nFe2O9h_0mAMnDTMX0vmQ59XmFWtZZe7Bi0UzkGQUvVVLfscwAVFgLbSO81-00y7-Rcj5ln-Dae67Sen9a8ekID44ERcBbJeWfzqKs5A6Wvue5HiXCzpgLoAeVph47EERT2T3gd5zQSIO1iGk4upn-Dyla9Ql-ZORKjOC1Ehr9FWYjHijjKLNiyyFurTICQDua3Jx3evqjVHBVP_T9s8Fjnnirp21eyJ76j6oiQs4ExhewrawdAbsKpOIYtuyCfvVNg4wccTbc56YhQ

BODY

SIGNATURE

```
{
  "typ": "JWT",
  "alg": "RS256",
  "kid": "QUND...TU5OA"
}, {
  "iss": "https://auth.digitale-doerfer.de/",
  "sub": "auth0|5aec49a4ef82150c69aa1dag",
  "aud": [ "https://api.digitale-doerfer.de/" ],
  "iat": 1525434811,
  "exp": 1525521211,
  "azp": "xYWUB28",
  "scope": "read:profile read:location"
  "http://digitale-doerfer.de/email_verified": false,
}
```

Signatur (Binärdaten) signiert mit privaten Schlüssel des Auth.-Servers
 Res.-Server kann den öffentlichen Schlüssels speichern
 und offline das Token verifizieren.

Issuer: Auth-Server
Subject: User-ID
Audience: Res.-Server API
Issued At: Timestamp
Expires: Timestamp
Authorized party: Client-ID
Scopes: erlaubte Ressourcen
Custom-Content

Refresh-Token, Motivation

Bisheriger Flow:

Wenn `access_token`
abgelaufen, erneuter Login
(=Benutzerinteraktion)
erforderlich!

The screenshot shows a login interface for 'Digitale Dörfer'. At the top, there is a logo and the text 'Digitale Dörfer'. Below the logo are two buttons: 'Anmelden' and 'Registrieren'. The main content area features social login options for Facebook (f) and Google (G), with the word 'oder' below them. There are two input fields: one for an email address (containing 'yours@example.com') and one for a password (containing 'Ihr Passwort'). Below the password field is a link that says 'Passwort vergessen?'. At the bottom, there is a prominent red button labeled 'Anmelden >'.

Refresh-Token, Kurzfassung

Durch

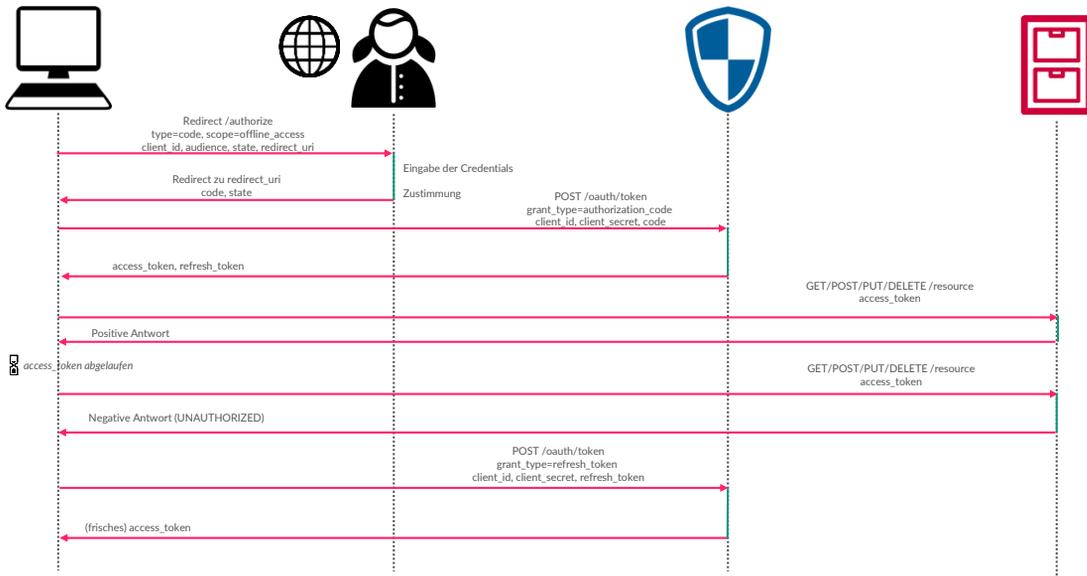
- Scope „offline_access“ und
- zusätzliche Sicherheitsmaßnahmen (client_secret)

erhält Client `access_token` und **refresh_token**.

