Federated Identity for IoT with OAuth

Paul Fremantle
CTO, WSO2 (paul@wso2.com)
PhD researcher, Portsmouth University
(paul.fremantle@port.ac.uk)
@pzfreo

How this will work

- Quick intro to Federated Identity and Access Management
- Even quicker introduction to OAuth2
- MQTT overview
- Demo
- Issues
- Next steps

UNITED FEDERATION OF PLANETS

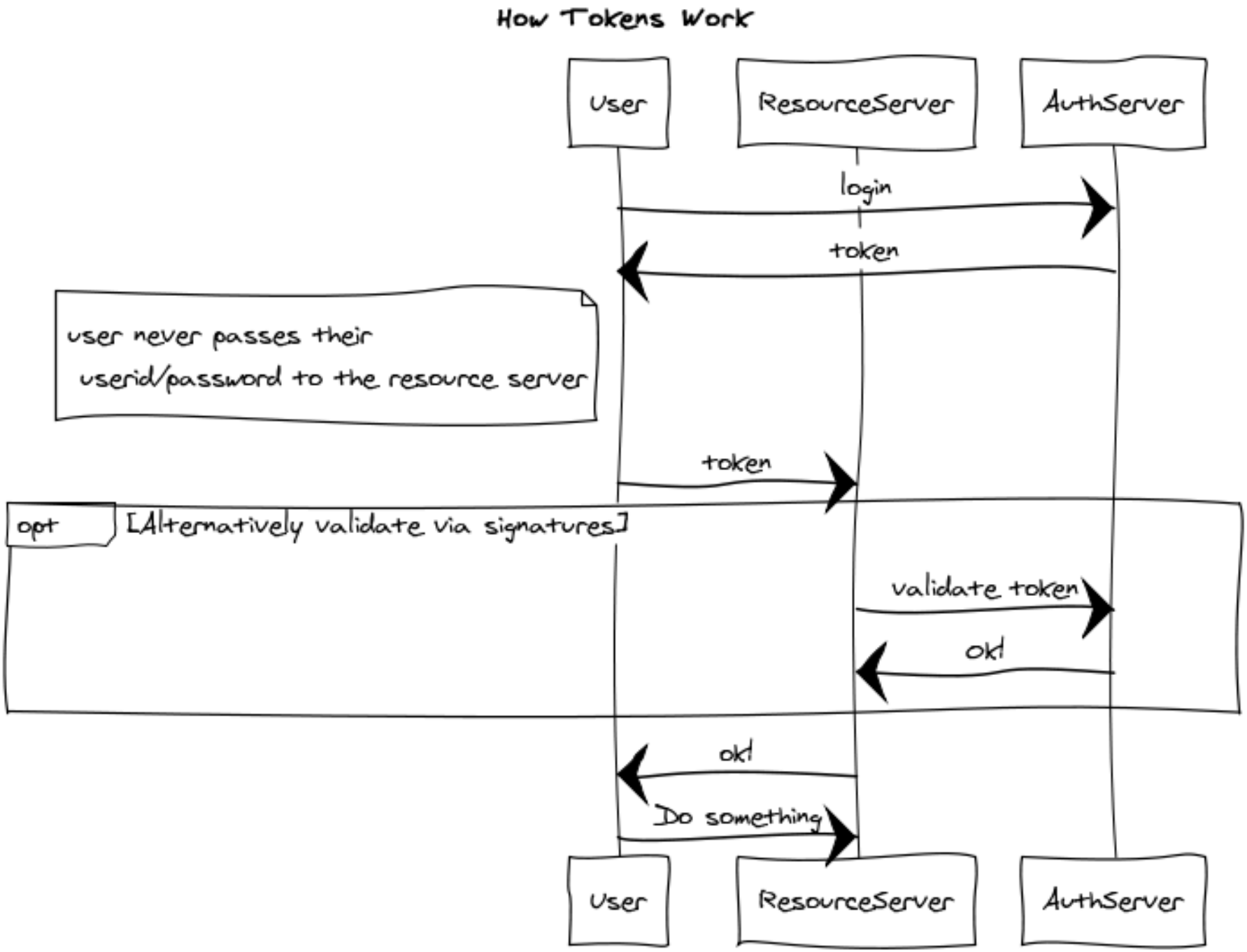
What is Federated Identity and Access Management (FIAM)?

Federated IAM aims to give You control over your credentials and access:

- You don't give your userid/pw to anyone
- You control the grant of permissions
- LinkedIn example
- OAuth2 emerging as widely used approach

Why FIAM for IoT?

