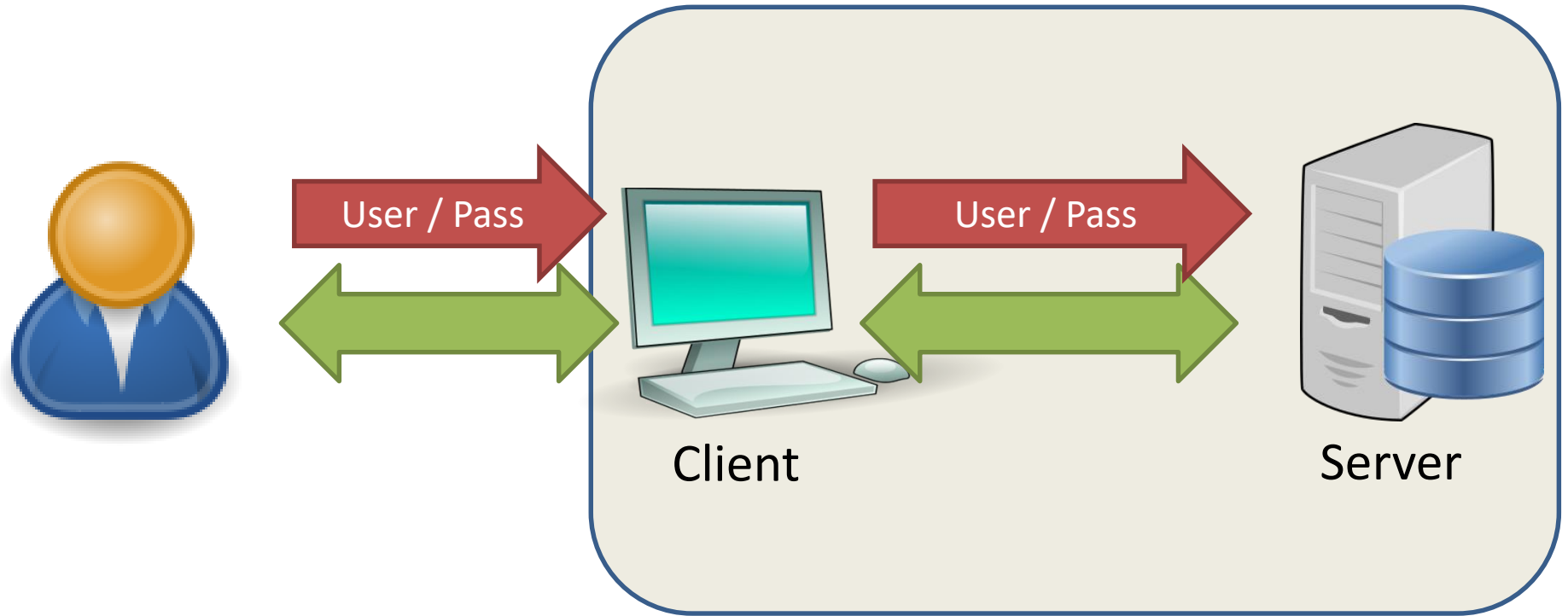


OAuth 2.0

Ralf Hoffmann

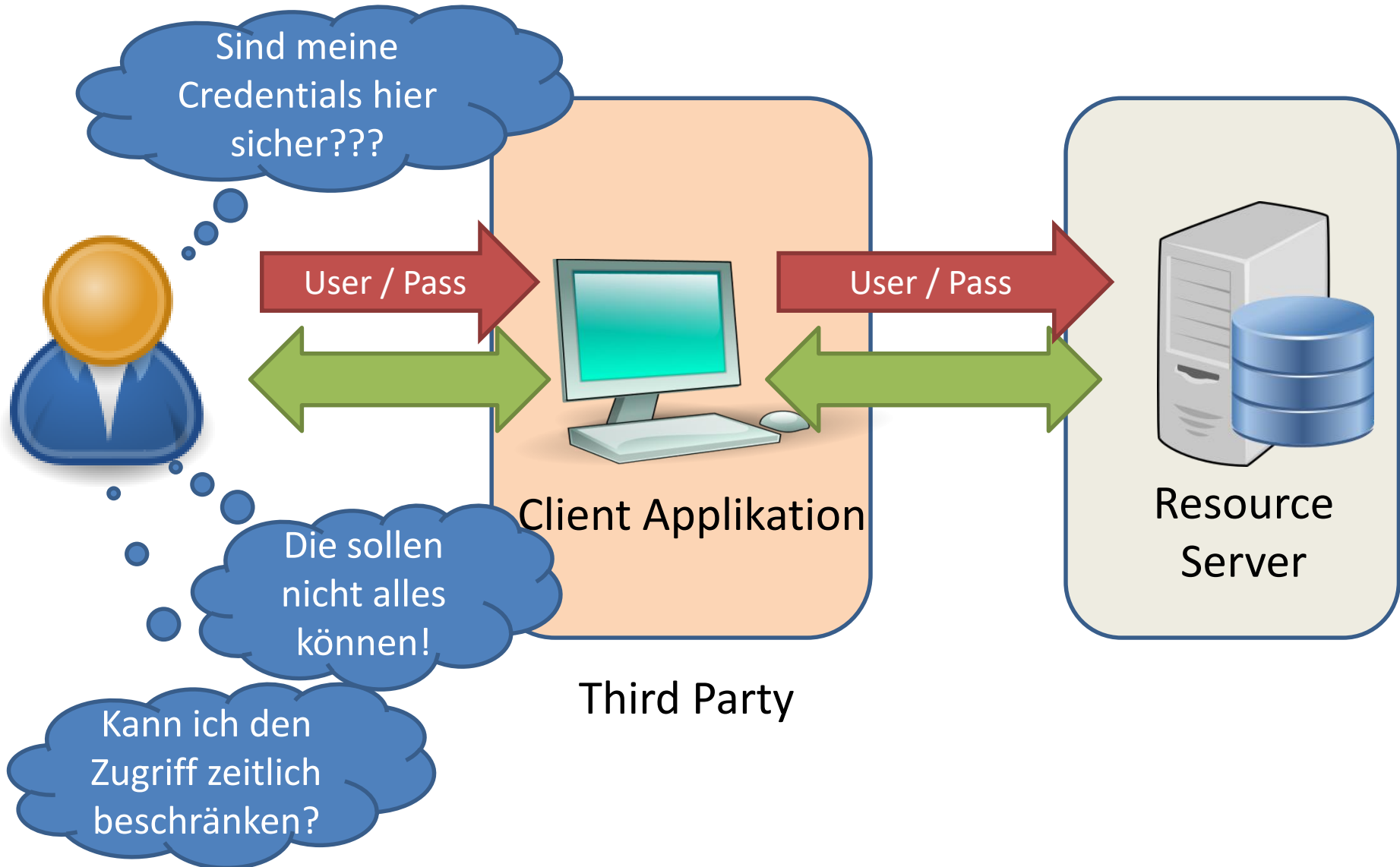
03 / 2017

Früher



Alles aus einer Hand

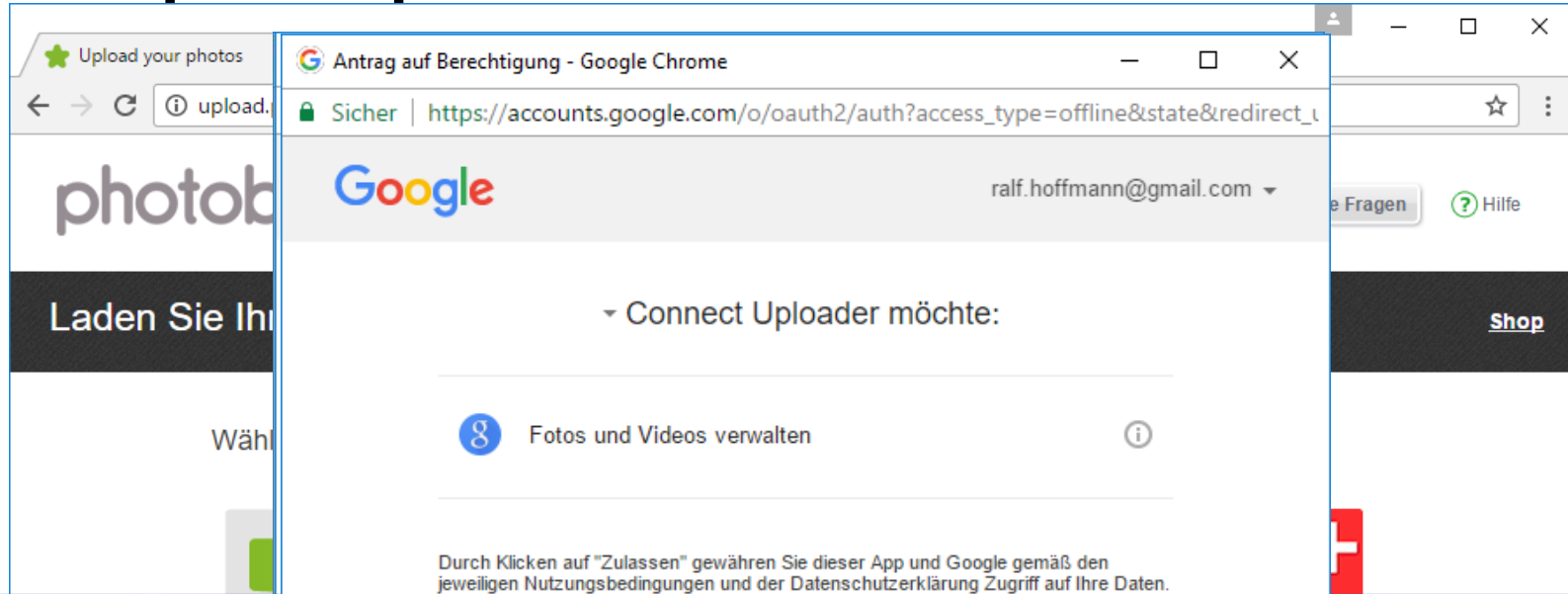
Früher / Heute



Lösung:

OAuth 2.0

Beispiel: photobox.com



https://accounts.google.com/o/oauth2/auth?access_type=offline&state&redirect_uri=https%3A%2F%2Fphotobox.com%2Fauth.html&response_type=code&client_id=2126&approval_prompt=auto&from_login=1&as=7458c390d&authuser=0

[plus%2Fauth.html&googleusercontent.com&google Fotos](#)

Beispiel: photobox.com

The screenshot shows the website **photobox.com** in a browser window. The address bar shows the URL `upload.photobox.com/de/#googleplus`. The page features the **photobox** logo and navigation links for **Anmelden**, **Live Chat**, **Häufige Fragen**, and **Hilfe**.

A dark banner at the top of the main content area reads **Laden Sie Ihre Bilder hoch** with a **Shop** link on the right. Below this, there are icons for various photo sources: **Computer**, **Facebook**, **Instagram**, **Flickr**, **Dropbox**, and **Google+**.

The **My Google+ albums** section displays two photo thumbnails of a blue elephant toy. The first is labeled **ProfilePhotos** and the second is labeled **ScrapbookPhotos**.

On the right side, a dark sidebar titled **Ausgewählte Fotos (0)** is visible. It contains a dashed box with a downward arrow and the text: **Wählen Sie links Ihre Fotos, die Sie hinzufügen möchten**. The sidebar also has **Upload starten** buttons at the top and bottom.

