

Plan B

Service to Service Authentication with OAuth

Zalando Tech Meetup Dortmund, 2016-05-12

ZALANDO

15 countries

3 fulfillment centers

18 million active customers

3 billion € revenue 2015

135+ million visits per month

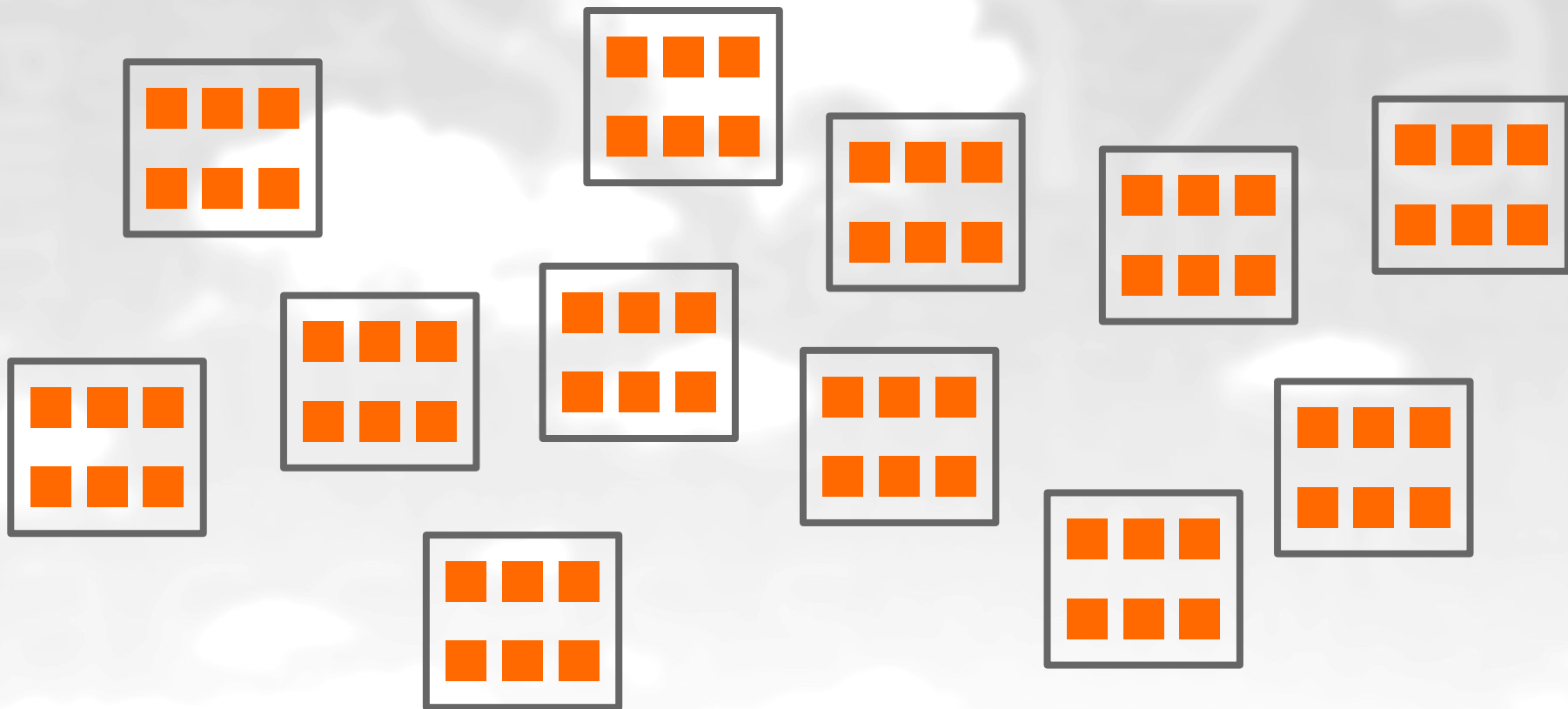
10.000+ employees in Europe



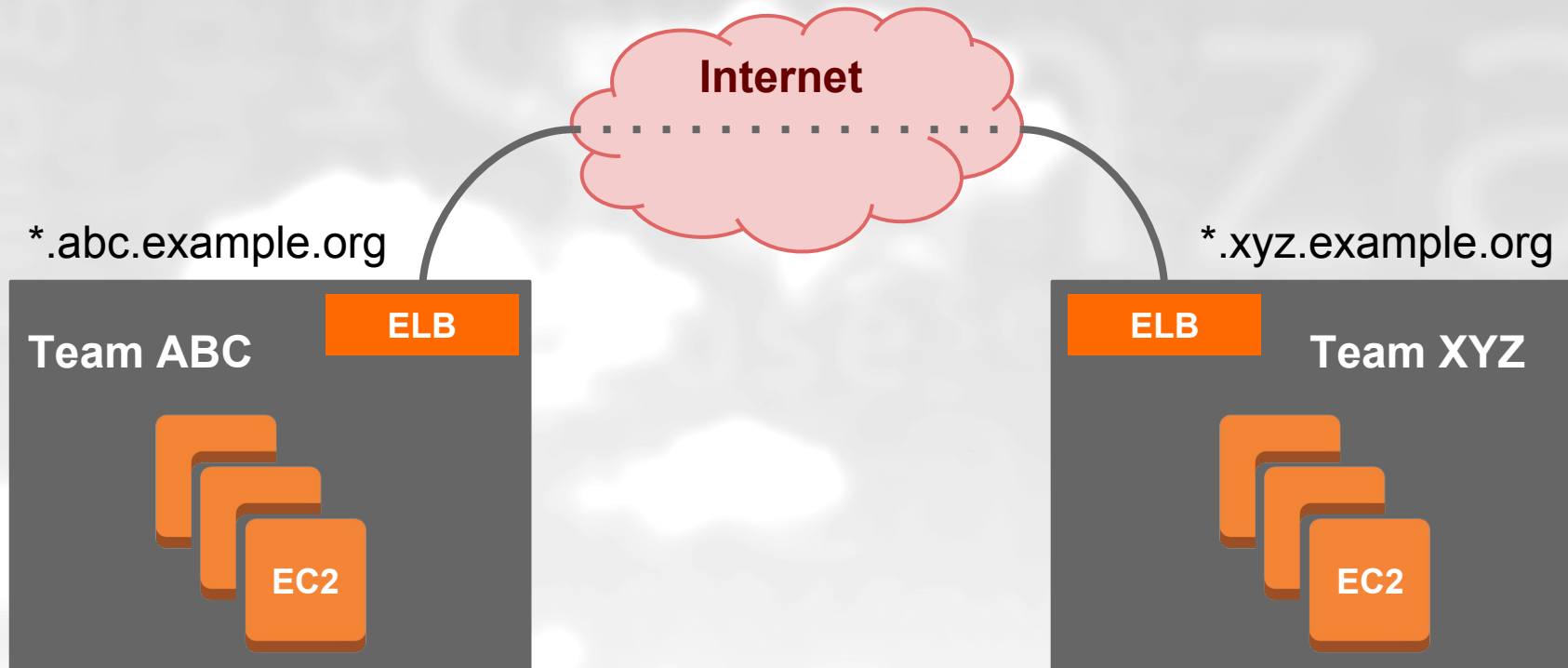
RADICAL AGILITY

AUTONOMY

ONE DATA CENTER PER TEAM



