Shibboleth & OAuth2 für die Autorisierung von Apps

Als Infrasturktur für die RWTHApp

Marius Politze
Bernd Decker

Übersicht

- OAuth2 zur Autorisierung an der RWTH Aachen
  - → Einleitung
  - → Architektur
- Authentifizierung für OAuth2 über Shibboleth
  - → Datenfluss & …
  - → … Beispiel RWTHApp
- Weitere Einsatzszenarien
  - → OAuth2 im DFN AAI
- Fazit
  - → Aktueller Stand
  - → Ausblick

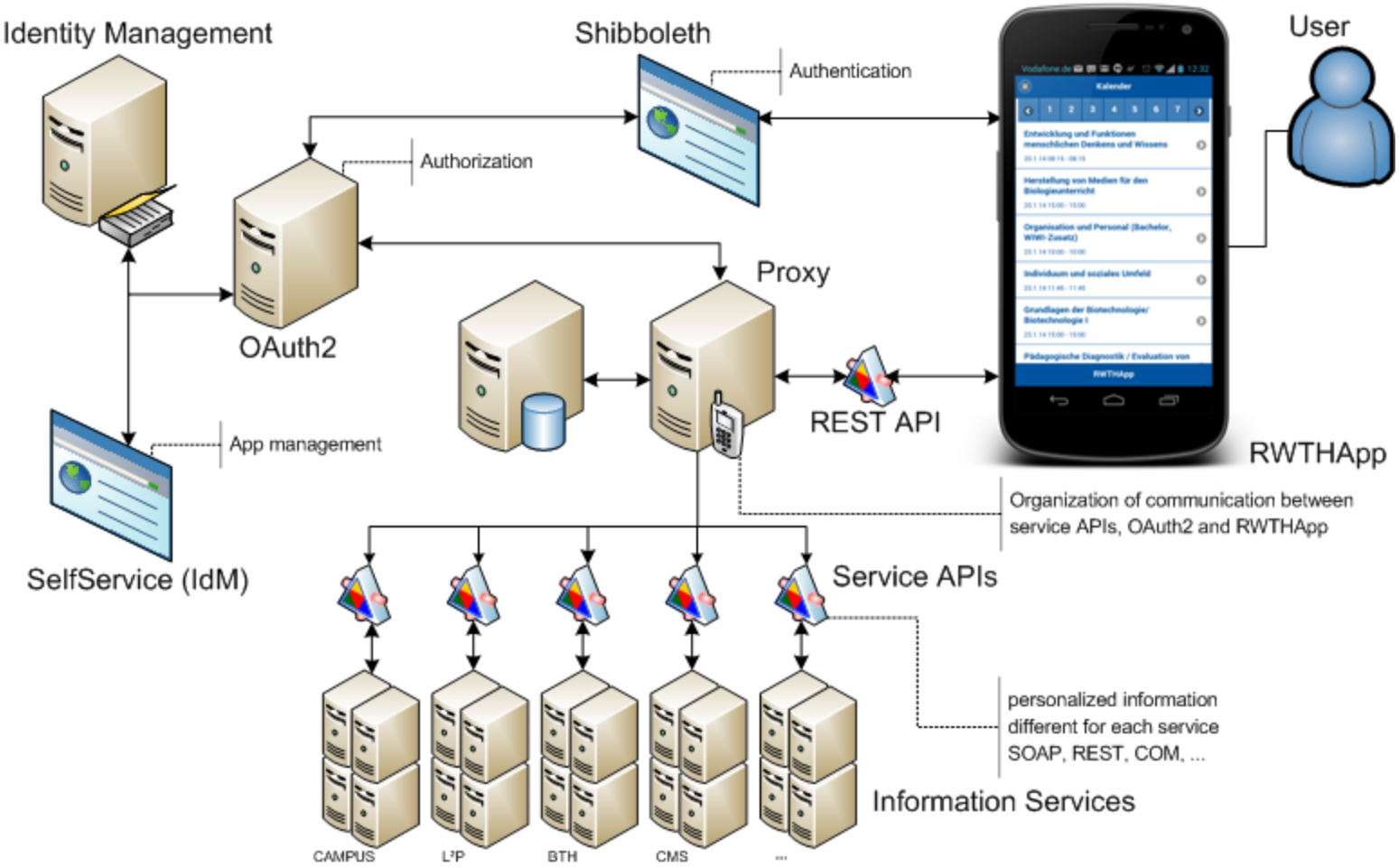
Warum?