Beispiel: photobox.com

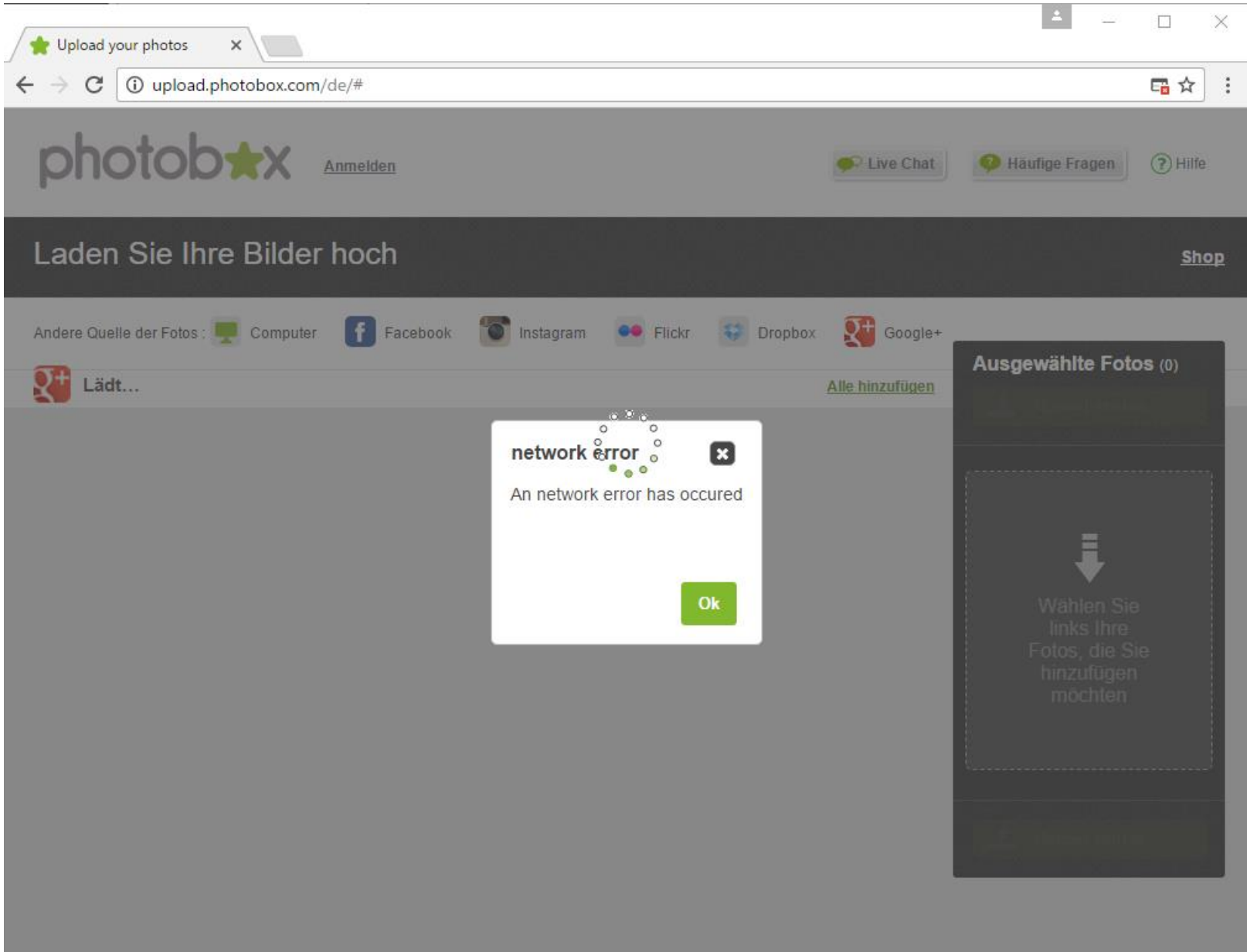
The screenshot shows a web browser window with the URL `https://myaccount.google.com/permissions?pli=1`. The page title is "Mit Ihrem Konto verbundene Apps". Below the title, there is a blue header bar with a back arrow and a question mark icon. The main content area contains a list of apps and their permissions. A green arrow points to the "Connect Uploader" app, which has a blue "ENTFERNEN" button next to it. Below the app name, there is a white box showing the app's access to "Google Fotos" and the authorization date "Vor 2 Minuten".

Mit Ihrem Konto verbundene Apps

Sie haben den unten aufgeführten Apps und Websites den Zugriff auf Ihr Google-Konto gestattet. [Weitere Informationen](#)

| | |
|---|---|
| Google Chrome | Hat vollständigen Zugriff auf Ihr Google-Konto |
| Connect Uploader | Hat Zugriff auf Google Fotos ENTFERNEN |
| Connect Uploader hat Zugriff auf: Google Fotos Fotos und Videos verwalten | |
| Autorisierungsdatum: | Vor 2 Minuten |
| Ficha1 | Hat Zugriff auf Google Docs, Google Drive, Allgemeine Informationen zum Konto |
| Google APIs Explorer | Hat Zugriff auf Google Docs, Google Drive |

