



Authentifizierung

Agenda

Authentifizierung

Beispielimplementierung Demo

Assignment

Authentifizierung



Was ist Authentifizierung?

- Prüfung und Abgleich von Anmeldeinformationen eines Benutzers gegen eine Authentifizierungsdatenbank
- Überprüfung der Identität
- Überprüfung von Zugriffsberechtigung auf:
 - Netzwerke
 - Server
 - Webseiten
 -



Abgrenzung Authentifizierung & Autorisierung

Authentifizierung: Überprüfung der Identität

Autorisierung: Überprüfung der Zugriffsrechte auf Ressourcen basiert auf Userberechtigungen, die im Userprofil hinterlegt sind

Reihenfolge:

1. Authentifizierung (Benutzer ist identifiziert und angemeldet)
2. Autorisierung (Anhand der Benutzerberechtigungen können nun Zugriffsrechte geprüft werden)



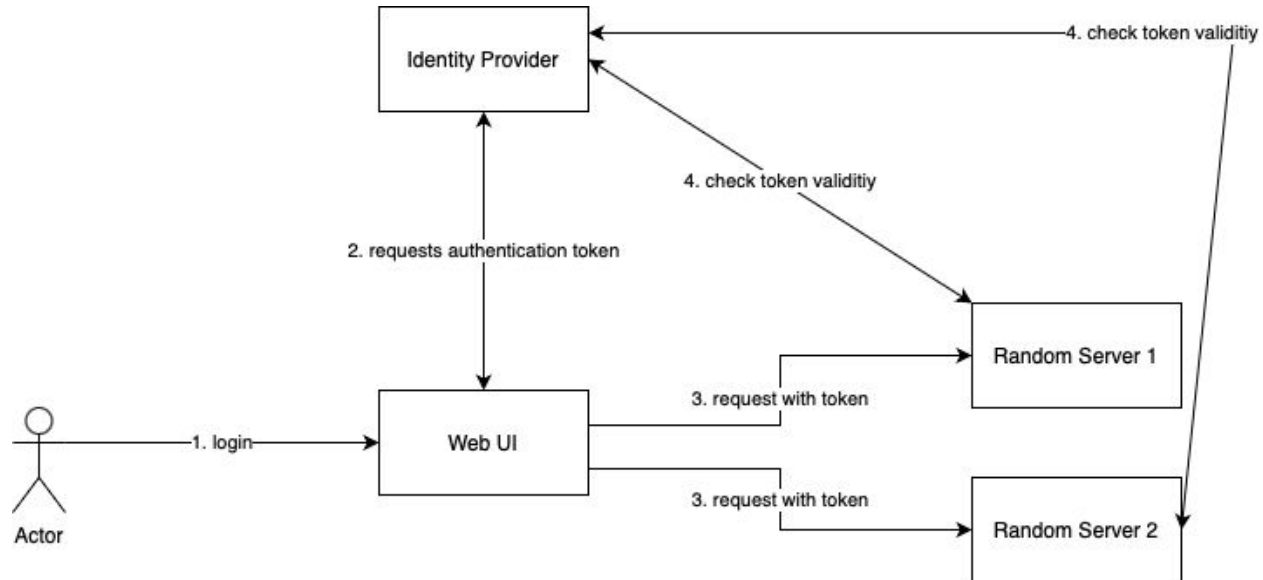
Früher

- Benutzer brauchte ein Benutzerkonto auf jedem Server
- Anmeldung durch Eingabe von UserID und Passwort

Heute

- Zentraler Authentifizierungsserver
- Der Benutzer fragt Authentifizierungstoken beim Authentifizierungsserver an
- Token wird bei jedem Request zu einem Server mitgeschickt und der Server überprüft diesen Token beim Authentifizierungsserver
- → Single Sign On (SSO)

Visualisierung Tokenauthentifizierung





Authentifizierungsfaktoren

- Daten, die zur Authentifizierung eines Benutzers verwendet werden
- Können sein:
 - Etwas, das man weiß (Wissensfaktor)
 - Beispiele: PIN, Passwort, Nutzernamen, geheime Frage
 - Etwas, das man hat (Besitzfaktor)
 - Beispiele: Sicherheitstoken, Mobiltelefon (SMS), App
 - Etwas, das man ist (Inhärenzfaktor)
 - Beispiele: Gesichtserkennung, Fingerabdruck
 - Standort: Wird oft als Ergänzung verwendet (sollte nie alleine verwendet werden)
 - Beispiele: GPS
 - Zeit: Wird oft als Ergänzung verwendet (sollte nie alleine verwendet werden)