- **Ausgangslage**
  - → RWTHApp soll entwickelt werden (CMS, LMS, BTH, …)
  - → Apps über „Screenscraping“ und mit Abfrage von RWTH-Credentials
  - → Entwicklung einer API für das E-Learning Portal L²P, für Seminare etc.
- **Problem**
  - → Wildwuchs, ohne Regelungen bzgl. Sicherheit, Datenschutz
  - → Verbieten quasi unmöglich
- **Maßnahme**
  - → Zentrales Angebot für Entwickler schaffen
  - → Komfortabel zu benutzen (einfach, stabil)

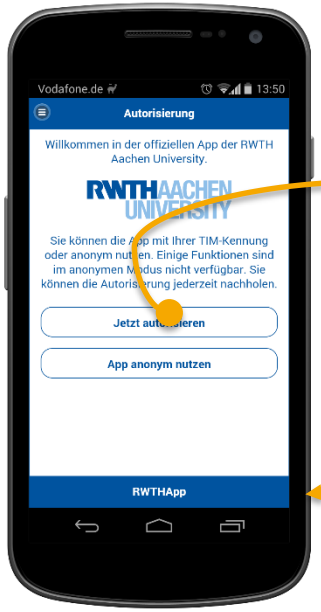
Anforderungen

- **Keine Weitergabe von Benutzernamen und Passwort an die App**
- **Credentials werden bei Verlust des Geräts nicht kompromittiert**
- **Apps explizit für bestimmte Anwendungen autorisieren**
- **(De-)Autorisierung einer App ohne Auswirkungen auf andere Apps**
- **Nur bekannte Apps erhalten Zugriff auf Quellsysteme**
- **Datenintegrität sicherstellen**

Architektur



Datenfluss



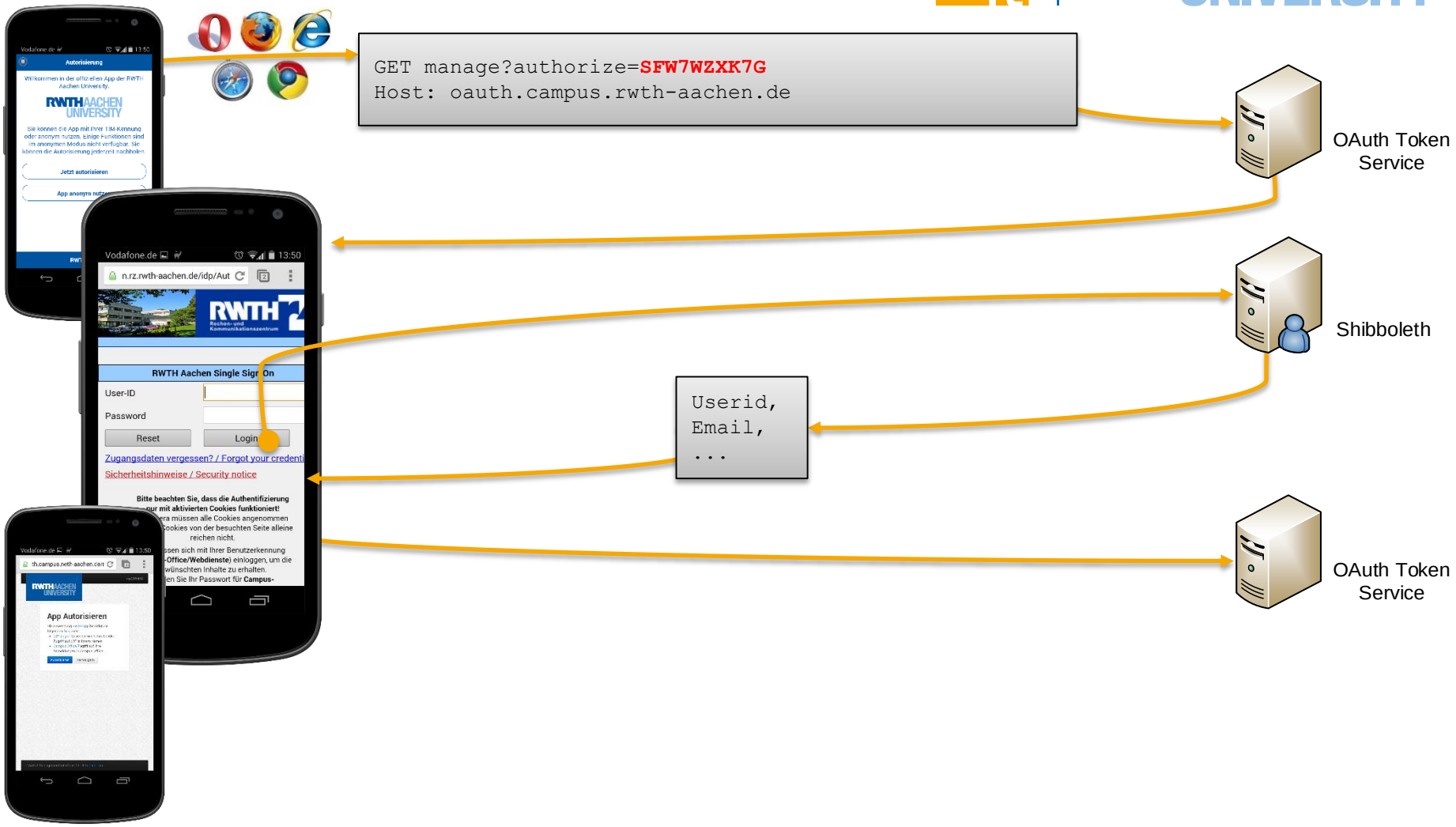

```
POST /oauth2waitress/oauth2.svc/code HTTP/1.1
Host: oauth.campus.rwth-aachen.de
Content-Type: application/x-www-form-urlencoded

client_id=QhV1IXlzticl9JCKgH01bhOMlu.app.rwth-aachen.de&
scope=l2p.rwth campus.rwth
```

