



The "OpenID Connect" protocol and its use.

Modul: Big Data Management und Analytics in datenzentrischen Wissenschaften

Dozent: Prof. Dr. Patrick Fuhrmann

Sommersemester 2021

Kathrin Klocke

OpenID Connect und OAuth 2.0

The diagram consists of three stacked rectangular boxes. The top box is orange and contains the OpenID logo (a stylized 'i' with an arrow) and the text 'OpenID' with a small '[2]' to its right. Below the logo is the text 'OpenID Connect 1.0'. The middle box is yellow and contains the OAuth 2.0 logo (a circular emblem with 'OAUTH' at the top and '2' in the center) and the text 'OAuth 2.0' with a small '[3]' to its right. The bottom box is grey and contains a REST client interface with a dropdown menu set to 'GET', a text input field containing 'Enter request URL', and a blue 'Send' button with a small '[4]' to its right. Below the interface is the text 'http://'.

Authentifizierung / Authentication:
Verifizierung der Identität

Single sign-on
(SSO) /
„Einmalanmeldung“

Autorisierung / Authorization:
Gewähren des Zugangs zu
Privilegien bzw. Ressourcen

Delegated
Authorization /
dienstübergreifende
Autorisierung

Rollen und Begriffe



End User

Ein menschlicher Teilnehmer. [2]



Entity

Ein Objekt, das eine separate und eindeutige Existenz hat und das in einem Kontext identifiziert werden kann, beispielsweise ein End User. [2]



Relying Party (RP) / Client

Eine OAuth-2.0-Client-Anwendung, die eine End-User-Authentifizierung und -Claims von einem OpenID-Provider anfordert. [2]



Claim

Eine Information, die in Bezug auf eine eine Entität behauptet wird. [2]



OpenID Provider (OP) / Identity Provider (IdP)

Ein OAuth-2.0-Autorisierungsserver, der in der Lage ist, den End User zu authentifizieren und einer Relying Party Claims über das Authentifizierungs-event und den End User zu liefern. [2]



ID Token

JSON Web Token (JWT), das Claims über das Authentifizierungs-event enthält. Es kann andere Claims enthalten. [2]

OpenID Connect Flows - Authentication Paths

Es gibt drei mögliche Authentication Paths:

- Authorization Code Flow
- Implicit Flow
- Hybrid Flow

Der `response_type` Wert im Authorization Request bestimmt welcher Flow verwendet wird.

Die Flows bestimmen, wie das ID Token und Access Token an den Client zurückgegeben werden. [2]

OpenID Connect Flows - Authentication Paths

Es gibt drei mögliche Authentication Paths:

- Authorization Code Flow
- Implicit Flow
- Hybrid Flow

Der `response_type` Wert im Authorization Request bestimmt welcher Flow verwendet wird.

response type value	Flow
code	Authorization Code
id token	Implicit
id token token	Implicit
code id token	Hybrid
code token	Hybrid
code id token token	Hybrid