ISOLATED AWS ACCOUNTS

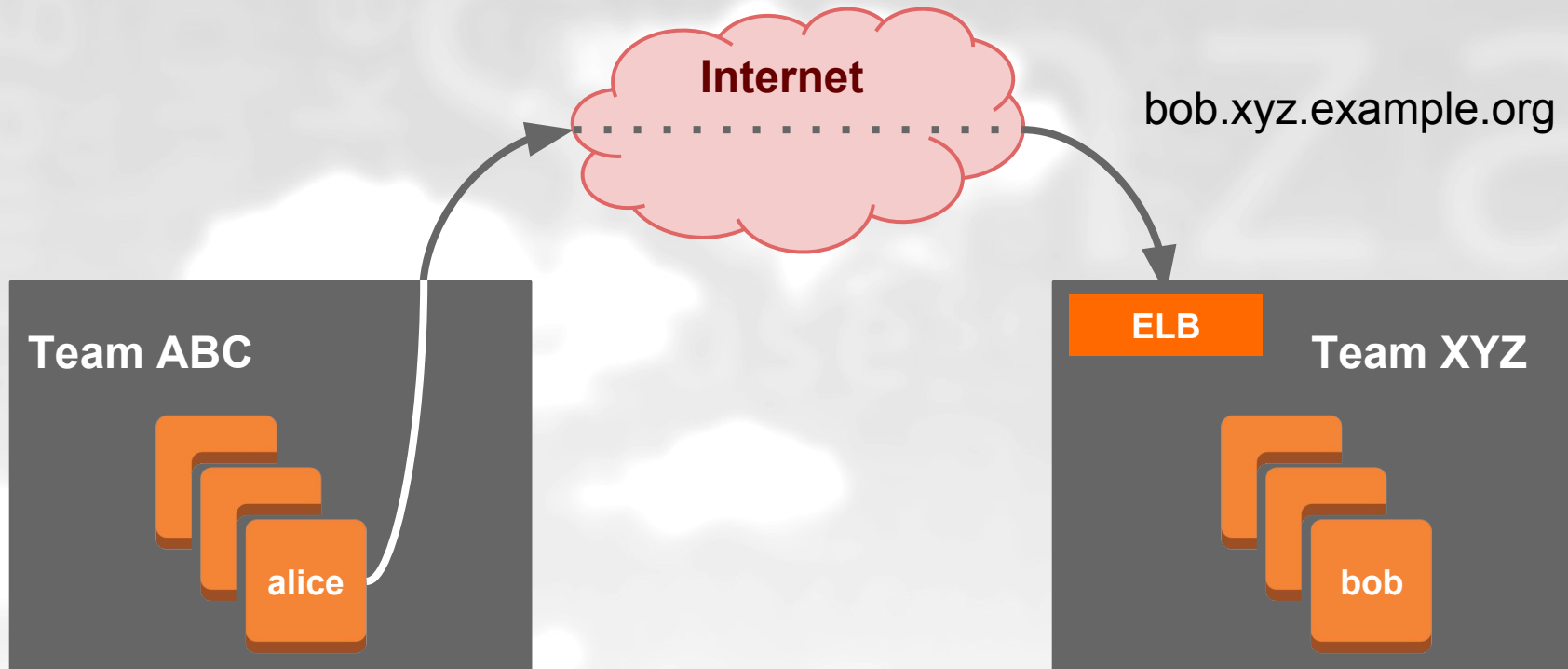


SOME NUMBERS..

- **1000+** in Zalando Tech
- **100+** AWS Accounts
- **300+** Applications



SERVICE TO SERVICE



AUTHENTICATION CANDIDATES

- HTTP Basic Auth
- SAML
- Kerberos
- OAuth 2.0
- “Notariat”

AUTHENTICATION CANDIDATES

- ~~HTTP Basic Auth~~
- ~~SAML~~
- ~~Kerberos~~
- OAuth 2.0
- ~~“Notariat”~~

OAUTH?