Beispiel: photobox.com

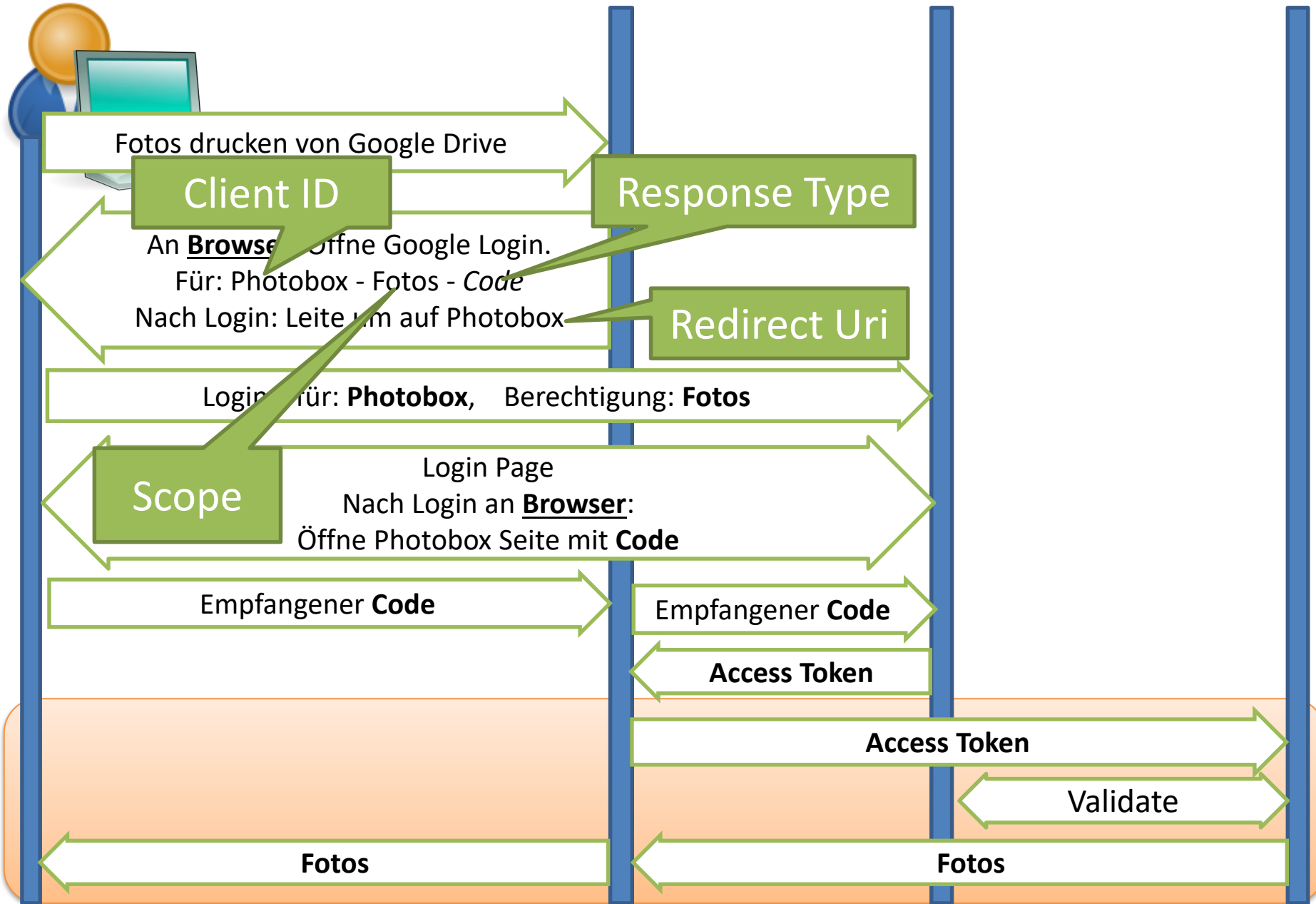


Ralf
(Resource Owner)

Client
(PhotoBox)

Authorization Server
(Google)

Resource Server
(Google Drive)