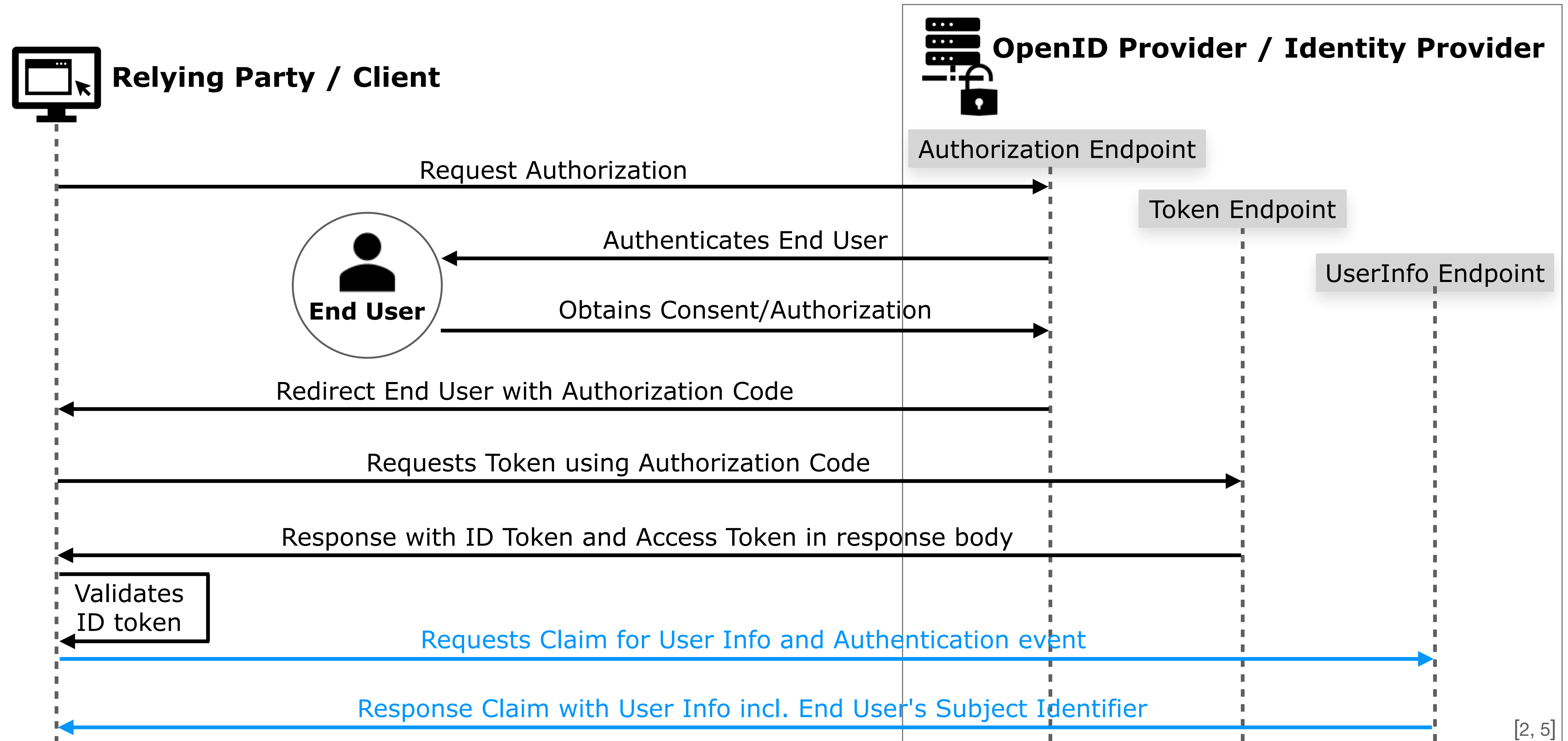
[2]

Die Flows bestimmen, wie das ID Token und Access Token an den Client zurückgegeben werden. [2]

