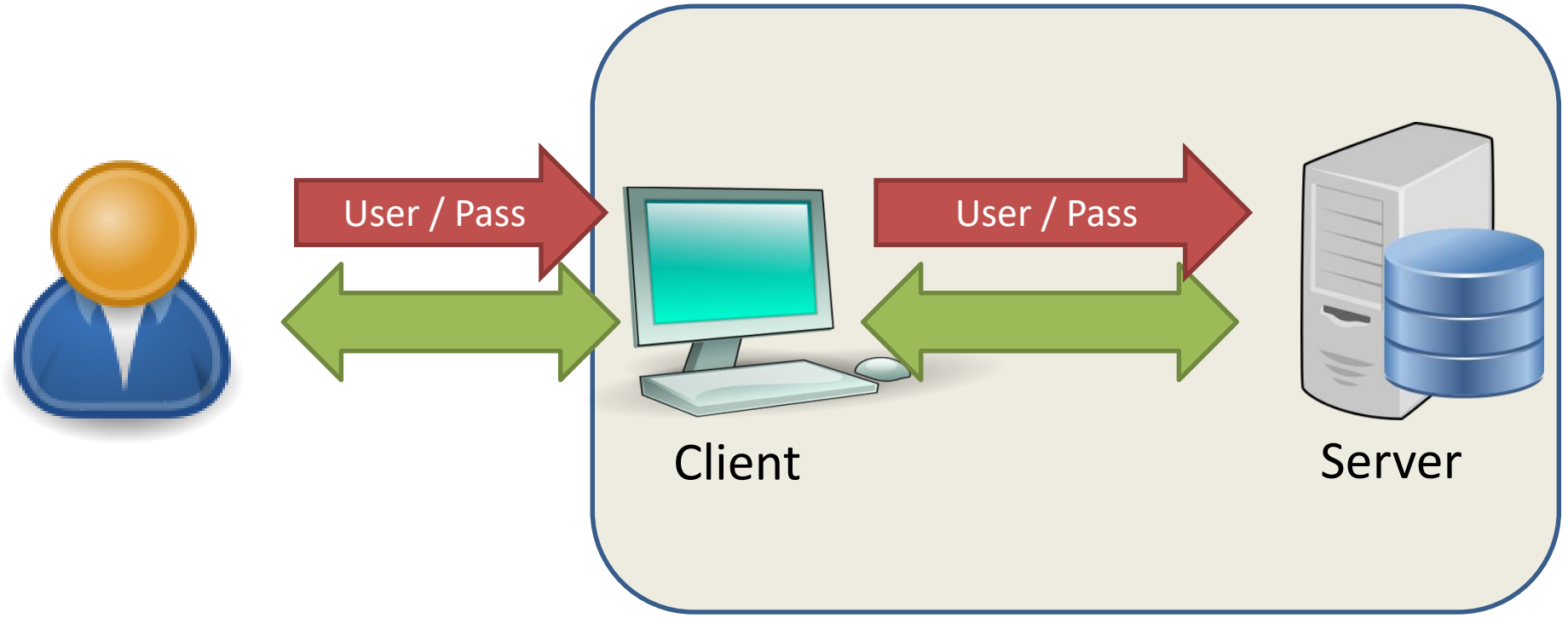
OAuth 2.0

Ralf Hoffmann

03 / 2017