*The
OAuth 2.0 authorization framework
enables a third-party application
to obtain limited access to
an HTTP service.*

- *oauth.net*

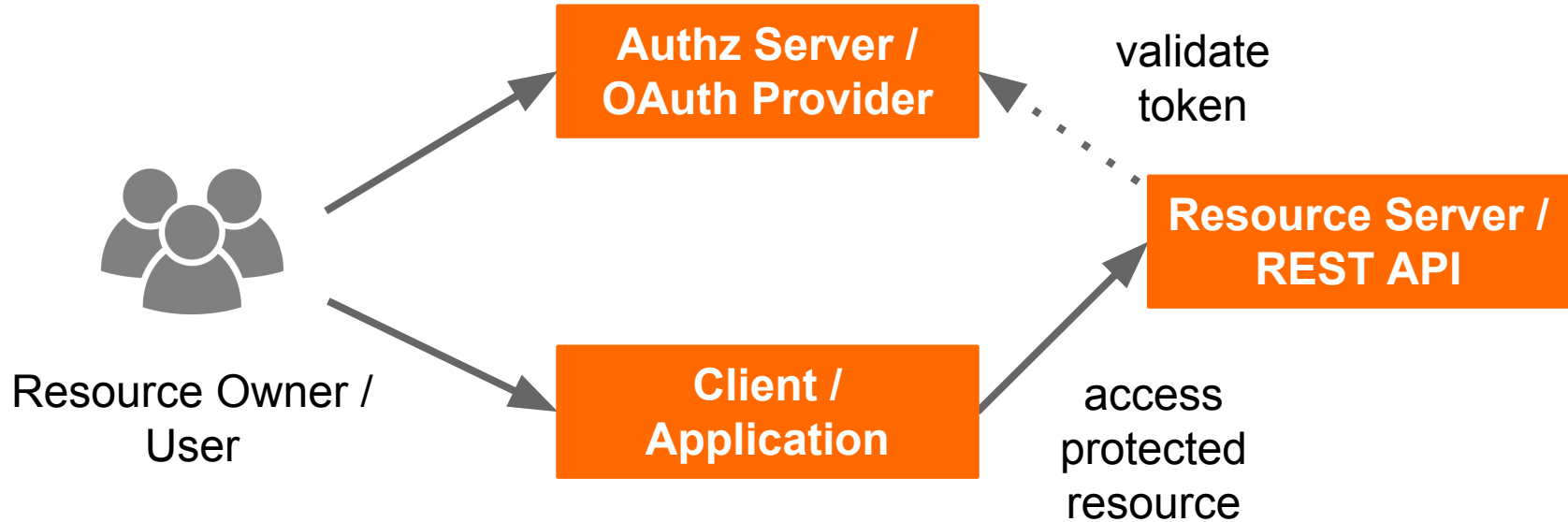
OAUTH ROLES

- **Resource Owner**
- **Client**
- **Resource Server**
- **Authorization Server**

OAuth ROLES

- Resource Owner \Leftrightarrow **User**
- Client \Leftrightarrow **Application**
- Resource Server \Leftrightarrow **REST API**
- Authorization Server \Leftrightarrow **OAuth Provider**

