cirosec

OAuth sicher mit Single-Page-Applications nutzen

Architektur-Pattern und Best Practices

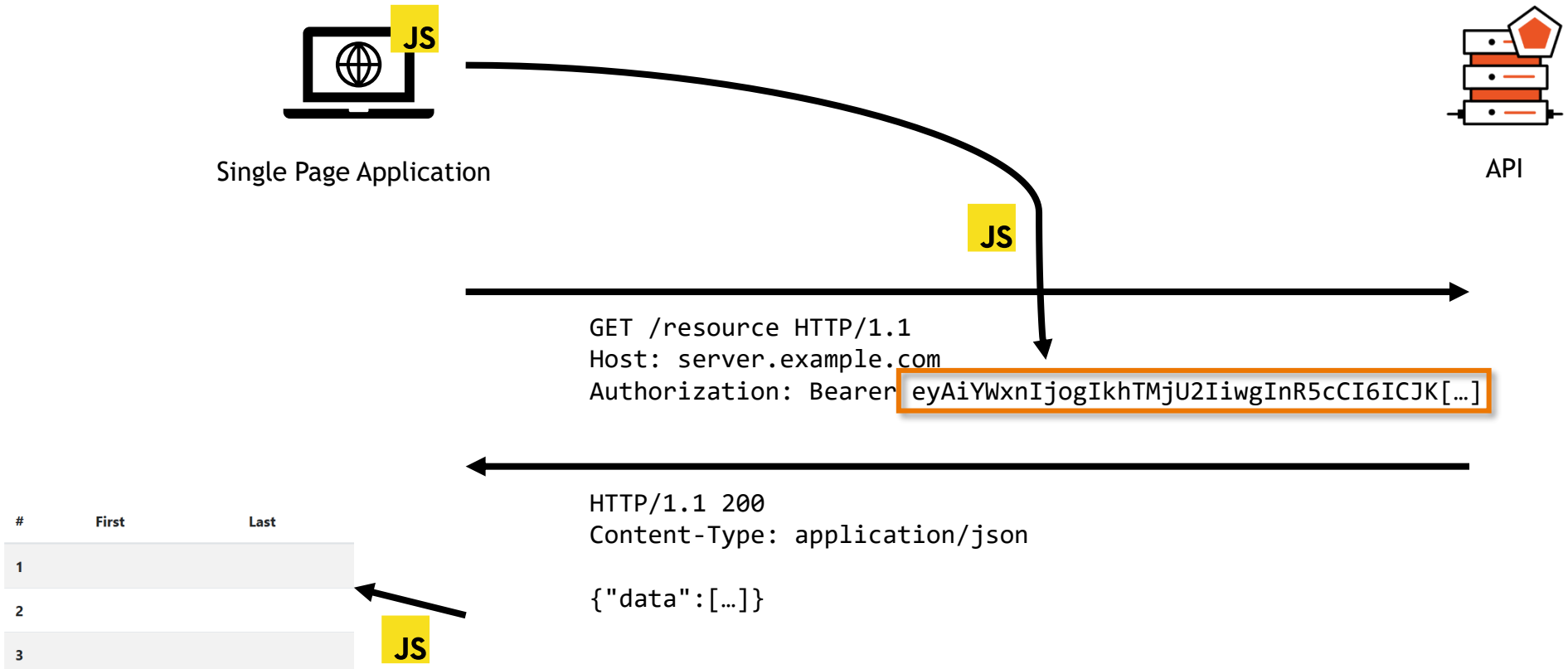
Benjamin Häublein

OWASP Stammtisch Heilbronn, 8.5.2025

Agenda

- Single Page Applications
- OAuth2 Grundlagen
- Pattern beim Einsatz von OAuth2 mit SPAs

Single Page Application (SPA)