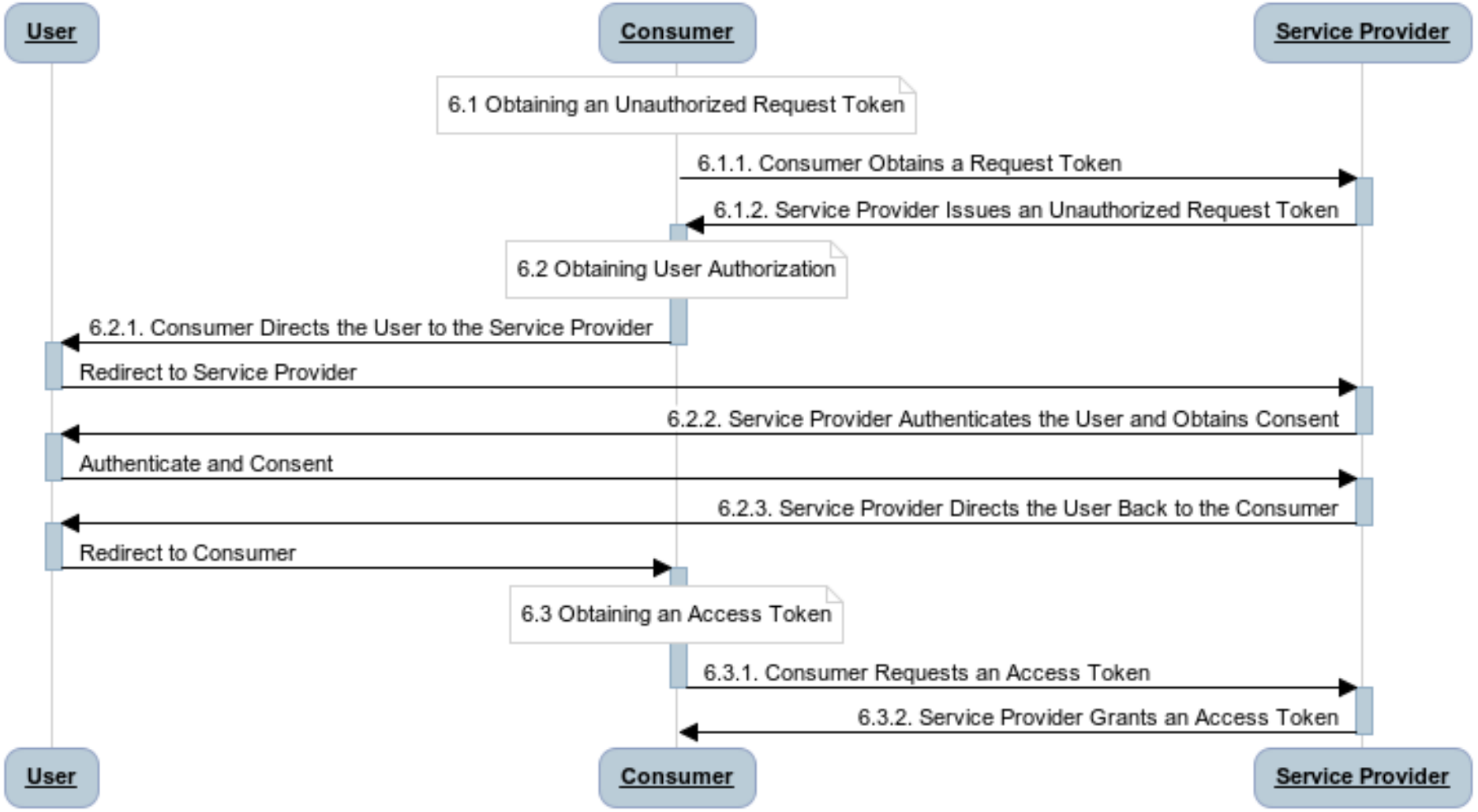
- Your device = Your data
- Tokens are better than u/p for devices
- Manage tokens and scopes independently of the device


How Tokens Work
User
ResourceServer
AuthServer
login
token
user never passes their
userid/password to the resource server
token
opt
[Alternatively validate via signatures]
validate token
ok!
ok!
Do something
User
ResourceServer
AuthServer
www.websequencediagrams.com

Why OAuth2?