OAUTH REDIRECT FLOW



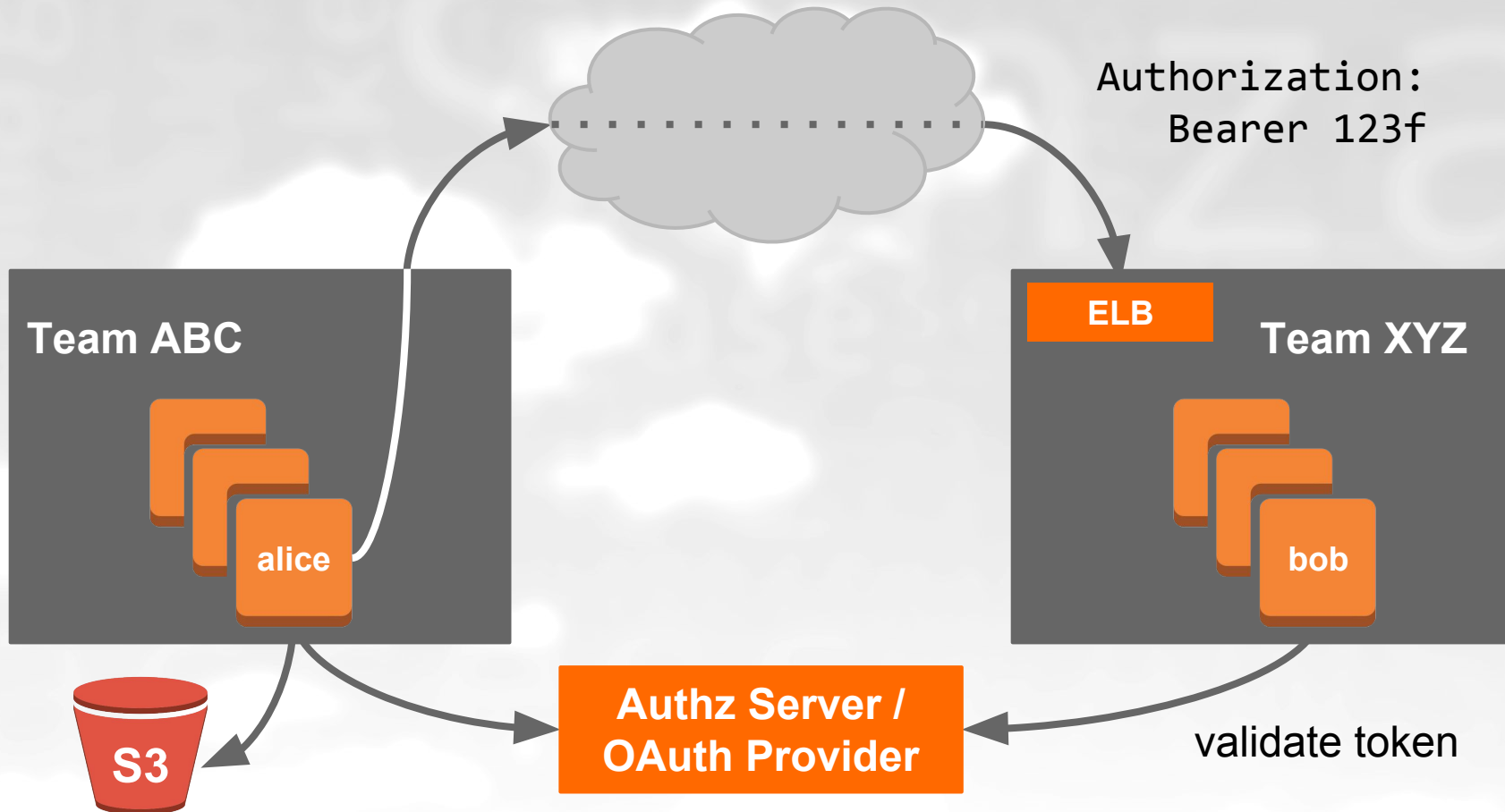
EXAMPLE OAUTH REDIRECT FLOW

<https://demo.zmon.io/>

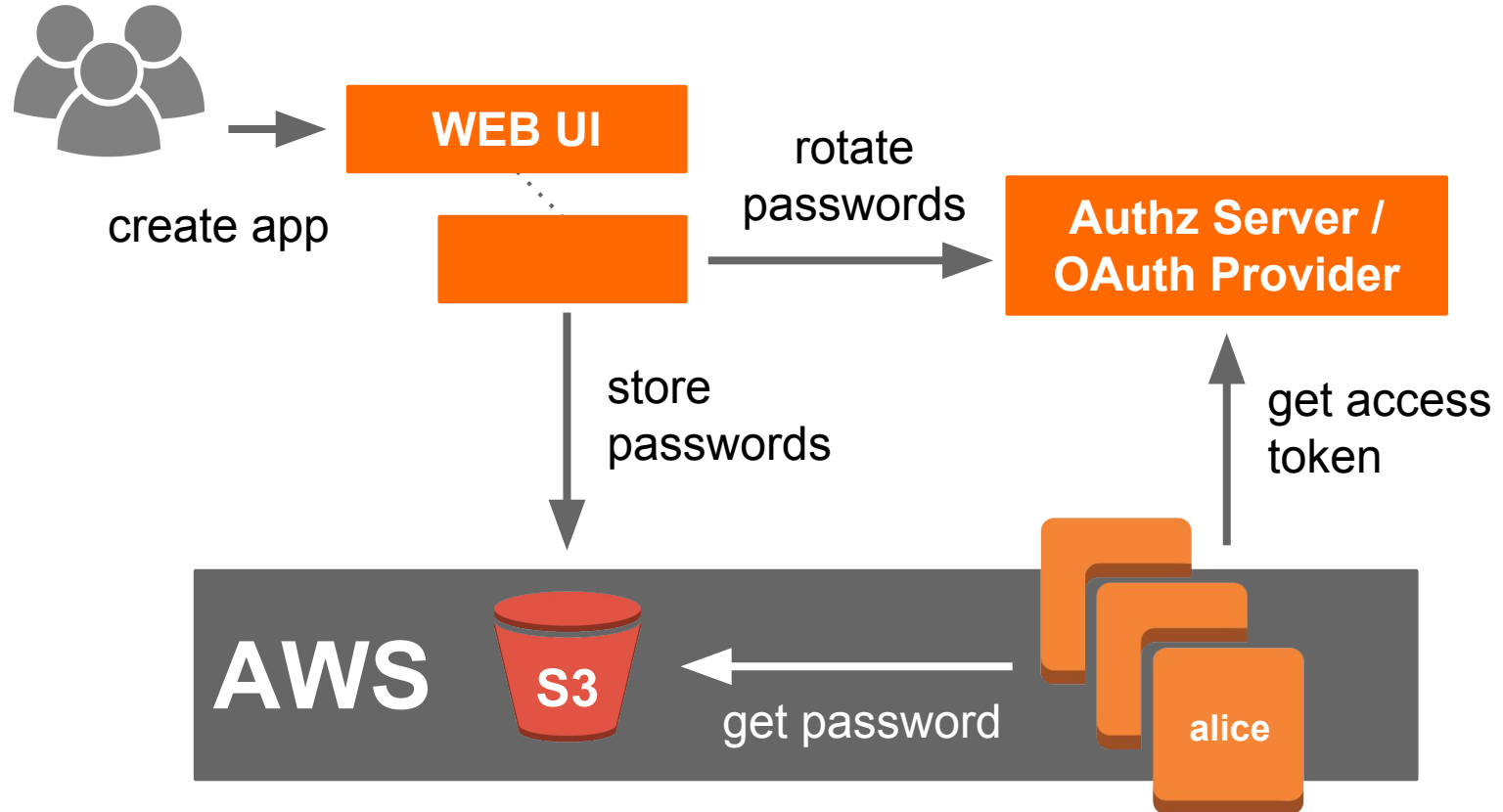
OAUTH FOR SERVICE TO SERVICE

- One **Service User** per Application
- **Resource Owner Password Credentials**
Grant Type
- Automatic **credential distribution**
and rotation