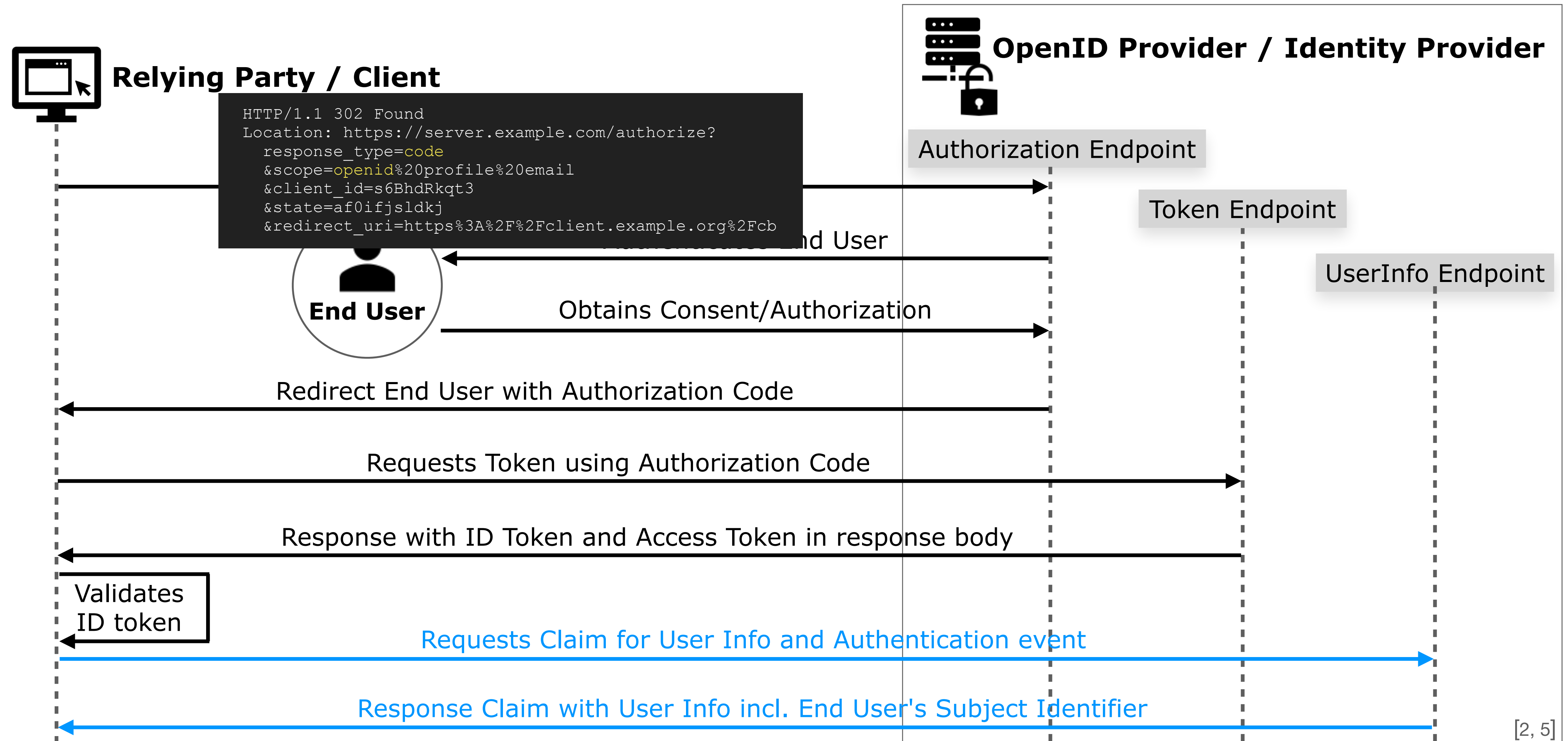
	Auth. Code	Implicit	Hybrid
All tokens returned from Authorization Endpoint	✗	✓	✗
All tokens returned from Token Endpoint	✓	✗	✗
Tokens not revealed to User Agent	✓	✗	✗
Client can be authenticated	✓	✗	✓
Refresh Token possible	✓	✗	✓
Communication in one round trip	✗	✓	✗
Most communication server-to-server	✓	✗	varies

[2]