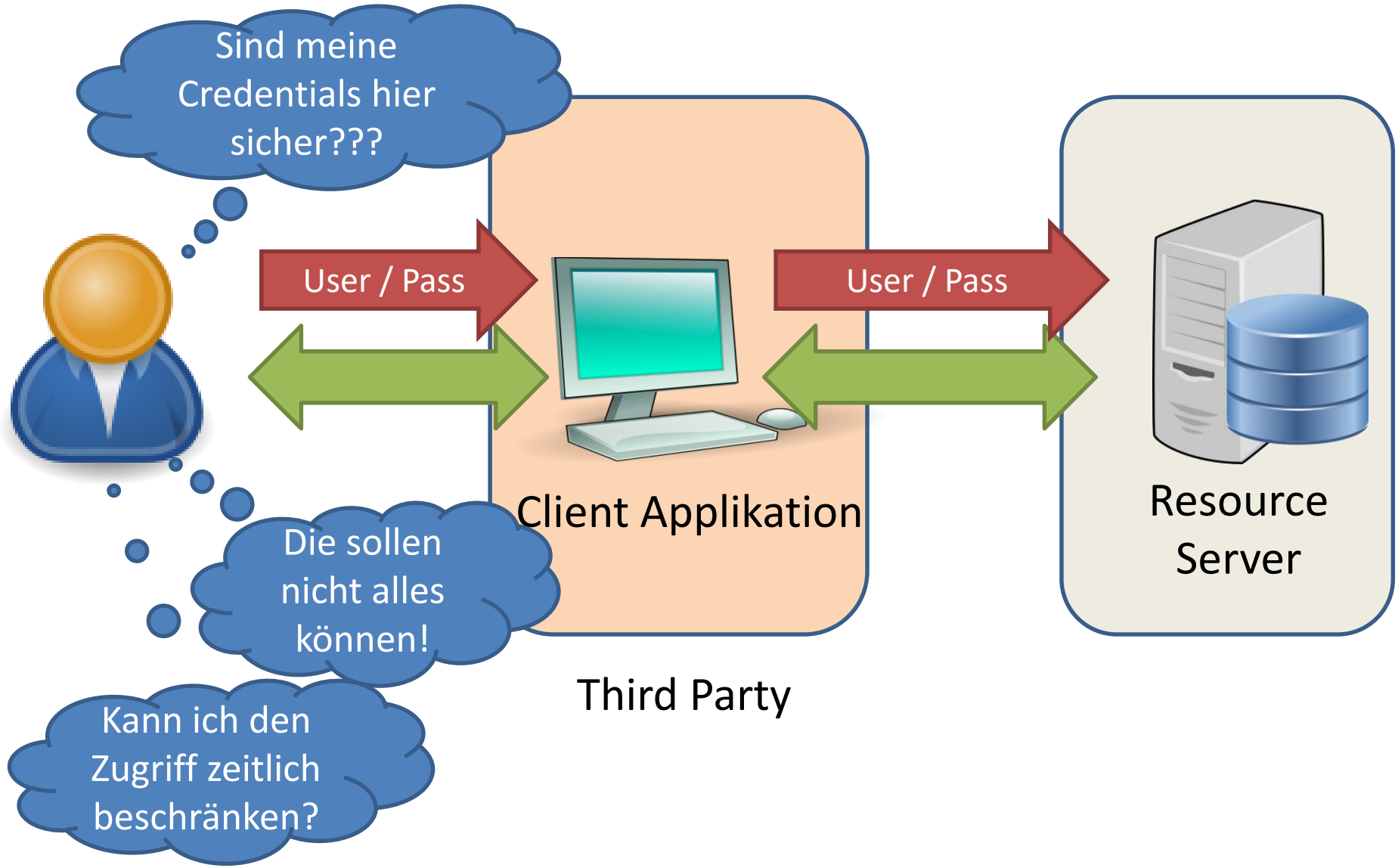
ralf.hoffmann@gmx.de

Früher



Alles aus einer Hand