SERVICE TO SERVICE



OAUTH CREDENTIAL DISTRIBUTION VIA S3 BUCKETS



OAUTH SERVICE TO SERVICE FLOW

- Alice **reads OAuth credentials** from S3
- Alice **gets access token** from Auth. Server
- Alice calls Bob with **Bearer token**
- Bob **validates token** against Auth. Server

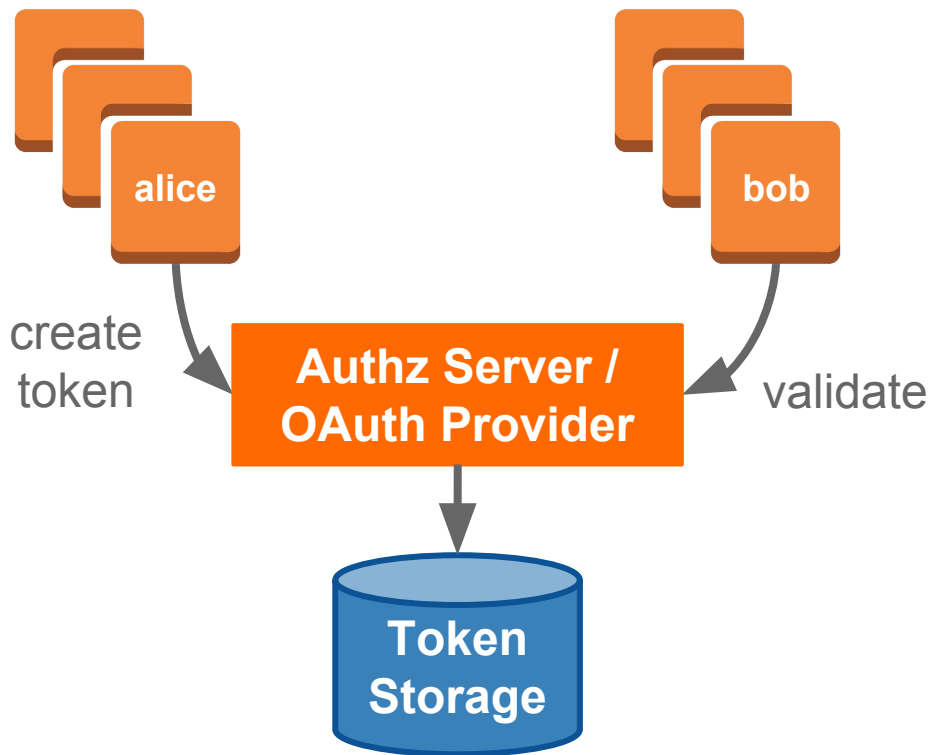
EASY ENOUGH

- Install some OAuth Provider
- Set up credential distribution
- PROFIT!!!



WHAT ABOUT

- Network Latency?
- Token Storage?
- Availability?

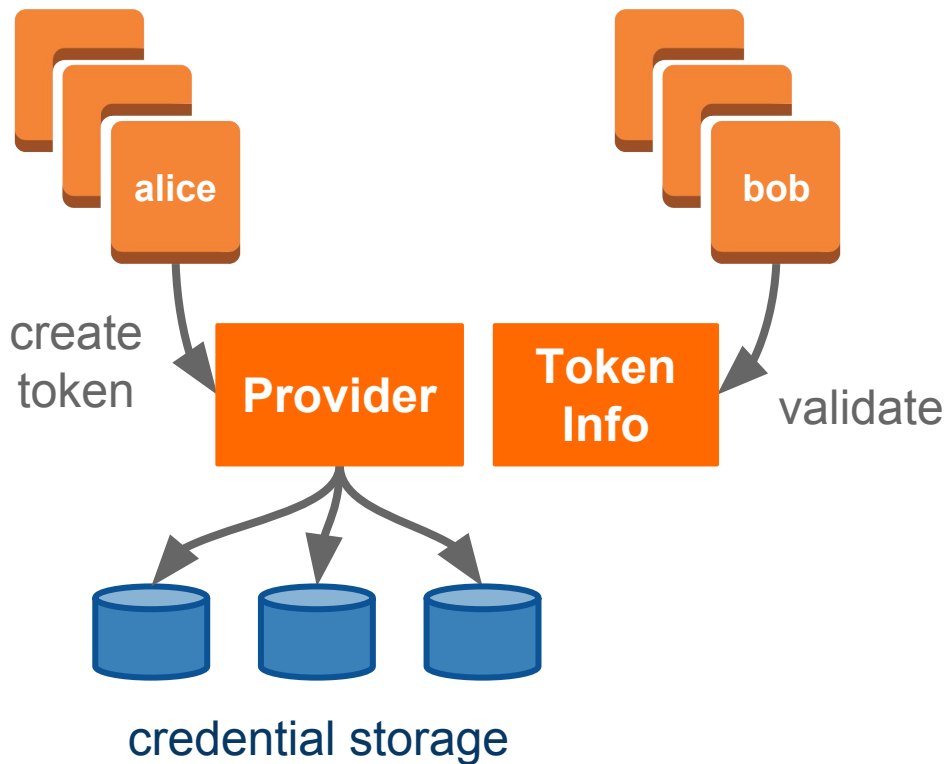


PLAN B: GOALS

- **Robustness** & resilience
- **Low latency** for token validation
- Horizontal **scalability**