Fotos drucken von Google Drive

Client ID

Response Type

An **Browser** 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“

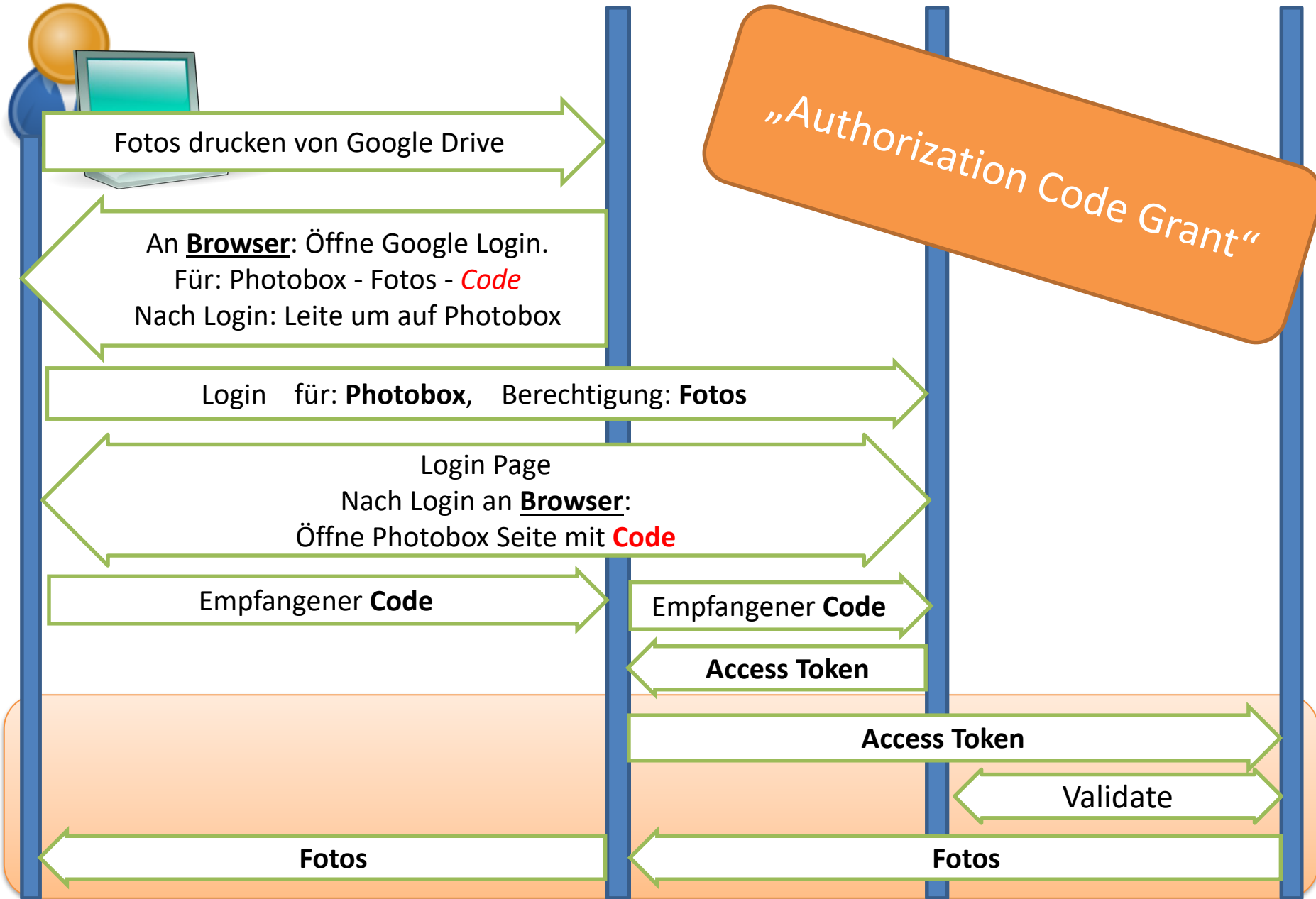
- **Zugriffsberechtigung**
 - Wie Geld / Scheck
- **Begrenzte Lebensdauer**
 - Evtl. „Refresh“ Token -> neues Access Token
- **Eingeschränkter Scope**
 - Z.B. nur Fotos, kein Kalender
- **Revoke**
 - Token für ungültig erklären
- **Inhalt des Tokens**
 - undefiniert!