Über das `refresh_token` bekommt der Client **ohne Benutzerinteraktion** ein neues `access_token`.

Ein Refresh-Token kann vom Resource Owner oder Auth.-Server-Admin zurückgerufen werden.

Refresh-Token-Flow



Vorteile

Vorteile

- App kann Passwort des Benutzers nicht abfangen
- Resource-Server braucht keine dauernde Online-Verbindung zum Authorization-Server
- Zentraler Login (Einheitliche Login-User-Experience über alle Anwendungen)
- Gute Einbindungsmöglichkeit von Drittanbieteranwendungen
- SSO über Browser-Cookie

Nachteile

Nachteile

- ⚠ Access-Token kann nicht widerrufen werden
 - Bei uns durch kurze Dauer und keine besonders hoher Sicherheitskritikalität verschmerzbar
- Benutzer verlässt die Anwendung, wenn er sich authentifiziert (vor allem auf Android auffällig)
 - Im Browser kein Problem (einfacher Redirect)
 - iOS: integrierte WebView
- Auth-Prozess aufwändiger zu implementieren
 - Hier helfen vorgefertigte Bibliotheken

Umsetzung



Was bietet Auth0?

- ready-to-use „Authentication as a Service“
- Fertiges Frontend (Login-/Registrierungs-Seiten) und Backend (token-Endpunkte, Benutzerverwaltung)
- Übersichtliche Verwaltungsoberfläche
- Toolsupport/Libraries für alle gängigen Programmiersprachen/Frameworks
- Login und E-Mails mit wenig Aufwand individualisierbar
- Sehr gute Erweiterbarkeit durch Hooks und Rules (in JavaScript geschrieben)

Entscheidung für Auth0?

- Bisheriges Authentifizierungsverfahren (Mischung aus Session-ID und Amazon Cognito) soll schnell abgelöst werden
- Evaluierte Alternativ-Lösungen weniger ausgereift oder höherer Anpassungsaufwand

Fallstricke

Doppelte Persönlichkeit

Benutzerregistrierung



Auth0

auth0|19448da23
lisa@example.org
1fj5d%!df

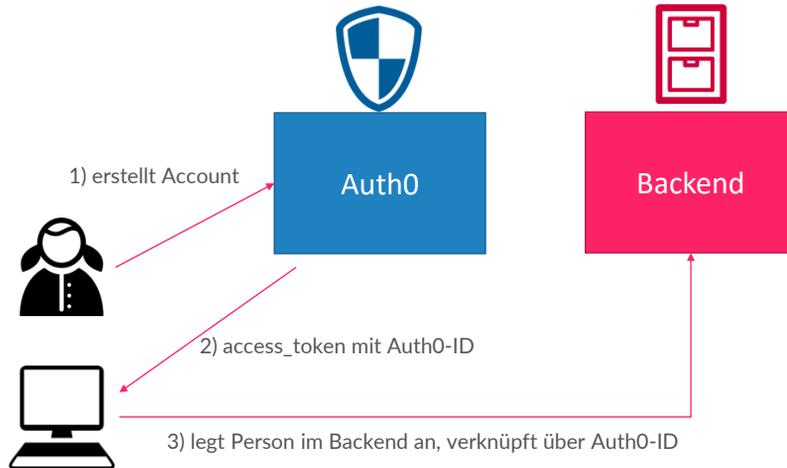


Backend

123a-abc1-78a3-cfa1
Lisa Müller
lisa@example.org
Lindenstraße 11, KL
+49 111 111456
auth0|19448da23
ROLE_MANAGER, VG_ADMIN