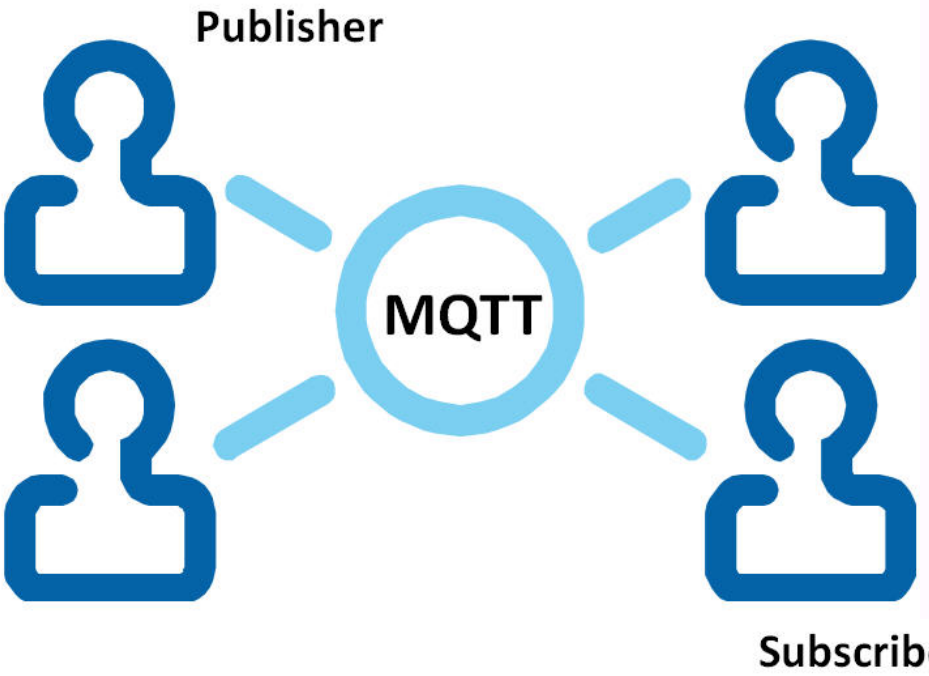
- Widely implemented
- Pretty good
  - Of course there is never 100% agreement
  - Or certainty with security protocols
- Not just HTTP:
  - http://tools.ietf.org/html/draft-ietf-kitten-sasl-oauth-12
  - OAuth2 used with SSL