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

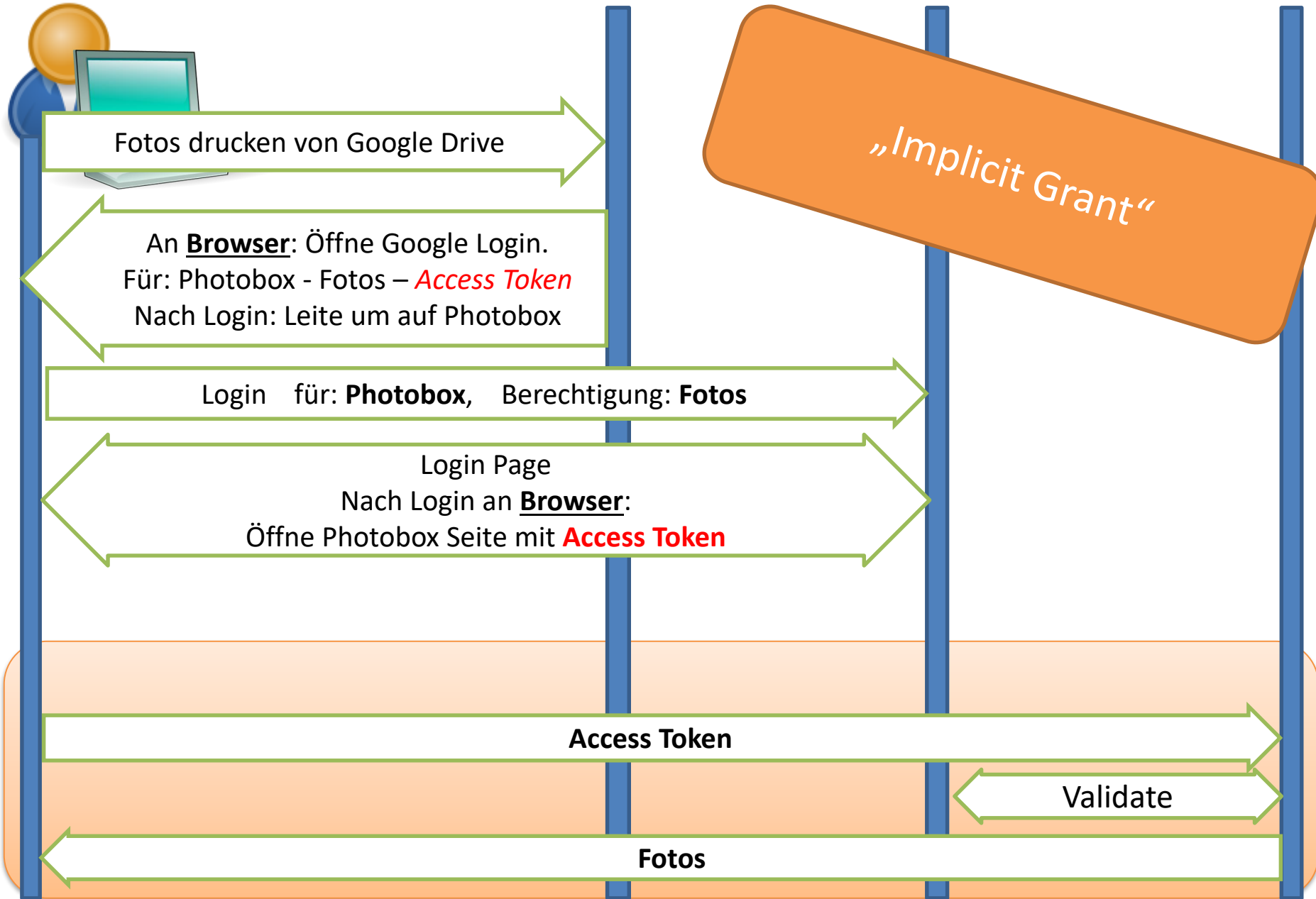
Fotos

Ralf
(Resource Owner)

Client
(PhotoBox)

Authorization Server
(Google)

Resource Server
(Google Drive)