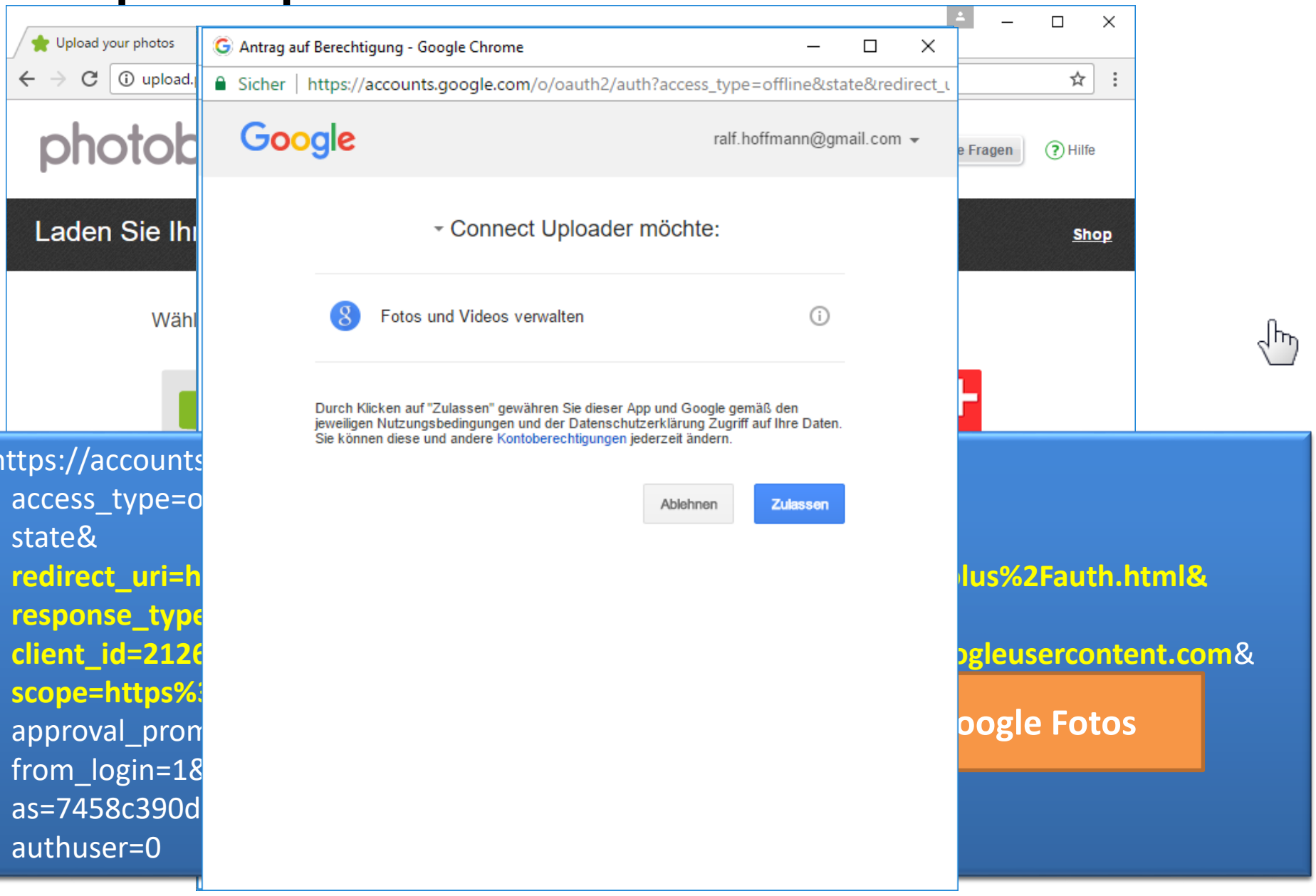
Früher / Heute



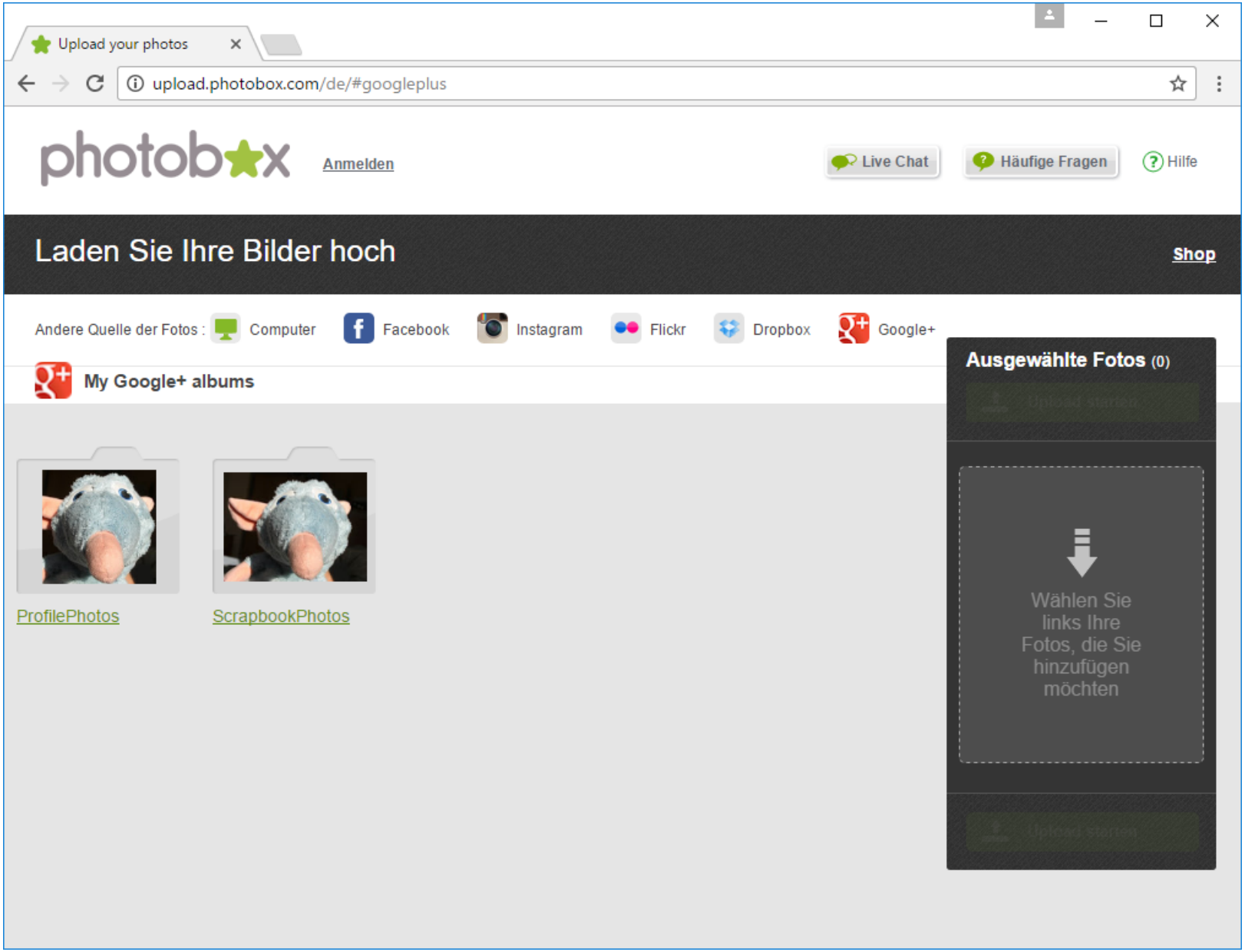
Lösung:

OAuth 2.0

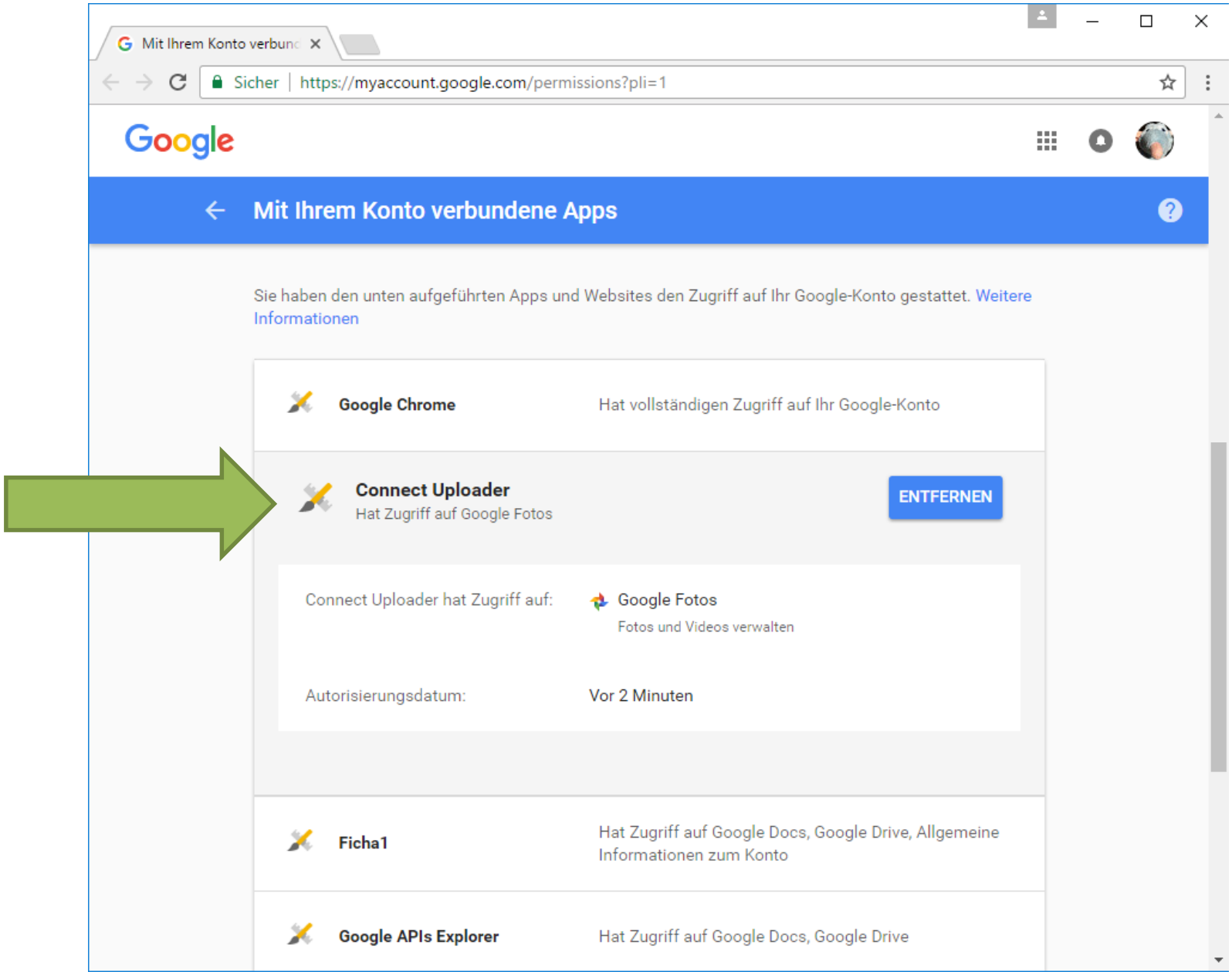
Beispiel: photobox.com



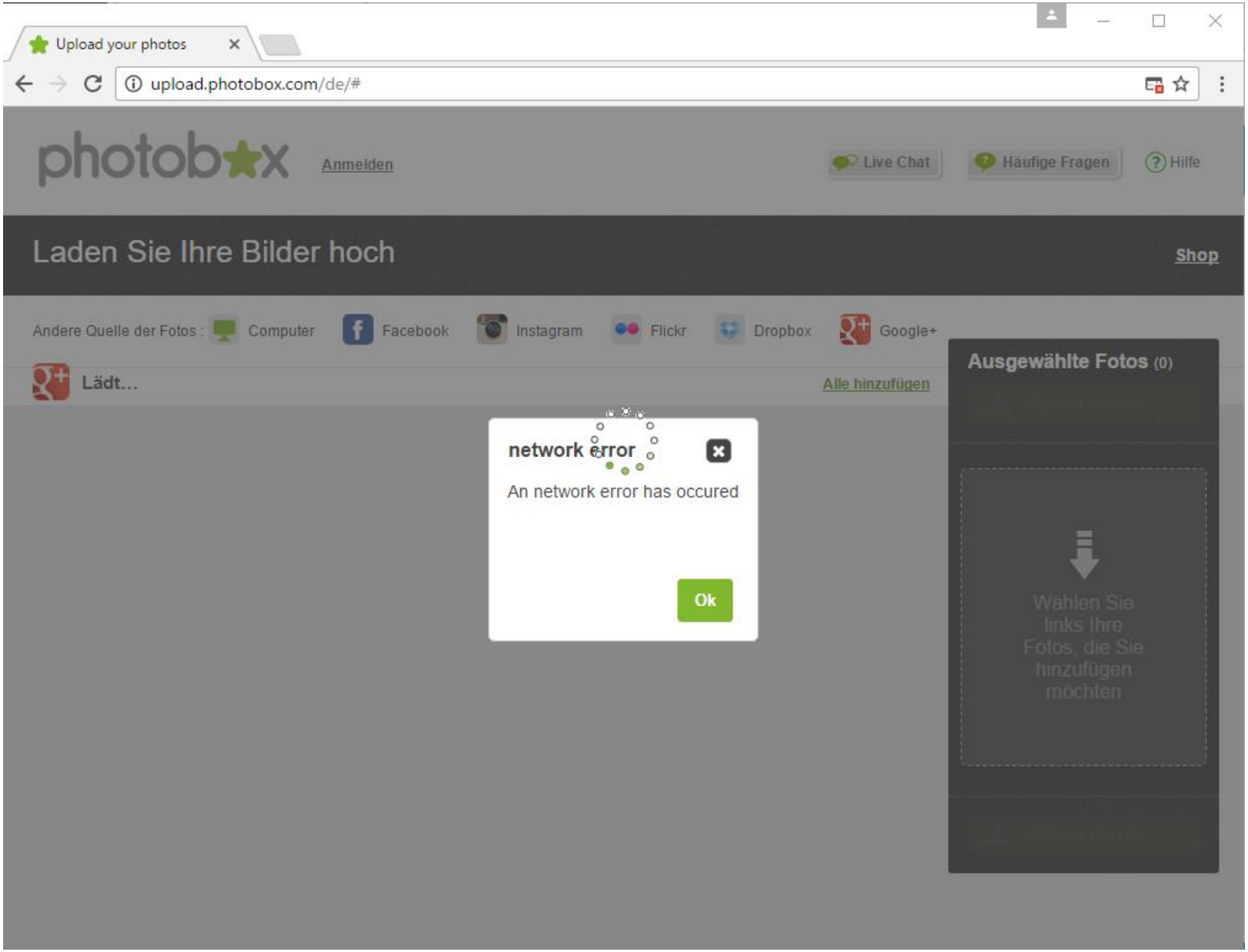
Beispiel: photobox.com

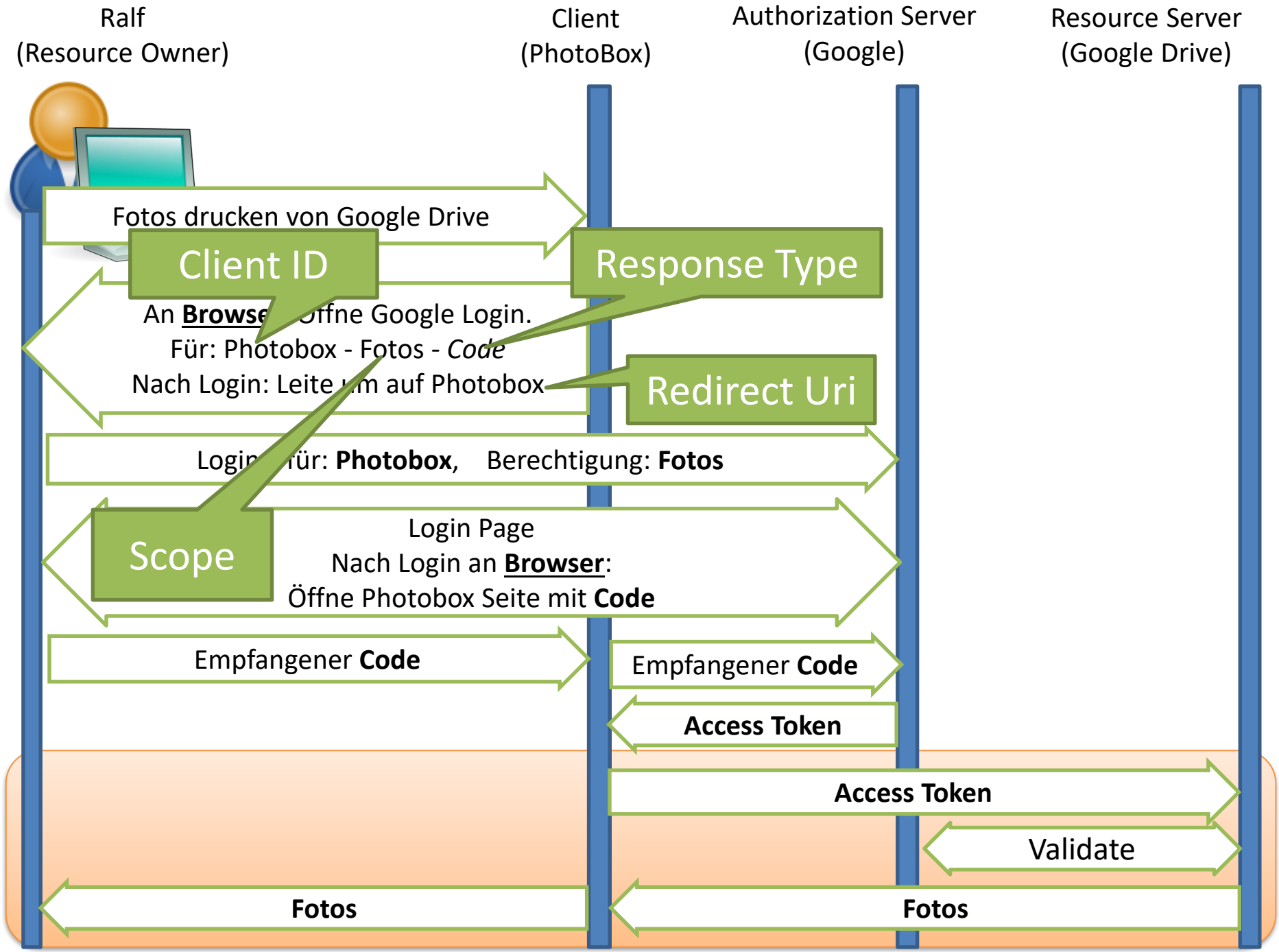


Beispiel: photobox.com



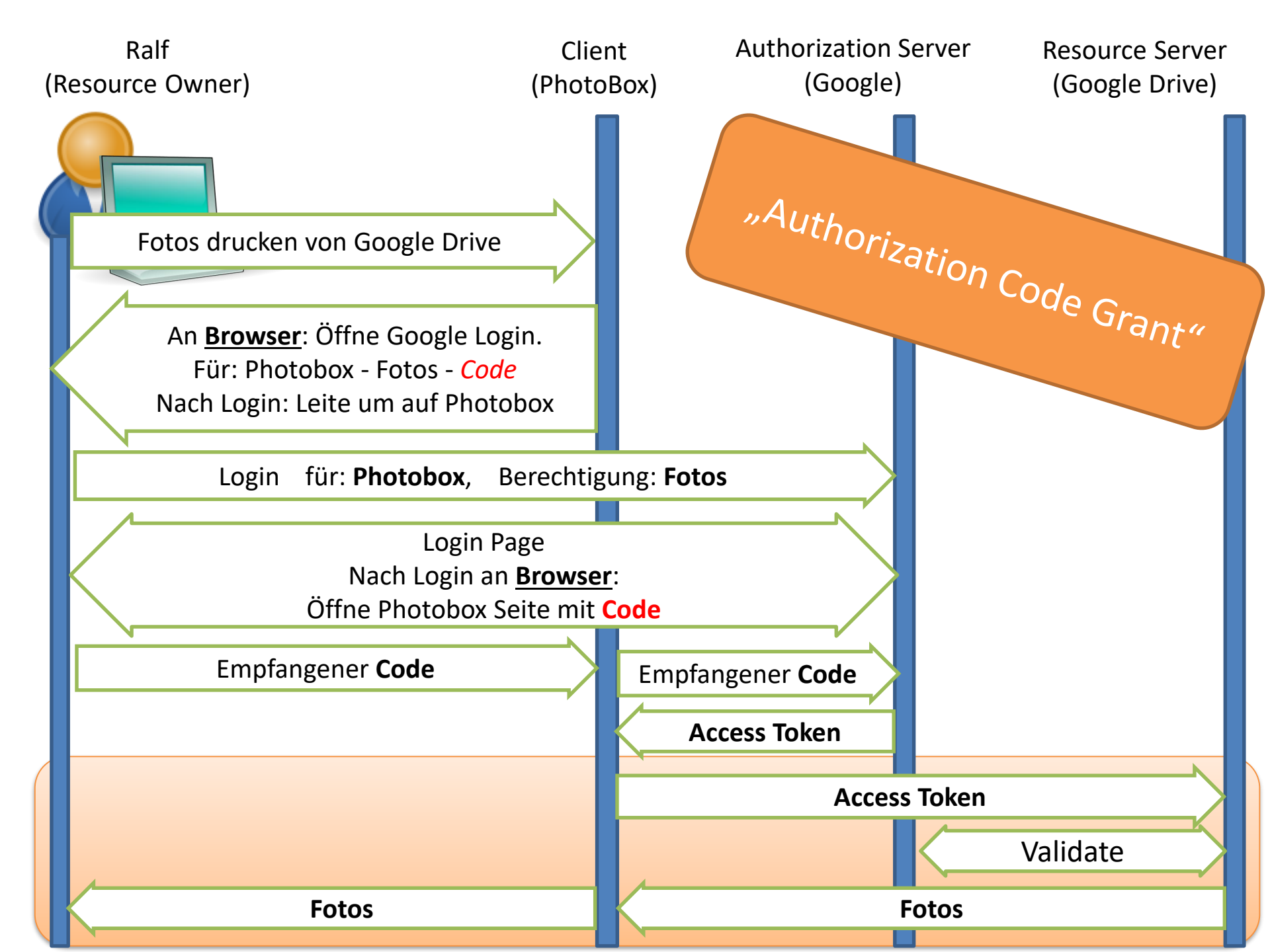
Beispiel: photobox.com

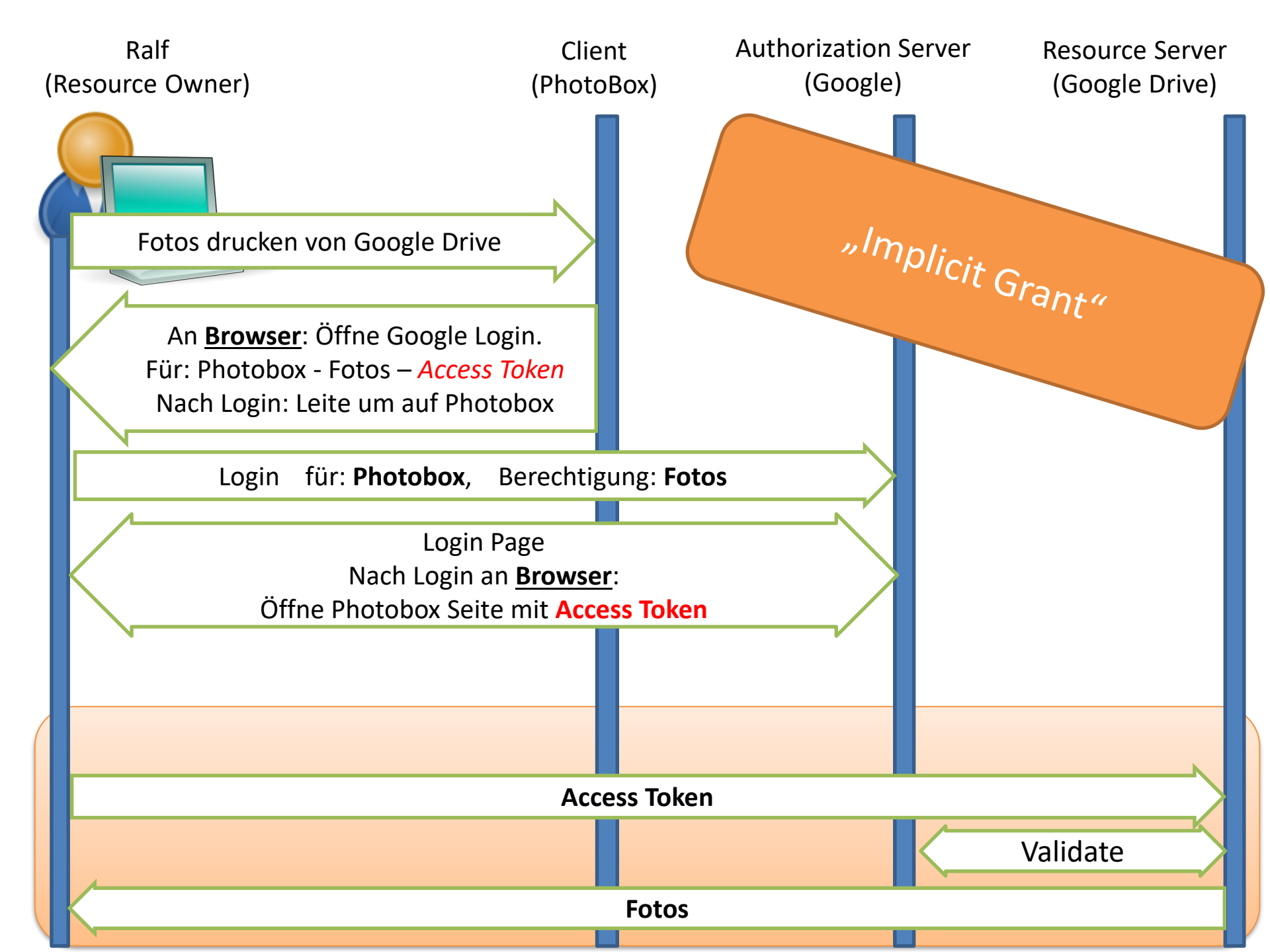


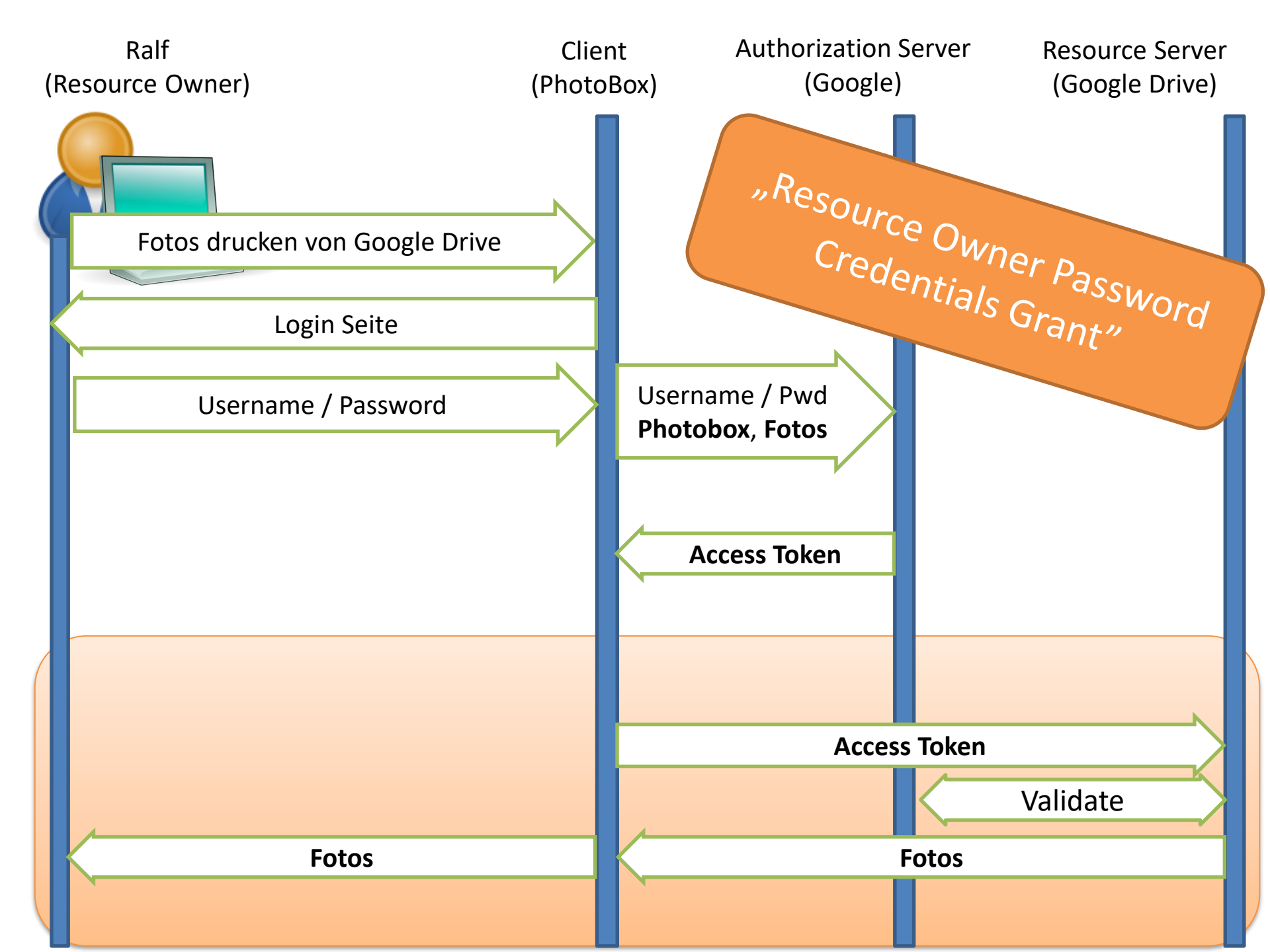

Ralf
(Resource Owner)
Client
(PhotoBox)
Authorization Server
(Google)
Resource Server
(Google Drive)
Fotos drucken von Google Drive
Client ID
Response Type
An **Browse** Öffne Google Login.
Für: Photobox - Fotos - *Code*
Nach Login: Leite um auf Photobox
Redirect Uri
Login für: **Photobox**, Berechtigung: **Fotos**
Scope
Login Page
Nach Login an **Browser**:
Öffne Photobox Seite mit **Code**
Empfangener **Code**
Empfangener **Code**
Access Token
Access Token
Validate
Fotos
Fotos

Was ist ein „Access Token“

- Zugriffsberechtigung
  - Wie Geld / Scheck
- Begrenzte Lebensdauer
