

## **Erste Analyse der API „Okta“**

### **Welche Organisation bietet den Service an?**

Der Service unter dem Namen „Okta Identity Cloud“ wird von dem gleichnamigen Unternehmen „Okta Inc.“ sowohl entwickelt, verwaltet als auch angeboten. Der Betrieb beschäftigt sich mit der Verbindung von Nutzern und dem Management von Nutzergruppen innerhalb eines gewünschten Systems, sodass dadurch die Unternehmen eben jener Systeme gewiss sein können, eine sichere Verbindung zwischen der eigenen Technologie und den Endnutzern vorweisen zu können.

(Quelle: <https://www.okta.com/company/>, Letzter Aufruf: 28.04.2018)

### **Was ist die hauptsächliche Funktion des Service?**

Die Hauptfunktion beinhaltet unter anderem die sichere Verbindung eines Nutzers mit einer gewünschten Software, eine Verwaltungsmöglichkeit aller registrierten Nutzer, als auch die Option durch die Analyse der Anmeldedaten Informationen über die Art und Weise der Nutzeranmeldung zu erheben.

(Quelle: <https://developer.okta.com/product/>, Letzter Aufruf: 28.04.2018)

### **Was sind wesentliche Elemente des Vertrages: z.B. Kosten, Datenschutz, Nutzungsrechte?**

Die Kosten zur Nutzung von Okta lassen sich in 3 Sparten unterteilen. Die erste sieht vor, lediglich maximal 7000 monatliche Nutzer verarbeiten zu können, dagegen allerdings frei zur Verfügung steht. Die zweite Sparte richtet sich an jene Software, welche monatlich mehr als 1000 Nutzer verzeichnen kann und bietet die Möglichkeit gegen eine etappenweise erhöhte Bezahlung dieses Pensum auf 50000 Nutzer pro Monat zu erhöhen. Sollte jedoch mehr Verkehr als das zu erwarten sein, bittet Okta darum, sie über das Kontaktformular getrennt zu kontaktieren. Okta behält sich des Weiteren vor, die durch die Nutzung entstandenen Daten aufzugreifen und verwenden zu dürfen. Im Falle der Einbindung eines Dritten werden die erhobenen Daten allerdings anonymisiert sodass nicht zurückverfolgt werden kann, von welchem Nutzer diese Daten stammen oder aus welchem Unternehmen diese entnommen worden.

(Quelle: <https://developer.okta.com/pricing/>, Letzter Aufruf: 28.04.2018; <https://developer.okta.com/terms/>, Letzter Aufruf: 28.04.2018)

### **URIs für Dokumentation und Endpunkt:**

Eigens generierter Endpunkt: dev-989237.oktapreview.com

Dokumentation: <https://developer.okta.com/documentation/>

## Beispielfunktionen des Service:

### Primäre Authentifizierung:

Jede Authentifizierungstransaktion beginnt mit einer primären Authentifizierung, welche das Hauptkennwort eines Benutzers überprüft. *Password Policy*, *MFA Policy*, und *Sign-On Policy* werden während der primären Authentifizierung ausgewertet, um festzustellen, ob bspw. das Kennwort des Benutzers abgelaufen, oder eine zusätzliche Überprüfung erforderlich ist. Der Transaktionsstatus der Antwort hängt vom Status des Benutzers, den Gruppenmitgliedschaften und den zugewiesenen Richtlinien ab.

Die Anfragen und Antworten variieren je nach Anwendungstyp und ob eine Passwortablaufwarnung gesendet wird.

Beispiel einer Anfrage zur primären Authentifizierung:

`POST /api/v1/authn`

#### Header:

```
"Accept: application/json"
"Content-Type: application/json"
```

#### Body:

```
{
  "username": "dade.murphy@example.com",
  "password": "correcthorsebatterystaple",
  "relayState": "/myapp/some/deep/link/i/want/to/return/to",
  "options": {
    "multiOptionalFactorEnroll": false,
    "warnBeforePasswordExpired": false
  }
}
```

Beispiel einer Antwort zur erfolgreichen primären Authentifizierung:

```
{
  "expiresAt": "2015-11-03T10:15:57.000Z",
  "status": "SUCCESS",
  "relayState": "/myapp/some/deep/link/i/want/to/return/to",
  "sessionToken": "00Fpzf4en68pCXTsMjcX8JPMctzN2Wiw4LD0BL_9pe",
  "_embedded": {
    "user": {
      "id": "00ub0oNGTSWTBKOLGLNR",
      "passwordChanged": "2015-09-08T20:14:45.000Z",
      "profile": {
        "login": "dade.murphy@example.com",
        "firstName": "Dade",
        "lastName": "Murphy",
        "locale": "en_US",
        "timeZone": "America/Los_Angeles"
      }
    }
  }
}
```