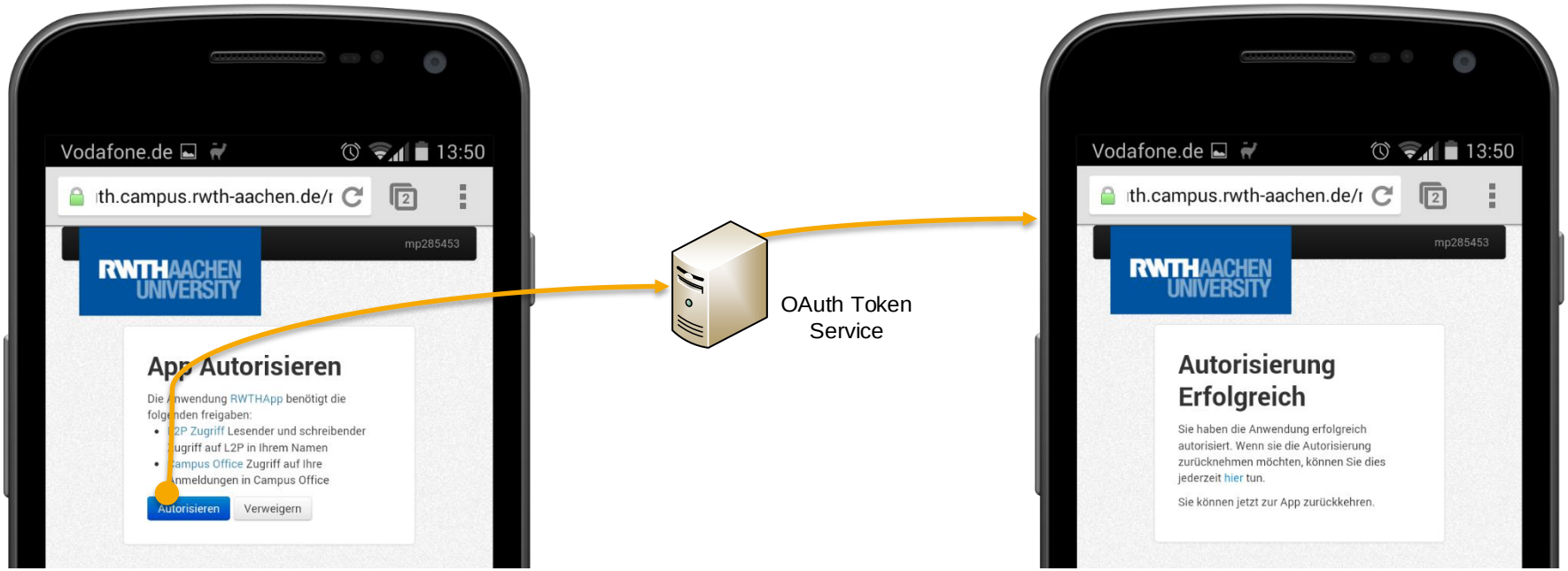
```
{
    "device_code" : "BaUAJHPFYFi6wKU0WY5xLC",
    "user_code" : "SFW7WZXK7G",
    "verification_url" : "https://oauth.campus.rwth-aachen.de/manage",
    "expires_in" : 1800,
    "interval" : 5
}
```