Three-legged OAuth



www.websequencediagrams.com

MQTT

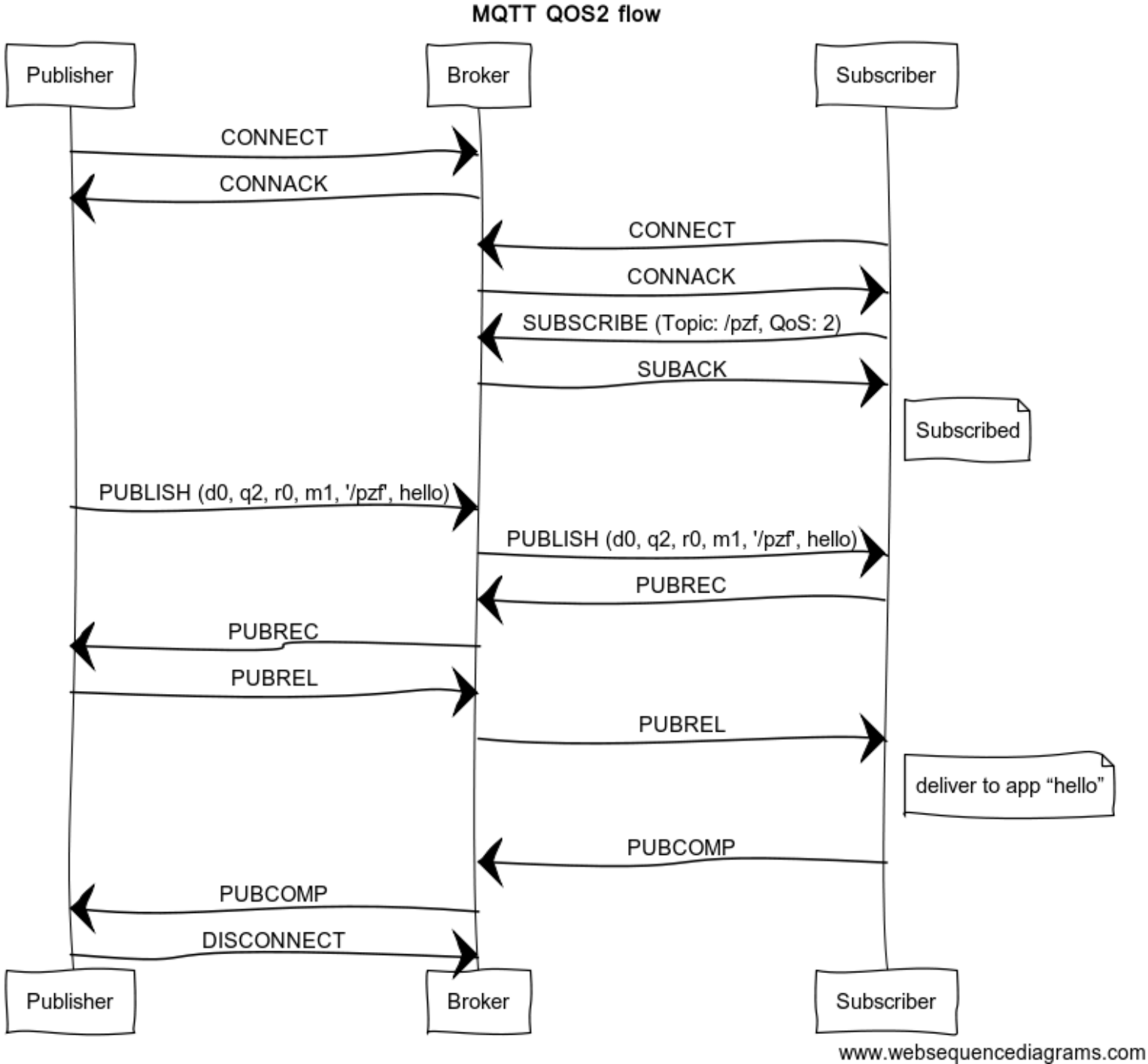


Messenger

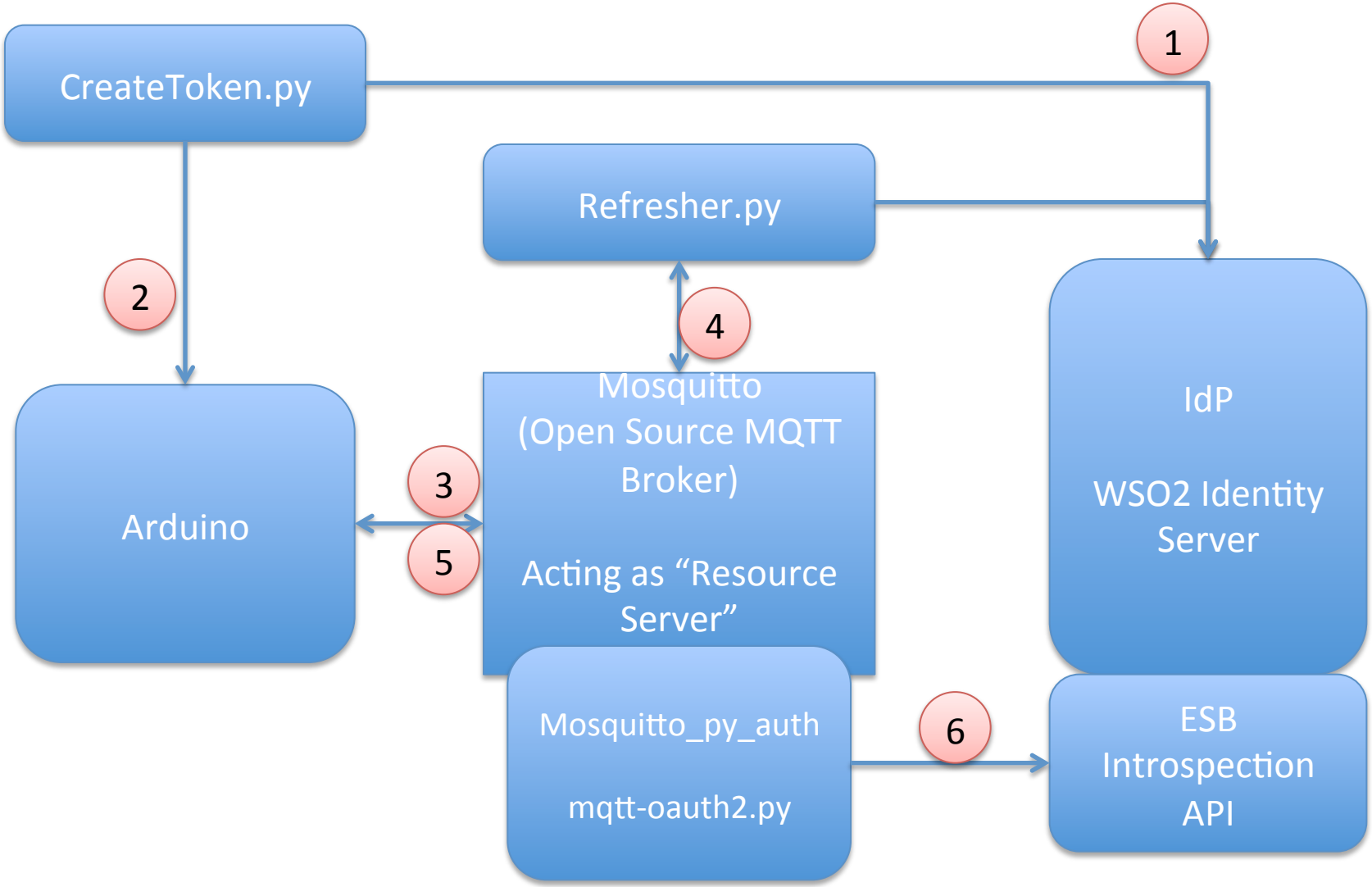
Free texting from Facebook

MQTT

- Very lightweight messaging protocol
  - Designed for 8-bit controllers, SCADA, etc
  - Low power, low bandwidth
  - Binary header of 2 bytes
  - Lots of implementations
    - Mosquitto from Eclipse
    - Apache ActiveMQ and Apollo
  - Clients:
    - Arduino, Perl, Python, PHP, C, Java, JS/Node.js, .Net, etc
- Plus an even lighter-weight version for Zigbee
  - MQTT-SN (Sensor Network)


MQTT QOS2 flow
Publisher
Broker
Subscriber
CONNECT
CONNACK
CONNECT
CONNACK
SUBSCRIBE (Topic: /pzf, QoS: 2)
SUBACK
Subscribed
PUBLISH (d0, q2, r0, m1, '/pzf', hello)
PUBLISH (d0, q2, r0, m1, '/pzf', hello)
PUBREC
PUBREC
PUBREL
PUBREL
deliver to app “hello”
PUBCOMP
PUBCOMP
DISCONNECT
Publisher
Broker
Subscriber
www.websequencediagrams.com

Demo components



Demo steps

- 1. Get an access-token / refresh-token
- 2. Encode it into the Arduino code, compile, burn
- 3. Reboot Arduino
- 4. Arduino tries access token
- 5. Arduino connects as “refresh user” and requests refresh token
- 6. Arduino receives updated access token and reconnects
- 7. Arduino starts to publish data (assuming it is allowed!)
- 8. Python client receives data using a previously authorized token

Step 1. Get a token

- Simple python script and web browser
- Encodes the requested permission “scopes” as b64 encoded JSON (ugly but works!)