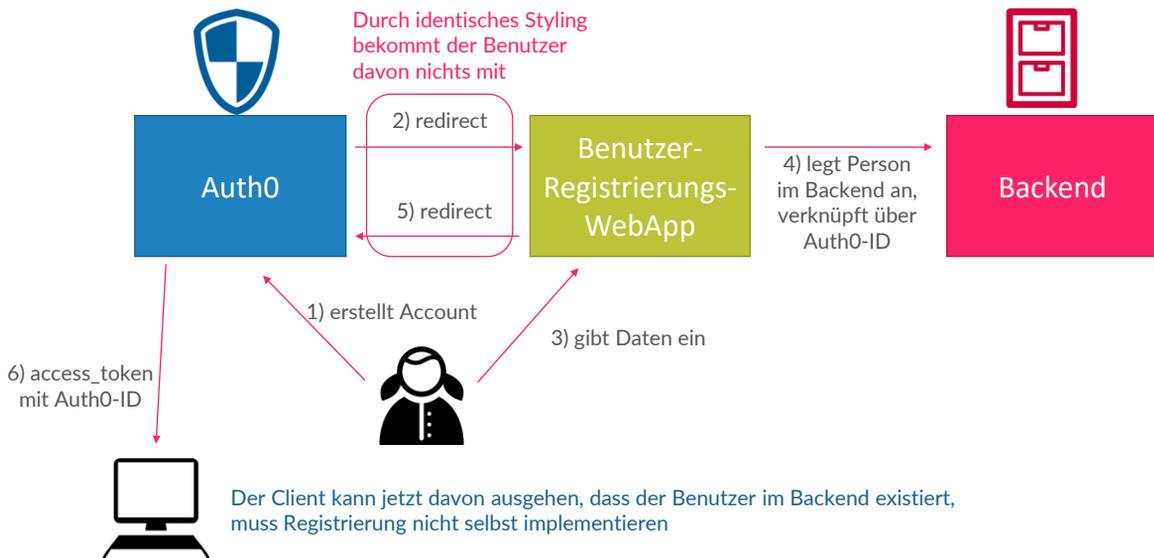
Benutzerregistrierung



Was passiert, wenn Registrierung fehlschlägt?
Mögliche Situation: Account existiert in Auth0, aber keine zugehörige Person im Backend

Jeder Client muss die Registrierung im Backend implementieren (Person anlegen mit Name, Adresse, Telefon, ...)

Benutzerregistrierung



User Experience - oder - „Wie zur Hölle hab ich mich da noch mal registriert?“



Emoji icon provided free by [EmojiOne](#)

Facebook?

The image shows a login form for 'Digitale Dörfer'. At the top is the logo, which consists of a green cube with white icons and the text 'Digitale Dörfer'. Below the logo are two tabs: 'Anmelden' (selected) and 'Registrieren'. Under the tabs are two social media icons: Facebook (f) and Google (G). Below the icons is the word 'oder'. There are two input fields: one for an email address with the placeholder 'yours@example.com' and one for a password with the placeholder 'Ihr Passwort'. Below the password field is a link that says 'Passwort vergessen?'. At the bottom is a red button with the text 'Anmelden >'.

Google?

Eigener
Account?

Fehlermeldungen

- ... können hier helfen (wenn sie gelesen werden 😊)

Außerdem:

- Erst eigener Account registriert, dann Social Login benutzte (gleiche E-Mail)
→ Accounts werden in Auth0 zusammengelegt

The screenshot shows a login interface for 'Digitale Dörfer'. At the top, there is a logo and a red banner with the text: 'UPS, DA LIEF ETWAS SCHIEF. BITTE PRÜFE DEINE E-MAIL BZW. DEIN PASSWORT. ODER HAST DU DICH ÜBER FACEBOOK BZW. GOOGLE BEI UNS REGISTRIERT? DANN MELDE DICH DAMIT AN.' Below the banner are two tabs: 'Anmelden' and 'Registrieren'. The 'Anmelden' tab is active. There are two social login buttons for Facebook and Google, with the text 'oder' below them. Below the social login options is an email input field containing 'example@gmail.com' and a password input field with masked characters. A link for 'Passwort vergessen?' is located below the password field. At the bottom, there is a red button labeled 'Anmelden >'.

**Wenn Entwickler mal schnell
einen API-Aufruf machen
wollen...**

Lösung für die Eingangsfragen

- Gleicher Login unabhängig von Client-Technologie
- Social-Logins nutzen
- Über Datenfreigabe entscheiden
- Kein Zugriff auf das Passwort des Benutzers
- Dauerhafter Login ohne Speichern des Passworts

Aber:

- Der Teufel steckt im Detail, daher
 - Prototypen bauen
 - Lösungen vergleichen (no „one size fits it all“)



Dr. Johannes C. Schneider

Software-Architekt

johannes.schneider@iese.fraunhofer.de

Fraunhofer IESE, Kaiserslautern



digitale-doerfer.de
fb.com/DigitaleDoerfer
twitter.com/digitaledoerfer