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

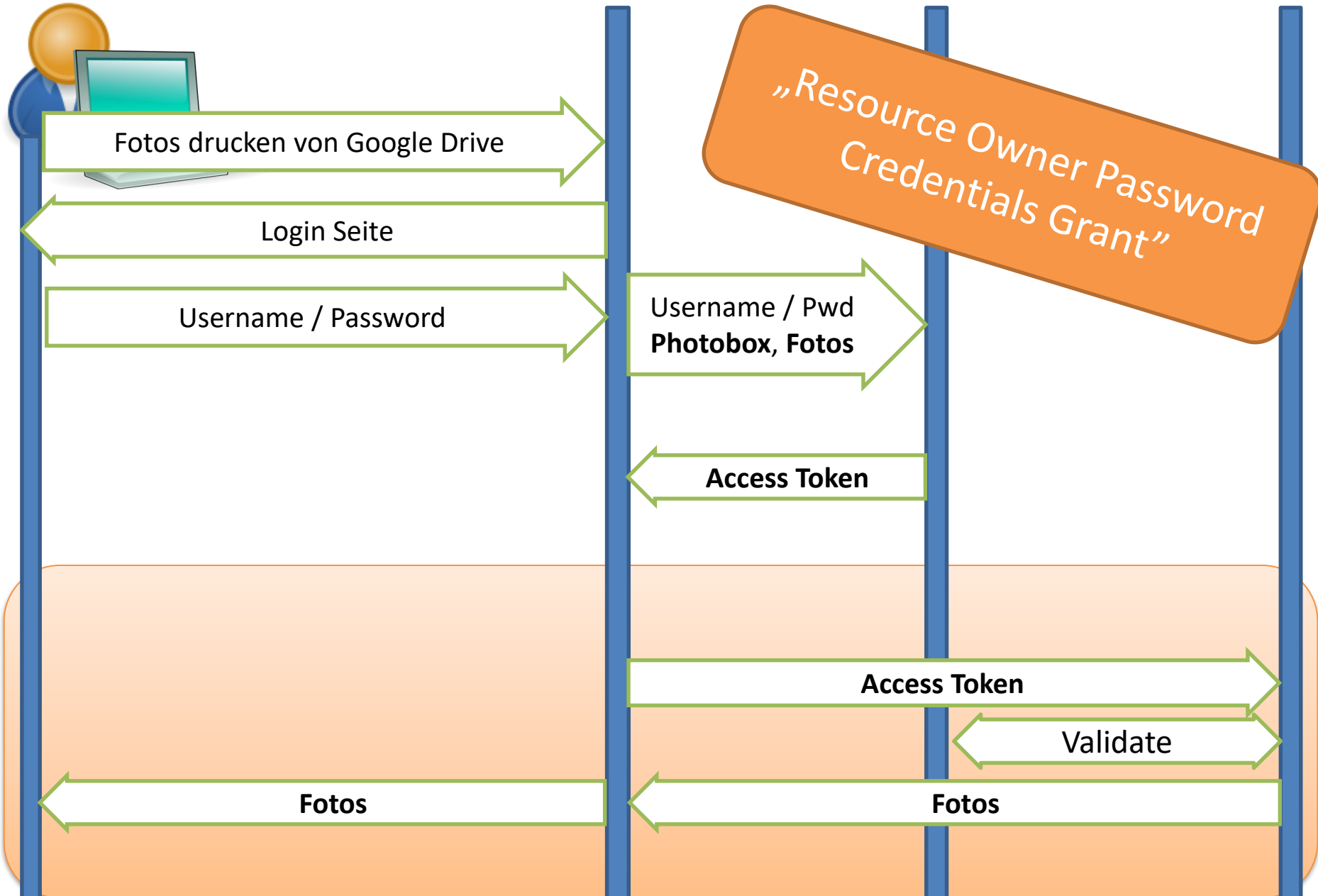
„Implicit Grant“

Ralf
(Resource Owner)

Client
(PhotoBox)

Authorization Server
(Google)

Resource Server
(Google Drive)



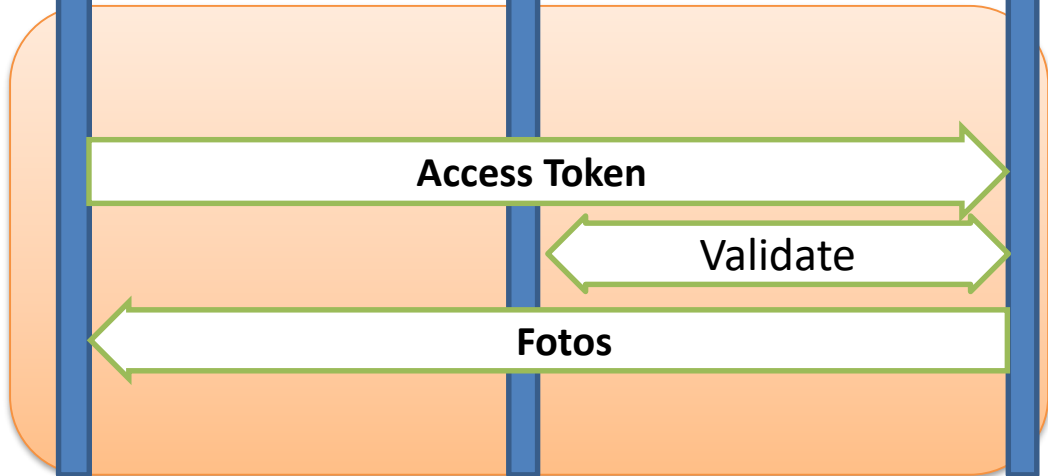
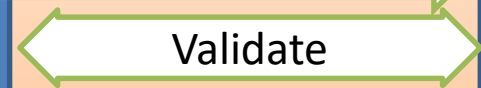