  - Evtl. „Refresh“ Token -> neues Access Token
- Eingeschränkter Scope
  - Z.B. nur Fotos, kein Kalender
- Revoke
  - Token für ungültig erklären
- Inhalt des Tokens
  - Undefiniert!


Ralf
(Resource Owner)
Client
(PhotoBox)
Authorization Server
(Google)
Resource Server
(Google Drive)
„Authorization Code Grant“
Fotos drucken von Google Drive
An **Browser**: Öffne Google Login.
Für: Photobox - Fotos - *Code*
Nach Login: Leite um auf Photobox
Login für: **Photobox**, Berechtigung: **Fotos**
Login Page
Nach Login an **Browser**:
Öffne Photobox Seite mit **Code**
Empfangener **Code**
Empfangener **Code**
Access Token
Access Token
Validate
Fotos
Fotos


Ralf
(Resource Owner)
Client
(PhotoBox)
Authorization Server
(Google)
Resource Server
(Google Drive)
„Implicit Grant“
Fotos drucken von Google Drive
An **Browser**: Öffne Google Login.
Für: Photobox - Fotos – *Access Token*
Nach Login: Leite um auf Photobox
Login für: **Photobox**, Berechtigung: **Fotos**
Login Page
Nach Login an **Browser**:
Öffne Photobox Seite mit **Access Token**
Access Token
Validate
Fotos


Ralf
(Resource Owner)
Client
(PhotoBox)
Authorization Server
(Google)
Resource Server
(Google Drive)
„Resource Owner Password Credentials Grant"
Fotos drucken von Google Drive
Login Seite
Username / Password
Username / Pwd
Photobox, Fotos
Access Token
Access Token
Validate
Fotos
Fotos

Ralf
(Resource Owner)

Client
(PhotoBox)

Authorization Server
(Google)

Resource Server
(Google Drive)

„Client Credentials Grant“

Client / Secret
Photobox, **Fotos**

Access Token

Access Token

Validate

Fotos

Anwendungsfälle

- Authorization Code Grant
  - Applikationen **mit eigenem** Server
- Implicit Grant
  - Browser Applikationen **ohne eigenen** Server
- Resource Owner Password Credentials Grant
  - Legacy
  - Alles aus einer Hand
- Client Credentials Grant
  - Services ohne User Interaktion

Was fehlt?

Keine User Information!

OpenID Connect