OAuth
Problemstellung

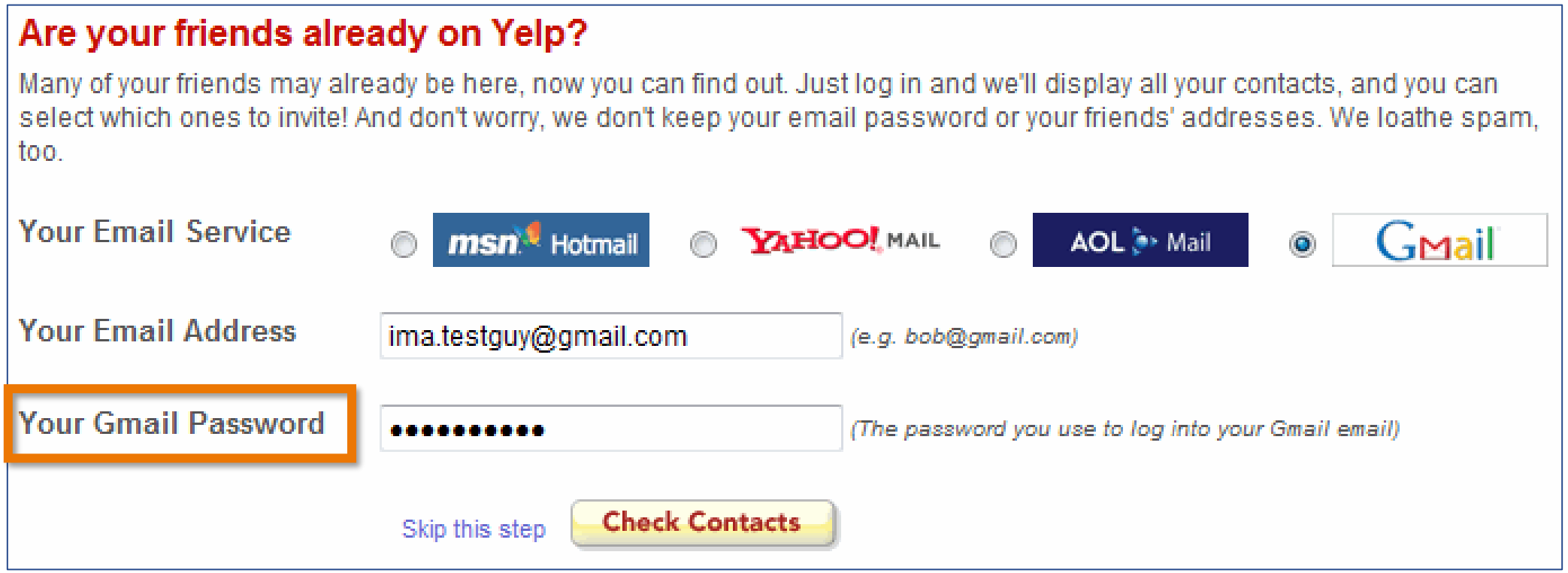
cirosec

Facebook/LinkedIn/…

möchte auf deine Gmail/… Kontakte zugreifen, um dein Netzwerk um Menschen die du kennst zu erweitern.

Wie macht man das?

OAuth
Lösung (2008)



https://blog.codinghorror.com/please-give-us-your-email-password/

OAuth

- „Delegierte Zugriffsberechtigung“
- Vergabe von Zugriffsberechtigungen durch den Benutzer des Dienstes an eine dritte Partei auf Ressourcen eines Dienstes

- OpenID
  - Delegation der Berechtigung zum Zugriff auf die Identität des Benutzers