PLAN B: APPROACH

- JWT access token
- No write operation
- Cassandra



JSON WEB TOKENS (JWT)

```
eyJraWQiOiJ0ZXN0a2V5LWVzMjU2IiwiaWxnIjoiriRV
MyNTYifQ.eyJzdWIiOiIzMDM1NzI5Mjg4Iiwic2Nvc
GUiOiIsib3BlbmlkIiwidWlkIiI0sImlzcyl6I6IkIiLCJ
yZWFSbSI6Ii9jdXN0b211cnMiLCJleHAiOi0jE0NTcxM
jc3MzEsIm1hdCI6MTQ1NzA5ODkzMX0.xDfBFH_cnfW
NnXcUdq7RShLGtx9d-
8RyQ13y4YRTXduQLKefbQqSsPuB56PKU-G3uI-
gjs7oEWfoiHVz8QdFRg
```

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "kid": "testkey-es256",
  "alg": "ES256"
}
```

PAYLOAD: DATA

```
{
  "sub": "3035729288",
  "scope": [
    "openid",
    "uid"
  ],
  "iss": "B",
  "realm": "/customers",
  "exp": 1457127731,
  "iat": 1457098931
}
```

VERIFY SIGNATURE

PLAN B TOKEN ENDPOINT

```
$ curl -u alice-service:mypw \
  -d 'grant_type=password&username=alice-service&password=123' \
  https://planb-provider.example.org/oauth2/access_token?realm=/services

{
  "access_token": "eyJraWQiOiOXN0a2V5LWVzMjU2..",
  "token_type": "Bearer",
  "expires_in": 28800,
  "scope": "cn",
  "realm": "/services"
}
```

JWT AS OAUTH ACCESS TOKEN

Authorization: Bearer ↵
a8dfcf02-2d21-fe12-8791-822f48749018

Authorization: Bearer ↵
eyJraWQiOiJ0ZXN0a2V5LWVzMjU2IiwiaWxnIjoiaRVMYNTYifQ.
eyJzdWIiOiJ0ZXN0MiIsInNjb3BlIjpjbImNuIi0sImIzcyI6IkkIiLCJyZWFsbSI6Ii9zZXJ2aWNlcyIsImV4cCI6MTQ1NzMxOTgxNCwiaWF0IjoxNDU3MjksImDE0fQ.
KmDsVB09RAOYwT0Y6E9tdQpg0rAPd8SExYhcZ9tXE06y9AWX4wBylnmNH
VoetWu7MwoexWkaKdpKk09IodMVug

36 chars vs ~300 chars

JWT: HOW TO VALIDATE?

- **JWT libs** exist for every major language
- De-facto standard: HTTP call to **Token Info**
- New OAuth RFC defines
Token **Introspection Endpoint**

PLAN B TOKEN INFO

GET /oauth2/tokeninfo?access_token=eyJraWQiOiJ0ZXN0a2VLWVzMjU2..