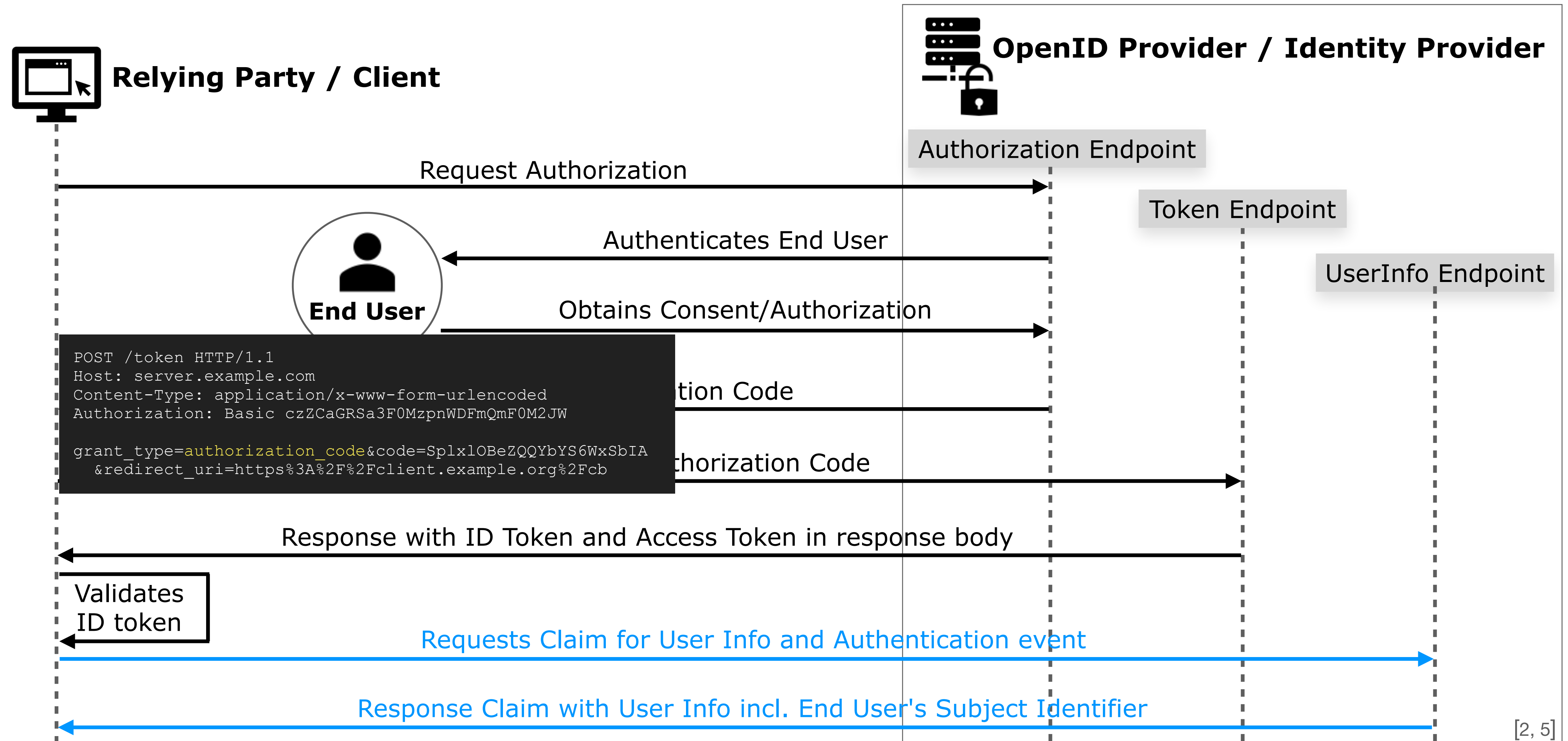
Ein Flow im Detail: Authorization Code Flow