What is OpenID Connect?

- OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. It allows Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner.

OpenID Connect

Also: Standard für **Identity Provider**

Was ist ein Identity Provider:

- Authentifiziert Benutzer
- Hält Informationen über den Benutzer
- Zuständig für viele verschiedene Resourcen
- Beispiele: Login with Google, Facebook etc.

Unterstützung durch:

- Microsoft, Google, Amazon, IBM, …

OpenID Connect

ID Token

- Json Web Token (JWT) = signiertes JSON
- Enthält “Claims”
  - User ID
  - Aussteller
  - Zeitstempel
  - Gültigkeitsdauer
  - Optional: Email, Name
  - Signatur

OpenID Connect

ID Token Beispiel:

```
{
   "sub"                          : "alice",
   "email"                        : "alice@wonderland.net",
   "email_verified"               : true,
   "name"                         : "Alice Adams",
   "given_name"                   : "Alice",
   "family_name"                  : "Adams",
   "phone_number"                 : "+359 (99) 100200305",
   "profile"                      : "https://c2id.com/users/alice",
   "https://c2id.com/groups" : [ "audit", "admin" ]
 }
```

OIDC Implementierungen

Microsoft

- Azure Active Directory

- Windows Server 2016

VIELE andere

Open Source (.Net)

- Identity Server
  - auch .Net Core
  - sehr erweiterbar!

Konsumieren in C#

Zu Fuß:

- Eingebetteter Browser
  Navigation auf Redirect Uri abfangen

- Externer Browser
  Http Listener in der App hört auf Redirect Uri

Mit Library

- IdentityModel.OidcClient2
- Auth0

Links

- OAuth 2.0 Spec:
  https://tools.ietf.org/html/rfc6749

- Open ID Connect erklärt:
  https://connect2id.com/learn/openid-connect

- Client Libraries
  https://github.com/IdentityModel/IdentityModel.OidcClient2

  https://auth0.com/

  https://docs.microsoft.com/de-de/azure/active-directory/develop/active-directory-devquickstarts-webapp-dotnet