OAuth
Grober Ablauf

Authorization Server

Resource Server

Resource Owner

Client

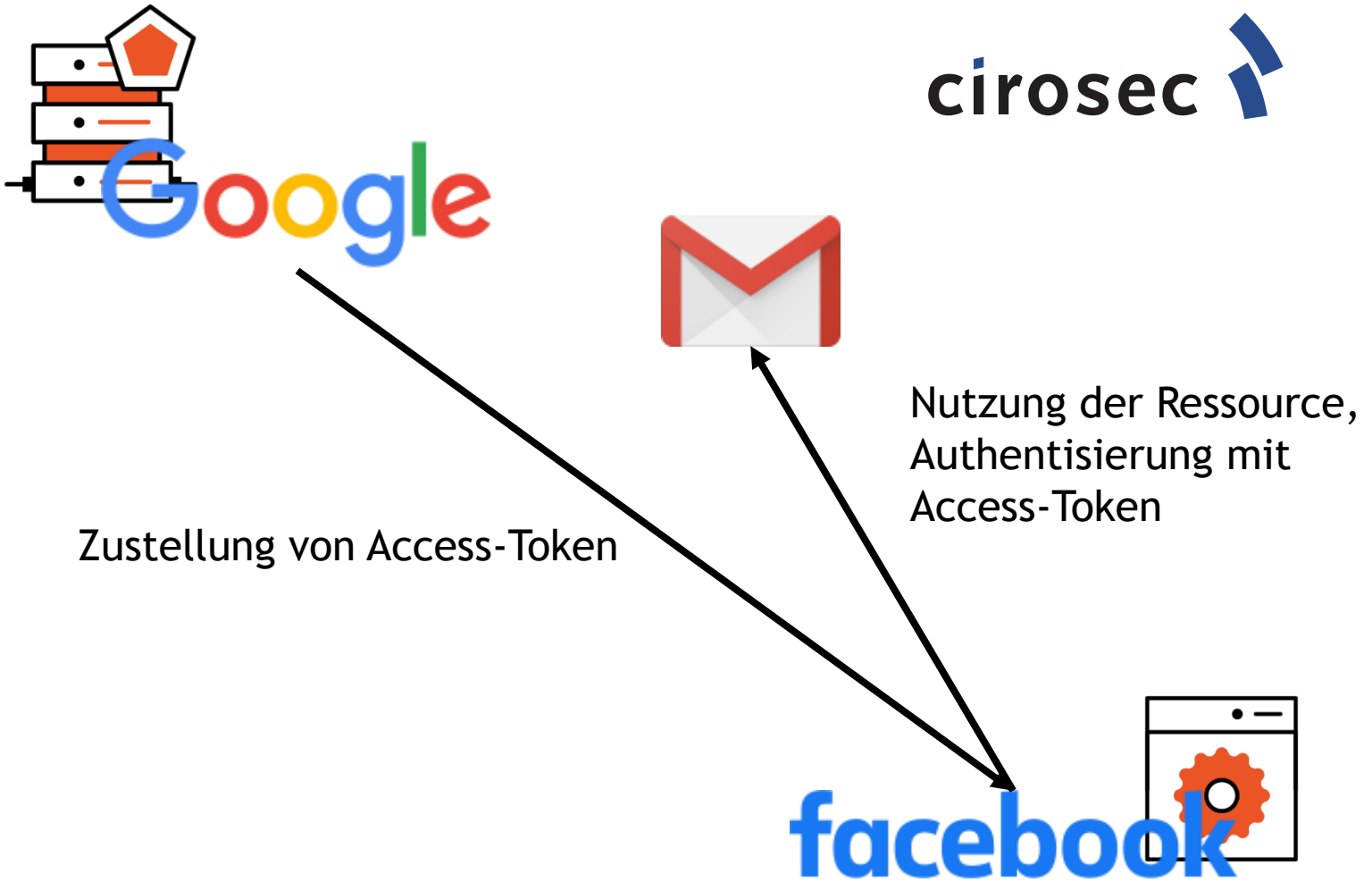
OAuth
Grober Ablauf

cirosec

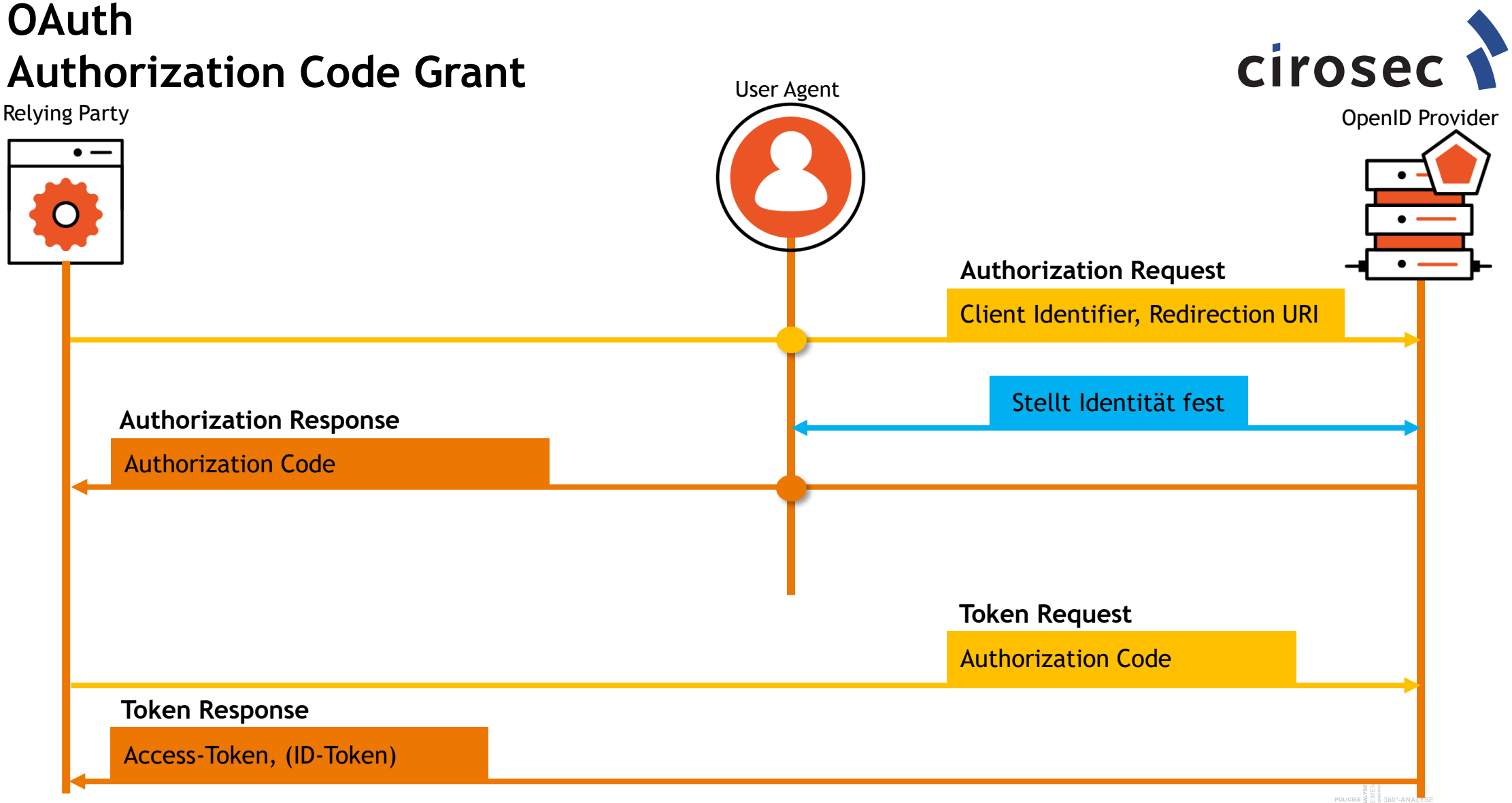
Besucht Facebook

Oauth
Grober Ablauf

Oauth
Grober Ablauf



OAuth
Authorization Code Grant

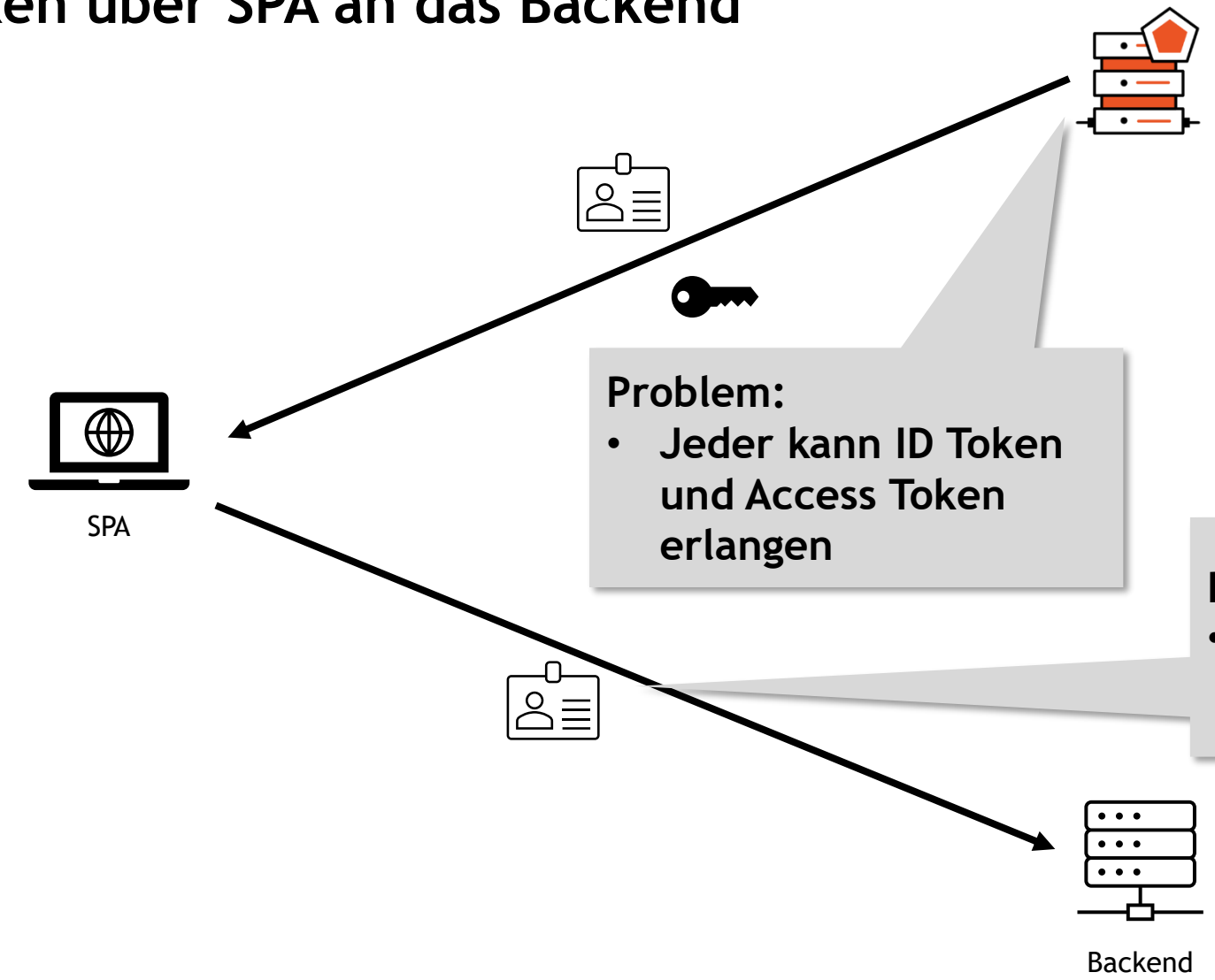


cirosec