Ein Flow im Detail: Authorization Code Flow

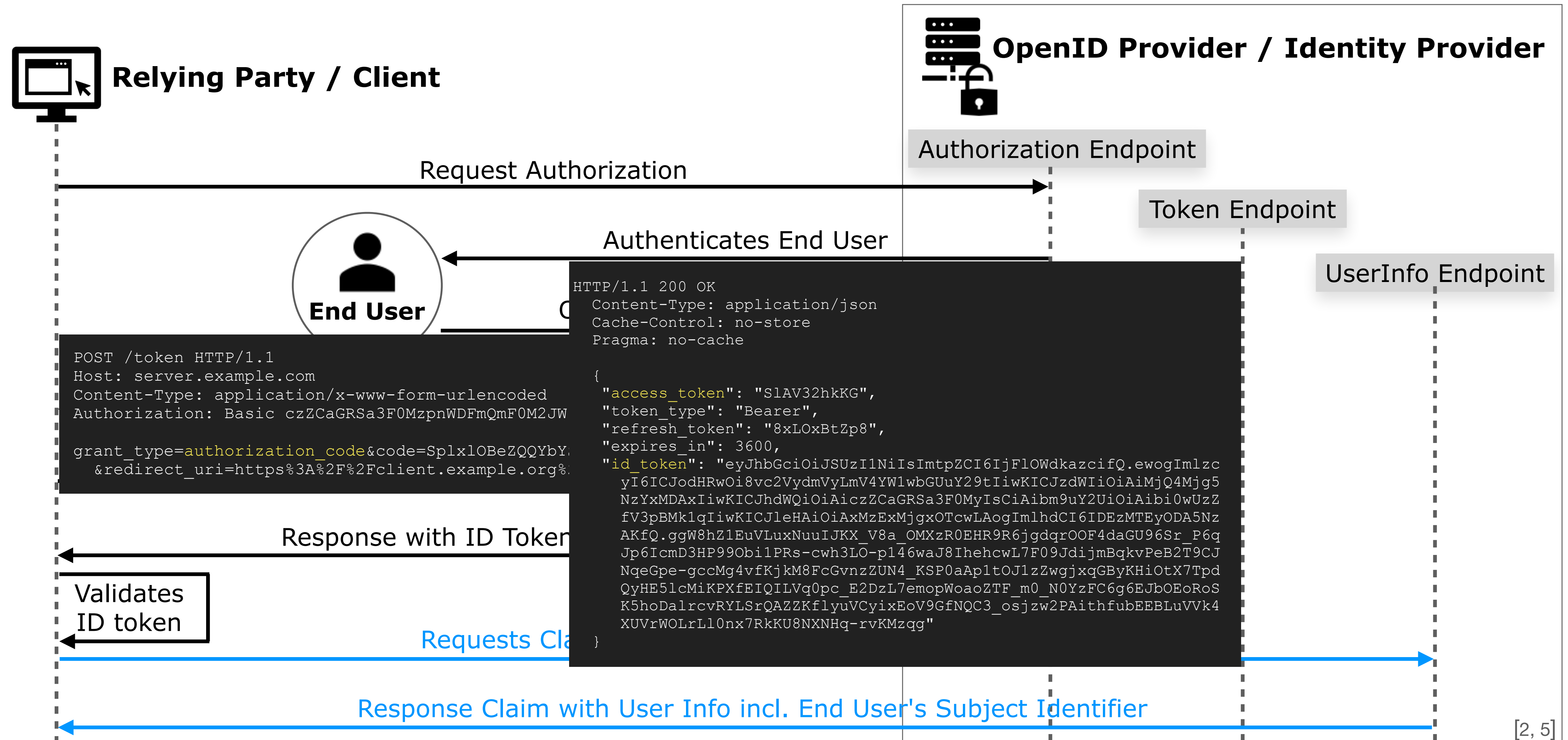