- scope = '[{"rw":"w","topic":"/pzf/#"}]’
- IdP = WSO2 Identity Server
  - open source Oauth server
- Redirects to a localhost server which prints the code

Step 2. Burn into Arduino

- Little program burns into EEPROM

Step 3, 4, 5, 6
Recode Arduino with App

- App tries access token to CONNECT
- If fails, retries as user “r” (refresh)
  - Ideally this would be a separate server / IdP-based broker
- Sends {clientid, refresh_token} to topic /r
- Subscribes to /c/{clientid}
- When new access_token arrives, saves in EEPROM and reconnects

Step 7. Arduino publishes data

- MPU 9150
- Yaw, Pitch, Roll
- Every publish is validated against the IdP
  - Should be cached by the resource server

Step 8. Python client subscribes

- Subscriber.py

Lessons learnt

- MQTT and MPU / I2C code is 97% of Duemilanove
  - Adding the final logic to do OAuth2 flow pushed it to 99%
  - No TLS in this demo is a big issue
- Different Oauth implementations behave differently (e.g. changing the refresh token every time you refresh)
- Need to be able to update the scope of token if this will work for long term embedded devices
- The refresh flow should not really go via the Resource server
  - Easy fix
- MQTT should have a well defined model for sending a message to just one client (securely)

Next steps

- Do the same for CoAP / other IoT protocols
- Implement solidly ☺
- Gain agreement on the specific MQTT
- Other FIAM approaches for IoT?
  - OpenID Connect?
- Please feel free to contact me:
  - @pzfreo
  - paul@wso2.com