OAuth Token Service

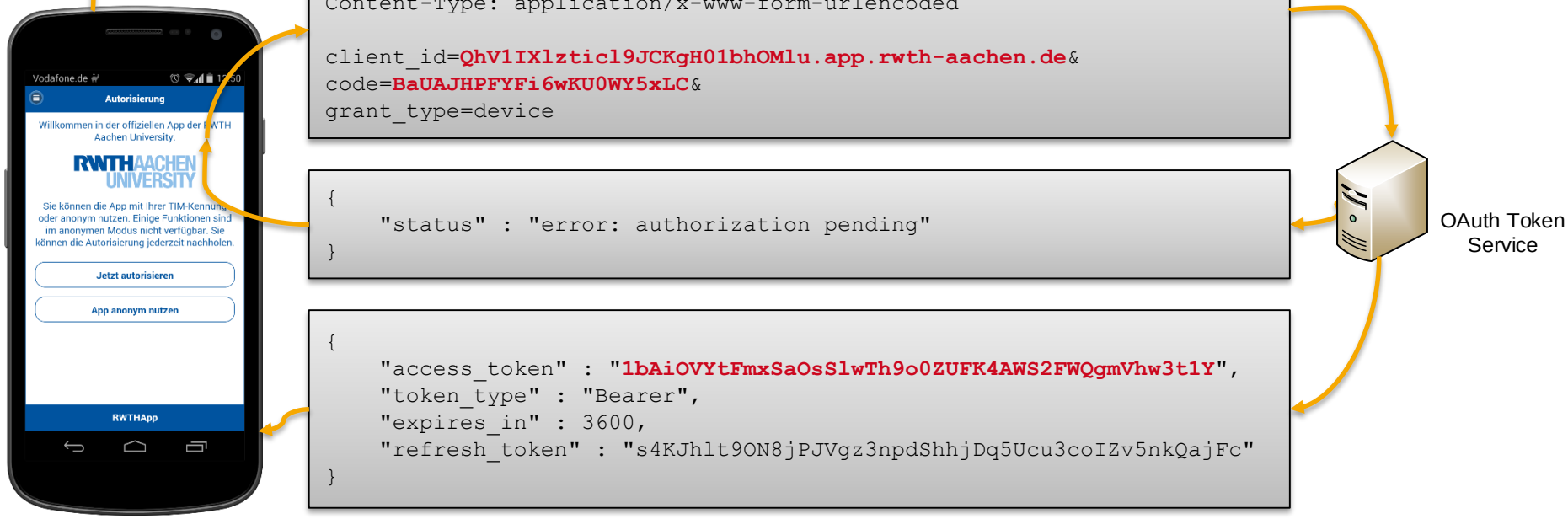
Datenfluss


GET manage?authorize=SFW7WZXK7G
Host: oauth.campus.rwth-aachen.de
OAuth Token Service
Shibboleth
Userid,
Email,
...
OAuth Token Service
RWTH Aachen Single Sign On
User-ID
Password
Reset
Login
Zugangsdaten vergessen? / Forgot your credenti
Sicherheitshinweise / Security notice
App Autorisieren

Datenfluss


Vodafone.de
13:50
th.campus.rwth-aachen.de/r
mp285453
RWTH AACHEN UNIVERSITY
App Autorisieren
Die Anwendung RWTHApp benötigt die folgenden freigaben:
L2P Zugriff Lesender und schreibender Zugriff auf L2P in Ihrem Namen
Campus Office Zugriff auf Ihre Anmeldungen in Campus Office
Autorisieren
Verweigern
OAuth Token Service
Vodafone.de
13:50
th.campus.rwth-aachen.de/r
mp285453
RWTH AACHEN UNIVERSITY
Autorisierung Erfolgreich
Sie haben die Anwendung erfolgreich autorisiert. Wenn sie die Autorisierung zurücknehmen möchten, können Sie dies jederzeit hier tun.
Sie können jetzt zur App zurückkehren.