Ein Flow im Detail: Authorization Code Flow



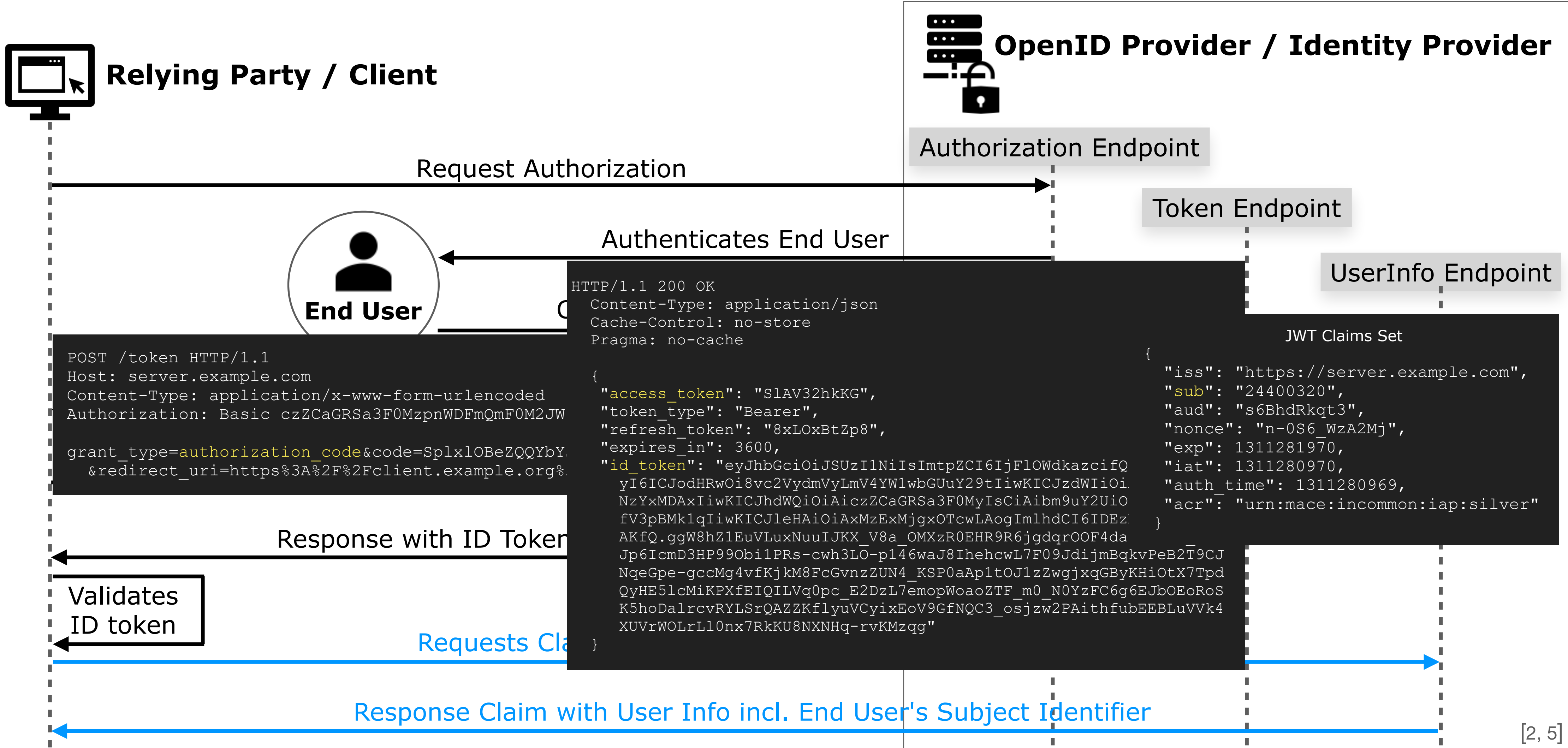
[2, 5]