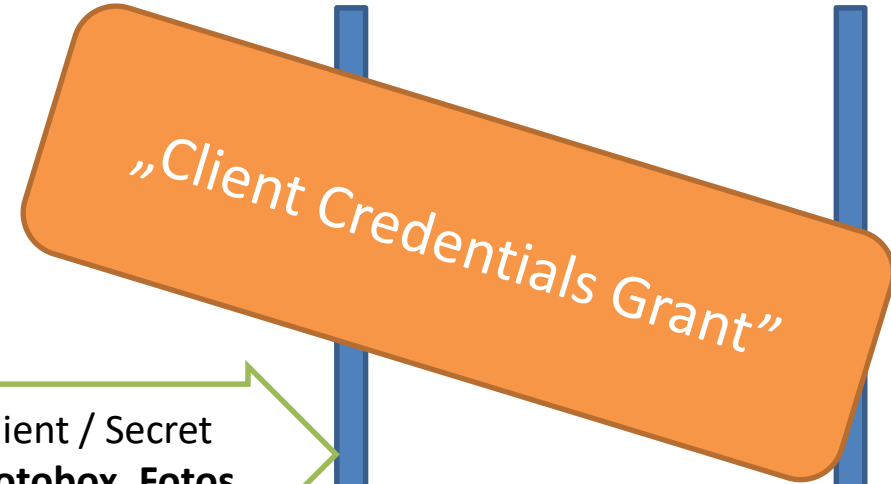
Ralf
(Resource Owner)



Client
(PhotoBox)

Authorization Server
(Google)

Resource Server
(Google Drive)



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 Ressourcen
- 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>