Multifaktorauthentifizierung

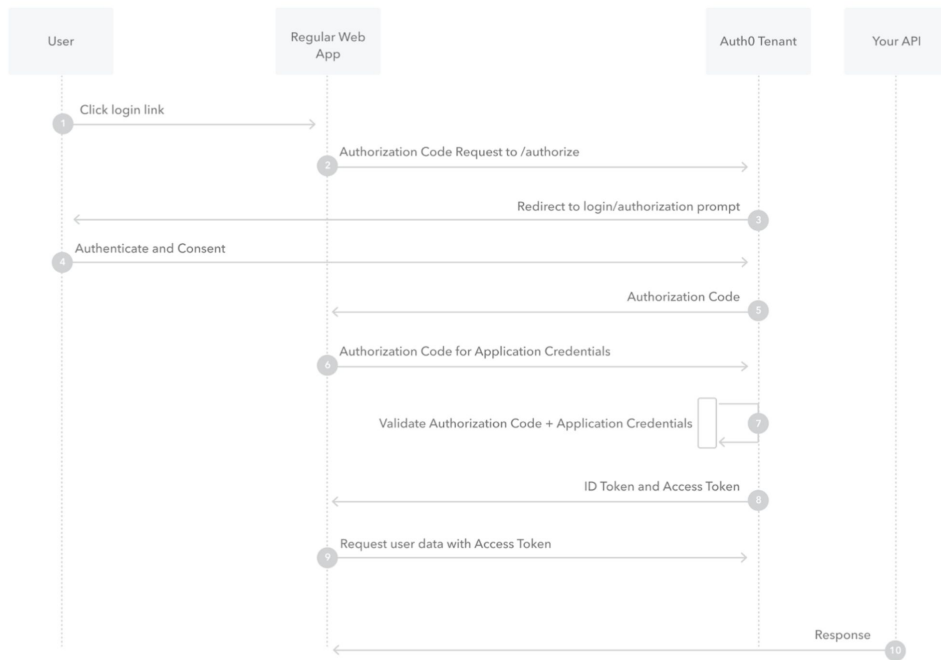
- Einsetzung zwei oder mehrerer Faktoren zur Authentifizierung
- Zwei Methoden des gleichen Faktortyps zählen nicht als Multifaktorauthentifizierung (z.B. Fingerabdruck- und Gesichtserkennung)



Authentifizierungsprotokolle

- Open Authorization (OAuth2)
 - Autorisierungsprotokoll
 - Nutzt Token zur Autorisierung für bestimmte Ressourcen (Tokenformat nicht vorgegeben)
 - Unterstützt verschiedene Autorisierungsvorgänge (verschiedene Schritte zur Autorisierung notwendig (Grants))
- OpenID Connect (OIDC)
 - Speziell für Web und Apps
 - Basiert auf OAuth2
 - Nutzt JSON Web Tokens (JWT)
 - Unterstützt verschiedene Authentifizierungsvorgänge (OIDC Flows)
- Security Assertion Markup Language (SAML2)
 - Komplexes Protokoll zur Single Sign On (SSO) mit großem Funktionsumfang
 - Wird in Unternehmen und im öffentlichen Sektor verwendet
 - Nutzt XML zur Übertragung von Nutzerdaten
- Fast Identity Online (FIDO)
 - Ziel: Abschaffung von Passwörtern
 - Authentifizierung via biometrischen Daten an Betriebssystemen (Apple TouchID, Windows Hello)

Authorization Code Flow





Maschinenauthentifizierung

- Asymmetrische Verschlüsselung (Public & Private Key)
 - Dokumente oder Verbindungen werden mit dem Public Key verschlüsselt
 - Dokumente können nur mit dazugehörigem Private Key entschlüsselt werden
- Public Key Infrastruktur (PKI)
 - Hierarchie von Zertifikaten
 - Wurzelzertifikat (Root) ist die Basis
 - Wird von Certificate Authority (CA) ausgestellt
 - Weitere Zertifikate in der PKI werden mit Root Zertifikat signiert
 - Empfänger (Server) prüft eingehende Verbindung beim Validierungsserver
 - → Authentifizierung möglich, ohne dass beide Parteien bekannt gemacht werden müssen