Typische OAuth2 / OpenID Connect Szenarien

Die fast alle problematisch sind

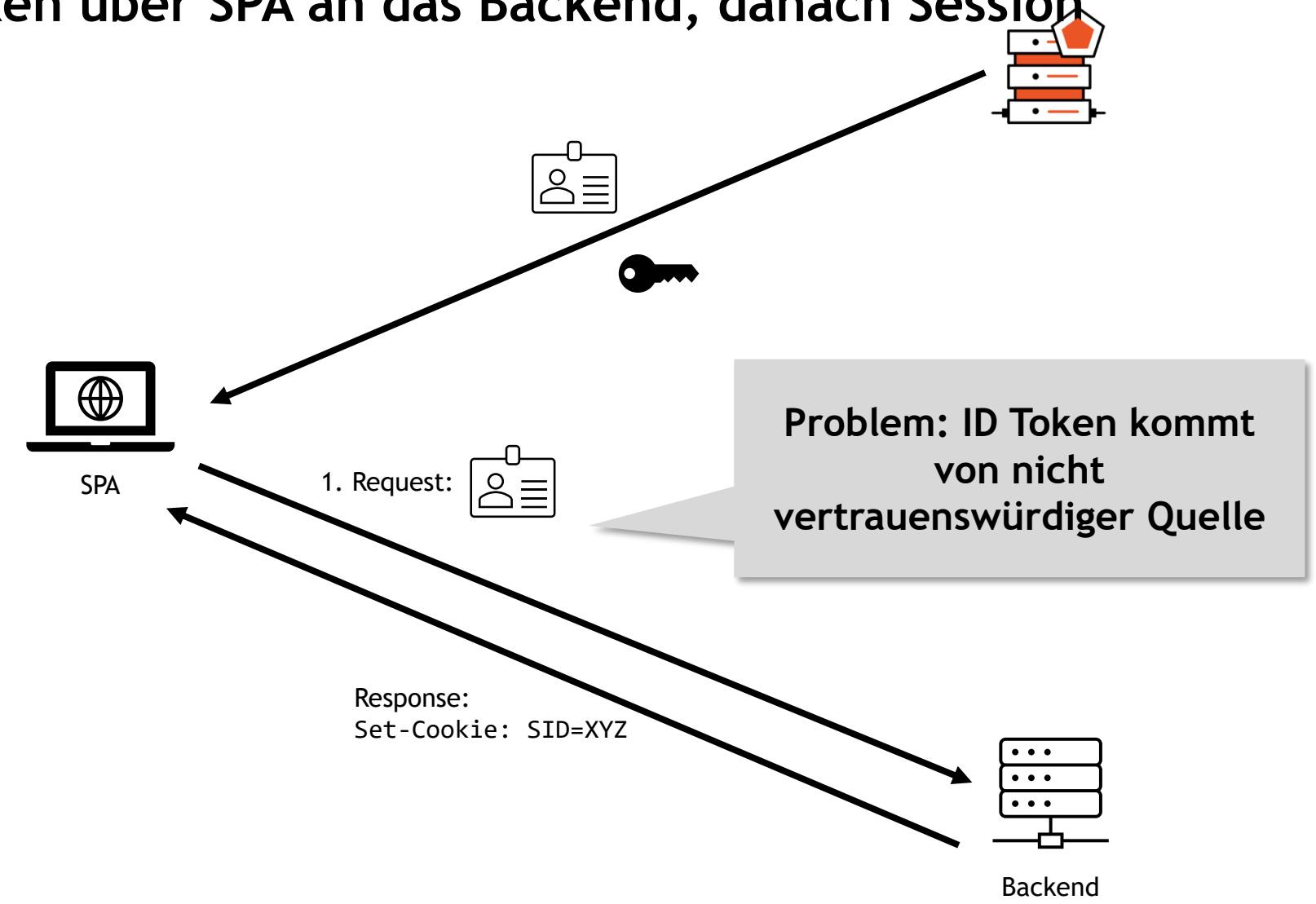
ID Token über SPA an das Backend



Access Token

ID Token

ID Token über SPA an das Backend, danach Session

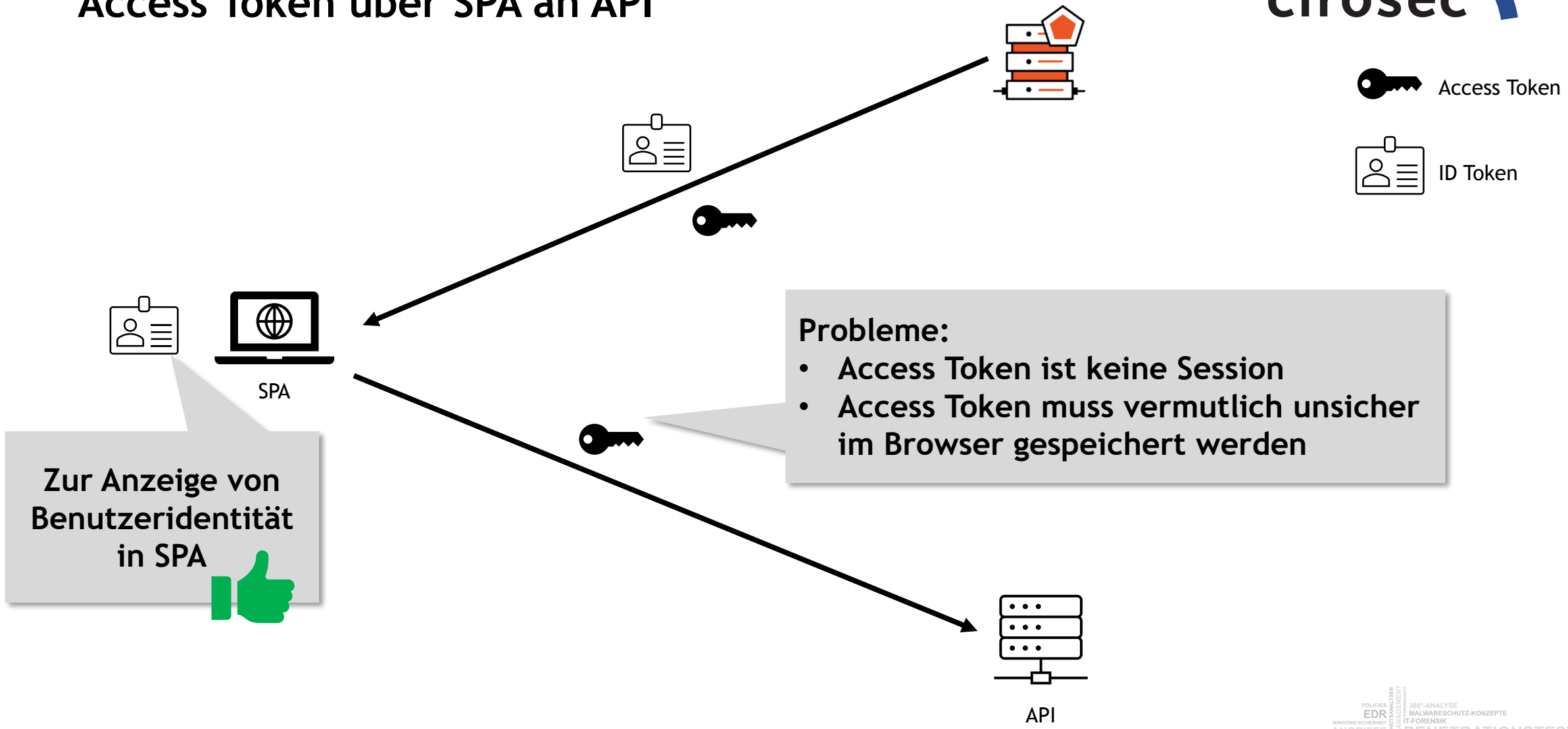


Access Token

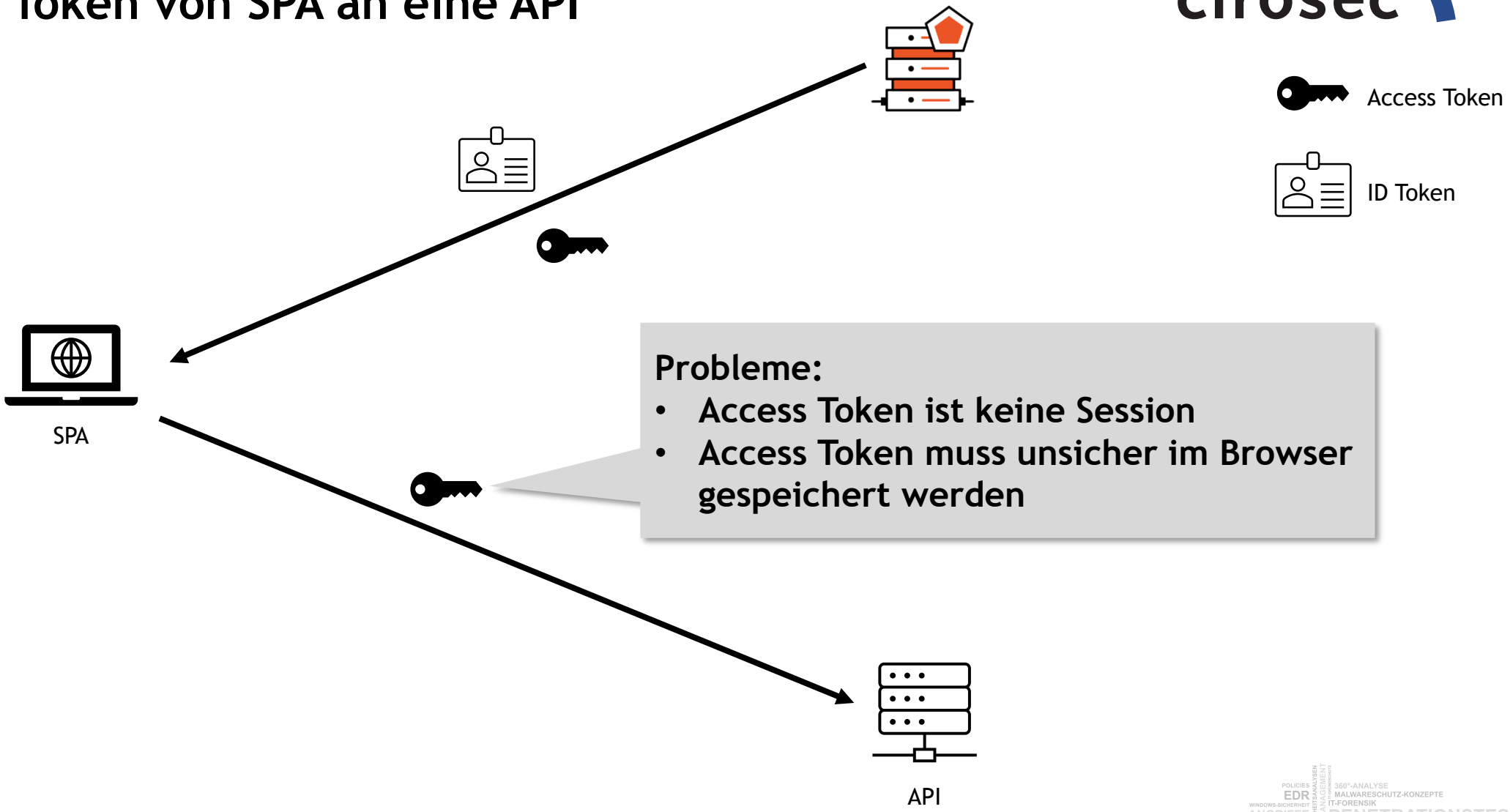
ID Token

Access Token über SPA an API