```
{  
  "expires_in": 28292,  
  "grant_type": "password",  
  "realm": "/services",  
  "scope": ["cn", "pets.read"],  
  "token_type": "Bearer",  
  "uid": "alice-service"  
}
```

REVOKING TOKENS

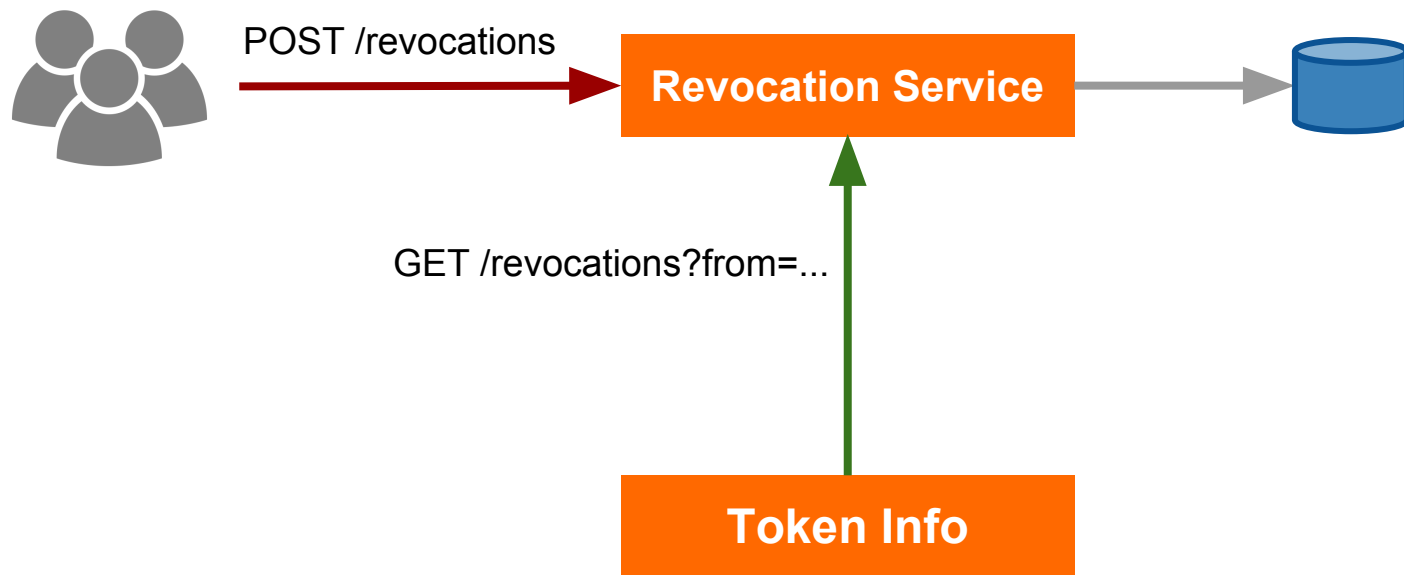
- Self-contained JWT tokens
- No revocation standard

REVOCATION LISTS

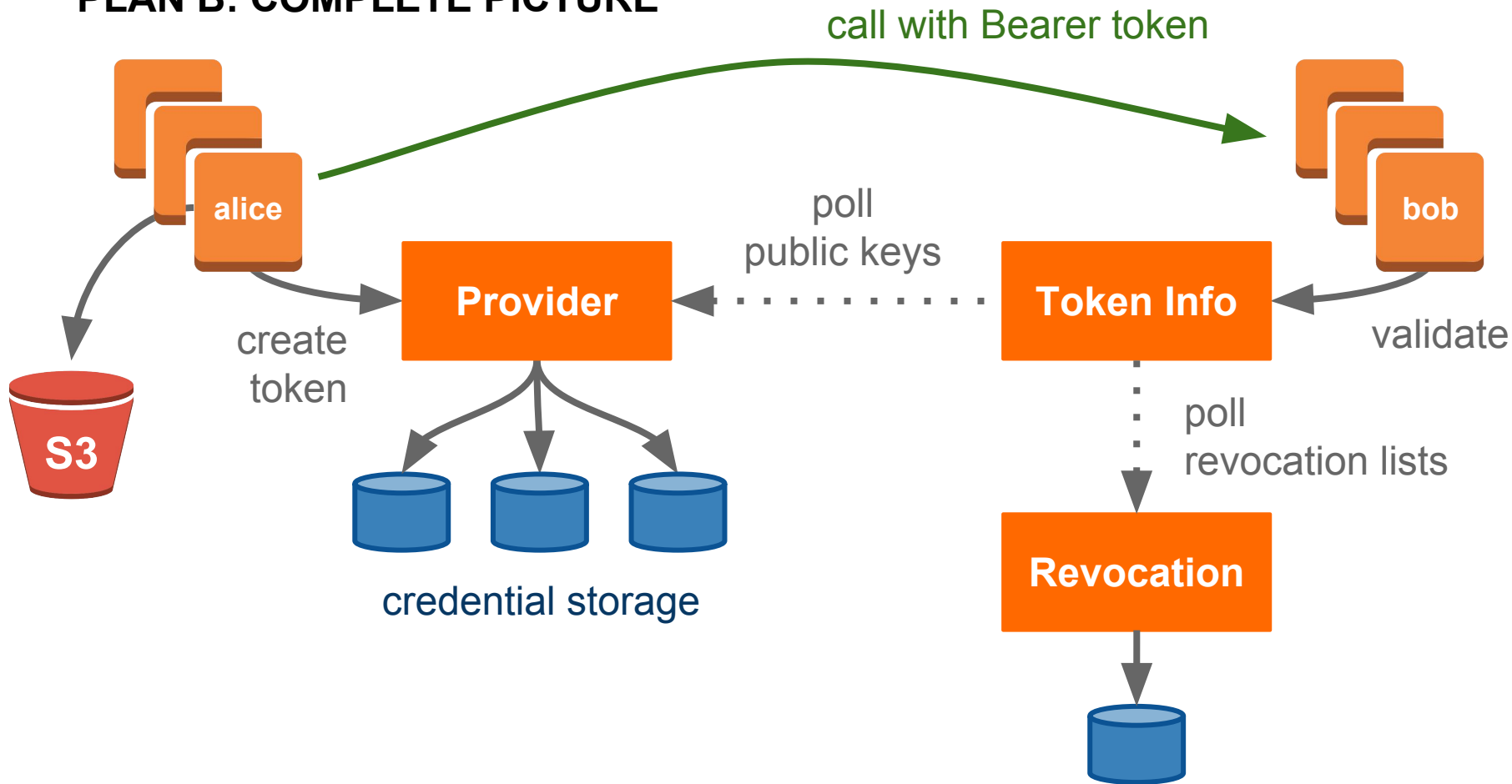
- Revoke single tokens
- Revoke tokens by claims

*“Revoke all tokens issued
before 1st of May for user John Doe”*

REVOCATION SERVICE



PLAN B: COMPLETE PICTURE



ALICE' PERSPECTIVE

- OAuth credentials in **CREDENTIALS_DIR**
- Token endpoint available at
OAUTH2_ACCESS_TOKEN_URL

BOB'S PERSPECTIVE

- Validation endpoint (Token Info) available at
TOKENINFO_URL

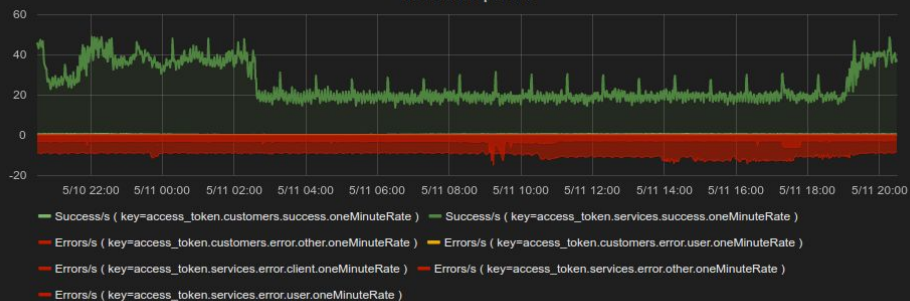
PLAN B: GOALS?

- **Robustness** & resilience
⇒ **Cassandra**, no SPOF
- **Low latency** for token validation
⇒ Token Info **next to application**
- Horizontal **scalability**
⇒ **Cassandra**, “stateless” **Token Info**

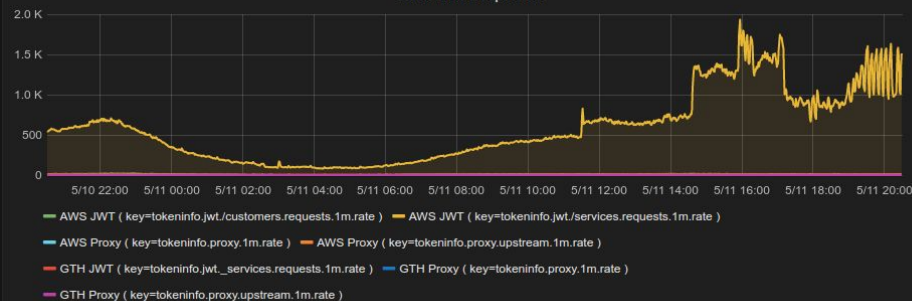
PLAN B IN PRODUCTION

- **>1300 active service users** (last 5 days)
- **8 h** JWT lifetime
- **40 rps** on Token Endpoint (Provider)
- **1500 rps** on Token Info (caching!)
- **0.5 ms** JWT validation (99%)
- **11 ms** Token Info latency (99%)

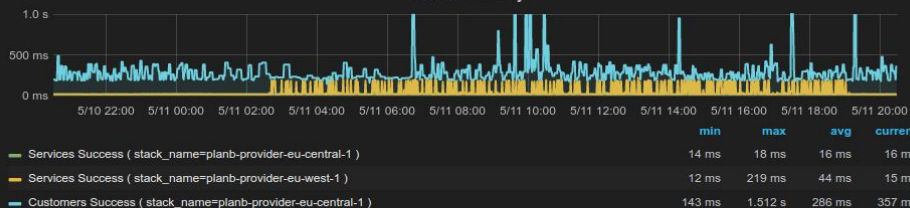
Provider Requests/s



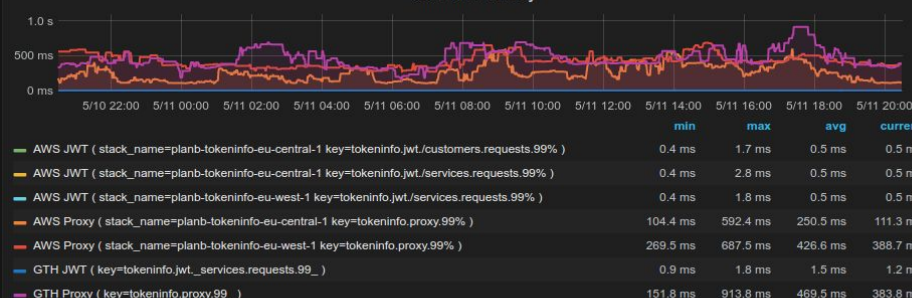
Token Info Requests/s



Provider Latency



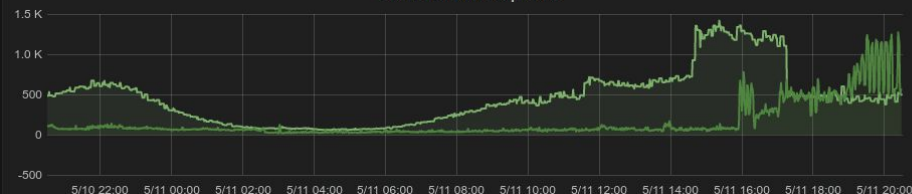
Token Info Latency