Datenfluss


Vodafone.de
Autorisierung
Willkommen in der offiziellen App der RWTH Aachen University.
RWTH AACHEN UNIVERSITY
Sie können die App mit Ihrer TIM-Kennung oder anonym nutzen. Einige Funktionen sind im anonymen Modus nicht verfügbar. Sie können die Autorisierung jederzeit nachholen.
Jetzt autorisieren
App anonym nutzen
RWTHApp
POST /oauth2waitress/oauth2.svc/token HTTP/1.1
Host: oauth.campus.rwth-aachen.de
Content-Type: application/x-www-form-urlencoded
client_id=QhV1IXlzticl9JCKgH01bhOMlu.app.rwth-aachen.de&
code=BaUAJHPFYFi6wKU0WY5xLC&
grant_type=device
{
"status" : "error: authorization pending"
}
{
"access_token" : "1bAiOVYtFmxSaOsSlwTh9o0ZUFK4AWS2FWQgmVhw3t1Y",
"token_type" : "Bearer",
"expires_in" : 3600,
"refresh_token" : "s4KJhlt9ON8jPJVgz3npdShhjDq5Ucu3coIZv5nkQajFc"
}
OAuth Token Service

Datenfluss

```
GET /proxy/api.svc/GetNewsFeed?
accessToken= 1bAiOVYtFmxSaOsSlwTh9o0ZUFK4AWS2FWQgmVhw3t1Y HTTP/1.1
Host: moped.ecampus.rwth-aachen.de
```

Informationsdienst

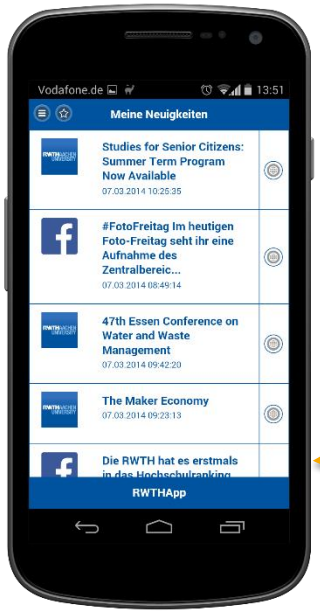
```
GET /oauth2waitress/oauth2.svc/token?
accessToken= 1bAiOVYtFmxSaOsSlwTh9o0ZUFK4AWS2FWQgmVhw3t1Y&
serviceId=asder34daf3hbdh34jsk5l.svc.rwth-aachen.de HTTP/1.1
Host: oauth.campus.rwth-aachen.de
```