cirosec

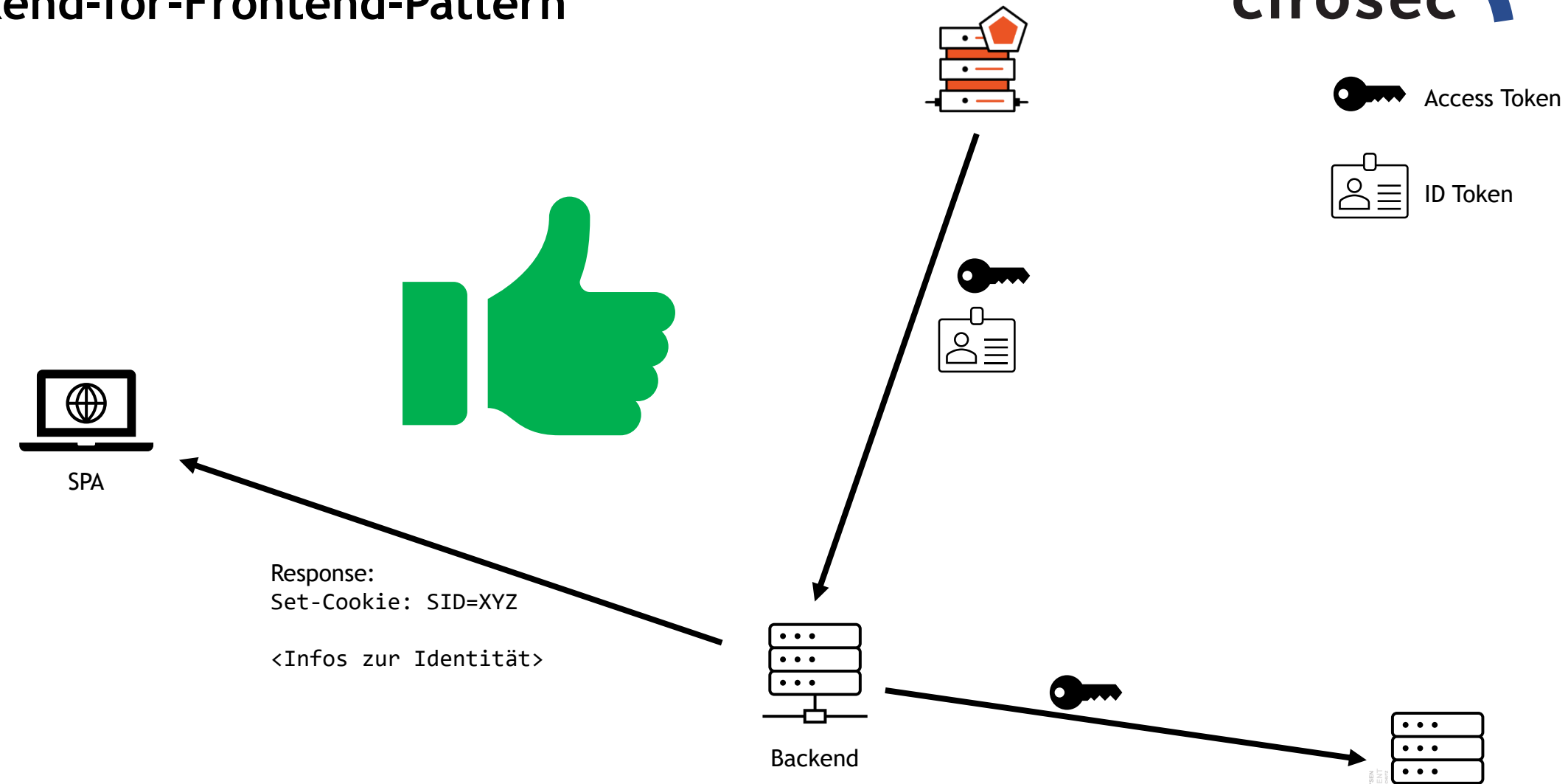


Access Token von SPA an eine API

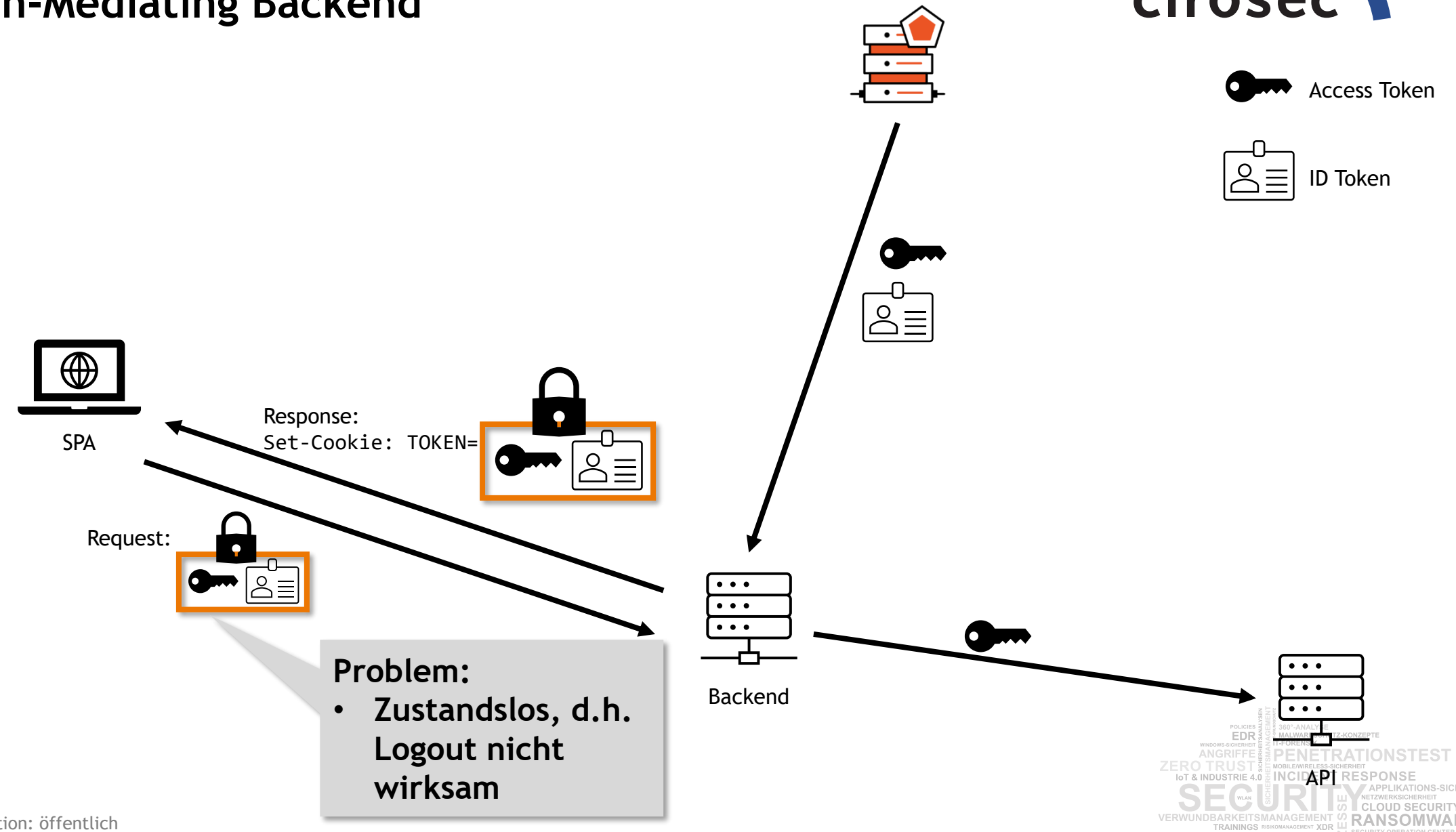


Backend-for-Frontend-Pattern

cirosec

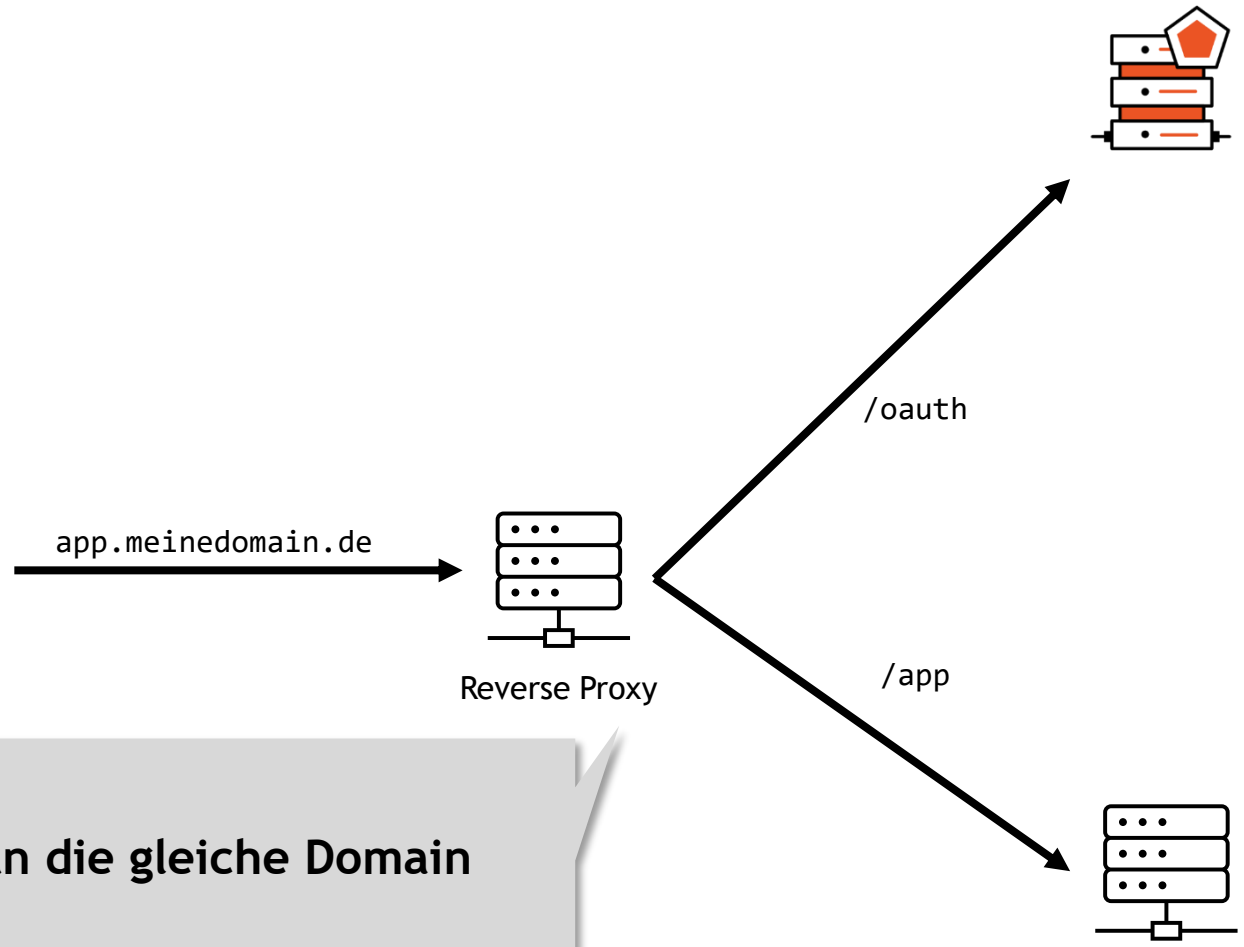


Token-Mediating Backend



Anwendung und IdP teilen sich eine Domain

cirosec



Access Token

ID Token

Problem:

- **Cookies sind an die gleiche Domain gebunden**
- **XSS in /app hat Auswirkung auf IdP**

cirosec

Schutzmaßnahmen bei SPA

Mögliche Schutzmaßnahmen für SPA (wenn Sie OAuth-Client sein müssen)

cirosec

- Proof Key for Code Exchange (PKCE, RFC 7636)
  - Bindung von Authorization Codes an die Instanz des Clients, der den OAuth-Flow gestartet hat
- Demonstrating Proof of Possession (DPoP, 9449)
  - Bindung von Access und Refresh Token an den Besitz von Privaten Schlüsseln

PKCE (Proof Key for Code Exchange)

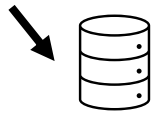
Code Verifier

Code Challenge
=HASH(Code Verifier)

Authorization Request

Code Challenge

Code Challenge



Token Request

Code Verifier

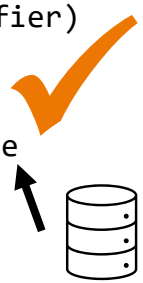
Code Verifier

Code Verifier

HASH(Code Verifier)

=

Code Challenge



Nachweis, dass Instanz des anfragenden und eintauschenden Clients „dieselbe“ ist.
(bis auf Weitergabe/Diebstahl des Code Verifier)

Benjamin Häublein

cirosec GmbH

https://www.cirosec.de/

info@cirosec.de

+49 7131 59455 0

Vielen Dank für Ihre Aufmerksamkeit!