Ein Flow im Detail: Authorization Code Flow



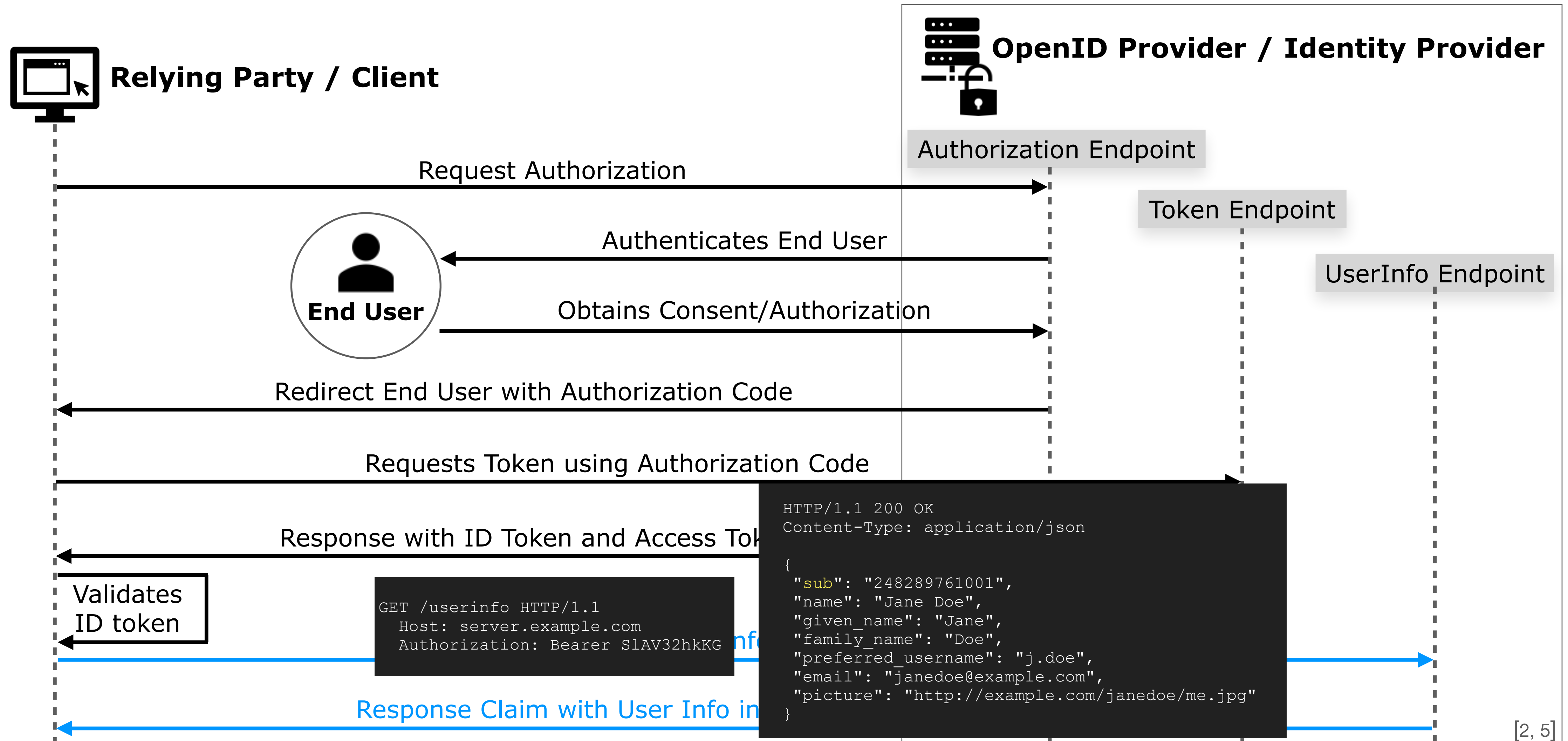
[2, 5]

Ein Flow im Detail: Authorization Code Flow



[2, 5]

Ein Flow im Detail: Authorization Code Flow



[2, 5]

Fragen?!

Vielen Dank

Quellen:

[1] https://openid.net/openid_connect_new-logo/ (abgerufen am 07.08.2021)

[2] „OpenID Connect Core 1.0 incorporating errata set 1“, https://openid.net/specs/openid-connect-core-1_0.html#Terminology (abgerufen am 07.08.2021)

[3] <https://oauth.net/2/> (abgerufen am 07.08.2021)

[4] Postman Application, Version 8.10.0

[5] „OPENID CONNECT (OIDC)“, <https://cloudsundial.com/node/7> (abgerufen am 07.08.2021)

Übersetzungen mit Hilfe von: <https://www.deepl.com/translator>



Hochschule für Technik
und Wirtschaft Berlin

University of Applied Sciences