Provider ELB Requests/s



Token Info ELB Requests/s




PLAN B PROVIDER

Created for Service2Service, but also supports:

- **Authorization Code Grant Type**
- **Implicit Grant Type**
- **User Consent**

PLAN B FOR CUSTOMERS

- 3rd party Mobile App
- OAuth Implicit Flow



The screenshot shows the login interface of the Zalando mobile app. At the top, there's a status bar with various icons and a 48% battery level. Below it, a navigation bar contains a back arrow and the text "Connect to Zalando". The main content area features the Zalando logo (an orange play button icon followed by the word "zalando" in lowercase). Below the logo are two input fields: "E-Mail-Adresse*" with the email "zr@qa-zalando.de" entered, and "Passwort*" which is empty. An orange button labeled "ANMELDEN" is positioned below the password field. Underneath the button is a link that says "Passwort vergessen?". At the bottom of the main content area is a grey button with the text "SIND SIE NEUKUNDE? JETZT REGISTRIEREN →". The very bottom of the screen has a light blue link that says "Or continue on the Zalando website".

Connect to Zalando

 zalando

E-Mail-Adresse*

zr@qa-zalando.de

Passwort*

ANMELDEN

[Passwort vergessen?](#)

SIND SIE NEUKUNDE? JETZT REGISTRIEREN →

[Or continue on the Zalando website](#)

PLAN B FOR CUSTOMERS

- Consent Screen
- Consent stored
in Cassandra



Questions?

Plan B Docs

planb.readthedocs.org

STUPS Homepage

stups.io

tech.zalando.com

@try_except_