OAuth Token Service

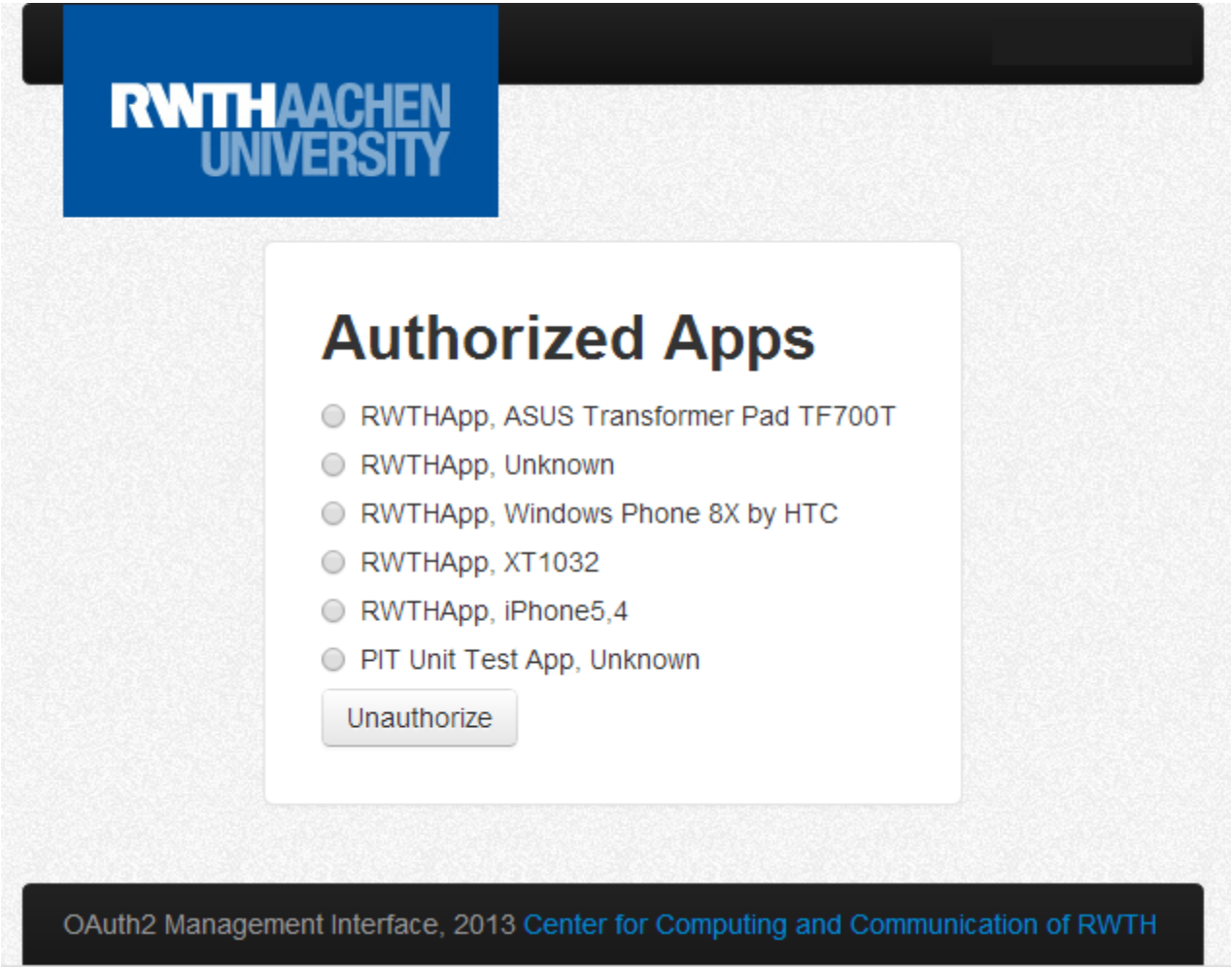
```
{
  uid: "abc123456"
}
```

Informationsdienst

```
{
  NewsFeed: [
    {Title: "Studies for Senior...", Date: "2014-03-07T15:35Z"},
    {Title: "#FotoFreitag Im heutigen...", Date: "2014-03-07T13:22Z"},
    ...
  ]
}
```



Autorisierte Apps



Weitere Einsatzszenarien

- **OAuth über WAYF**
  - → Globale E-Learning Szenarien an der RWTH Aachen
  - → Gigamove App
- **OAuth as a Service (Eine geteilte OAuth Instanz)**
  - → Terminplaner
  - → Videokonferenzen
- **OAuth Cluster (Viele vernetzte Instanzen)**
  - → Eduroam for devices
  - → VPN
- **…?**

Aktueller Stand

- **Installationen seit Veröffentlichung**
  - → 6300 seit November 2013 
  - → 3000 seit Januar 2014 
  - → 140 seit Februar 2014 
- **OAuth Schnittstelle**
  - → ~11.000 Aktive Autorisierungen (personalisiert)
  - → ~30.000 Requests pro Tag, davon ca. 3.000 anonym
- **Probleme**
  - → Viele zufriedene Nutzer ;-)

Ausblick

- **Veröffentlichen der API für Entwickler / Studenten**
- **Anbinden weiterer Informationsdienste in der RWTH**
  - → Bibliothek
  - → Nahverkehr
  - → Studentenwerk
  - → …
- **Feintuning, Reporting**